Annex 6.

Twinning project "Implementation of the best European practices with the aim of strengthening the institutional capacity of the apparatus of the Ukrainian Parliament Commissioner for human rights to protect human rights and freedoms (apparatus)"
No. EuropeAid/137673/DD/ACT/UA

2.3.4. Developing recommendations as regards improving the existing or employing new instruments for restoring human rights, in the spheres of personal data protection, access to public information and the prevention of all forms of discrimination in particular

Document	RECOMMENDATIONS ON AMENDMENT OF THE LAW OF UKRAINE ON PROTECTION OF PERSONAL DATA and RECOMMENDATIONS ON AMENDMENT OF THE LAW OF UKRAINE ON ACCESS TO PUBLIC INFORMATION
Short description of the document	This Document contains recommendations on amendment of the law of Ukraine on protection of personal data and recommendations on amendment of the law of Ukraine on access to public information
Author	Valerija Gedeikė, Waltraut Kotschy
Date	July 2018, Kyiv

RECOMMENDATIONS ON AMENDMENT OF THE LAW OF UKRAINE ON PROTECTION OF PERSONAL DATA

1. Paragraph 1 of Article 1 (**Subject-matter and objectives**) of the Law of Ukraine on protection of personal data (hereafter – the Law) is re-formulated in order to harmonize with Article 1 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (hereafter – the Convention 108) and Article 1 of the General data protection regulation (hereafter – the GDPR).
The right to respect for private life and the right to personal data protection, although closely related, are distinct rights. Both strive to protect similar values, i. e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion. The two rights differ, however, in their purpose and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. The protection of personal data is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed. The processing must comply with the essential components

of personal data protection, namely independent supervision and the respect for the data subject's rights.[1]

Taking into account the above deliberations it is essential to define the objectives of the Law as protection of fundamental rights and freedoms of natural persons and in particular their rights to privacy AND to the protection of personal data.

2. Introducing a new Article 3 on **territorial scope,** in order to define clearly the dividing line between the application of the data protection law of Ukraine and the data protection law of other countries, especially EU Member States, to controllers and processors. It is necessary to define the territorial scope of the Law is necessary since data processing has become a cross-border activity carried out by many kinds of businesses. This question is particularly relevant for business activities of foreign companies in Ukraine and Ukrainian companies acting abroad .

The definition of an establishment of a controller or processor is also introduced for this purpose.

3. The definitions of the GDPR are transposed and aligned with Ukraine requirements, taking into account the existing relevant definitions in other laws of Ukraine.

4. Since the goal is to transpose the GDPR, the principles relating to processing of personal data and main data processing rules shall be revised and harmonised with the GDPR. Rapid technological developments and globalisation require a strong and more coherent data protection framework, backed by strong enforcement, given the importance of creating the trust[2]. The GDPR is intended to modernise the data protection legal framework considering new technologies and strengthen data subject's control over his or her own data.

It is highlighted in the draft that any processing activity, including data transfer, shall be carried out in accordance with the Law.

5. A more detailed description of **valid consent**, as established in Article 7 of the GDPR, was included into the draft; it is in line with data protection law and practise in Ukraine.

6. Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data[3]. **Special protection of children** in this context has been introduced in accordance with Article 8 of the GDPR determining special conditions to child's consent in relation to the offer of electronic information services directly to a child. The definition of electronic information services has been harmonised with the Law of Ukraine on e-commerce.

7. The rules on the **lawful processing of special categories data** (Art. 9) have been aligned with the GDPR, although in a slightly simplified formulation.

8. As processing of personal data relating to criminal convictions and offences is regulated by special rules in the GDPR, a separate article on personal data relating to criminal convictions and offences has been introduced to the draft, aiming to determine that processing of these data must always be authorised by law.

9. The description of the **rights of data subjects** and how they may be exercised has been largely taken over from the GDPR with some clarifications and some slight simplifications of formulation.

10.Special clarification has been added as to the question who can make use of the right to access to personal data in accordance with Article 15 of the GDPR: it is highlighted that only the data subject and his/her representative, but no third party has this right.

11. The provisions of the GDPR on **automated individual decision-making** have been simplified in formulation, though without changing its essence.

---

1 *Handbook on European data protection law,* 2018 edition.

2 Recital 7 of the GDPR

3 Recital 38 of the GDPR

12. **Restrictions of rights of data subjects and obligations of controllers have been modified**: the provisions of Ukrainian Law on personal data protection and provisions of the GDPR were combined for this purpose.
13. A new obligation of controllers and processors to record data processing activities is introduced in accordance with the GDPR.
14. The controller's obligation to notify the Commissioner of data processing activities determined by the valid Law of Ukraine on Protection of personal data is modified. The **notification** by the controller and publication by the Commissioner is proposed in Article 30 only for processing activities which constitute a high risk for the data subjects. The Commissioner shall determine the list of such high risk processing operations.
15. Requirements for secure data processing are harmonised with the GDPR along with a definition of the relevant responsibilities of controllers and processors. It is highlighted in Article 27 that if a processor violates the Law by infringing the remit of his mandate by determining the purposes and means of processing by himself, this **processor shall be considered to have become a controller** in respect of that processing with all consequences of processing data without sufficient legal basis.
16. A new obligation of controllers to notify the Commissioner and data subjects (if needed) of a **personal data breach** is introduced in accordance with the GDPR. A new definition of a personal data breach is introduced for that purpose. The Commissioner shall determine and publish the assessment criteria for large scale breach of security which shall lead to the obligation to notify of a personal data breach.
17. The status and tasks of **data protection officer** are harmonised with requirements of GDPR, highlighting the independence of the officer and his tasks of monitoring the data processing compliance with the Law and of reporting to the head of the controller; responsibility for lawful processing stays with the head of the controller.
18. The concept of **codes of conduct** is harmonised with the GDPR, introducing the adherence to the code of conduct approved by the Commissioner as important factor for the extent of liability, also as a means of introducing the safeguards for data transfer.
19. Rules for **transfers of personal data** to third countries or international organisations are harmonised with the GDPR. Data transfers to data recipients in Member States of the European Economic Area, as well as in countries that have signed the Convention 108 shall not require any specific authorisation. The Commissioner is to determine and publish the list of the third countries, territories and specified sectors within a third country, and of those international organisations for which it he or she has decided that an adequate level of protection is ensured. The Commissioner shall also adopt standard data protection clauses as a means for a controller or processor to provide appropriate safeguards and that enforce data subject rights and effective legal remedies for data subjects in case when personal data are intended to be transferred to a recipient in a third country in the absence of an adequacy decision.
20. Personal data which are processed **for journalistic or academic, artistic or literary purposes** fall within the scope of the Law, though exceptions for application of some articles of the Law are made provided that the balance between the right to data protection and privacy and the right to freedom of expression is ensured.
21. The **supervision of the implementation of the Law** is entrusted to the Commissioner. It is highlighted that the Commissioner acts through competent officials who are part of the Commissioner's office. The Commissioner in its function as data protection supervisory authority is given several new powers such as to make decisions on the imposition of administrative fines, to draw up and publish methodological recommendations on data processing and protection of personal data, to participate in the drafting of laws and legal acts of the Cabinet of Ministers of Ukraine regulating protection of personal data.
22. Data subject's rights to effective remedies, right to compensation and controller's or processor's liability are harmonised with the GDPR.

23. General conditions for imposing administrative fines are harmonised with the GDPR.
24. General rules on procedure of imposing administrative fines and the procedure itself are introduced to the Law. It is emphasised that fines may be imposed both on natural and legal persons infringing the Law.

RECOMMENDATIONS ON AMENDMENT OF THE LAW OF UKRAINE ON ACCESS TO PUBLIC INFORMATION

1. The Law of Ukraine on access to public information ((hereafter – the Law on access) defines the procedure of implementation and provision of the common right to access to the information which is in the possession of public authorities, other processors of public information, specified by this Law, and to the information that is of public interest. Taking into account the scope of this Law it must be harmonised with the Law on protection of personal data.
Provisions of the Law on access contradicting or repeating provisions of the Law must be abolished for the purpose of harmonisation.
2. Provisions regulating the person's right to access his/her data must be abolished providing that the execution of this right is regulated by provisions of the Law on protection of personal data.
3. The concept of public information with restricted access must be supplemented with a new category – personal information.
4. Special rules on access to personal information by third parties shall be introduced into the Law on access. It is highlighted that the access to personal information may be granted on grounds of legitimate interest of the requester or other persons, including public interest, in disclosure of personal information, provided that the interest in disclosure overrides the personal information subject's interests or fundamental rights and freedoms, which require protection of personal information.

LAW OF UKRAINE ON PROTECTION OF PERSONAL DATA

CHAPTER I
General provisions

Article 1. Subject-matter and objectives

This Law regulates the legal relations concerning the protection of natural persons with regard to the processing of personal data and aims thereby to protect the fundamental human rights and freedoms of natural persons, particularly the right to data protection and to privacy.

Article 2. Material scope

1. This Law applies to personal data processing activities performed, fully or partially, by automated means, as well as to processing of personal data stored in a file folder or assigned to be included in it, with the use of non-automated means.
2. This Law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

Article 3. Territorial scope

This Law applies to the processing of personal data for the purpose of the activities of an establishment of a controller or processor in Ukraine, regardless of whether the processing takes place in Ukraine or not. Where processing for such an establishment is wholly or partly performed outside Ukraine, Chapter V of this Law will apply.

Article 4. Definitions

The following definitions are used in the present Law:

- **'personal data'** means any information relating to an identified or identifiable natural person (**'data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **'profiling'** means 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'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law.

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

- **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- **'third party'** means 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'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a written or oral statement (explicit consent) or by a clear affirmative action (conclusive consent), signifies agreement to the processing of personal data relating to him or her;

- **'personal data breach'** means a large scale 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. The Ukrainian Parliament Commissioner for human rights shall determine and publish the assessment criteria for the large scale breach of security.

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

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

-'**establishment of a controller or processor'** means a stable place where business or other activities are really and effectively exercised; the legal form, whether through a branch or a subsidiary with a legal personality, is not determining factor in that respect;

- **'electronic information service'** means a service usually provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of service. 'at a distance' means that the service is provided without the parties being simultaneously present. 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means. 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

CHAPTER II
Principles

Article 5. Principles relating to processing of personal data

1. Personal data shall be:

1) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'), every processing operation has to be carried out in accordance with the Law;

2) 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 46, not be considered to be incompatible with the initial purposes ('purpose limitation');

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4) 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 ('accuracy');

5) 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 ('storage limitation');

6) 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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('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:

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

2) 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;

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

4) processing is necessary in order to protect the vital interests of the data subject;

5) 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 and is determined by law;

6) 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. The basis for the processing referred to in point (3) and (5) of paragraph 1 shall be laid down by law. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (5) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Law, *inter alia*: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing.

3. The processing of personal data for a purpose other than that for which the personal data have been collected can be carried out if:

1) this further processing is compatible with the prior processing; or

2) it is based on the data subject's consent; or

3) is determined by law insofar as necessary in a democratic society in the interests of national security, economic welfare and protection of human rights and freedoms of data subjects or other persons as referred to in Article 23.

4. The Ukrainian Parliament Commissioner for human rights shall determine the assessment criteria for compatible further processing of personal data.

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. Oral or written request for the data subject's consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and be formulated in clear and plain language.

3. Any part of a declaration of consent which constitutes an infringement of this Law shall not be binding.

4. 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.

5. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Article 8. Conditions applicable to child's consent in relation to electronic information services

1. Where point (1) of Article 6(1) applies, in relation to the offer of electronic information 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 holder of parental responsibility over the child.

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

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:

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

2) 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 law pursuant to law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

3) 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;

4) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association 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;

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

6) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

7) 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 law or pursuant to contract with a health professional and subject to the obligation of professional secrecy law or rules established by competent bodies.

8) 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 law;

9) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 46.

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

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only when the processing is authorised by law -. Any comprehensive register of criminal convictions shall be processed by 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 of this Article, 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

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 and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

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 a the Ukrainian Parliament Commissioner for human rights and seeking a judicial remedy.

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.

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 a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Ukrainian Parliament Commissioner for human rights shall determine the information to be presented by the icons and the procedures for providing standardised icons.

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:

1) the identity and the contact details of the controller;

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

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

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

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

6) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision as referred to in Article 40.

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:

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

2) 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;

3) where the processing is based on point (1) of Article 6(1) or point (1) 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;

4) the right to lodge a complaint with the Ukrainian Parliament Commissioner for human rights;

5) 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;

6) the existence of automated decision-making, including profiling, referred to in paragraph 1 and 3 of Article 22 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:

1) the identity and the contact details of the controller;

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

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

4) the categories of personal data concerned;

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

6) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision as referred to in Article 40.

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:

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

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

3) 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;

4) where processing is based on point (1) of Article 6(1) or point (1) 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;

5) the right to lodge a complaint with a the Ukrainian Parliament Commissioner for human rights;

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

7) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (3) 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:

1) 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;

2) 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

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

3. 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:

1) the data subject already has the information;

2) 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 46 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;

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

4) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Ukrainian law, including a statutory obligation of secrecy.

Article 15. Right of access by the data subject

1. The data subject or his or her representative after proving his or her capacity as representative shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. No one else can claim access to data on grounds of this provision. Where a request is made by the data subject or his or her representative, access shall be given to the personal data and the following information:

1) the purposes of the processing;

2) the categories of personal data concerned and the content of the data processed about the data subject;

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

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

5) the of the rights of the data subject according to Articles 16 to 22;

6) the right to lodge a complaint with the Ukrainian Parliament Commissioner for human rights;

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

8) the existence of automated decision-making, including profiling, referred to in of Article 22 and, 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 a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 41 relating to the transfer.

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.

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

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:

1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

2) the data subject withdraws consent on which the processing is based according to point (1) of Article 6(1), or point (1) of Article 9(2), and where there is no other legal ground for the processing;

3) 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);

4) the personal data have been unlawfully processed;

5) the personal data have to be erased for compliance with a legal obligation in law to which the controller is subject;

6) the personal data have been collected in relation to the offer of electronic information 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:

1) for exercising the right of freedom of expression and information;

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

3) for reasons of public interest in the area of public health in accordance with points (7) and (8) of Article 9(2);

4) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 46 in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

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

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:

1) 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;

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

3) 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;

4) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

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 or for the protection of the rights of another natural or legal person or for reasons of important public interest of Ukraine.

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:

1) the processing is based on consent pursuant to point (1) of Article 6(1) or point (1) of Article 9(2) or on a contract pursuant to point (2) of Article 6(1); and

2) 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 referred to in paragraph 1 of this Article 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 referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 21. Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (5) or (6) 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.

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 electronic information 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 46, the data subject, on grounds relating to his or her particular situation, 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:

1) is authorised by law; or

2) based on the performance of a contract or explicit consent of the data subject, provided that safeguards for the data subject's rights and freedoms and legitimate interests are in place, 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.

3. Decisions based on the processing of special categories of personal data referred to in Article 9(1), shall be made according to the requirements of point 2 of paragraph 2 and apply only to the contracts mentioned in Article 9(2).

Article 23. Restrictions on the implementation of rights of data subjects and obligations of controllers

1. Restrictions on the implementation of rights of data subjects referred to in Articles 12-22 or obligation of a controller referred to in Article 34 of the Law shall be implemented only in cases foreseen by law insofar as necessary in a democratic society in the interests of national security, economic welfare and protection of human rights and freedoms of data subjects or other persons.

2. In particular, any legislative measure referred to in paragraph 1 must contain specific provisions as mentioned in the third sentence of Article 6 (2).

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.

2) Adherence to approved codes of conduct as referred to in Article 38 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.

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 law to which the controllers are subject. 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. 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 rights of the data subject.

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 law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

1) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

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

3) takes all measures required pursuant to Article 32;

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

5) 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;

6) assists the controller in ensuring compliance with the obligations pursuant to Articles 31 to 33 taking into account the nature of processing and the information available to the processor;

7) 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 law requires storage of the personal data;

8) 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.

With regard to point (8) of the paragraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Law or other data protection provisions.

3) 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 law, 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.

4. Adherence of a processor to an approved code of conduct as referred to in Article 38 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

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

6. If a processor violates this Law by infringing the remit of his mandate by determining the purposes and means of processingby oneself, the processor shall be considered to be a controller in respect of that processing with all consequences of processing data without sufficient legal basis.

Article 28. 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 law.

Article 29. Records of data processing activities

1. Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

1) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

2) the basis of lawful processing according to Article 6(1) and Articles 9 or 10; in case if the basis of lawful processing is provided in accordance with point 3 or 5 of Article 6(1), the relevant law must be stated;

3) the purposes of the processing;

4) a description of the categories of data subjects and of the categories of personal data;

5) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

6) where applicable, the identification of the third country or international organisation, which personal data are transferred to and, in the case of transfers referred to in the second subparagraph of Article 43(1), the documentation of suitable safeguards;

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

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

2. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

1) the name and contact details of the processor and of each controller on behalf of which the processor is acting, and the data protection officer;

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

3) where applicable, the identification of the third country or international organisation, which personal data are transferred to and, in the case of transfers referred to in the second subparagraph of Article 43(1), the documentation of suitable safeguards;

4) 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 shall make the record available to the Ukrainian Parliament Commissioner for human rights on request.

Article 30. Notification of Data Processing

1. Data processing operations, which are of particular risk to the rights and freedoms of data subjects, may be carried out only when after the data controller has notified the Ukrainian Parliament Commissioner for human rights by transmitting the relevant records of processing activities and the notification was published in accordance with the procedure established by the Ukrainian Parliament Commissioner for human rights.

2. Types of data processing operations, which are of particular risk to the rights and freedoms of data subjects, shall be determined by the Ukrainian Parliament Commissioner for human rights.

3. Publication of notifications pursuant to this Article shall take place on the official website of the Ukrainian Parliament Commissioner for human rights in a manner determined by the Ukrainian Parliament Commissioner for human rights.

4. The decision of the Ukrainian Parliament Commissioner for human rights to publish or refuse to publish notifications pursuant to this Article shall be made within two months of the date of receipt of the notification. The decision of the Ukrainian Parliament Commissioner for human rights to refuse to publish the information notified pursuant to this Article shall be reasoned. If neither a publication nor a refusal is effected after the period of two months the controller may proceed to process data according to the content of the notification.

Article 31. Cooperation with the Ukrainian Parliament Commissioner for human rights

The controller and the processor shall cooperate, on request, with the Ukrainian Parliament Commissioner for human rights in the performance of his/her tasks.

Section 2
Security of personal data

Article 32. Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

2) the pseudonymisation and encryption of personal data;

3) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

4) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

5) 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 an approved code of conduct as referred to in Article 38 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

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 law.

Article 33. Notification of a personal data breach to the Ukrainian Parliament Commissioner for human rights

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 Ukrainian Parliament Commissioner for human rights, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Ukrainian Parliament Commissioner for human rights 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:

1) 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;

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

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

4) 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 Ukrainian Parliament Commissioner for human rights 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 additionally to the obligation referred to in Article 33 communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article 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 (2), (3) and (4) 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:

1) 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;

2) 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;

3) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the Ukrainian Parliament Commissioner for human rights, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3
Data protection officer

Article 35. Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

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

2) 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

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

2. The Ukrainian Parliament Commissioner shall determine and publish the assessment criteria for the large scale data processing.

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

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

2. 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.

3. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Ukrainian Parliament Commissioner for human rights. The publishing on the controller's or the processor's website would be considered as good practice.

Article 36. 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 37 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 those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his 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 law.

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 37. Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

1) 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 data protection provisions;

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

3) to cooperate and act as the contact point for the Ukrainian Parliament Commissioner for human rights on issues relating to data processing.

Section 4

Codes of conduct and certification

Article 38. Codes of conduct

1. Associations and other bodies representing categories of controllers or processors or branches of business may prepare codes of conduct, applicable to their members, for the purpose of creating detailed rules for lawful and fair data processing and specifying the application of this Law, such as with regard to:

1. fair and transparent processing;
2. the legitimate interests pursued by controllers in specific contexts;
3. the collection of personal data;
4. the pseudonymisation of personal data;
5. the information provided to the public and to data subjects;
6. the exercise of the rights of data subjects;
7. the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
8. the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
9. the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
10. the transfer of personal data to third countries or international organisations; or
11. 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 pursuant to Articles 50 and 52.

2. Such codes of conduct may be submitted for approval to the Ukrainian Parliament Commissioner for human rights. The Ukrainian Parliament Commissioner for human rights shall approve the code of conduct if the code stablishes lawful, fair and transparent

processing in accordance with the requirements of the Law. Adherence to an approved code of conduct shall be considered as mitigating factor when deciding on the imposition of an administrative fine as referred to in point (10) Article 54(2).

Article 38a. Purpose of certification

For the purpose of demonstrating compliance with the Law of Ukraine On personal data protection the data processing activities operated by a controller or processor may be certified by a certification body. Such certification may also present itself as a seal or mark.

Article 38b. Accreditation of certification bodies

1. Certification bodies are accredited by The Ukrainian Parliament Commissioner for human rights if they fulfil the criteria for accreditation. The Ukrainian Parliament Commissioner for human rights shall determine and publish the accreditation criteria. These criteria shall comprise the assessment of independence of decision making, level of expertise in the area of data protection and, additionally, assessment of a certification procedure, which must ensure adequate and justified certification.

2. Accreditation shall be issued for a maximum period of five years. It can be renewed. It can also be revoked if the criteria for accreditation are no longer fulfilled.

3. The Ukrainian Parliament Commissioner for human rights shall provide a public register of all accredited certification bodies on its website.

Article 38c. Certification of processing schemes

1. Certification shall be carried out in accordance with the certification procedure approved by the Ukrainian Parliament Commissioner for human rights in the course of the body's accreditation.

2. Before granting certification of a data processing scheme of a controller or processor, the certification body shall notify the Ukrainian Parliament Commissioner for human rights with a reasoned statement of the intention to certify. Certification may be issued if the Ukrainian Parliament Commissioner for human rights does not prohibit it within a period of one month since the day of notification. The decision of the Ukrainian Parliament Commissioner for human rights to prohibit certification shall be reasoned and shall be sent to the certification body and to the controller or processor applying for certification.. The decision of the Ukrainian Parliament Commissioner for human rights to prohibit certification may be appealed to administrative court by the certification body as well as the controller or processor applying for certification according to the procedure laid down by law.

3. Certification shall be issued for a maximum period of three years. It can be renewed in accordance with the certification procedure set down in paragraph 1 of Article 38b. Certification can also be revoked by the certification body or by the Ukrainian Parliament Commissioner for human rights if the requirements for certification are no longer fulfilled.

4. Data processing activities which are based on certified processing schemes are subject to investigation and assessment by the Ukrainian Parliament Commissioner for human rights in the same way as activities which are based on non-certified processing schemes. When deciding on the imposing and/or the amount of an administrative fine the Ukrainian Parliament Commissioner for human rights shall give due regard to the fact, that the controller or processor followed a certified processing scheme during the processing activity.

CHAPTER V
Transfers of personal data to third countries or international organisations

Article 39. General principle for transfers

1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third 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 third country or an international organisation to another third 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. Member States of European Economic Area, as well as countries that have signed the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) shall be recognised as those ensuring the appropriate level of protection of personal data. Personal data transfer to data recipients in these countries shall not require any specific authorisation.

Article 40. Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Ukrainian Parliament Commissioner for human rights has decided in coordination with the other Member States of the Council of Europe Convention 108, that the a third country, a territory or one or more specified sectors within that third country, or international organisation in question ensures an adequate level of protection. Transfer of personal data to such places shall not require any specific authorisation.

2. The Ukraine Parliament Commissioner for human rights shall publish the list of the third countries, territories and specified sectors within a third country and international organisations for which it he or she has decided that an adequate level of protection is ensured.

Article 41. Transfers subject to appropriate safeguards

1. A controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the Ukrainian Parliament Commissioner for human rights, by:

1) standard data protection clauses adopted by the Ukrainian Parliament Commissioner for human rights and committed by the controller or processor, subject to this Law, and the controller, processor or recipient of personal data in the third country or international organisation;

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

3) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor in the third country in order to apply the rules of code of conduct and to provide and enforce the rights of data subjects and effective legal remedies for data subjects.

3. Subject to the authorisation from the Ukrainian Parliament Commissioner for human rights, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

1) contractual clauses between the controller or processor, subject to this Law, and the controller, processor or the recipient of the personal data in the third country or international organisation; or

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

Article 42. Transfers or disclosures not authorised by law

Any judgment of a court or tribunal and any decision of an administrative authority of a third 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 agreement, such as a mutual legal assistance treaty, in force between the requesting third country and Ukraine, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 43. Derogations for specific situations

1. In the absence of appropriate safeguards pursuant to Article 41, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

1) 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;

2) 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;

3) 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;

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

5) the transfer is necessary for the establishment, exercise or defence of legal claims;

6) 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;

7) the transfer is made from a register which according to law 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 law for consultation are fulfilled in the particular case.

2. A transfer pursuant to point (7) of paragraph 1 shall not involve the entirety or considerable part of the personal data contained in the register.

3. The public interest referred to in point (4) of paragraph 1 shall be recognised in law to which the controller is subject.

CHAPTER VI
Provisions relating to specific processing situations

Article 44. Processing and freedom of expression and information

When personal data are processed for journalistic or academic, artistic or literary purposes, Articles 8, 12 to 23, 25, 29, 39 to 43 and 46 of the Law shall not apply provided that the balance between the right to data protection and privacy and the right to freedom of expression is ensured.

Article 45. Processing and public access to official documents

Personal data in official documents held by a public authority or body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with the requirements of Article 6(1) and 9(2) of this Law, requirements of the Law of Ukraine on access to public information and requirements of law

to which the public authority or body is subject and in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Law.

Article 46. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

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. Personal data must be altered immediately in a manner which makes it impossible to identify the data subject where the data processing purposes can be fulfilled without personal data.

Article 47. Processing of data on private life for professional qualities assessment

Processing of data on private life of individual for professional qualities assessment is prohibited unless explicitly foreseen by law.

Article 48. Obligations of secrecy

1. Data processing by employees of the data controller and/ or data processor shall be performed according to their professional duties and obligations under labour law, especially as determined by the data controller and/ or data processor. These employees shall not disclose personal data which became known to them in the course of performance of their duties except for cases determined by law. This obligation shall remain valid after termination of their duties, except for cases established by law.
2. The infringement of this obligation shall be subject to liability as laid down by law.

CHAPTER VII
Supervision of implementation of this Law

Section 1
Competence and powers

Article 49. Supervisory Authority and powers Thereof

2. The implementation of this Law, shall be supervised and monitored by the Ukrainian Parliament Commissioner for human rights in its function as data protection supervisory authority in the sense of the Chapter IV of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). In this function the Commissioner is acting through competent officials who are part of the Ukrainian Parliament Commissioner's for human rights office. Decisions by these officials are made on behalf of the Ukrainian Parliament Commissioner for human rights.
3. The Ukrainian Parliament Commissioner for human rights acting through his/ her office shall have the following powers in the field of data protection:
1) to receive proposals, and other requests of individuals and legal entities concerning the protection of personal data and to take decisions on the results of their consideration;
2) to hear complaints about alleged infringements of this Law, which are brought before the Commissioner within 3 years after the infringement took place according to the complaint and within one year after the complainant gained knowledge about the event causing the alleged infringement;

3) to carry out on-site and off-site, scheduled, unscheduled inspections of the controller and/or the processor on the basis of a request or on the initiative of the Ukrainian Parliament Commissioner for human rights, in a manner determined by the Ukrainian Parliament Commissioner for human rights; the Ukrainian Parliament Commissioner for human rights in accordance with law shall be granted access to the premises where data processing is carried out;

4) to get on his/her request and have access to any information (documents) of the controller or processor that is necessary for supervision of personal data processing, including access to personal data, relevant databases or filing systems, information with restricted access.

5) to issue binding instructions (compliance notice) on prevention or elimination of infringements of the legislation on protection of personal data, including changing, removal or destruction of personal data, ensuring rights of data subjects, personal data transfer, suspension or termination of the processing of personal data;

6) to accredit certification bodies pursuant to Article 38b and to withdraw accreditation if the requirements for accreditation are no longer met

7) to prohibit or withdraw a certification pursuant to Articles 38c, if the requirements for the certification are not or are no longer met

8) to make decisions on the imposition of administrative fines;

9) to approve codes of conduct which provide sufficient safeguards pursuant to Article 38(2);

10) to approve of the transfer of personal data to third countries or international organisations as foreseen in paragraph 3 of Article 41.

11) to adopt legal acts, regulating personal data protection, in cases determined by this Law;

12) to provide recommendations on practical application of the legislation on protection of personal data, to explain the rights of data subjects, rights and obligations of data controllers, data processors, data protection officers and other persons;

13) draw up and publish methodological recommendations on data processing and protection of personal data;

14) to cooperate with data protection officers; to process information about data protection officers;

15) to submit proposals to the Parliament of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, other public authorities regarding the drafting, amending and repealing of laws or other legal acts, regulating protection of personal data, provided that their provisions are related to the issues falling within the competence of the Ukrainian Parliament Commissioner for human rights;

16) to participate in drafting of laws and legal acts of the Cabinet of Ministers of Ukraine regulating protection of personal data, provided that their provisions are related to the issues falling within the competence of the Ukrainian Parliament Commissioner for human rights;

17) to carry out the monitoring of new practices, trends and technologies of protection of personal data;

18) to organize and ensure the cooperation with foreign data protection authorities, particularly, in connection with implementation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and Additional Protocol to it, other international agreements of Ukraine on personal data protection;

19) to participate in the work of international organizations on personal data protection.

2. The Ukrainian Parliament Commissioner for Human Rights includes in his/her annual report on state of observance and protection of human and citizens' rights and

freedoms in Ukraine the report on the state of observance of legislation on personal data protection.

Section 2
Remedies and liability

Article 50. Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Ukrainian Parliament Commissioner for human rights, if the data subject considers that the processing of personal data relating to him or her infringes this Law.

2. The Ukrainian Parliament Commissioner for human rights shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 51.

Article 51. Right to an effective judicial remedy against the Ukrainian Parliament Commissioner for human rights

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the Ukrainian Parliament Commissioner for human rights concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the Ukrainian Parliament Commissioner for human rights does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 50.

Article 52. Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with the Ukrainian Parliament Commissioner for human rights pursuant to Article 50, each data subject shall have the right to an effective judicial remedy 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 this Law.

Article 53. 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 this 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 suffered, 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.

Section 3
Administrative fines

Article 54. General conditions for imposing administrative fines

1. The Ukrainian Parliament Commissioner for human rights shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Law referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in point 5 of paragraph 1 of Article 49. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

1) 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;

2) the intentional or negligent character of the infringement;

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

4) 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;

5) any relevant previous infringements by the controller or processor;

6) the degree of cooperation with the Ukrainian Parliament Commissioner for human rights, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

7) the categories of personal data affected by the infringement;

8) the manner in which the infringement became known to the Ukrainian Parliament Commissioner for human rights, in particular whether, and if so to what extent, the controller or processor notified the infringement, including the fulfilment of obligation on notification of a personal data breach as referred to in Article 33;

9) where measures referred to in point (5) of paragraph 2 of Article 49 have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

10) adherence to approved codes of conduct pursuant to Article 38 or to a processing scheme certified pursuant to Article 38c.

11) 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.

Article 55. General rules on procedure of imposing administrative fines

1. The Ukrainian Parliament Commissioner for human rights, acting through his/ her office, is entitled to impose administrative fines for the infringements of this Law in accordance with procedure laid down in this Law.

2. Fines may be imposed on individuals infringing this Law or on legal persons, if the infringement is caused either by direct order of a decision making organ of the legal person or is the result of inadequate control mechanisms for processing operations within the institutions of the legal person.

3. Persons involved in the procedure for the imposition of administrative fine may have a representative. The power of attorney or any other document confirming the representative's authorisation shall be submitted to the Ukrainian Parliament Commissioner for human rights.

4. A decision to impose an administrative fine can be made within 3 years since the day of commitment of the infringement, or if the infringement of Law is of a continuous nature – the last occurrence of the infringement.

Article 56. Procedure for imposing administrative fines

1. The Ukrainian Parliament Commissioner for human rights shall start the procedure for imposing an administrative fine by sending an official document to the person who is suspected of committing an infringement of the Law, informing about the opening of the procedure and requesting to submit within a time period set out in the document, shall not be less than 10 working days after receiving the official document, the information in writing concerning the following:

1) explanations regarding the circumstances of the alleged infringement of the Law answering to the deliberations and questions contained in the document,; and

2) information relevant to the imposition of an administrative fine, especially its amount;

3) the person who is suspected of committing an infringement of the Law may request on an oral hearing procedure giving the reasons why it should be considered necessary.

2. Failure of the person who is suspected of committing an infringement of the Law to provide explanations and other information set in paragraph 1 within the set period of time shall not preclude the continuation of the procedure and imposition of an administrative fine.

3. At the request of a suspected person or on the initiative of the Ukrainian Parliament Commissioner for human rights, due to the complexity of the circumstances referred to or other important circumstances, when it is necessary to hear oral submissions of the person, suspected of conducting an infringement of the Law, or when a case can be disposed better by holding oral proceedings, the Ukrainian Parliament Commissioner for human rights may decide to hold an oral hearing of a case. When a case is being heard orally, the person suspected of committing an infringement of the Law, the complainant (if any) and other interested parties (if any) must be informed of the place, date and time of the hearing of the case not later than 10 working days before the day of the hearing.

4. The person suspected of committing an infringement of the Law, and other persons, whose participation in the hearing is necessary to dispose the case properly, can participate in the hearing of the case and submit their explanations.

5. Failure to appear in the hearing by the person suspected of committing an infringement or the representative of the person shall not preclude the hearing and disposition of the case, provided that the person suspected of committing an infringement has been duly notified of the hearing and no proof that proof that the person suspected of committing an infringement or the representative of the person could not arrive for important reasons was provided.

6. If written proceedings are held the Ukrainian Parliament Commissioner for human rights shall make a decision on administrative fine imposition within the period of 20 working days since the end of the period set in the document setting out the proposal for the imposition of an administrative fine referred to in paragraph 1 of this Article. The decision of the Ukrainian Parliament Commissioner for human rights shall be sent to the person, in respect of whom a decision has been made, and the complainant (if any).

The decision of the Ukrainian Parliament Commissioner for human rights on the imposition of administrative fine must be reasoned. It must contain: the name of the issuing authority; date and place of the hearing; information about the person, in respect of whom a

decision has been made; the decision which was made on the imposition or non-imposition of an administrative fine; the legal basis for the decision; infringements of personal data and / or privacy protection, if any; the circumstances of the infringement; evidence gathered and their assessment; explanations (if any) of the person suspected of committing the infringement and other persons, their assessment; the time period and procedure for appeal.

7. The decision of the Ukrainian Parliament Commissioner for human rights on the imposition of administrative fine may be appealed to court according the procedure laid down by law.

Article 57. Execution of the decision on the imposition of administrative fine

The individual or legal person fined by the decision of the Ukrainian Parliament Commissioner for human rights shall pay the fine within one month since the day the decision was sent or served to the person, to whom an administrative fine was imposed. In case of a failure to fulfil the obligation he Ukrainian Parliament Commissioner for human rights start an enforcement procedure as laid down by law. The administrative fine shall be paid to the state budget.

CHAPTER VIII
Final provisions

Article 58. Entry into force and application

This Law shall enter into force on _____.

DRAFT AMENDMENT OF LAW OF UKRAINE ON ACCESS TO PUBLIC INFORMATION

Article 1.

Article 2 shall be supplemented with paragraph 3:

"3. This Law shall not apply to the person's right to access his/her data. This right shall be executed as laid down in the Law of Ukraine on personal data protection."

Article 2.

1. Paragraph 1 of Article 6 shall be supplemented with subparagraph 4:

"4) personal information."

2. Article 6 shall be supplemented with paragraph 1a:

"1a. Restriction of access to personal information may only be executed according to the provisions of the Law of Ukraine on personal data protection as set out in Article 9^1 of the present Law"

Article 3.

The Law shall be supplemented with an Article 91:

"Article 91. Personal information

1. Personal information means personal data in the sense of the Law of Ukraine on personal data protection.

2. Access to personal information by third parties shall be granted if such information is reliably de-personalized or if the access complies with the requirements of the Law of Ukraine on personal data protection. In the absence of consent of the data subject or a special

legal provision determining or allowing the access to personal information by third parties, the access to personal information may be granted on the ground of legitimate interest of requester or other persons, including the public interest, in disclosure of personal information, provided that the interest in disclosure override the personal information subject's interests or fundamental rights and freedoms, which require protection of personal information. The requester's interest in disclosure shall be considered overridden by personal information subject's interests or fundamental rights and freedoms, if the disclosure would unduly harm the data subject. The risk of prosecution for alleged offences or crimes shall not be considered as personal information subject's overriding interest or fundamental rights and freedoms, which require protection of personal information.

3. In case a request for access to personal information by third parties is based on legitimate interests of the requester, the personal information subject must be informed about the request and has the right to object to the disclosure and giving the reasons of overriding interests in protection within 10 days after receiving the information. The information processor shall decide whose legitimate interests prevail. The decision may be appealed to the Ukraine Parliament Commissioner for human rights.

Article 4.

1. Article 10 shall be repealed.
2. Paragraph 3 of Article 101 shall be repealed.
3. Article 10 1 shall become Article 10

Article 5.

Paragraph 2 of Article 19 shall be amended and worded as follows:

"Requests for information shall not be reasoned except for requests for personal information."

Article 6.

Paragraph 5 of Article 19 shall be supplemented with subparagraph 2a:

"2a) the reason for the request for personal information."

Article 7.

Paragraph 1 of Article 22 shall be supplemented with a subparagraph 1a:

"1a) the requirements set out in Article 91 for the disclosure of personal information to a third party are not met.