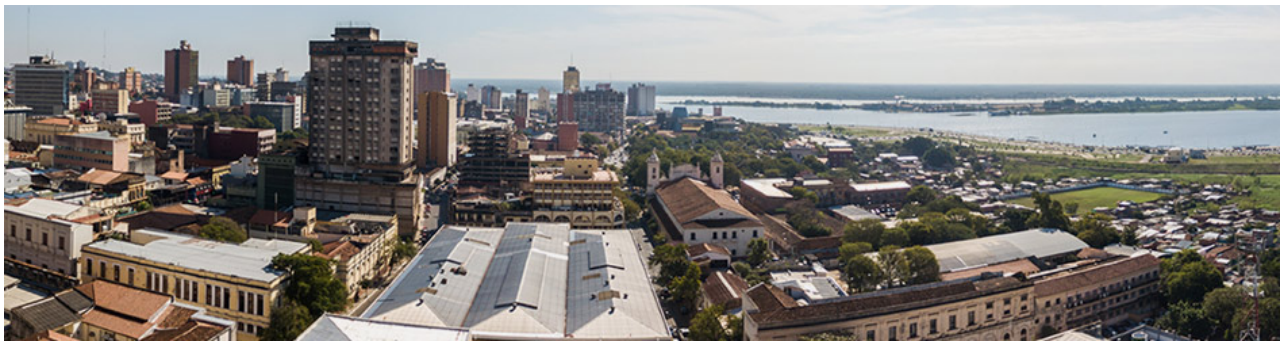
DATA PROTECTION LAWS OF THE WORLD

Moldova

MOLDOVA



Last modified 18 January 2024

LAW

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 the near future we expect the adoption of a new Law on Personal Data Protection which will transpose the provisions of the GDPR with some adjustments to Moldovan conditions.

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.

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.

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 shall be abolished. However, according to the new provision, the controller shall consult with the NCPDP before starting any operations on processing of personal data in case if the data protection impact assessment indicates the processing would generate an increased risk.

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

- The description of category of the data to be processed, the purpose of processing and legitimate interest (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.

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 & 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, in order to take steps at the request of the data subject prior to entering into a contract;
- 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;
- statistical, historical or scientific-research purposes, except where the personal data remains anonymous for a longer period of processing

Processing of special categories of personal data shall be prohibited, except for cases provided by the Law.

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 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.

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 is used as a reference for the minimum-security measures to be implemented by the controller.

BREACH NOTIFICATION

Data controllers shall submit to the NCPDP an annual report on any security incidents involving information systems during that year.

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 750.

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.

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.

KEY CONTACTS

ACI Partners
www.aci.md

Marina Zanoga
Senior Associate
ACI Partners
T +373 22 279 323
mzanoga@aci.md

Nicolina Țurcan
Associate
ACI Partners
nturcan@aci.md

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.