Comparing privacy laws:
GDPR v. Law on Personal Data

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

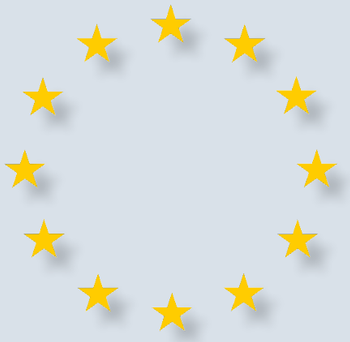
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which entered into effect on 25 May 2018, governs the protection of personal data in EU and EEA Member States. The Law No. 133 of 8 July 2011 on Personal Data Protection ('the Law on Personal Data') which entered into force on 14 April 2012 is the primary legislation governing data processing in Moldova. The National Center for Personal Data Protection ('NCPDP') is the national data protection regulator in the region, and has corrective, advisory, and investigatory powers including the conducting of compliance investigations, issuance of decisions, as well as corrective orders.

In general terms, there are broad similarities between the GDPR and the Law on Personal Data, as the Law on Personal Data is based on 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 ('Data Protection Directive'). Specifically, the two legislations outline similar terms including data controller, data processor, processing, and special category data. In addition, both legislations address matters such as data subject rights, provide lawful bases for data processing, and allow data transfers based on an adequate level of protection. Nevertheless, the Law on Personal Data and the GDPR differ in important ways. Specifically, the obligations imposed on data controllers under the Law on Personal Data are less extensive than those provided in the GDPR, and omit obligations including in relation to conducting Data Protection Impact Assessments ('DPIA'), data breach notifications, mandatory data protection officer ('DPO') appointment, and record-keeping. Furthermore, rights such as the right to data portability are notably absent from the Law on Personal Data.

This overview organises provisions from the Law on Personal Data and the GDPR into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Law on Personal Data.

Key for giving the consistency rate

Consistent: The GDPR and the Law on Personal Data bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the Law on Personal Data bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

Fairly inconsistent: The GDPR and the Law on Personal Data bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

Inconsistent: The GDPR and the Law on Personal Data bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.

Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

Fairly consistent

1.1. Personal scope

The GDPR and Law on Personal Data provide similar definitions of data controllers, data processors, and data subjects. However, the GDPR clarifies that it will apply to the processing of natural persons' data regardless of their nationality and residents in the EU, while the Law on Personal Data is silent on these matters.

GDPR	Law on Personal Data
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 3(5): 'controller' a natural or legal person governed by public law, or by private law, including public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data expressly provided by applicable law.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 3(6): 'processor' natural or legal person governed by public law, or by private law, including public authority and its territorial subdivisions, which processes personal data on behalf of the controller, on instructions from the controller.
Data subject	
Article 4(1): 'personal data' means 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 3(1): 'personal data' 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.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Article 3(5): 'controller' means a natural or legal person governed by public law, or by private law, including public authority, agency or any other body.

GDPR	Law on Personal Data
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	The Law on Personal Data does not explicitly refer to the nationality of data subjects.
Place of residence	
See Recital 14, above.	The Law on Personal Data does not explicitly refer to the data subject place of residence.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The Law on Personal Data does not explicitly address its applicability to deceased persons. However, Articles 5(3) and 11(4) of the Law outline requirements for the processing of the data subject's personal information after death.

1.2. Territorial scope

The GDPR and the Law on Personal Data both have extraterritorial application, applying to data controllers that are not established within their respective jurisdictions, in certain circumstances. Notably, however, the Law on Personal Data does not explicitly regulate goods and services or monitoring from abroad, whereas the GDPR explicitly outlines such activities as within its scope.

GDPR	Law on Personal Data
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.	Article 2(2)(a): The Law on Personal Data will apply to the processing of personal data carried out in the context of the activities performed by the controllers established on the territory of the Republic of Moldova.
Extraterritorial	
See Article 3, above.	Article 2(2)(b-d): The Law on Personal Data will apply: • to the processing of personal data carried out within the diplomatic missions and consular offices of the Republic of Moldova, as well as carried out by other controllers that do not have permanently establishment on the territory of the Republic of Moldova, but are situated in a place where the domestic law of the Republic of Moldova applies by virtue of international public law; • to the processing of personal data carried out by controllers that are not established on the territory of the Republic of Moldova, making use of equipment situated on the territory of the Republic of Moldova, unless such equipment is used only for purposes of transit through the territory of the Republic of Moldova; and • to the processing of personal data in the context of actions of prevention and investigation of criminal offences, enforcement of convictions and other activities within criminal or administrative procedures, in terms of the law.

GDPR	Law on Personal Data
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The Law on Personal Data does not refer to the provision of goods and services from abroad.
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The Law on Personal Data does not refer to monitoring from abroad.

Fairly consistent

1.3. Material scope

The Law on Personal Data and the GDPR adopt similar definitions of general and sensitive personal data, data processing, and depersonalisation of data, although defined as pseudonymisation of data under the GDPR. In addition, both legislations provide general exceptions for the processing of personal data for purely personal or household activities and enhanced protection for the processing of special categories of personal data.

GDPR	Law on Personal Data
Personal data/ personal information	
Article 4(1): 'personal data' means 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 2(1): 'personal data' 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.
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Article 2(3): 'processing of personal data' any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, keeping, restoring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Special categories of data	
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Article 2(2): 'special categories of personal data' data revealing racial or 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.

GDPR	Law on Personal Data

Anonymised data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Law on Personal Data does not explicitly define anonymised data.

Pseudonymised data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Article 2(10): 'depersonalisation of data' is such alteration of personal data so that details of personal or material circumstances can no longer be linked to an identified or identifiable natural person or so link can only be made within an investigation with disproportionate efforts, expense and use of time.

Automated processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Article 2(1): The Law on Personal Data regulates relations arising in course of the processing operations of personal data performed wholly or partly by automatic means, and otherwise than by automatic means, which form part of a filing system or are intended to be included in such a filing system.

General exemptions

Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or (c) by a natural person in the course of a purely personal or household activity.	Article 4: The Law on Personal Data shall not apply • to the processing of personal data carried out by controllers exclusively for personal and family needs, where the rights of personal data subjects are not violated thereby; • to the processing of personal data assigned to state secret, according to an established procedure, excepting the information referred to in Article 2(d); • to the processing operations and cross-border transmission of personal data referring to the perpetrators or victims of genocide, crimes against humanity and war crimes.

2. Key definitions

Fairly consistent

2.1. Personal data

The Law on Personal Data largely contains similar definitions to those provided in the GDPR, including personal data, special category data, and third party. However, the Law on Personal Data does not define 'online identifiers.'

GDPR	Law on Personal Data

Personal data/ personal information

Article 4(1): 'personal data' means 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 2(1): 'personal data' 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.

Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	AArticle 2(2): 'special categories of personal data' data revealing racial or 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

Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	The Law on Personal Data does not explicitly refer to online identifiers.

GDPR	Law on Personal Data
Filing system	
Article 4(6): 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.	Article 3(4): 'personal data filing system' any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Recipient	
Article 4(9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.	Article 3(8): 'recipient' a natural or legal person governed by public law, or by private law, including public authority and its territorial subdivisions, to whom personal data are disclosed, whether a third party or not. The bodies responsible for the national defence, state security and public order, the prosecution bodies and the courts, which may receive personal data in the framework of exercising their duties established by law, shall not be regarded as recipients.
Third Party	
Article 4(9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.	Article 3(7): 'third party' natural or legal person governed by public law, or by private law, other than the personal data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the personal data.

2.2. Pseudonymisation

The Law on Personal Data and the GDPR provide a definition for pseudonymisation/ depersonalisation of personal data. However, the GDPR requires the implementation of technical and organisational measures to ensure that personal data is not attributable to a data subject, while the Law on Personal Data does not.

GDPR	Law on Personal Data
Anonymisation	
Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Law on Personal Data does not explicitly define anonymisation.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Article 2(10): 'depersonalisation of data' is such alteration of personal data so that details of personal or material circumstances can no longer be linked to an identified or identifiable natural person or so link can only be made within an investigation with disproportionate efforts, expense and use of time

2.3. Controllers and processors

Fairly inconsistent

The Law on Personal Data and the GDPR adopt similar concepts of 'controller' and 'processor.' In addition, both legislations outline requirements for the establishment of controller/processor contracts in certain circumstances. Notably, however, the Law on Personal Data does not explicitly define or address DPIAs, or DPOs.

GDPR	Law on Personal Data

Data controller

GDPR	Law on Personal Data
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 3(5): 'controller' a natural or legal person governed by public law, or by private law, including public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data expressly provided by applicable law.

Data processor

GDPR	Law on Personal Data
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 3(6): 'processor' natural or legal person governed by public law, or by private law, including public authority and its territorial subdivisions, which processes personal data on behalf of the controller, on instructions from the controller.

Controller and processor contracts

GDPR	Law on Personal Data
Article 28(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]	Article 30(3): The carrying out of processing by way of a processor must be governed by a contract or legal act stipulating, in particular that: • the processor shall act only on instructions from the controller; and the obligations set out in Article 30(1) of the Law shall also be incumbent on the processor.

GDPR	Law on Personal Data

Data Protection Impact Assessment ('DPIA')

GDPR	Law on Personal Data
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	The Law on Personal Data does not refer to DPIAs.

Data Protection Officer ('DPO')

GDPR	Law on Personal Data
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	The Law on Personal Data does not refer to DPOs. However, Government Decision of 14 December 2010 No. 1123 approving the Requirements for Ensuring the Security of Personal Data and their Processing in Information Systems of Personal Data (available in Romanian here and Russian here) (an unofficial English translation is available here) ('the Decision') provides recommendations for the appointment an individual(s) responsible for undertaking the measures necessary to comply with Law.

2.4. Children

Unlike the GDPR, the Law on Personal Data does not provide a definition of children, nor do they implement special requirements for the processing of children's information.

GDPR	Law on Personal Data

Children's definition

The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

The Law on Personal Data does not specifically define 'minor'

Consent for processing children's data

Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

The Law on Personal Data does not specifically address consent requirements for minors.

However, Article 24 of the Law states that categories of the processing operations of personal data subject to transborder transfer and the categories of the processing operations of personal data likely to present specific risks to the rights and freedoms of individuals shall be subject to a prior checking include:

- processing operations of minors' personal data within direct marketing activities; and
- processing operations of personal data referred to in letter a) and personal data of minors collected via internet or electronic messaging.

Privacy notice (children)

Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

The Law on Personal Data does not provide specific requirements in relation to privacy notices for children.

2.5. Research

The Law on Personal Data and the GDPR both provide exemptions to data processing for historical and scientific research purposes. In addition, the two legislations permit further processing and require the implementation of appropriate safeguards. Unlike the GDPR, however, the Law on Personal Data does not provide a definition of such data and does not place limits on data subject right on this basis.

GDPR	Law on Personal Data

Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

The Law on Personal Data refers to processing of personal data for statistical activity, historical, or scientific research but does not provide definitions thereof.

Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

Article 4(1)(b): [...] Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible with the purpose of the collection if is carried out in compliance with the provision of the Law on Personal Data, including those for notifying the NCPDP, and observing safeguards for personal data processing, provided by by-laws regulating the statistical activity, historical, or scientific research.

Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

Article 4(1)(e): Storage of personal data for longer period for purposes of statistical, historical, or scientific research, shall be performed in compliance with appropriate safeguards for personal data processing, provided by by-laws regulating these fields, and only for as long as necessary to achieve those purposes.

GDPR	Law on Personal Data

Appropriate safeguards (cont'd)

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

Data subject rights (research)

Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

The Law on Personal Data does not provide generally restrictions on data subject rights when processing personal information for statistical activity, historical or scientific research.

However, Article 13(2): Where personal data concerning health is processed for the purpose of scientific-research, where there is clearly no risk of breaching the rights of the personal data subject, and the data is not used for taking measures or decisions regarding any particular individual, communication of information specified in Article 13(1) [the right to access] may be done within a period of time longer than the one stipulated by the Law on Access to Information 2008 (as amended), to the extent to which it could affect the good carrying-out or results of the research, but not later than the research is over.

3. Legal basis

Fairly consistent

The Law on Personal Data and the GDPR provide very similar lawful grounds for the processing of personal data, and enhanced protection for the processing of special categories of personal data. In addition, both legislations provide exemptions to processing for journalistic, literary, or artistic purposes and outline conditions for obtaining consent from data subjects.

GDPR	Law on Personal Data

Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 5(1): Personal data shall be processed with the consent of personal data subject.

Article 5(5): The personal data subject's consent is not required where:

(a) the processing is necessary for the 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;

(b) the processing is necessary for carrying out an obligation of the controller, under the law;

(c) the processing is necessary in order to protect the life, physical integrity, or health of the personal data subject;

(d) the processing is necessary for the 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 are disclosed;

(e) the processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party to whom personal data are disclosed, except where such interest is overridden by the interests for fundamental rights and freedoms of the personal data subject; and

(f) the processing is necessary for statistical, historical or scientific-research purposes, except where the personal data remain anonymous for longer period of processing.

Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

There are specific requirements for processing special categories of data, see Article 6 of the Law on Personal Data for further information.

GDPR	Law on Personal Data

Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 3(9): 'personal data subject's consent' any freely given, expressly and unconditionally indication of will, in written or electronic form, according to the requirements of the electronic document, by which the personal data subject signifies his agreement to personal data relating to him being processed.

Journalism/ artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Article 10: The processing of personal data and freedom of expression provisions referred to in Articles 5, 6 and 8 shall not apply if the processing of personal data is carried out, exclusively for journalistic, artistic, or literary purposes [...].

4. Controller and processor obligations

4.1. Data transfers

The Law on Personal Data and the GDPR both provide for transfers based on adequate protection and contractual clauses. However, the Law on Personal Data does not outline other mechanisms such as Binding Corporate Rules ('BCRs') or Codes of Conduct to enable international data transfers. In addition, both legislations do not provide data localisation requirements.

GDPR	Law on Personal Data

Adequate protection

Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Article 32(3): Transborder transmission of personal data undergoing processing or are intended for processing after transfer may take place only with the authorisation of the NCPDP, as provided for by law, and only if the country in question ensures an adequate level of protection of personal data subjects' rights and of data intended for transfer.

Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

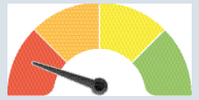
(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

Article 32(6): The NCPDP may authorise, as provided for by law, the transfer of personal data to another state, which legislation does not ensure at least the same level of protection as the one offered by the Law of the Republic of Moldova, where the controller provides sufficient guarantees regarding the protection and the exercise of the personal data subjects' rights, that are laid down by contracts concluded between controllers and natural or legal persons, on which provision the transfer is carried out.

GDPR	Law on Personal Data
Other mechanisms for data transfers (cont'd)	
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. (3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
Data localisation	
Not applicable.	Not applicable.

4.2. Data processing records



While the GDPR requires both data controllers and data processors to maintain data processing records, the Law on Personal Data does not provide such an obligation. Conversely, the Law on Personal Data outlines requirements for data processing notifications while the GDPR contains no equivalent requirement.

GDPR	Law on Personal Data
Data controller obligation	
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; and (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The Law on Personal Data does not contain specific record-keeping requirements for private entities. However, Article 15(4) of the Law on Personal Data states public authorities shall keep record of the application of exceptions set in paragraph 15 (1) and shall inform the NCPDP, within ten days, about the personal data processed in terms of this Article.

GDPR	Law on Personal Data

Data processor obligation

GDPR	Law on Personal Data
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The Law on Personal Data does not contain specific record-keeping requirements for private entities.

Records format

GDPR	Law on Personal Data
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The Law on Personal Data does not contain specific record-keeping requirements for private entities.

Required to make available

GDPR	Law on Personal Data
Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	The Law on Personal Data does not contain specific record-keeping requirements for private entities.

GDPR	Law on Personal Data

Exemptions

GDPR	Law on Personal Data
Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	The Law on Personal Data does not contain specific record-keeping requirements for private entities.

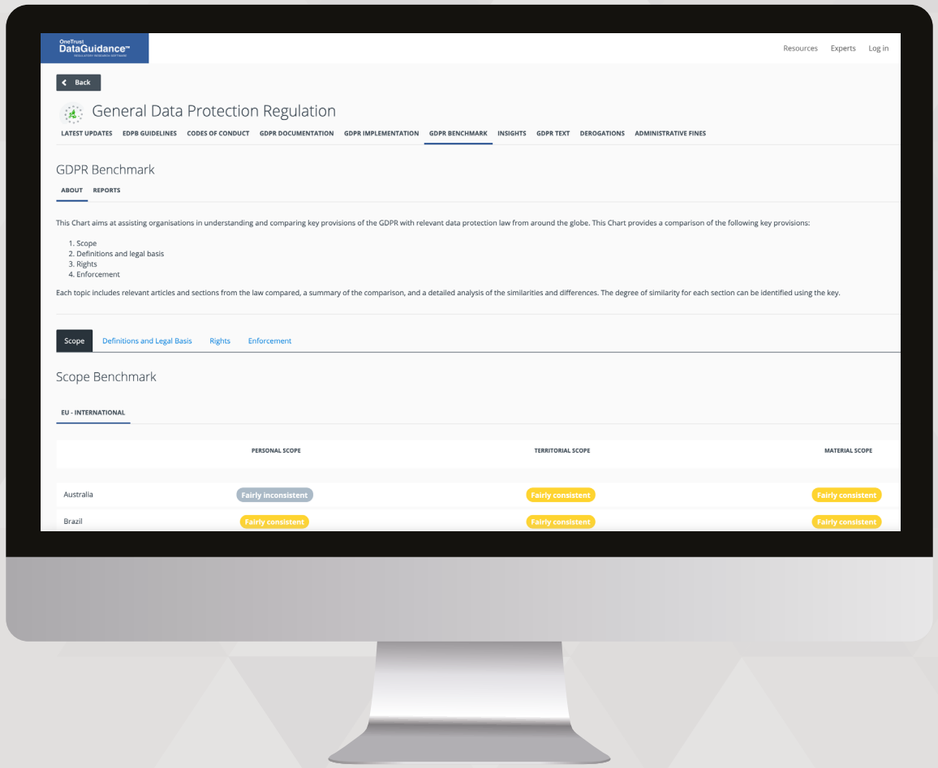
General Data Processing Notification ('DPN')

GDPR	Law on Personal Data
Not applicable.	Article 23(1): Controllers must notify the NCPDP, personally or through the representatives authorised by them (processors), before carrying out the processing of personal data intended to serve a purpose. The processing of other categories of personal data than those notified before shall be carried out under a new notification.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions

- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.3. Data protection impact assessment

Unlike the GDPR, the Law on Personal Data does not require or refer to DPIAs or contain any similar requirements.

GDPR	Law on Personal Data

When is a DPIA required

Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

The Law on Personal Data does not contain specific DPIA requirements.

DPIA content requirements

Article 35(7): The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

The Law on Personal Data does not contain specific DPIA requirements.

GDPR	Law on Personal Data

DPIA content requirements (cont'd)

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Consultation with authority

Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].

Article 24(1): If, based on the notification, the NCPDP establishes that the processing falls under one of the categories referred to in Article 24(2), it shall mandatory order the conduct of a prior checking, informing the controller or the processor within five days from the date of submission of notification. [Article 24(2) outlines when such prior consultation will be needed].

4.4. Data protection officer appointment

Unlike the GDPR, the Law on Personal Data does not require or refer to DPOs. However, guidelines released by the NCPDP provides recommendations regarding DPO appointments.

GDPR	Law on Personal Data

DPO tasks

Article 39(1): The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority; and

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The Law on Personal Data does not refer to DPOs.

However, the Decision provides recommendations for the appointment an individual(s) responsible for undertaking the measures necessary to comply with Law on Personal Data.

When is a DPO required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

The Decision does not explicitly address when a DPO will be required.

However, Data protection officer (only available in Romanian here) ('the Guide on Data Protection Officer') states that organisations are expected to designate such responsible person where:

GDPR	Law on Personal Data

When is a DPO required (cont'd)

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

- the processing of personal data constitutes the main activities of the controller which, by their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the main activities of the controller or of the processor involves the processing of special categories of data.

Group appointments

Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

The Decision does not explicitly address group appointments

Notification of DPO

Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

The Decision does not explicitly address notification of DPOs.

However, the Guide on Data Protection Officer states the NCPDP data controllers to make efforts to identify and appoint a responsible person as it is a useful indication for demonstrating compliance with data protection laws.

Qualifications

Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

The Decision does not explicitly address the qualification of a DPO

However, Article 17 of the Decision states that the personal data holder will nominate a responsible person for elaboration, implementing and monitoring compliance with the provisions of security policy of personal data, directly subordinated to the head of institution that will not have other responsibilities incompatible with the functional tasks of policy implementation.

4.5. Data security and data breaches

Both the GDPR and the Law on Personal Data provide a detailed list of security measures that should be undertaken to avoid data breaches. However, unlike the GDPR, the Law on Personal Data does not require data breaches to be notified to authorities or data subjects.

GDPR	Law on Personal Data
Security measures defined	
Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Article 30(1): while the processing of personal data, the controller must implement appropriate technical and organisational 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.
Data breach notification to authority	
Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	The Law on Personal Data does not explicitly provide a general data beach notification requirement. However, Article 90 of the Decision states Annually, by 31 January, reports on security incidents of personal data information systems will be presented to NCPDP by the personal data holders. Based on this report, the NCPDP undertakes the necessary measures that are compelled by the Law on personal data protection.
Timeframe for breach notification	
See Article 33(1) above.	Please see Article 90 of the Decision above.
Notifying data subjects of data breach	
Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	The Decision does not explicitly address notification to data subjects.
Data processor notification of data breach	
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The Decision does not explicitly address data breach notification by data processors.
Exceptions	
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	The Decision does not outline any exemptions regarding security incident notifications.

4.6. Accountability

Fairly inconsistent

The Law on Personal Data does not contain an express principle of accountability as in the GDPR. However, the Law on Personal Data provides requirements for controllers to ensure compliance with the law.

GDPR	Law on Personal Data
Principle of accountability	
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	Article 4(2): The controllers have the obligation to ensure that Article 4(1) is complied with.
Liability of data controllers and data processors	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	Article 33: For violation of this law, the convicted persons are liable under the civil, administrative, or criminal law.

5. Rights

Fairly consistent

5.1. Right to erasure

The GDPR and the Law on Personal Data provide a right to erasure. In terms of the right to erasure, both legislations provide grounds for the exercising, a right to be informed about, and a requirement to notify other controllers of this right, among other things. Nevertheless, the GDPR outlines a clear timeframe and format for responding to such requests, whereas the Law on Personal Data does not address this.

GDPR	Law on Personal Data
Grounds for erasure	
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	Article 14(1): Any personal data subject has the right to obtain from the controller or his representative, on request and free of charge the rectification, update, blocking or erasure of personal data, the processing of which does not comply with this law, in particular because of their incomplete or inaccurate nature.

GDPR	Law on Personal Data

Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Article 12(1)(3)(b): Where personal data is collected directly from the personal data subject, the controller or the processor must provide the data subject with [...] additional information, such as existence of the rights of access to data, the right of intervention upon data and the right to object, as well as conditions under which such rights may be exercised.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 14(a): Any personal data subject has the right to obtain from the controller or his representative, on request and free of charge the rectification, update, blocking or erasure of personal data, the processing of which does not comply with this law, in particular because of their incomplete or inaccurate nature.

Response timeframe

Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

The Law does not provide specific timeframes.

GDPR | Law on Personal Data

Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Law does not provide specific format requirements for the format of response.

Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Article 14 (b): [...] notification of the third parties to whom the personal data have been disclosed, about any operations performed under Article 14(a), except where such notification proves to be impossible or involves disproportionate effort towards the legitimate interest that might be violated.

Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 15(1): The provisions referred to in [...] 14 shall not apply where the processing of personal data is carried out in the course of activities provided for in Article 2 (2) (d), for the purposes of national defence, state security and public order, protection of the rights and freedoms of personal data subject or of other persons, if their application affects the efficiency of action or the objective pursued in fulfilment of legal duties of a public authority.

Article 15(4): As soon as the reasons that justified the enforcement of Article 15(1) and (2) of this Article no longer exist the controllers shall take the necessary measures in order to ensure the observance of personal data subject's rights provided for in Articles 12 – 14.

GDPR	Law on Personal Data

Exceptions (cont'd)

Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The Law on Personal Data does not provide specific exceptions to a right to erasure.

5.2. Right to be informed

Fairly inconsistent

The Law on Personal Data and the GDPR require data controllers to provide information about processing activities to data subjects, irrespective of whether information is collected directly or indirectly from the data subject. Both legislations also provide detailed disclosure of information that must be given to data subjects and general exceptions to this requirement. However, the GDPR establishes intelligibility obligations as well as requirements on the format in which information is communicated whereas the Law on Personal Data does not.

GDPR	Law on Personal Data

Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

The Law does not explicitly specify when information should be provided.

GDPR	Law on Personal Data

Informed prior to/ at collection (cont'd)

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

What information is to be provided

See Article 13(1) and (2) above.

Article 12: Where the personal data are collected directly from the personal data subject, the controller or the processor must provide the data subject with the following information, except where he already has it:

- the identity of the controller or of the processor, as the case may be;
- the purpose of processing for which the data are collected;
- additional information, such as:
- recipients or categories of recipients of personal data;
- existence of the rights of access to data, the right of intervention upon data and the right to object, as well as conditions under which such rights may be exercised; and
- whether the answers to the questions intended to collect data are mandatory or voluntary, as well as the possible consequences of denial to respond.

GDPR	Law on Personal Data

When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

Article 12(2): Where personal data is not collected directly from the personal data subject, the controller or the processor must, at the time of data collection or, if a disclosure to the third parties is envisaged, no later than the time when the data are first disclosed provide the personal data subject with information on the categories of personal data which are intended to be collected or disclosed, as well as with the information specified in Article 12 (1) except Article 12(3)(c).

Intelligibility requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Law does not outline any intelligibility requirements.

Format

The requirements of Article 13 do not apply where the data subject already has the information.

The requirements of Article 14 do not apply where:

(a) the data subject already has the information;

The Law does not provide specific format requirements.

Exceptions

The requirements of Article 13 do not apply where the data subject already has the information.

The requirements of Article 14 do not apply where:

General

Article 15(1): The provisions referred to in [...] 12 shall not apply where the processing of personal data is carried out in the course of activities provided for in Article 2 (2) (d), for the purposes of national defence, state security

GDPR	Law on Personal Data

Exceptions (cont'd)

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

and public order, protection of the rights and freedoms of personal data subject or of other persons, if their application affects the efficiency of action or the objective pursued in fulfilment of legal duties of a public authority.

Article 15(4): As soon as the reasons that justified the enforcement of Article 15(1) and (2) of this Article no longer exist the controllers shall take the necessary measures in order to ensure the observance of personal data subject's rights provided for in Articles 12 – 14.

When data is from third party

Article 12(3): Article 12(2) shall not apply where:

(a) the personal data subject has already the information;
(b) processing of personal data is carried out for statistical, historical or scientific-research purposes;

(c) provision of information that proves to be impossible or involves disproportionate effort towards the legitimate interest that might be violated; and

(d) recording or disclosure of personal data is expressly stipulated by law.

Fairly consistent

5.3. Right to object

Like the GDPR, the Law on Personal Data establishes a right to object to processing, as well as related provisions such as objecting to direct marketing and restricting processing. The Law on Personal Data is less detailed on how this right should be exercised and it does not explicitly refer to the withdrawal of consent.

GDPR	Law on Personal Data

Grounds for right to object/ opt out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Article 16(1): The personal data subject shall have the right to object at any time and free of charge on compelling legitimate grounds relating to his particular situation to the processing of personal data relating to him, save where otherwise provided by law. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

Withdraw consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 5(2): The consent given for personal data processing may be withdrawn at any time by the personal data subject. The withdrawal of consent shall not be retroactive.

Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

Article 14: Any personal data subject has the right to obtain from the controller or his representative, on request and free of charge the rectification, update, blocking, or erasure of personal data, the processing of which does not comply with this law, in particular because of their incomplete or inaccurate nature.

GDPR	Law on Personal Data
Restrict processing (cont'd)	
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	
Object to direct marketing	
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Article 16(2): The personal data subject has the right to object at any time and free of charge without any justification to the processing of personal data relating to him for the purpose of direct marketing. The controller or the processor is obliged to inform the person concerned about the right to object such operation before his personal data are to be disclosed to third parties.
Inform data subject of right	
See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	Article 12(1)(3)(b): Where personal data is collected directly from the personal data subject, the controller or the processor must provide the data subject with [...] additional information, such as existence of the rights of access to data, the right of intervention upon data and the right to object, as well as conditions under which such rights may be exercised.
Fees	
See Article 12(5) in section 5.1. above.	Article 16(2): The personal data subject shall have the right to object at any time and free of charge.
Response timeframe	
See Article 12(3) in section 5.1. above.	See section 5.1 above.
Format of response	
See Article 12(1) in section 5.1. above.	See section 5.1 above.
Exceptions	
See Article 12(5) in section 5.1. above.	The Law does not provide any exceptions for the right to object.

5.4. Right of access

Similar to the GDPR, the Law on Personal Data establishes grounds for the right of access. More specifically, both legislations require that data subjects be informed of this right, and details requirements for the charging of fees as well as exceptions to this right. Notably, the Law on Personal Data does not address verification of data subjects, or formats and timeframes for the response. In addition, the GDPR, sets out a more extensive list of information that must be provided in comparison to the Law on Personal Data.

GDPR	Law on Personal Data
Grounds for right of access	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Article 13(1): Any personal data subject has the right to obtain from the controller, upon request, without delay and free of charge: (a) confirmation as to whether or not data relating to him are being processed and information as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; (b) communication to him in an intelligible form and in a way that does not require additional equipment, of the data undergoing processing, and of any available information as to their source; (c) information on the logic involved in any automatic processing of data concerning the personal data subject; (d) information on legal consequences for the personal data subject generated by processing of these data; and (e) information on the exercise of the right of intervention upon the personal data.
Information to be accessed	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:	.See Article 13(1) above.

GDPR	Law on Personal Data

Information to be accessed (cont'd)

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source; and

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Inform data subject of right

See Article 12(1) in section 5.1.

Article 12(1)(3)(b): Where personal data is collected directly from the personal data subject, the controller or the processor must provide the data subject with [...] additional information, such as existence of the rights of access to data, the right of intervention upon data and the right to object, as well as conditions under which such rights may be exercised.

Fees

See Article 12(5) in section 5.1. above.

See Article 13(1) above.

Verify data subject request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

The Law does not provide specific verification requirements.

Response timeframe

See Article 12(3) in section 5.1. above.

See Article 13(1) above.

Format of response

See Article 12(1) in section 5.1. above.

See section 5.1 above.

Exceptions

See Article 12(5) in section 5.1. above.

Article 13(2): Where the personal data concerning health are processed for the purpose of scientific-research, where there is clearly no risk of breaching the rights of the personal data subject, and the data are not used for taking measures or decisions regarding any particular individual, communication of information specified in Article 13(1) may be done within a period of time longer than the one stipulated by the Law on access to information, to the extent to which it could affect the good carrying-out or results of the research, but not later than the research is over. The personal data subject must give his consent to the processing of health related data for scientific-research purposes, as well as to the possible delay, for this reason, of the communication of information provided for in Article 13(1).

5.5. Right not to be subject to discrimination

Consistent

Similar to the GDPR, the right not to be subject to discrimination in exercising rights is not explicitly mentioned in the Law on Personal Data. However, such a right can be inferred based on the protection from adverse effects on individuals' personal rights and interests under the GDPR, while no equivalent provision is provided in the Law on personal data. Nevertheless, the GDPR and Law on Personal Data provide a right not to be subject to automated decision-making.

GDPR	Law on Personal Data

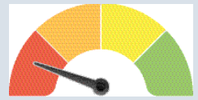
Definition of right

GDPR	Law on Personal Data
The GDPR only implies this right and does not provide an explicit definition for it.	The Law does not refer to this right nor imply a require not to be subject to discrimination

Automated processing

GDPR	Law on Personal Data
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Article 17 (1): Any person shall have the right to request for the rescinding, in whole or in part, of any individual decision which produces legal effects concerning his rights and freedoms, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him such as his performance at work, creditworthiness, conduct, or other similar aspects.

5.6. Right to data portability



Inconsistent

Unlike the GDPR, the Law on Personal Data does not explicitly refer to a right to data portability.

GDPR	Law on Personal Data

Grounds for portability

GDPR	Law on Personal Data
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	The Law does not explicitly provide for the right to data portability.

Inform data subject of right

GDPR	Law on Personal Data
See Article 12(1) in section 5.1.	The Law does not explicitly provide for the right to data portability.

Fees

GDPR	Law on Personal Data
See Article 12(5) in section 5.1. above.	The Law does not explicitly provide for the right to data portability.

Response timeframe

GDPR	Law on Personal Data
See Article 12(3) in section 5.1. above.	The Law does not explicitly provide for the right to data portability.

Format

GDPR	Law on Personal Data
See Article 20(1) above.	The Law does not explicitly provide for the right to data portability.

GDPR	Law on Personal Data
Controller to controller	
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	The Law does not explicitly provide for the right to data portability.
Technically feasible	
See Article 20(2) above.	The Law does not explicitly provide for the right to data portability.
Exceptions	
See Article 12(5) in section 5.1. above.	The Law does not explicitly provide for the right to data portability.

6. Enforcement

6.1. Monetary penalties

Unlike the GDPR, the Law on Personal Data does not explicitly address the issuance of monetary penalties. However, the Law on Personal Data provides for liability under civil, administrative, or criminal law.

GDPR	Law on Personal Data
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The Law does not explicitly provide of monetary penalties. However, Article 33 of the Law states that for violation of this law, the convicted persons are liable under the civil, administrative, or criminal law.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	The Law does not explicitly provide of monetary penalties.
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX;	The Law does not explicitly provide of monetary penalties.

GDPR	Law on Personal Data

Fine maximum (cont'd)

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.

The Law does not explicitly provide of monetary penalties.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

The Law does not explicitly provide of monetary penalties.

Mitigating factors (cont'd)

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Imprisonment

Not applicable.

The Law does not address imprisonment.

However, Article 33 of the Law states that for violation of this law, the convicted persons are liable under the civil, administrative, or criminal law.

DPO liability

Not applicable.

The Law does not explicitly address DPO liability

6.2. Supervisory authority

The Law on Personal Data provides for the establishment of the NCPDP. Similar to the GDPR, the NCPDP has investigatory, corrective, and advisory powers, and must submit annual reports.

GDPR	Law on Personal Data
Provides for data protection authority	
Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	Article 19(1): Control over compliance of personal data processing with the requirements of this law is performed by the NCPDP that carries out its activity under the conditions of impartiality and independence.
Investigatory powers	
Article 58(1): Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Article 20(1): The NCPDP has the following duties: (a) to supervise the compliance of the legislation on the protection of information and to monitor its application, especially the right to information, the right of access to data, the right of intervention upon the data and the right to object; (b) to authorise the processing operations of personal data as provided for by law; (c) to develop guidelines necessary to bring personal data processing in compliance with the provisions of this law, without affecting the area of competence of other bodies; (d) to provide information to personal data subjects on their rights; (e) to order the suspension or cessation of personal data processing performed with violation of the provisions of this law; (f) to keep the register of personal data controllers, which form and content is approved by the Government of Moldova; (g) the register shall be public, except for the information referred to in Article 23(2)(l)(g) to issue orders in the area of personal data protection, and standard forms for notifications and for its own registers; (h) to receive and analyse notifications on personal data processing;

GDPR	Law on Personal Data
Investigatory powers (cont'd)	
	(i) to carry out control of the lawfulness of personal data processing in accordance with the Law, which develops and approves it; (j) to make proposals on improving the enacted legislation in the area of personal data protection and processing; (k) to cooperate with public authorities, mass media, non - government organiations ('NGO'), as well as with similar foreign institutions; (l) to compile and analyse annual activity reports of public authorities with regard to the protection of individuals in respect of personal data processing; (m) to notify the law enforcement bodies if there are indication of committing crimes related to infringement of personal data subjects' rights; (n) to establish contraventions and to draw up minutes according to the Contravention Code of the Republic of Moldova; (o) to inform public authorities, on the situation existing in the field of the protection of personal data subjects' rights, as well as to respond to their claims and requests; (p) to survey the fulfilment of requirements set by the Government with regard to the personal data security within their processing; (q) to inform regularly the institutions and the society about its activity, the issues and priority concerns in the area of the protection of individual's rights; (r) to provide assistance and to perform the requests for assistance in terms of enforcement of the Convention for the protection of individuals with regard to automatic processing of personal data ('Convention 108'); and (s) to carry out other duties as provided for by law. Article 20(2): (2) The NCPDP has the following competences: (a) to request and receive, free of charge, from natural or legal persons governed by public law, or by private law, information necessary for the exercise of its duties; (b) to obtain from controllers the support and information necessary for the exercise of its duties;

GDPR	Law on Personal Data

Investigatory powers (cont'd)

	(c) to recruit specialists and experts in the activity of prior checking and control of the lawfulness of personal data processing in areas which require special expertise, with whom it shall conclude agreements of confidentiality; and (d) to request from controllers the rectification, blocking or destruction of personal data which are inaccurate or obtained unlawfully.

Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;	See Article 20(1) above.

GDPR | Law on Personal Data

Corrective powers (cont'd)

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.	

Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contractual clauses referred to in point (a) of Article 46(3);	See Article 20(1) above.

Authorisation/ advisory powers (cont'd)

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

See Article 20(1) above.

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

Tasks of authority (cont'd)

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

GDPR	Law on Personal Data

Tasks of authority (cont'd)

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

Annual report

Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Article 21(3): The NCPDP shall submit to the Parliament of Moldova, the President of the Republic of Moldova, and the Government, annually, until 15 March, the activity report for the preceding calendar year, which shall be published free of charge in the Official Gazette of the Republic of Moldova and on the website of the NCPDP.

6.3. Civil remedies for individuals

Fairly consistent

The Law on Personal Data and the GDPR both provide data subjects with a right of action, right to receive compensation for damage suffered as a result of non-compliance, and outline the liability of processors. However, the Law on Personal Data does not address matters such as data subject representation, or specific compensation amounts for data subjects.

GDPR	Law on Personal Data

Provides for claims/ cause of action

Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Article 18: Any person who has suffered damage as a result of an unlawful processing operation of personal data or his rights and interests guaranteed by this law have been violated, shall have the right to refer in a court in order to repair the material and moral damages.

Material and non-material damage

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

See Article 18 above.

Mandate for representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

The Law does not explicitly address the right to mandate representation.

Specifies amount for damages

Not applicable.

The Law does not specify the amount of damages.

GDPR	Law on Personal Data

Processor liability

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	Article 2(3): The provisions of this law are applicable to the processor, without prejudice to legal actions which could be initiated against the controller himself.

Exceptions

Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The Law does not address exemption from liability.