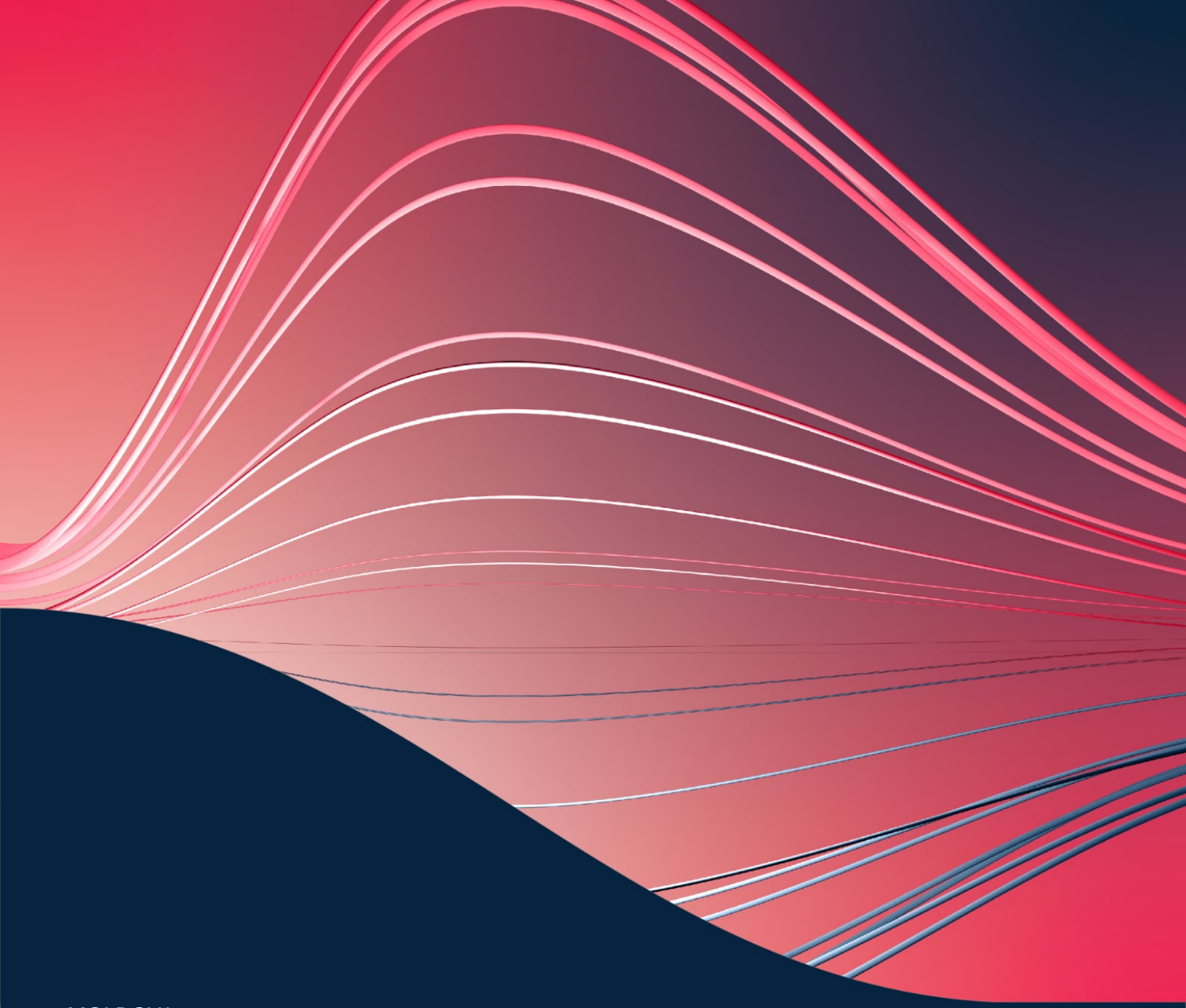


MOLDOVA

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.

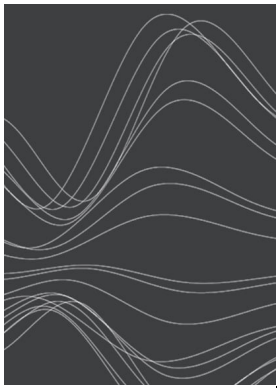
Africa key contact

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

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

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

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

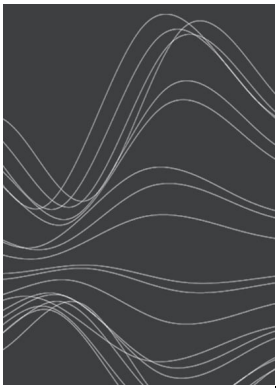
Middle East key contact

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

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

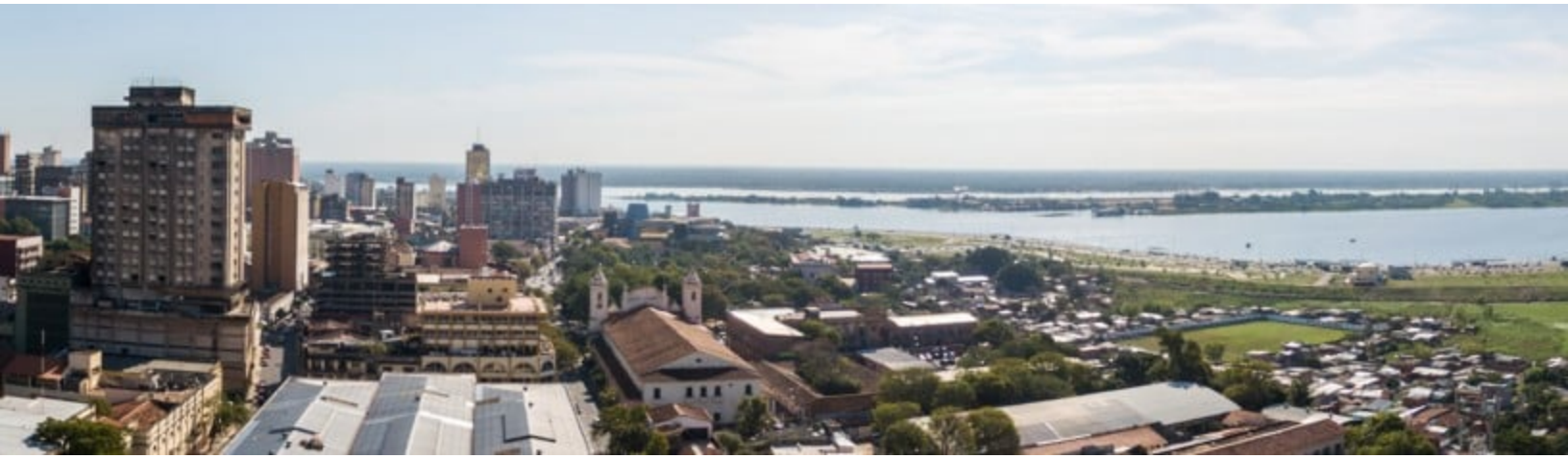
Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



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

Moldova

LAST MODIFIED 16 JANUARY 2025



Data protection laws

The main national legal acts regulating personal data protection in Moldova are:

- the Constitution of the Republic of Moldova (Article 28);
- the Law No. 133 of 08 July 2011 on Personal Data Protection;
- the Law No. 182 of 10 July 2008 regarding the approval of the National Centre for Personal Data Protection regulation, structure, staff-limit and its financial arrangements;
- the Government Decision No. 296 of 15 May 2012 on the approval of the Regulation regarding the Register of evidence of the personal data controllers;
- the Governmental Decision No. 1123 of 14 December 2010 on the approval of the requirements for the assurance of personal data security and their processing within the information systems of personal data.

The law on Personal Data Protection is the core legal act establishing the legal framework of personal data protection in Moldova. It has been adopted to harmonize the national regulations with the provisions of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In addition to Law No 133 of 8 July 2011 on Personal Data Protection, a new data protection law has been enacted. Specifically, on 25 July 2024, Law No 195 on Personal Data Protection was adopted and is scheduled to come into effect on 23 August 2026 (the "New Data Protection Law"). This new legislation partially incorporates the provisions of the European General Data Protection Regulation (GDPR) into national law, while introducing certain specific provisions that deviate from the GDPR framework.

Please note that Moldova is not an EU country and European provisions on personal data protection are not directly applicable in Moldova.

Definitions

Definition of personal data

Personal data is defined as “any information relating to an identified or identifiable natural person (“personal data subject”)”. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The New Data Protection Law introduces the following definition for personal data, similar to the one regulated by the GDPR: "any information relating to an identified or identifiable natural person" (“*data subject*”). An identifiable natural person is one who can be "identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person”.

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data. Such special categories include data related to race, ethnic origin, political opinions, religious or philosophical beliefs, social belonging, data concerning health or sex life, as well as data relating to criminal convictions, administrative sanctions or coercive procedural measures.

The New Data Protection Law does not regulate the definition of sensitive personal data anymore. Instead, the following new definitions are introduced, similarly to the notions regulated by the GDPR:

“Genetic data” – means the personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample collected from the natural person in question.

“Biometric data” – means the personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

“Data concerning health” – means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

National data protection authority

The National Centre for Personal Data Protection (“NCPDP”) is the national data protection authority. The permanent headquarters of the Centre are located in Chisinau, 48, Serghei Lazo str., MD-2004, T: +37322820801, F: +37322820807, www.datepersonale.md.

Registration

As of January 10, 2022, the requirement of mandatory registration or notification of personal data databases has been abolished.

Instead, according to the new legal provisions, before starting the data processing operations, the data controller shall perform a data protection impact assessment, analysing thereby the envisaged actions to be performed and their eventual impact on the data subject.

The data protection impact assessment should contain at least the following information:

- The description of envisaged processing operations, the purpose of processing and legitimate interest of the data controller (if any);
- The description of the necessity and proportionality of processing operations in relation to the purpose of processing;
- Risk assessment for the rights and freedoms of data subjects, in particular, the source of those data, nature, specific degree of likelihood of materialization of the increased risk and the severity of that risk;
- The description of risk prevention measures, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the provisions of the data protection law.

The NCPDP has additionally approved and published a list of types of personal data processing operations, which are subject to the mandatory data protection impact assessment requirement. The list may be consulted at the following link.

Furthermore, the data controller shall consult with the NCPDP before starting any operations on processing of personal data if the data protection impact assessment indicates that the processing would generate an increased risk, and the data controller considers that such risk cannot be mitigated through reasonable means, considering the available technologies and implementation costs.

Data protection officers

The appointment of an internal data protection officer is required, in the following cases:

- the processing is carried out by a public authority or institution, with the exception of courts acting in their judicial capacity;
- the main activities of the Data Controller or data processors consist of processing operations which, by virtue of their nature, their scope and / or their purposes, necessitate regular and systematic monitoring of data subjects on a large scale; and
- the main activities of the Data Controller or data processor consist of large-scale processing of special categories of data.

Collection and processing

Personal data shall be processed with the consent of the personal data subject, unless an exception applies.

The consent of the data subjects is not necessary where the processing is necessary for:

- performance of a contract to which the personal data subject is party, or implementation of pre-contractual measures, taken at the data subject's request;
- carrying out an obligation of the controller, under the law;
- protection of the life, physical integrity or health of the personal data subject;
- performance of tasks carried out in the public interest or in the exercise of public authority prerogatives vested in the controller or in a third party to whom the personal data is disclosed;
- the purposes of legitimate interest pursued by the controller or by the third party to whom personal data is disclosed, except where such interest is overridden by the interests for fundamental rights and freedoms of the personal data subject;
- conducting the external public audit;
- statistical, historical or scientific-research purposes, provided that the personal data remains anonymous throughout the processing;
- data exchange, performed in accordance with the applicable legislation on data exchange and interoperability.

Processing of special categories of personal data shall be prohibited, except for cases provided by the Law. Furthermore, Law on Personal Data Protection currently expressly establishes special rules for processing the following: personal data concerning health, data concerning criminal convictions and offences or related security measures, data comprising the national identification number.

Personal data undergoing processing must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and / or further processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits the identification of personal data subjects for no longer than is necessary for the purposes for which the data was collected and further processed.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without the prior consent of the data subject unless one of the following exclusions applies:

- processing relates to data which is voluntary and manifestly made public by the personal data subject;

- the personal data is rendered anonymous.

The controller must implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data.

Transfer

Transfers of personal data by a controller or a processor are permitted taking into account the principle of free movement of data to EU countries and to third countries that ensures an adequate level of protection of personal data subjects' rights and of data intended for transfer.

The NCPDP is in charge of maintaining the list of the countries that ensures an adequate level of protection of personal data subject's rights. The list of such jurisdictions has been elaborated by the NCPDCP. The list may be consulted, by accessing the following link.

The Law on Personal Data Protection also includes a list of context specific derogations, permitting transfers to countries that do not ensure an adequate level of protection:

- if the transfer is provided under an international treaty to which Moldova is a signatory;
- the data subject consents to the transfer;
- if the transfer is necessary for the conclusion or performance of an agreement or contract concluded between the personal data subject and the controller or between the controller and a third party in the interest of the personal data subject;
- if the transfer is necessary in order to protect the life, physical integrity or health of the personal data subject;
- if the transfer is carried out solely for journalistic, artistic, scientific and archive purposes of public interest;
- if the transfer is made to other companies from the same group as the data controller, provided that the mandatory corporate rules are observed;the transfer is necessary for the accomplishment of an important public interest, such as national defence, public order or national security, carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court, on the condition that the personal data is processed solely in relation to this purpose and only for longer period is necessary to achieve it;
- if the transfer is necessary for the establishment, exercise or defence of legal claims, whether when the courts are acting in their judicial capacity, or in the context of administrative or extrajudicial proceedings, including proceedings involving regulatory authorities;
- if the processing takes place under the contract standard for cross-border data transmission, elaborated and approved by the NCPDCP, concluded by the data controller.

If only a data transfer agreement is to be concluded, our recommendation is to use as a template of data processing agreement the template approved by the NCPDCP. NCPDCP has elaborated the Standard Data Transfer Agreement, that may be used by the data controllers. Transferring data under this template elaborated by the NCPDCP shall be considered as an additional safeguard for the legitimacy of the transfer. The template Standard Data Transfer Agreement may be accessed here.

Security

The controller must implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data. The NCPDP has approved guidelines on the security measures to be implemented by the controller or processor, for the protection and processing of personal data within information systems. The guidelines may be accessed here.

Where processing is to be carried out on behalf of the controller, the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures. The processing of personal data by a processor shall be governed by a contract concluded with the controller, ensuring in particular the following:

- that the processor only acts on the instructions from the controller;
- that the obligations related to mandatory technical and organisational measures to be undertaken, in order to ensure a level of security appropriate to the risk and nature of the data processed, shall also apply to the processor.

According to the New Data Protection Law, and save for the exceptions expressly established by law, where a controller or processor not registered in the Republic of Moldova is processing personal data of subjects who are in the Republic of Moldova, it should designate a representative in Moldova, provided that the processing activities are related to the following:

- offering of goods or services, irrespective of whether a payment of the data subject is required to such subjects in the Republic of Moldova; or
- to the monitoring of data subjects' behaviour, as far as their behaviour takes places within the Republic of Moldova.

Breach notification

Current provisions

Personal data processing activities conducted by controllers or processors are subject to oversight by the NCPDP. In the event that the NCPDP identifies legal violations following its control, it shall issue a decision ordering the suspension of the data processing operations in question. Such a decision shall also include specific instructions for rectifying the identified violations.

The suspension of data processing operations shall remain in effect until the circumstances that served as the basis for the decision have been remedied. The

controller or processor is required to address and rectify these circumstances within 30 days from the date on which the suspension decision was issued by the NCPDP.

Failure to take the necessary remedial measures within the specified period may result in the NCPDP issuing a decision to terminate the respective data processing operations. Additionally, the NCPDP may order the blocking or destruction of invalid or unlawfully obtained personal data.

Also, under the current Data Protection Law, data subjects have the right to lodge a complaint with the NCPDP if they believe that personal data processing operations have been conducted unlawfully. Such complaints must be submitted within 30 days from the date the data subject became aware of the alleged violation.

New legal provisions

In addition to the above, the New Data Protection Law (to enter into force on 23 August 2026) expressly includes the "personal data breach" definition and concept. Under the new provisions, where a personal data breach occurs, the controller shall without undue delay, and, where feasible, not later than 72 hours after having become aware of it, notify the NCPDP, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Such notification shall include at least the following details:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller, to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Furthermore, where a personal data breach is likely to result in a high risk for the rights and freedoms of the individual, save for the exceptions provided by law, the controller shall communicate the personal data breach to the data subject, without undue delay. Such communication shall describe in a clear and plain language the nature of the personal data breach and shall contain at least the details indicated above (which has been communicated to the NCPDP).

Enforcement

The NCPDP is responsible for the enforcement of the Law on Personal Data Protection. The NCPDP is entitled to:

- carry out checks;
- consider complaints from data subjects;
- require the submission of necessary information about personal data processing by the data controller;

- require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data;
- file court actions;

Violation of personal data protection legislation may result in administrative liability. The maximum administrative penalty that can be imposed, as at the date of this review, is MDL (Moldovan lei) 15,000 which is about EUR 780.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The NCPDP may also suspend or prohibit the processing of data if the rules on personal data protection are breached.

In addition to above, the New Data Protection Law introduces revised penalties for violations of data protection rules. Pursuant to the new legal provisions, infringements of statutory data protection norms may result in administrative fines of up to MDL 2,000,000 (approximately EUR 104,339), or, in the case of undertakings, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These provisions are not yet in effect and will become enforceable as of 23 August 2026.

The New Data Protection Law also establishes a transitional period concerning the application of penalty amounts. During the first three years following the entry into force of these provisions, the penalty amounts will be applied incrementally. The sanctions will gradually increase each year until they reach the maximum amounts specified above.

Electronic marketing

The Law regarding information society services dated July 22, 2004 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce. In particular:

- commercial electronic messages are allowed only subject to the preliminary consent of a subscriber or addressee to receive such messages;
- the recipient shall have easy access to information regarding the individual or legal entity sending the message;
- commercial electronic messages regarding sales, promotional gifts, premiums etc. shall be unequivocally identified as such and the conditions for receiving of such promotions shall be clearly stated to avoid their ambiguous understanding.

Online privacy

At the date of this review, Moldovan law does not specifically regulate online privacy.

There are no specific requirements on data location, except for the requirement of the prior authorization of the cross-border transfer of data.

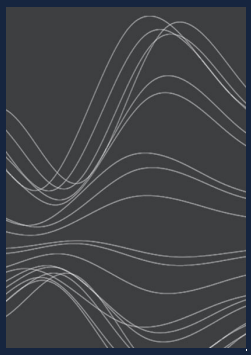
Data protection lawyers

Doina Doga
Senior Associate
ACI Partners
ddoga@aci.md
View bio

Nicolina urcan
Senior Associate
ACI Partners
nturcan@aci.md

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