Republic of Moldova

PARLIAMENT

LAW No. 195 of 25.07.2024
on personal data protection

Published: 23.08.2024 in the Official Gazette No. 367-369 art. 574

The Parliament adopts this organic law.

This Law transposes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in the Official Journal of the European Union L 119/1 of 4 May 2016, CELEX: 32016R0679.

Chapter I
GENERAL PROVISIONS

Article 1. Subject-matter and purpose of the Law

(1) This Law lays down the legal framework on the following:
a) protection of natural persons with regard to the processing of personal data;
b) the organisation and operation of the National Centre for Personal Data Protection (hereinafter also referred to as *"the Centre"*);
c) supervision of the implementation of legislation on personal data protection;
d) legal liability and sanctions for violation of legislation on personal data protection.

(2) The purpose of this Law is to ensure the protection of the fundamental rights and freedoms of natural persons, and, in particular, the right to intimate, family and private life, in relation to the processing of personal data.

Article 2. Material scope

(1) This Law 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.

(2) This Law does not apply to the processing of personal data:
a) classified as state secrets, which is performed according to the Law no. 245/2008 on state secrets, to the extent necessary and proportionate for the protection of national security and defence;
b) by a natural person in the course of a purely personal or household activity;
c) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
d) of deceased persons, except in the case provided for in Article 52.

(3) This Law is without prejudice to the provisions of Law no. 284/2004 on information society services, in particular to the provisions related to liability of service providers and intermediaries provided for in Articles 14 to 17 of this law.

Article 3. Territorial scope

(1) This Law applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Republic of Moldova, regardless of whether the processing takes place in the Republic of Moldova or not.

(2) This Law applies to the processing of personal data of data subjects who are in the Republic of Moldova by a controller or processor not established in the Republic of Moldova, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Republic of Moldova; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Republic of Moldova.

(3) This Law applies to the processing of personal data by diplomatic missions and consular posts of the Republic of Moldova, as well as by other controllers or processors not established in the Republic of Moldova, if the legislation of the Republic of Moldova applies by virtue of public international law.

Article 4. Definitions

For the purposes of this Law, the following notions mean:

personal data – any information relating to an identified or identifiable natural person (hereinafter – *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;

processing – 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;

restriction of processing – the marking of stored personal data with the aim of limiting their processing in the future;

profiling – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

pseudonymisation – 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;

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;

controller – 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 normative acts, the controller or the specific criteria for its nomination are provided by those normative acts;

processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

establishment – the place of the effective and real exercise of activity through stable arrangements.

recipient – a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance to normative acts 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;

third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

consent – 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;

personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

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

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

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

national identification number – the number by which a natural person is identified in certain filing systems and which has general application, such as: state identification number, ID card series and number, passport number, driver’s license number;

representative – a natural or legal person established in the Republic of Moldova who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Law;

enterprise – a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

group of undertakings – a controlling undertaking and its controlled undertakings;

binding corporate rules – means personal data protection policies which are adhered to by a controller or processor established on the territory of the Republic of Moldova for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

total turnover – a turnover as defined in Article 4 of the Law no. 183/2012 on competition;

information society service – a service as defined in Article 4 of Law no. 284/2004 on information society services;

direct marketing – the communication, by telephone, post or any other mean of direct communication, of advertising or marketing messages (promoting goods or services) shared with particular persons;

international organisation – an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Chapter II
PRINCIPLES

Article 5. Principles relating to processing

(1) Personal data shall be:
a) processed lawfully, fairly and in a transparent manner in relation to the data subject (principle of lawfulness, fairness and transparency);
b) 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 54 (1), not be considered to be incompatible with the initial purposes (principle of purpose limitation);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimisation);
d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (principle of accuracy);
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 54 (1) subject to implementation of the appropriate technical and

organisational measures required by this Law in order to safeguard the rights and freedoms of the data subject (principle of storage limitation);

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of integrity and confidentiality).

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (principle of accountability).

Article 6. Lawfulness of processing

(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;

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.

(2) Personal data may be processed pursuant to paragraph (1) (e) if the processing is necessary for:

a) the performance of a task carried out in the public interest arising from the normative acts; or

b) the exercise by the controller of the functions or tasks provided for in the normative acts.

(3) The basis for the processing referred to in point (c) and (e) of paragraph 1 and paragraph 2 shall be laid down in the legislation of the Republic of Moldova.

(4) Paragraph (1) (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

(5) Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on legislation which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 (1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia*:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

b) e context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

d) the possible consequences of the intended further processing for data subjects;

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7. Conditions for consent

(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Law shall not be binding.

(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.

(4) When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8. Child's consent in relation to information society services

(1) 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 14 years old. Where the child is below the age of 14 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the legal representative of the child.

(2) The controller shall make reasonable efforts to verify that consent is given or authorised by the legal representative of the child, taking into consideration available technology.

(3) Paragraph 1 shall not affect the general contract law such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9. Processing of special categories of personal data

(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.

(2) Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where normative acts provide that the prohibition referred to in paragraph (1) may not be lifted by the data subject;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by normative acts or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a political party, trade union, religious cult or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims in administrative, judicial or out-of-court proceedings or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of normative acts which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of normative acts or pursuant to contract with a health service provider and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of normative acts which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on law and in accordance with Article 54 (1).

(3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under normative acts or by another person also subject to an obligation of secrecy under normative acts.

Article 10. Processing of personal data relating to criminal convictions and offences

(1) Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 (1) shall be carried out only under the control of public

authority or when the processing is authorised by normative acts providing for appropriate safeguards for the rights and freedoms of data subjects.

(2) Any comprehensive register of criminal convictions shall be kept only under the control of public authority.

Article 11. Processing which does not require identification

(1) If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Law.

(2) Where, in cases referred to in paragraph 1, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Chapter III
RIGHTS OF THE DATA SUBJECT

Section 1
Transparency and modalities for the exercise of the rights of the data subject

Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject

(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.

(2) The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11 (2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

(3) The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay, but 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.

(4) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Centre and filing a lawsuit.

(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.

(6) Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(7) The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner an overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

(8) The Centre may approve acts for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2
Information and access to personal data

Article 13. Information to be provided where personal data are collected from the data subject

(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 another country or international organisation and the existence or absence of an adequacy decision by the Centre, or in the case of transfers referred to in Article 46, 47 or 49 (2), 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;

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 the Centre;

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.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(4) Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14. Information to be provided where personal data have not been obtained from the data subject

(1) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with 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) the categories of personal data concerned;

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

f) where applicable, that the controller intends to transfer personal data to another country or international organisation and the existence or absence of an adequacy decision by the Centre, or in the case of transfers referred to in Article 46, 47 or 49 (2), reference to the appropriate or suitable safeguards and the means 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 provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

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

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

c) 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 and to object to processing as well as the right to data portability;

d) where 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;

e) the right to lodge a complaint with the Centre;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) 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.

(3) The controller shall provide the information referred to in paragraphs 1 and 2:

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

(4) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(5) Paragraphs 1 to 4 shall not apply where and insofar as:

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 54 (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 normative acts which provide appropriate measures to protect the data subject’s legitimate interests; or

d) where the personal data must remain confidential subject to a legal obligation of professional secrecy regulated by normative acts, including a legal obligation of secrecy.

Article 15. Right of access by the data subject

(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:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in other 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 the Centre;

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

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.

(2) Where personal data are transferred to another country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3
Rectification and erasure

Article 16. Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17. Right to erasure (“right to be forgotten”)

(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 normative acts 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).

(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.

(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 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 54 (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;
e) for the establishment, exercise or defence of legal claims in administrative, judicial or out-of-court proceedings.

Article 18. Right to restriction of processing

(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 in administrative, judicial or out-of-court proceedings;
d) the data subject has objected to processing pursuant to Article 21 (1) pending the verification whether the legitimate rights of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims in administrative, judicial or out-of-court proceedings or for the protection of the rights of another natural or legal person or for reasons of important public interest.
(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17 (1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20. Right to data portability

(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.

(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.

(3) The exercise of the right to data portability shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(4) The right to data portability shall not adversely affect the rights and freedoms of others.

Section 4
Right to object and automated individual decision-making

Article 21. Right to object

(1) The data subject shall have the right to object, on personal grounds, 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 in administrative, judicial or out-of-court proceedings.

(2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(3) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

(4) 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.

(5) In the context of the use of information society services, and notwithstanding the provision of Law no. 284/2004 on information society services, the data subject may exercise his or her right to object by automated means using technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 54 (1), the data subject, on personal grounds, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22. Automated individual decision-making, including profiling

(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.

(2) Paragraph 1 shall not apply if the decision:
a) is necessary for entering into, or performance of, a contract between the data subject and a controller;
b) is authorised by normative acts which also lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9 (1), unless point (a) or (g) of Article 9 (2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5
Restrictions

Article 23. Restrictions

(1) The obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, may be restricted by law, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the Republic of Moldova, in particular an important economic or financial interest of the Republic of Moldova, including monetary, budgetary and taxation matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

(2) Any law referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
a) the purposes of the processing or categories of processing;
b) the categories of personal data;
c) the scope of the restrictions introduced;
d) the safeguards to prevent abuse or unlawful access or transfer;
e) the specification of the controller or categories of controllers;
f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
g) the risks to the rights and freedoms of data subjects;
h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Chapter IV
CONTROLLER AND PROCESSOR

Section 1
General obligations

Article 24. Responsibility of the controller

(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law. Those measures shall be reviewed and updated where necessary.

(2) Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

(3) Adherence to approved codes of conduct as referred to in Article 40 or certification mechanisms approved under Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25. Data protection by design and by default

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at

the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Law and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(3) An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26. Joint controllers

(1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Law, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by normative acts. The arrangement may designate a contact point for data subjects.

(2) The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

(3) Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Law in respect of and against each of the controllers.

Article 27. Representatives of controllers or processors not established in the Republic of Moldova

(1) Where Article 3 (2) applies, the controller or the processor shall designate in writing a representative established in the Republic of Moldova.

(2) The obligation laid down in paragraph 1 shall not apply to:
a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9 (1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;
b) a public authority or institution
c) controllers and processors which are established in the European Economic Area member states; or

d) controllers and processors which have the designated representative with an establishment in the European Economic Area member states.

(3) The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, Centre and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Law.

(4) The designation of a representative by the controller or processor shall be without prejudice to the right to lodge a complaint with the Centre, or to file a lawsuit against the controller or processor.

Article 28. Processor

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the data subject's rights.

(2) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) Processing by a processor shall be governed by a contract or other legal act under the legislation of the Republic of Moldova, 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 as well as the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data carried out under the terms of Chapter V, unless the processor is required to process the data pursuant to normative acts. In such a case, the processor shall inform the controller of that legal requirement before processing, unless the normative acts prohibit such information on important grounds of public interest;

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality;

c) takes all measures required pursuant to Article 32;

d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the normative acts require storage of the personal data;

h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Law on data protection.

(4) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under the legislation of the Republic of Moldova, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Law. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Adherence of a processor to an approved code of conduct as referred to in Article 40 or a certification mechanism approved under Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

(6) Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 may be based, in whole or in part, on standard contractual clauses referred to in paragraph 7, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

(7) The Centre shall approve standard contractual clauses for the matters referred to in paragraph 3 and 4.

(8) The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

(9) Without prejudice to Articles 76, 86 to 88, if a processor infringes this Law by determining the purposes and means of personal data processing, the processor shall be considered to be a controller in respect of that processing.

Article 29. Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by normative acts.

Article 30. Records of processing activities

(1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility; the record shall include 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 other countries or international organisations;

e) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in Article 49 (2), the documentation of suitable safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organisational security measures referred to in Article 32 (1).

(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 processors are acting, and, where applicable, of the controller's or the processor's representative;

b) the categories of processing activities carried out on behalf of each controller;

c) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in Article 49 (2), the documentation of suitable safeguards;

d) where possible, a general description of the technical and organisational security measures referred to in Article 32 (1).

(3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

(4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the Centre on request.

(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.

Article 31. Cooperation with the Centre

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the Centre in the performance of its tasks.

Section 2
Security of personal data

Article 32. Security of processing

(1) Taking into account the state of the technological development, 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 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.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) Adherence to a code of conduct approved under Article 40 or a certification mechanism approved under Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.

(4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by normative acts.

Article 33. Notification of a personal data breach to the Centre

(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 Centre, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(3) The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(5) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Centre to verify compliance with this Article.

Article 34. Communication of a personal data breach to the data subject

(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.

(2) The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33 (3).

(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 be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the Centre, having considered the likelihood of the personal data breach resulting in a high risk, may require the controller to inform the data subject or may decide that one of the conditions referred to in paragraph 3 is met.

Section 3
Data protection impact assessment and prior consultation

Article 35. Data protection impact assessment

(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.

(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(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.

(4) The Centre shall approve a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

(5) The Centre may approve a list of the kind of processing operations for which no data protection impact assessment is required.

(6) Lists approved pursuant to paragraphs 4 and 5 shall be published in the Official Gazette of the Republic of Moldova and on the official website of the Centre.

(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;
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 Law taking into account the rights and legitimate interests of data subjects and other persons concerned.

(8) When assessing the impact of processing operations carried out by controllers or processors, due account shall be taken of compliance by controllers or processors with codes of conduct, if approved in accordance with Article 40, in particular with a view to a data protection impact assessment.

(9) Where appropriate, the controller shall seek the views of data subjects or their representatives on the envisaged processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(10) In the case of processing pursuant to point (c) or (e) of Article 6 (1), the provisions of paragraphs 1 to 7 shall not apply if a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of the normative acts providing the legal basis for the processing, unless the normative acts provide that a data protection impact assessment shall be carried out prior to the processing activities.

(11) Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36. Prior consultation

(1) The controller shall consult the Centre prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(2) Where the Centre is of the opinion that the envisaged processing referred to in paragraph 1 would infringe this Law, in particular where the controller has insufficiently identified or mitigated the risk, the Centre shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable, to the processor, and may use any of its powers provided for in Article 60. That period may be extended by six weeks, taking into account the complexity of the envisaged processing. The

Centre shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request together with the reasons for the delay. Those periods may be suspended until the Centre has obtained information it has requested for the purposes of the consultation.

(3) When consulting the Centre pursuant to paragraph 1, the controller shall provide the Centre with:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing activities, in particular for processing within a group of undertakings;

b) the purposes and means of the envisaged processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Law;

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

e) the data protection impact assessment; and

f) any other information requested by the Centre.

(4) Drafts of normative acts containing provisions relating to the processing of personal data are submitted to the Centre for an opinion under the terms of Law no. 100/2017 on normative acts.

Section 4
Data protection officer

Article 37. Designation of the data protection officer

(1) The controller and the processor shall designate a data protection officer if:

a) the processing is carried out by a public authority or institution, except for courts in the administration of justice;

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 or personal data relating to criminal convictions and offences referred to in Article 10.

(2) A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each of their establishments.

(3) Where the controller or the processor is a public authority or institution, a single data protection officer may be designated for several such authorities or institutions, taking account of their organisational structure and size.

(4) In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by normative acts, shall designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

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

(6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

(7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Centre.

Article 38. Position of the data protection officer

(1) The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of his or her tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

(4) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Law.

(5) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with normative acts.

(6) The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39. Tasks of the data protection officer

(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 Law and to other provisions of normative acts on data protection;

b) to monitor compliance with this Law, with other provisions of normative acts on data protection 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 on request as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d) to cooperate with the Centre;

e) to act as the contact point for the Centre 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.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5
Codes of conduct and certification

Article 40. Codes of conduct

(1) The Centre shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Law, taking into account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

(2) Associations and other bodies representing categories of controllers or processors may draw up codes of conduct, or amend such codes, for the purpose of specifying the application of this Law, such as with regard to:

a) fair and transparent processing;

b) the legitimate interests pursued by controllers in specific contexts;

c) the collection of personal data;

d) the pseudonymisation of personal data;

e) the information provided to the public and to data subjects;

f) the exercise of the rights of data subjects;

g) the information provided to, and the protection of, children, and the manner in which the consent of the legal representatives of children is to be obtained;

h) the measures and procedures provided for in Articles 24 and 25 and the measures to ensure security of processing provided for in Article 32;

i) the notification of personal data breaches to Centre and the communication of such personal data breaches to data subjects;

j) the transfer of personal data to other countries or international organisations; or

k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects provided for in Articles 72 and 74.

(3) In addition to the controllers and processors covered by this Law, codes of conduct approved pursuant to paragraph 5 may also be adhered to by controllers or processors that are not subject to this Law pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to other countries or international organisations under the terms provided for in point (d) of Article 46 (2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

(4) A code of conduct provided for in paragraph 2 shall contain mechanisms which enable the body referred to in Article 41 (1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the Centre.

(5) Associations and other bodies referred to in paragraph 2 which intend to draw up a code of conduct or to amend an existing code shall submit the draft code or amendment to the Centre. The Centre shall provide an opinion on whether the draft code or amendment complies with this Law and shall approve it, if it finds that it provides sufficient appropriate safeguards.

(6) Where the draft code or amendment is approved in accordance with paragraph 5, the Centre shall register and publish the code on its official website.

(7) The Centre shall keep a record of the codes of conduct and approved amendments in a register and shall ensure the publication on its official website of the updated and consolidated texts of the codes of conduct following the approval of amendments thereto.

Article 41. Monitoring of approved codes of conduct

(1) Without prejudice to the tasks and powers of the Centre provided for in Articles 59 and 60, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Centre.

(2) A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:
a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Centre;
b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
c) established procedures and structures to handle and resolve complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
d) demonstrated to the satisfaction of the Centre that its tasks and duties do not result in a conflict of interests.

(3) The Centre shall approve the requirements for accreditation of a body as referred to in paragraph 1.

(4) Without prejudice to the tasks and powers of the Centre, a body as referred to in paragraph 1 shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the Centre of such actions and the reasons for taking them.

(5) The Centre shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are no longer met or where actions taken by the body infringe this Law.

(6) This Article shall not apply to processing carried out by public authorities and institutions.

Article 42. Certification

(1) The Centre shall encourage the establishment of personal data protection certification mechanisms and of personal data protection seals and marks, for the purpose of demonstrating compliance with this Law of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

(2) In addition to adherence by controllers or processors subject to this Law, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 may be established for the purpose of demonstrating the existence of appropriate safeguards provided

by controllers or processors that are not subject to this Law pursuant to Article 3 within the framework of personal data transfers to other countries or international organisations under the terms referred to in point (e) of Article 46 (2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

(3) The certification shall be voluntary and available via a process that is transparent.

(4) A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Law and is without prejudice to the tasks and powers of the Centre.

(5) A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the Centre, on the basis of certification criteria approved by the Centre.

(6) The controller or processor which submits its processing activities to the certification mechanism shall provide the certification body, or where applicable, the Centre, with all information and access to its processing activities which are necessary to conduct the certification procedure.

(7) Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies or by the Centre where the criteria for the certification are not or are no longer met.

(8) The Centre shall collate all certification mechanisms and personal data protection seals and marks in a register and shall publish them on its official website.

Article 43. Certification bodies

(1) Without prejudice to the tasks and powers of the Centre provided for in Articles 59 and 60, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the Centre in order to allow it to exercise its powers pursuant to point (h) of Article 60 (2) where necessary, issue and renew certification.

(2) Certification bodies shall be accredited by the National Accreditation Centre where they have:

a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the National Centre for Personal Data Protection;

b) undertaken to respect the criteria approved under Article 42 (5);

c) established procedures for the issuing, periodic review and withdrawal of personal data protection certification, seals and marks;

d) established procedures and structures to handle and resolve complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

e) demonstrated, to the satisfaction of the National Centre for Personal Data Protection, that their tasks and duties do not result in a conflict of interests.

(3) The accreditation of certification bodies as referred to in paragraphs 1 and 2 shall take place on the basis of certification requirements approved by the Centre. Those

requirements shall complement those envisaged in Law no. 235/2011 on accreditation and conformity assessment activities and the technical rules that describe the methods and procedures of the certification bodies.

(4) The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Law. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

(5) The certification bodies referred to in paragraph 1 shall provide the National Centre for Personal Data Protection with the reasons for granting or withdrawing the requested certification.

(6) The requirements referred to in paragraph 3 and the criteria referred to in Article 42 (5) shall be published by the National Centre for Personal Data Protection on its official website.

(7) The National Accreditation Centre, including at the request of the National Centre for Personal Data Protection, shall revoke the accreditation granted to a certification body pursuant to paragraph 1, where conditions for accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Law.

(8) The National Centre for Personal Data Protection may adopt technical standards for certification mechanisms and personal data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks.

Chapter V
TRANSFERS OF PERSONAL DATA TO OTHER COUNTRIES OR TO INTERNATIONAL ORGANISATIONS

Article 44. General principle for transfers

(1) Any transfer of personal data which are undergoing processing or are intended for processing after transfer to another country or to an international organisation shall take place only if, subject to the other provisions of this Law, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the other country or an international organisation to another country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Law is not undermined.

(2) This Chapter shall not apply to transfers of personal data to Member States of the European Economic Area. No special authorisation is required for such transfers.

Article 45. Transfers on the basis of an adequacy decision

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

(2) When assessing the adequacy of the level of protection, the Centre shall, in particular, take account of the following elements:

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

b) the existence and effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the Centre;

c) the international commitments the country or international organisation concerned has entered into, or other obligations arising from international treaties as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data; and

d) the adequacy decisions of the European Commission.

(3) The Centre, after assessing the adequacy of the level of protection, may decide that another country, a territory or one or more specified sectors within a country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The decision shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the foreign country or international organisation. The decision shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2.

(4) The Centre shall, on an ongoing basis, monitor developments in other countries and international organisations that could affect the functioning of decisions issued pursuant to paragraph 3 and decisions issued before the entry into force of this Law.

(5) The Centre shall, where available information reveals, in particular following the review referred to in paragraph 3, that a country, a territory or one or more specified sectors within a country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2, to the extent necessary, repeal or amend the decision referred to in paragraph 3 without retro-active effect.

(6) The Centre may, in conjunction with the competent authorities of the Republic of Moldova, enter into consultations with the country or international organisation with a view to remedying the situation giving rise to the decision issued pursuant to paragraph 5.

(7) A decision issued pursuant to paragraph 5 is without prejudice to transfers of personal data to the country, a territory or one or more specified sectors within that country, or the international organisation in question pursuant to Articles 46 to 49.

(8) The Centre shall publish in the Official Gazette of the Republic of Moldova and on its official website a list of the countries, territories and specified sectors within a country and

international organisation for which it has decided that an adequate level of protection is or is no longer ensured.

Article 46. Transfers subject to appropriate safeguards

(1) In the absence of a decision pursuant to Article 45 (3), a controller or processor may transfer personal data to another 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 the Centre, by:

a) a binding and enforceable legal act between public authorities or institutions;

b) binding corporate rules in accordance with Article 47;

c) standard personal data protection clauses approved by the Centre or adopted by the European Commission;

d) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the other country to apply the appropriate safeguards, including as regards data subjects' rights; or

e) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the other country to apply the appropriate safeguards, including as regards data subjects' rights.

(3) Subject to the authorisation from the Centre, 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 other country or international organisation; or

b) provisions to be inserted into administrative arrangements between public authorities or institutions which include enforceable and effective data subject rights.

Article 47. Binding corporate rules

(1) The Centre shall approve binding corporate rules provided that they:

a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

c) fulfil the requirements provided for in paragraph 2.

(2) The binding corporate rules referred to in paragraph 1 shall specify at least:

a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the country or countries in question;

c) their legally binding nature, both internally and externally;

d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the Centre and to file a lawsuit in accordance with Article 74, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

f) the acceptance by the controller or processor established on the territory of the Republic of Moldova of liability for any breaches of the binding corporate rules by any member concerned not established in the Republic of Moldova. The controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) is provided to the data subjects in addition to Articles 13 and 14;

h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint examination;

i) the complaint procedures;

j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Centre;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Centre;

l) the cooperation mechanism with the Centre to ensure compliance with the rules by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the Centre the results of verifications of the measures referred to in point (j);

m) the mechanisms for reporting to the Centre any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in another country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Article 48. Transfers or disclosures not authorised by normative acts

Any judgment of a court and any decision of a public authority of a country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international treaty, such as a mutual legal assistance treaty, in force between the requesting country and the Republic of Moldova, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49. Derogations for specific situations

(1) In the absence of an adequacy decision pursuant to Article 45 (3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to another country or an international organisation shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of a legal claim in an administrative, judicial or out-of-court proceeding;

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which according to normative acts is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by normative acts for consultation are fulfilled in the particular case.

(2) Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the paragraph 1 of this Article is applicable, a transfer to another country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the Centre of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

(3) A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

(4) Points (a), (b) and (c) of paragraph 1 and paragraph 2 shall not apply to activities carried out by public authorities in the exercise of their public powers.

(5) The public interest referred to in point (d) of paragraph 1 shall be provided for in the normative acts.

(6) In the absence of an adequacy decision, normative acts may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to another country or an international organisation.

(7) The controller or processor shall document the assessment as well as the suitable safeguards referred to in the paragraph 2 in the records referred to in Article 30.

Article 50. International cooperation for the protection of personal data

In relation to other countries and international organisations, the Centre shall take appropriate steps to:

a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with other countries.

Chapter VI
SPECIFIC CASES
OF PERSONAL DATA PROCESSING

Article 51. Processing and freedom of expression

(1) For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, this Law shall not apply if the following cumulative conditions are met:

a) the controller processes personal data with the intention of publishing journalistic, academic, artistic or literary material;

b) publication of the material would be in the public interest;

c) the application of the provisions of this Law is incompatible with the realization of journalistic purposes or the purpose of academic, artistic or literary expression.

(2) The Centre shall be competent to supervise processing operations carried out pursuant to paragraph 1.

(3) The data subject shall be entitled to file a lawsuit pursuant to Article 74 and to claim compensation pursuant to Article 76, if he or she considers that his or her personal data have been processed in breach of paragraph 1 of this Article.

(4) This Article is not applicable to legal relationships of access to information of public interest. In this case, the conditions pursuant to Article 52 shall be applied.

Article 52. Processing and access to information of public interest

(1) Personal data held by controllers may be disclosed under the conditions of Law no. 148/2023 on access to information of public interest, except for special categories of personal data referred to in Article 9 (1) of this Law.

(2) Paragraph 1 shall not apply to data subjects' requests for access to their own personal data. In this case, the provisions of sections 1 and 2 of the Chapter III shall be applied.

Article 53. Processing of the national identification number

(1) Processing of a national identification number, including through the collection or disclosure of documents containing it, may be carried out in the situations provided for in Article 6 (1).

(2) Processing of a national identification number, including through the collection or disclosure of documents containing it, for the purpose provided for in point (f) of Article 6 (1), in particular for the legitimate interests pursued by the controller or a third party, shall be carried out under the following safeguards set up by the controller:

a) implementation of appropriate technical and organisational measures to comply especially with the data minimisation principle and to ensure the security and confidentiality of personal data processing under Article 32;

b) determination of storage periods according to the nature of the data and the purpose of the processing, as well as of specific periods where personal data must be erased or reviewed with a view to their erasure;

c) regular training on the obligations of persons who, under the direct authority of the controller or processor, process personal data.

Article 54. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(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 Law, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in 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. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, Articles 15, 16, 18 and 21 shall not apply, subject to the conditions and safeguards referred to in paragraph 1 of this Article, in so far as the rights provided for in these Articles are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(3) Where personal data are processed for archiving purposes in the public interest, Articles 15, 16, 18 and 21 shall not apply, subject to the conditions and safeguards referred to in paragraph 1 of this Article, in so far as the rights provided for in these Articles are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(4) Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Chapter VII
NATIONAL CENTRE FOR PERSONAL DATA PROTECTION

Section 1
General provisions

Article 55. Status of the Centre

(1) The National Centre for Personal Data Protection is a public authority that operates at the national level as a single structure, independent from other public authorities and from other legal and natural persons.

(2) The Centre is a legal person of public law and has a seal with the image of the State Coat of Arms of the Republic of Moldova.

(3) The headquarters of the Centre is located in Chisinau.

Article 56. Funding of the Centre's activity

(1) The Centre shall be financed from the state budget.

(2) The Centre shall develop, approve and manage the budget according to the principles, rules and procedures provided for in the Law no. 181/2014 on public finance and fiscal responsibility.

(3) The economic and financial activity of the Centre shall be subject to the audit by the Court of Accounts.

Article 57. Budget and structure of the Centre

The budget and the structure of the Centre shall be approved by the Director of the Centre.

Section 2
Mission, tasks and powers of the Centre

Article 58. Mission of the Centre

(1) The Centre shall ensure the supervision and monitoring of the implementation of this Law and of other normative acts on personal data processing, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of personal data.

(2) The Centre shall not be competent to supervise processing operations of courts in the administration of justice.

Article 59. Tasks of the Centre

(1) To achieve its mission, the Centre shall:
a) monitor and enforce the application of this Law;
b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, especially to activities addressed specifically to children;
c) advise the Parliament, the Government and other public authorities 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 Law;

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

f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 72, 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 a supervisory authority from other countries is necessary;

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

h) conduct investigations on the application of this Law, including on the basis of information received from supervisory authority from other country 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) approve standard contractual clauses referred to in Article 28 (7) and in point (c) of Article 46 (2);

k) approve 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) approve the requirements for accreditation of the bodies for monitoring codes of conduct pursuant to Article 41 and of the certification bodies pursuant to Article 43;

q) conduct the accreditation of the bodies for monitoring codes of conduct pursuant to Article 41 and of the certification bodies 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;

t) keep internal records of infringements of this Law and of measures taken, especially the warnings issued and the sanctions imposed in accordance with Article 60 (2);

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

(2) The performance of the tasks of the Centre shall be free of charge for the data subject and, where applicable, for the data protection officer.

(3) Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Centre may charge a reasonable fee based on administrative costs, or refuse to examine the request. The Centre shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 60. Powers of the Centre

(1) The Centre shall have 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 Law;

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 normative acts.

(2) The Centre shall the following corrective powers:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Law;

b) to issue warnings to a controller or a processor where processing operations have infringed provisions of this Law;

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 Law;

d) to order the controller or processor to bring processing operations into compliance with the provisions of this Law, 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 in the manner required by law;

f) to impose a temporary or definitive limitation including a ban on processing in the manner required by law;

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;

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 a fine pursuant to Articles 86 to 88, 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 another country or to an international organisation.

(3) The centre shall have 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 Parliament, the Government or other public authorities as well as to the public on any issue related to the protection of personal data;

c) to issue an opinion and approve draft codes of conduct pursuant to Article 40 (5);

d) to accredit certification bodies pursuant to Article 43;

e) to issue certifications and approve criteria of certification in accordance with Article 42 (5);

f) to approve standard data protection clauses referred to in Article 28 (7) and in point (c) of Article 46 (2);

g) to authorise contractual clauses referred to in point (a) of Article 46 (3);

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

i) to approve binding corporate rules pursuant to Article 47.

(4) The powers of the Centre shall be exercised, according to the legislation, by the Director or Deputy Directors of the Centre, data protection inspectors and other staff of the Centre.

Article 61. Activity report

(1) The Centre shall submit by March, 31, to the Parliament and the Government the annual activity report for the previous year regarding its activities, which includes, at least, information on the types of infringement notified and types of measures taken in accordance with Article 60 (2).

(2) The activity report shall be published on the official website of the Centre.

Section 3
Organization of the Centre

Article 62. Leadership of the Centre

(1) The Centre shall be headed by a Director, assisted by two Deputy Directors.

(2) The positions of Director and Deputy Directors of the Centre shall be positions of public dignity and incompatible with any other position or remunerated activity, except for teaching, scientific and creative activities.

(3) The Director and Deputy Directors of the Centre, in the performance of their duties, shall be independent of any direct or indirect influence and shall not seek or take instructions from anybody.

(4) The Director and Deputy Directors of the Centre shall, both during and after their terms of office, comply with professional secrecy with regard to confidential information coming to their knowledge in the course of the performance of their duties or in the exercise of their powers, in particular with regard to the reporting by natural persons of infringements of this Law.

Article 63. Appointment of the Director of the Centre

(1) The Director of the Centre shall be appointed by the Parliament through a competition for a 7-year term of office. A person may not be appointed as Director of the Centre for two consecutive terms.

(2) A person may apply for the position of Director of the Centre, if he or she:
a) is a citizen of the Republic of Moldova;
b) is not subject to a remedial measure in the form of guardianship;
c) has a law degree;
d) has at least 5 years employment record in the field of law;
e) has an irreproachable reputation;
f) is not a member of a political party;
g) is medically fit for the performance of the duties, according to the health certificate issued in accordance with the law;

h) knows Romanian language.

(3) A person shall be deemed not to have an irreproachable reputation, within the meaning of point (e) of paragraph 1, if he or she:

a) has a criminal record;

b) has been deprived by a final court decision of the right to hold certain positions or to perform certain activities, as a main or additional penalty;

c) has been found by a final act to have infringed the legal regime of conflicts of interest, incompatibilities, restrictions and limitations;

d) is subject to an irrevocable court decision ordering confiscation of unjustified wealth;

e) had negative results of the professional integrity test for violation of the obligation referred to in point (a) of Article 7 (2) of the Law no. 325/2013 on the evaluation of institutional integrity, for the last 5 years, in his or her professional integrity record.

f) is prohibited from holding a public office or a public dignity office, given a finding of the National Integrity Authority.

(4) The competition for the selection of the Director of the Centre shall be organised by the Committee for Legal Affairs, Appointments and Immunities of the Parliament at least three months before the expiry of the term of office of the acting Director.

(5) The competition shall be conducted in a public way. Information on the organisation and conduct of the competition, the requirements for candidates and the documents to be submitted shall be published on Parliament's official website and in the media at least 30 days before the date of the competition.

(6) The competition shall be deemed valid if at least two candidates take part in it. If insufficient applications for the competition have been submitted or the candidates do not meet the requirements stipulated in this Law, a repeat competition shall be announced and held within 30 days.

(7) Candidates' CVs shall be published on Parliament's official website for public consultation.

(8) The candidates shall be assessed by the Committee for Legal Affairs, Appointments and Immunities.

(9) After the assessment, the Committee shall propose to Parliament the candidate for appointment as Director of the Centre.

(10) The proposed candidate shall be appointed as Director of the Centre by a majority vote of the elected members. If the required number of votes for the appointment of the Director has not been obtained, the Committee for Legal Affairs, Appointments and Immunities shall, within 15 days, announce the organisation and conduct of a new competition in accordance with this Article.

(11) On the day of appointment, the Director of the Centre shall take the following oath of office before the Parliament:

„I swear to faithfully and honestly perform my functional duties, serve the Republic of Moldova, comply with the Constitution and laws of the Republic of Moldova, protect fundamental human rights and freedoms, democracy and the well-being of the people."

(12) Refusal to take the oath of office shall entail the invalidity of the appointment.

Article 64. Appointment of Deputy Directors of the Centre

(1) The Deputy Directors of the Centre shall be appointed by Parliament on a proposal from the Director of the Centre for a 7-years period.

(2) A person who meets the conditions provided for in the Article 63 (2) and (3) may be appointed as deputy Director of the Centre.

(3) The person proposed by the Director of the Centre shall be appointed as Deputy Director by a majority vote of the elected members.

Article 65. Duties of the Director and Deputy Directors of the Centre

(1) The Director of the Centre shall perform the following duties:
a) conduct, organise and control the Centre's activity;
b) represent the Centre at national and international levels;
c) ensure the monitoring of the implementation of this Law and other normative acts on personal data processing;
d) issue orders, decisions and dispositions pursuant to and for the purposes of the execution of the law;
e) approve methodological guidelines in order to ensure the proper interpretation and implementation of this Law and other normative acts on personal data processing;
f) approve or amend the staffing of the Centre according to the established structure and staff-limit;
g) approve the regulations of the subdivisions of the Centre;
h) appoint data protection inspectors, modify, suspend and terminate their service, in accordance with the law;
i) appoint civil servants and contractual personnel of the Centre's apparatus, modify, suspend and terminate their service or employment, in accordance with the law;
j) resolve the issues relating to the determination of increments and the payment of bonuses in accordance with the law;
k) organise and implement the internal management control system and is liable for the management of the Centre's budget and public assets under its administration;
l) manage public finances and administer the Centre's public assets according to the good governance principles;
m) may delegate some of his or her duties to the Deputy Directors of the Centre or to civil servants of the Centre;
n) other duties stipulated by legislation.

(2) The Deputy Directors of the Centre shall assist the Director in the management of the Centre and shall exercise the powers delegated to them by the Director. In the absence of the Director of the Centre or in the event of a vacancy in his or her office, all his or her functions shall be exercised by the Deputy Director appointed by order of the Director of the Centre.

Article 66. Termination of the term of office of the Director and Deputy Directors of the Centre

(1) The term of office of the Director or Deputy Directors of the Centre shall cease in the event of:

a) resignation;
b) dismissal;
c) expiry of the term of office;
d) achievement of retirement age;
e) death.

(2) The Director or a Deputy Director of the Centre shall be dismissed if he or she:
a) has committed a serious breach of his or her functional duties stipulated by law;
b) has not submitted a declaration of assets and personal interests or has refused to submit it;
c) has become a member of a political party;
d) has become subject to a final criminal conviction;
e) no longer meets the conditions referred to in Article 63 due to circumstances that have arisen;
f) for health reasons, is unable to exercise his or her duties for more than three consecutive months;
g) is declared missing in accordance with the law.

(3) The grounds referred to in paragraphs 1 to 2 shall be established at a plenary session of Parliament, based on the report of the Committee for Legal Affairs, Appointments and Immunities, by adopting of a decision of Parliament noting the occurrence of the situation that gives grounds for the termination of the term of office. The termination of the term of office of the Director or Deputy Directors of the Centre shall be adopted by Parliament by a majority of the elected members.

(4) If the term of office of the Director of the Centre expires, he or she shall continue to exercise his or her duties until a new Director of the Centre is appointed.

(5) The term of office of the Deputy Directors of the Centre shall cease together with that of the Director of the Centre, but they shall continue to exercise their duties until the appointment of new Deputy Directors.

Article 67. Centre’s personnel

(1) The Centre’s personnel consists of persons with public dignity positions, civil servants and contractual personnel.

(2) The duties and tasks of the Centre’s personnel shall be established in the internal regulation approved by order of the Director of the Centre.

Article 68. Data protection inspector

(1) The data protection inspector shall be responsible for handling complaints relating to alleged infringements of this Law, investigating the application of the legislation on personal data protection, and for other tasks provided for by legislation.

(2) The position of data protection inspector is a public office, exercised in accordance with this Law and the Law no. 158/2008 on the public office and the status of civil servant.

(3) The data protection inspector shall receive a service card, as prescribed, by the Centre.

Article 69. Appointment of the data protection inspector

(1) A person may apply for the position of data protection inspector if he or she meets all of the following conditions:
a) is a citizen of the Republic of Moldova
b) is domiciled in the Republic of Moldova;
c) is not subject to a remedial measure in the form of guardianship;
d) has a law or IT degree;
e) has an irreproachable reputation;
f) knows Romanian language.
(2) A person shall be deemed not to have an irreproachable reputation, within the meaning of point (e) of paragraph 1, if he or she:
a) has a criminal record;
b) has been deprived by a final court decision of the right to hold certain positions or to perform certain activities, as a main or additional penalty;
c) has been found by a final act to have infringed the legal regime of conflicts of interest, incompatibilities, restrictions and limitations;
d) is subject to an irrevocable court decision ordering confiscation of unjustified wealth;
e) has entries on negative results of the professional integrity test for violation of the obligation referred to in point (a) of Article 7 (2) of the Law no. 325/2013 on the evaluation of institutional integrity, within the last 5 years, in his or her professional integrity record;
f) is prohibited from holding a public office or public dignity office, given a finding of the National Integrity Authority.

Article 70. Liability of data protection inspectors

(1) The data protection inspector shall be liable for the lawfulness of actions taken within the investigation procedures and for the quality of the investigation performed.

(2) The data protection inspector shall bear disciplinary, contraventional, civil or criminal liability in accordance with the legislation.

Article 71. Status of the Centre's personnel

The activity of the Centre's personnel shall be subject to the regulations of this Law and, as the case may be, of the Law no. 199/2010 on the status of persons with public dignity positions, Law no. 158/2008 on the public office and the status of civil servant, and labour legislation.

Chapter VIII
LEGAL REMEDIES, LIABILITY AND SANCTIONS

Section 1
General provisions

Article 72. Right to lodge a complaint with the Centre

(1) Without prejudice to Article 74, every data subject shall have the right to lodge a complaint with the Centre, if the he or she considers that the processing of personal data relating to him or her infringes this Law.

(2) Statute of limitations for lodging a complaint shall make up one year from the date on which the person could have become aware of the alleged infringement, but no later than 3 years from the date of the alleged infringement.

(3) In the case of an alleged continuing or prolonged infringement, statute of limitations period shall start from the date of the last action or inaction.

(4) If the complaint is lodged after the expiry of the statute of limitations referred to in in paragraphs (2) and (3), the Centre shall reject the complaint.

(5) The Centre shall inform the complainant on the progress and the outcome of the complaint, including the possibility of challenging the Centre's acts in accordance with Article 73.

(6) The provisions of the Administrative Code shall apply only insofar as they are not contrary to the provisions of this Law.

Article 73. Right to challenge the actions or inactions of the Centre

(1) Actions or inactions of the Centre may be challenged directly before the court, in accordance with the Administrative Code, without preliminary procedure.

(2) Where the Centre does not handle the complaint or inform the complainant on the progress and the outcome of the complaint within three months in accordance with Article 72, the person concerned may challenge the Centre's inactions directly before the court, in accordance with the Administrative Code, without preliminary procedure.

Article 74. Right to file a lawsuit against a controller or processor

Without prejudice to Articles 72 and 73 and to alternative dispute resolution procedures, each data subject shall have the right to file a lawsuit in the competent court, where he or she considers that his or her rights under this Law have been infringed as a result of the processing of his or her personal data in non-compliance with the Law.

Article 75. Representation of data subjects

The data subject shall be entitled to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the legislation, 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 72 to 74 on his or her behalf, and to exercise the right to receive compensation referred to in Article 76 on his or her behalf where provided for by normative acts.

Article 76. Right to compensation and liability

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

(2) Any controller involved in processing shall be liable for the damage caused by processing which infringes the Law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(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.

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage caused, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

(6) Court proceedings for exercising the right to receive compensation shall be brought before the competent courts in accordance with the law.

Section 2

Preliminary examination, investigation and decision-making

Article 77. Initiation of the examination procedure

(1) The Centre shall initiate the procedure for the examination of alleged infringements of this Law or of other normative acts on personal data processing:
a) upon complaint by a data subject; or
b) *ex officio*.

(2) According to Article 81, the Centre may initiate the examination *ex officio* on the basis of available information relating to the alleged infringement of the legislation.

Article 78. Stages of the examination procedure

(1) The procedure for the examination of alleged infringement of personal data processing legislation shall include:
a) preliminary examination; and/or
b) investigation.

(2) The investigation of the infringement shall be ordered under Article 81. In other cases, the investigation shall be omitted.

Article 79. Lodging a complaint

(1) The complaint lodged with the Centre in accordance with Article 72 shall include the following elements:

a) surname and name of the data subject;

b) place of residence of the data subject and e-mail address, if the reply is requested by this means;

c) specification of all the factual and legal circumstances relating to the alleged infringement of the legislation relating to the processing of personal data concerning the data subject;

d) information identifying the controller or processor, to the extent possible;

e) information on the lodging of the complaint within the statute of limitations referred to in Article 72 (2) and (3).

f) measures to be taken by the Centre;

g) where applicable, information on the requests submitted to the controller or processor and the result of such requests;

h) where applicable, other relevant information, in particular whether the subject-matter of the complaint has been or is being examined by a court or whether the complainant has taken other measures, including their results, if any;

i) signature of the data subject or his or her legal or authorised representative, and electronic signature in the case of complaints submitted by e-mail.

(2) The complaint shall be accompanied, where appropriate, by:

a) the legal representative's supporting document, power of attorney or proxy based on the electronic signature of the authorised representative;

b) the mandate granted pursuant to Article 75;

c) documents and evidence which are deemed useful by the complainant for the support of his complaint.

(3) The Centre shall facilitate the lodging of complaints by making the complaint form available to the public, including in electronic form, without excluding other means of communication.

Article 80. Preliminary examination of the complaint

(1) The preliminary examination of the complaint concerning the alleged infringement of the legislation on the processing of personal data shall be carried out within 30 days from the date of registration of the complaint.

(2) During the preliminary examination of the complaint, the Centre shall establish whether there are reasonable grounds to suspect an infringement of the legislation on the processing of personal data.

(3) Anonymous complaints or complaints lodged without specifying the postal or e-mail address of the data subject shall not be examined.

(4) Where the complaint does not meet the requirements referred to in the points (c) to (f) and (i) of Article 79 (1) or the points (a) or (b) of Article 79 (2), the data subject shall be informed of the defects and shall be given a reasonable time limit to rectify them. Where the data subject fails to rectify the defects within the specified time limit, the complaint shall not be examined and the data subject shall be informed thereof.

(5) Where the Centre considers that, based on the information submitted by the complainant and other relevant information, there are no reasonable grounds for suspecting an infringement of the legislation on the processing of personal data, it shall reasonably reject the complaint and inform the data subject thereof.

(6) In order to reject a complaint on the grounds that the conduct complained of does not infringe the legislation on the processing of personal data or does not fall within their scope of application, the Centre is not obliged to take into account circumstances that have not been brought to its attention by the complainant.

(7) Where, during the preliminary examination of the complaint or the investigation under Article 81, appears reasonable suspicion that an offence has been committed, the Centre shall refer the matter to the prosecuting authority. In this case, the preliminary examination or investigation shall continue. The prosecuting authority shall inform the Centre of the decision taken.

Article 81. Investigation

(1) Investigation is the collection and administration of information on the lawfulness of the processing of personal data obtained under the provisions of this Law.

(2) Where after the preliminary examination of the complaint it is considered that the information submitted by the data subject and that obtained during the preliminary examination reveal reasonable grounds to suspect an infringement of the legislation on personal data protection, the Centre shall issue an order on initiation of the investigation.

(3) *Ex officio* investigations may be carried out:
a) as the result of the transmission of personal data breach notifications;
b) for the verification of data and information on alleged infringement of the legislation on personal data processing obtained by the Centre from sources other than those which are the subject-matter of the complaint or notification of personal data breach, such as referrals or information provided by another supervisory or public authority, correspondence received by the Centre, the media, access to the Internet, findings made due to other investigations or any other information. Such sources may be grounds for the opening of an *ex officio* investigation provided that the circumstances or the information contained therein reasonably indicate an alleged infringement of the legislation on personal data processing;
c) for international cooperation in the field of personal data protection, joint operations and mutual assistance.

(4) The order to open an *ex officio* investigation shall include the necessary analysis and reasoning regarding the compliance with the conditions provided for in paragraph 3.

(5) The *ex officio* investigation may be opened only within the statute of limitations referred to in Article 72 (2) and (3).

(6) The order to open the investigation shall not establish an infringement of the legislation on personal data processing. The infringement of the legislation on personal data processing shall be established by the Centre’s decision.

(7) During the investigation, the Centre shall first consider the possibility of carrying it out by requesting documentation and other information directly from the person under investigation and other persons involved in the investigation or by other methods which make

it possible to obtain such data. Where the documentation and information for the establishment of the compliance with the legislation by the person under investigation is insufficient, or given the investigation type and risk analysis, the Centre shall perform the on-the-spot investigation by issuing an appropriate mandate. The on-the-spot investigation may be carried out only if there are grounds to believe that documents can be found or information deemed necessary for the investigation of the alleged infringement of the legislation on personal data protection initiated by the order, can be obtained. This fact does not need to be demonstrated to the subject of the investigation. In the case of direct requests for information without on-site visit, the Centre shall specify the data referred to in paragraph 8, except as indicated in point (a).

(8) The mandate for on-the-spot investigation shall include at least:
a) number and date of issue
b) identification data of the Centre;
c) reference to the legal provisions under which the investigation is carried out;
d) grounds to initiate the investigation;
e) details of the data protection inspectors carrying out the on-the-spot investigation (surname, name and position);
f) data on the natural or legal person under investigation (where applicable, name of the person; fiscal code; establishment/address of the subdivision under investigation and its code, where applicable, other contact details);
g) subject-matter of the investigation;
h) purpose of the investigation and issues to be investigated;
i) the date of commencement and envisaged duration of the investigation.

(9) The mandate for the on-the-spot investigation shall be submitted under signature to the person under investigation or to the legal or authorised representative. In case of refusal to receive and sign the mandate, a minute shall be drawn up in the presence of two witnesses. The presence of witnesses shall not be required in the case of video and audio recording of the refusal.

(10) The data protection inspectors, within the limits of their powers under paragraphs 7 and 8, shall be entitled to:
a) obtain access to all personal data and information required for the conduct of the investigation, irrespective of the storage medium, including any documents, filing systems, software products, equipment and data processing means;
b) have access to any premises and rooms related to the subject-matter and purpose of the investigation, which are owned or used by the persons under investigation;
c) ask for and obtain the information, documents and explanations requested, within the time limit set, which shall be reasonable in terms of the amount and complexity. The time limit may be extended at the reasoned request of the person under investigation;
d) hear the person under investigation or his or her legal or authorised representative with regard to the facts which are relevant to the subject-matter of the investigation and, where appropriate, to record the answers, including by audio and/or video means, with the prior information of the person heard. Upon request, a copy of the recording shall be submitted to the person under investigation;
e) request and obtain information relating to the subject-matter and purpose of the investigation, stored on computers or other electronic devices, in a form that allows its retrieval, transport and examination;
f) request support of the competent subdivisions of the Ministry of Internal Affairs, which are obliged to provide the necessary assistance to the data protection inspectors within the investigation. Experts in specific fields empowered by the Centre may also be trained for

the investigation, that shall ensure the confidentiality of the information obtained during the investigation.

(11) During the investigation, data protection inspectors shall:
a) inform the person under investigation of his or her rights and obligations;
b) to introduce the delegation who carries out the on site investigation, or in the case of a request for documentation and other information directly from the person under investigation, the information referred to in paragraph (8) letters b) - i);
c) carry out the investigation in accordance with the powers provided for by this Law, taking into account its subject-matter and purpose.

(12) During the investigation, the person under investigation shall be entitled to:
a) obtain a copy of the mandate for on-the-spot investigation or the information referred to in points (b) to (i) of paragraph 8;
b) present evidence in the course of the investigation;
c) provide explanations recorded in any form relating to the subject-matter and purpose of the investigation;
d) be assisted by lawyers or other representatives authorised by law.

(13) The person under the on-the-spot investigation may be assisted by a lawyer. The absence of a lawyer does not prevent the conduct of the investigation.

(14) All legal persons governed by public or private law and natural persons shall submit to the investigation carried out by the Centre, including by ensuring the conditions for the proper conduct of the investigation.

(15) The on-the-spot investigation shall be carried out during the working hours of the person under investigation or, failing that, between 09:00 a.m. and 05:00 p.m., in the presence of the person under investigation or his or her representative. The investigation may continue after office hours or after 05:00 p.m., as appropriate, only with the consent of the person under investigation or his or her representative.

(16) Access by data protection inspectors to the home or residence of the natural person, without his or her consent, shall be allowed only on the basis of a court order issued in accordance with paragraphs 17 to 20 and presented to the natural person concerned.

(17) Where inspectors are prevented in any way from the performance of their duties, and there is a reasonable suspicion that information, documents, equipment, means or media which are related to the subject-matter of the investigation and could be relevant to prove a serious infringement of this Law are kept in premises, land or means of transport occupied by natural persons, the Centre may request a court order under the conditions of this Law by submitting an application to the court within whose territorial judicial district the Centre's headquarters is located. The application for authorisation shall include all the information that may justify the investigation, and the judge seized shall verify whether the application is justified.

(18) The court order can only be issued if:
a) there is a reasonable suspicion that in the premises, land or means of transport to be investigated contain information, documents, equipment, means or media which are related to the subject-matter of the investigation and which were requested by the Centre in accordance with this Law, but were not submitted within the prescribed time limit;

b) there is a reasonable suspicion that in the premises, land or means of transport to be investigated contain information, documents, equipment, means or media which are related to the subject-matter of the investigation and which may be requested by the Centre under this Law, which would not have been submitted, if requested, but would have been concealed, removed, altered or destroyed; or

c) the access by data protection inspectors to the premises, land or means of transport to be investigated has been restricted by the natural or legal persons under investigation, and there is a reasonable suspicion that the premises, land or means of transport concerned contain information, documents, equipment, means or media which are related to the subject-matter of the investigation and which were requested by the Centre under this Law.

(19) The court order shall include the purpose and subject-matter of the investigation, the authorisation issued as well as the right to appeal the order. The court order shall be valid for one month from the date of issue.

(20) In the event of a request for a court order, the court shall verify if the order for investigation is genuine and the coercive measures envisaged are not arbitrary or excessive given the subject-matter of the investigation. During the check of the proportionality of the coercive measures, the court may ask the Centre for detailed explanations, in particular with regard to the grounds for suspecting an infringement of this Law, as well as the seriousness of the suspected infringement, the importance of the evidence sought, the nature of the involvement of the person under investigation in the case and the reasonable probability that information, documents, equipment, means or media relating to the subject-matter of the investigation are kept at the place for which the court order is sought.

(21) The court order issued in accordance with paragraphs 17 to 20 may be challenged on appeal to the Central Court of Appeal, which shall not suspend execution, unless the appeal court orders otherwise.

(22) Paragraphs 17 to 21 shall apply accordingly in the case of a request, from the providers of electronic communications networks and/or services, of traffic data and/or location data related to the electronic communications services provided or to access to the respective data.

(23) The investigation result shall be recorded in the draft decision on the investigation, which shall state whether or not an infringement has been found and the corrective measures and sanctions applied. The draft decision shall be sent to the data subject and to the controller or processor who has been subject to the investigation, with a 30-day period for objections from the date of dispatch. The period referred to in paragraph 25 shall be suspended from the date of dispatch of the draft decision to the parties until the date of submission of any objections to the draft decision or, if observations are not submitted within the time limit, until the date of expiry of the time limit set for the submission of observations.

(24) During the conduct of the investigation, the Data Protection Inspector shall comply with the legal provisions and perform the required investigative actions. Any outside interference in the investigative activity shall be prohibited and punishable by law.

(25) The time limit for the conduct of the investigation shall be up to 6 months from the date of initiation of the investigation. It can be reasonably extended by up to one month, but not more than 12 months from the date of initiation, depending on the complexity of the case, the amount of information to be obtained and examined, the behaviour of the participants in the

investigation procedure and other relevant aspects. The Centre shall inform the data subject of the extension of the time limit and the reasons for such extension.

Article 82. Request for information

(1) To exercise its duties, the Centre shall be entitled to request and obtain, free of charge and ensuring the confidentiality of information, from natural and legal persons governed by public and private law any necessary documents and information, including in digital form, which are accessible and may be relevant to law enforcement, without them being able to invoke the confidentiality of criminal proceeding, banking secret, commercial secret, tax secret, medical secret, professional secret (with the exception of the professional secret referred to in Article 55 of the Law no. 1260/2002 on Advocacy), personal data and other information with limited accessibility.

(2) The Centre shall request the necessary information in writing, state the legal basis and purpose of the request for information, set a reasonable time limit for the provision of the information which make up at least 5 working days, and specify the sanctions provided for by law.

(3) Requests for information shall be proportionate and shall not oblige the person under investigation to admit that he or she has committed an infringement, but this person shall answer factual questions and provide documents even if the latter could be used to establish the existence of an infringement against them or another person.

(4) In the course of investigations, an exchange of communications between the person under investigation and his or her lawyer made within the scope of and for the sole purpose of exercising the right of defence of the person under investigation which relates to the subject-matter of the investigation, may not be used as evidence to establish a breach of legislation on personal data protection. Where the person under investigation fails to prove the security of the communication, it shall be sealed and withdrawn in duplicate.

The minutes of the on site investigation shall set a time-limit within which the person subject to the investigation is to submit evidence and explanations demonstrating the protected nature of the communication. The Director of the Center shall decide, as a matter of urgency, on the protected character of the communication on the basis of the request and of the evidence and arguments provided by the person under investigation. If the Director of the Center rejects the request with regard to the protected character of the communication, the unsealing of the document may take place only after the expiry of the time limit within which the order may be contested or, if the decision is contested, after the judgment of the court has become final. The order of the Director of the Center rejecting the request with regard to the protected character of the communication may be appealed within 15 days of its announcement, without following the prior procedure, in accordance with the provisions of the Administrative Code.

Article 83. Confidentiality

(1) Persons who, by virtue of their rights and duties under this Law, have become aware of the information of the investigation, as well as other persons who have become aware of such information, shall ensure its confidentiality, in accordance with the legislation.

(2) The case materials accumulated during the investigation may not be withdrawn, intercepted, obtained and/or used for any other subsequent purpose, if it could worsen the situation of the data subject, unless this is required for the administration of justice.

(3) The Data Protection Inspector, the data subject or other persons who, by virtue of their rights and duties under this Law, have become acquainted or aware of the information of the investigation may not be heard or interrogated by other bodies or organisations with regard to the substance of the information of the investigation, except in court.

Article 84. Issuance and notification of decisions

(1) Upon completion of the investigation, the Centre shall issue a reasoned decision on whether there has been an infringement of the legislation on personal data processing and on the application of the measures provided for in Section 3, as appropriate.

(2) The decision shall be issued by the Director of the Centre, the Deputy Director or by the supervisory staff of the Centre, in accordance with the powers granted by order of the Director of the Centre. The decision shall be communicated to the data subject and the person under investigation within 10 working days of the date of issuance.

(3) The Centre shall publish the summary of the decisions adopted, reflecting the nature of the infringements detected, the grounds of the decision, the measures ordered and the penalties applied.

Article 85. Execution of the Centre's decisions

(1) The decisions shall be executed within the time limit specified therein, with the obligation to inform the Centre in writing of the actions taken. The Centre may set a time limit for the execution of the decision of up to 6 months, taking into account the complexity of the actions to be performed, the degree of danger of the infringements requiring removal, the possibilities of the person under investigation to perform the prescribed actions, as well as previous prescriptions issued in similar cases. In complex cases, where the Centre's decision provides for the implementation of complex corrective measures, the Centre may extend the time limit for execution of the decision beyond the 6-months term, at the justified request of the controller or the processor.

(2) The time limit for voluntary execution of the fine shall be at least 2 months from the date of notification of the decision.

(3) The decisions of the Centre shall be enforced in accordance with the Execution Code.

(4) As regards the collection of fines imposed, the Centre's decisions shall be executed in accordance with the procedure of enforcement of monetary claims based on public law decisions, approved by the Government.

Section 3
Pecuniary penalties

Article 86. Fine

(1) The fine is the pecuniary sanction imposed on the controller by the Centre in the event of an infringement of this Law.

(2) The fine imposed by the Centre shall be paid to the state budget.

Article 87. General conditions for applying fines

(1) The Centre shall ensure that the imposition of fines pursuant to this Section in respect of infringements of this Law referred to in Article 88 shall in each individual case be effective, proportionate and dissuasive.

(2) Fines shall, depending on the circumstances of each individual case, be applied in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 60 (2). In the case of a minor infringement or where the fine likely to be imposed would place a disproportionate burden on a natural person, a warning may be issued instead of a fine. For the purposes of imposing a fine and determining the amount of the fine, the following circumstances shall be taken into account in each individual case:

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;

f) the degree of cooperation with the Centre, 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 Centre, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 60 (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.

(3) Fines may only be imposed where it is established that the controller has intentionally or negligently committed an infringement referred to in Article 88.

(4) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Law, the total amount of the fine shall not exceed the amount specified for the gravest infringement.

Article 88. Infringements subject to fines

(1) Infringements of the following provisions shall, in accordance with Article 87, be subject to fines up to 1 000 000 MDL, or in the case of an undertaking, up to 1% of the total turnover in the year preceding the sanctioning, whichever is higher:

a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) the obligations of the certification body pursuant to Articles 42 and 43;

c) the obligations of the monitoring body pursuant to Article 41 (4).

(2) Infringements of the following provisions shall, in accordance with Article 87, be subject to fines up to 2 000 000 MDL, or in the case of an undertaking, up to 2% of the total turnover in the year preceding the sanctioning, 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 another country or an international organisation pursuant to Articles 44 to 49;

d) obligations referred to in Chapter VI;

e) non-compliance with a corrective measure or a temporary or definitive limitation on processing or the suspension of data flows by the Centre within legally permissible limits, pursuant to Article 60 (2) or failure to provide access in violation of Article 60 (1).

(3) Infringement of a corrective measure adopted by the Centre as referred to in Article 60 (2) shall, in accordance with Article 87, be subject to fines up to 2 000 000 MDL, or in the case of an undertaking, up to 2 % of the total turnover in the year preceding the sanctioning, whichever is higher.

(4) Without prejudice to the corrective powers of the Centre referred to in Article 60 (2), penalties provided for in this Article shall also be applied to public authorities and institutions in accordance with this Law.

(5) Where the total turnover achieved in the year preceding the sanctioning is not recorded, the last year preceding the sanctioning in which the undertaking achieved a turnover shall be taken into account.

Chapter IX

FINAL AND TRANSITIONAL PROVISIONS

Article 89. Final provisions

(1) This Law shall enter into force on the expiry of 24 months from the date of its publication in the Official Gazette of the Republic of Moldova.

(2) The Government, before the entry into force of this Law, shall:

a) submit to the Parliament proposals for bringing the legislation in line with this Law;

b) bring its normative acts in line with this Law;

(3) The Centre, before the entry into force of this Law, shall approve necessary normative acts for the execution of this Law.

(4) This Law shall not impose additional obligations on natural or legal persons with regard to processing in connection with the provision of publicly available electronic communications services in public electronic communications networks, with respect to matters for which they are subject to specific obligations with the same objective as provided for in the Law no. 241/2007 on electronic communications.

Article 90. Transitional provisions

(1) The Director and the Deputy Director of the Centre in office on the date of entry into force of this Law shall remain in office for the period for which they were appointed.

(2) The staff of the Centre in office at the time of the entry into force of this Law shall be assigned to new posts according to the staffing schedule, in compliance with the provisions of the Law no. 158/2008 on the public office and the status of civil servant and the labour legislation.

(3) On the date of entry into force of this Law, the following shall be repealed:

a) Law no. 182/2008 regarding the approval of Regulation of the National Centre for Personal Data Protection, structure, staff-limit and its financial arrangements;

b) Law no. 133/2011 on personal data protection;

c) Articles 74^1 to 74^3 and Article 423^4 of the Contravention Code no. 218/2008.

(4) From the moment of entry into force of this Law, the following shall apply from the final amount of the pecuniary sanction determined by the Centre:

a) from the first year – 10% of the amount of the fine;

b) from the second year – 40% of the amount of the fine;

c) from the third year – 100% of the amount of the fine.

(5) The acts issued by the Centre pursuant to Article 32 (3) and point (i) of Article 32 (5) of Law no 133/2011 on personal data protection shall remain in force after the entry into force of this Law.

(6) Complaints lodged with the Centre before the date of entry into force of this Law shall be examined and resolved in accordance with the procedural rules provided by this Law and with the substantive rules, including those on liability for breach of data protection legislation provided for by the law in force at the date of the breach.

(7) Civil and administrative litigation cases are examined and resolved in accordance with the provisions of the law in force on the date of the appearance of the litigious legal relationship.

(8) Where processing is based on consent pursuant to Law no. 133/2011 on personal data protection, the data subject shall not be required to give consent again if the method in which consent was given complies with this Law and allows the controller to continue such processing after the date of entry into force of this Law.

PRESIDENT OF THE PARLIAMENT Igor GROSU

No. 195. Chisinau, 25th July, 2024.