Council of Europe Project
"Supporting Implementation of the European Human Rights Standards in Ukraine"

24 April 2023

OPINION
ON THE DRAFT LAW OF UKRAINE "ON PERSONAL DATA PROTECTION"
(NO. 8153 AS OF 25 OCTOBER 2022)

TABLE OF CONTENT

1. INTRODUCTION

The Council of Europe implements the project "Supporting implementation of the European Human Rights Standards in Ukraine" (hereinafter the Project), funded under the Council of Europe Action Plan for Ukraine "Resilience, Recovery and Reconstruction" (2023-2026). The Project aims at supporting the human rights institutions in effectively implementing their mandate, including by providing expertise on harmonisation of the legal framework with the European standards.

This opinion was requested by the Committee of the Verkhovna Rada of Ukraine on Human Rights, De-occupation and Reintegration of the Temporarily Occupied Territories of Ukraine, National minorities, and Interethnic relations on 26 January 2023.

Ms Dijana Šinkūnienė, the Director of the State Data Protection Inspectorate of the Republic of Lithuania and Ms Nana Botchorichvili, Data Protection and Privacy Attorney, as the Consultants of the Council of Europe were asked to deliver the opinion vis-à-vis its compliance of the Draft law "On Personal Data Protection" ("the Draft law") with the Council of Europe and other European standards.

The opinion is limited and does not extend to cover the full revision of the draft legislative package on data protection. The Council of Europe remains committed to finalise this comprehensive exercise through a follow-up exchange with the Ukrainian authorities, discussing key aspects of the data protection reform.

The purpose of this opinion is to analyse the Draft law and to provide recommendations on its improvement. The primary basis for this opinion are the Council of Europe and European Union standards, in particular the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS No. 108) as amended by the Protocol CETS No. 223, adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018), and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In addition, taking into consideration the EU legal acts to be implemented by the Draft Law[1], the following relevant EU provisions were taken into account for the purpose of this opinion: the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April

[1] Information provided in the Explanatory Note to the Draft Law of Ukraine „On Personal Data Protection" (Annex 1), p. 2,3.

2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive), as well as Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive).

For the sake of ensuring consistency, the authors of this opinion considered recommendations issued in 2020 on the previous version of the draft Law of Ukraine "On Personal Data Protection"[2], as well as discussions with Ukrainian counterparts held in 2021[3]. The authors are also aware of the Draft Law on the supervisory authority "On the National Commission for Personal Data Protection and Access to Public Information" (No. 6177 dated 18.10.2021) which has been developed and is under consideration by one of the Committees of the Verkhovna Rada of Ukraine[4].

The Draft Law, when adopted, will serve as a basis for the protection of personal data both in the public and private sectors, as well as for legislative bodies when adopting legal acts regulating personal data processing and security.

[2] Legal review on the Draft Law of Ukraine "On Personal Data Protection" No. 5628 as of 07 June 2021 with recommendations to make it aligned with the Council of Europe and European standards, prepared by Ms Nataša Pirc Musar, and Ms Dijana Šinkūnienė, 16 October 2020 (provided before the registration of the Draft Law in the Verkhovna Rada of Ukraine).

[3] Online consultations were held on 29 April 2021, the Table of comments of the Draft Law of Ukraine "On Personal Data Protection" 5628 as of 07.06.2021 and the legal opinion thereto Joint European Union and the Council of Europe Project is provided in Annex 2.

[4] Information provided in the Explanatory Note to the Draft Law of Ukraine „On Personal Data Protection" No.8153 as of 25 October 2022 (Annex 1), p. 8.

2. LIST OF ABBREVIATIONS

Draft Law	Draft Law of Ukraine "On Personal Data Protection"
Convention 108+	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), adopted on 28 January 1981 in Strasbourg, as amended by the Protocol CETS No. 223.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of naturalpersons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Law Enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
E-Privacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as further amended in 2006 and 2009

Explanatory Report	Explanatory Report to Convention 108+ endorsed by the Committee of Ministers in its 128th Session (Elsinore, 18 May 2018)
Table of comments	Table of comments of the Draft Law of Ukraine "On Personal Data Protection" 5628 as of 07.06.2021 and the legal opinion thereto Joint European Union and the Council of Europe Project provided as Annex 2

3. COMMENTS BY ARTICLE TO THE DRAFT LAW OF UKRAINE "ONPERSONAL DATA PROTECTION"

3.1. PREAMBLE AND SECTION I GENERAL PROVISIONS

Preamble of the Draft Law is in compliance with the Convention 108+ and GDPR.

Article 1. Scope of the Law

The Article is in compliance with the Convention 108+ and with the GDPR.

Article 2. Definitions

According to the definition provided in this Article, "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow identifying or verifying that natural person, including by the following parameters: digital signature of a person, digital image of a person's face, digital fingerprints. The wording "<…> including by the following parameters: digital signature of a person, digital image of a person's face, digital fingerprints" suggests that these parameters themselves shall be considered biometric data, but such an approach would not be correct. It should be noted that a digital signature usually means an electronic signature, which shall not be considered biometric data (this conclusion could be supported by the provisions of paragraph 6 of the same Article which provides that the term "digital signature" shall be used with the meanings provided in the Law of Ukraine "On Electronic Trust Services"). Concept of "digital fingerprints" has a meaning that describes data relating to the user browsing the Internet and using various digital devices. According to paragraph 59 of the Explanatory Report, the processing of images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual, therefore the mere digital image of a person's face should not be considered as biometric data.

Following the definition of biometric data provided in Article 4 (14) of the GDPR, '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, i.e. facial images and dactyloscopic data (fingerprints) are provided as examples of characteristics of a natural person which should undergo specific technical processing in order to be considered biometric data.

Definition of "biometric data" shall be amended deleting its last part "including by the following parameters: digital signature of a person, digital image of a person's face, digital

fingerprints" or using the wording that would not be confusing. It is recommended to use the definition of "biometric data" provided in the Table of comments[5].

According to this Article, "restriction of processing" means designation of the stored personal data in order to restrict their further processing. Article 4 (3) of GDPR and Article 3 (3) of the Law Enforcement Directive provide that "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future.

In order to avoid confusion, it is recommended to amend definition "restriction of processing" using the word "marking" instead of "designation".

Definition of **'**law enforcement agency' provided in this Article foresees that 'law enforcement agency' means a public authority vested with the tasks related to prevention, detection, termination, uncovering and investigation of criminal offences falling within its competence; ensuring protection of human rights and freedoms, combating crime, maintaining public security and order; authorised to enforce criminal sanctions; initiate and conduct pre-trial investigation and inquiry, ensure procedural management of pre-trial investigation; public authority of special purpose with law enforcement functions that ensures national security of Ukraine; intelligence and counterintelligence agencies. Following definition of 'personal data processing for the law enforcement purposes', ensuring protection of human rights and freedoms is also named as one of the elements of personal data processing for the law enforcement purposes[6].

According to Article 3 (7) of the Law Enforcement Directive 'competent authority' means: a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

[5] **'Biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological characteristics of a natural person, which allow identifying or verifying that natural person (see p. 4).

[6] According to Article 2 (1) of the Draft Law, 'personal data processing for the law enforcement purposes' means processing of the personal data by the law enforcement agencies aimed at prevention, detection, termination, uncovering and investigation of criminal offences, enforcement of criminal sanctions; ensuring protection of human rights and freedoms, combating crime, maintaining public security and order; initiating and conducting pre-trial investigation and inquiry, procedural management of pre-trial investigation; intelligence operations; ensuring national security.

Although respect for human rights must be ensured when processing personal data by law enforcement agencies, however, it is not a task of competent authorities according to the Law Enforcement Directive. Therefore, we would advise to amend definition of 'law enforcement agency' and definition 'personal data processing for the law enforcement purposes' by adding 'ensuring the lawful exercise of human rights and fundamental freedoms' instead of '<u>ensuring protection of human rights and freedoms</u>'.

Article 3. Legislation on personal data protection

This Article does not need to be modified or amended.

Article 4. Principles relating to the processing of personal data

This Article does not need to be modified or amended.

3.2. SECTION II GROUNDS OF THE PROCESSING OF PERSONAL DATA

Article 5. Grounds for the processing of personal data

According to Article 5 (5), processing of personal data based on the consent of the personal data, as well as based on necessity to protect the vital interests of the personal data subject or another natural person may be carried out only in case of absence of other grounds provided for by paragraph one of this Article. Following this provision, it could be concluded that other grounds for legitimate processing have priority over the consent and protection of vital interests' grounds.

Article 5 (2) of the Convention 108+ provides that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law. Article 6 (1) of GDPR sets out conditions for lawfulness of processing. Convention 108+ and GDPR do not give priority to any of the grounds for legitimate data processing, i.e. all legal grounds are equal.

Article 5 (5) of the Draft Law is not fully in line with Article 5 (2) of the Convention 108+ and Article 6 (1) of GDPR and therefore should be deleted.

Article 6. Consent to the processing of personal data

Following Article 6 (3) (1) the consent is not considered free if the personal data subject is dependent on or subordinated to the controller to whom the consent is given. It should be noted that in cases of subordination (for example in employer-employee relationship) freely given consent can still be possible. Guidelines 05/2020 on consent under Regulation 2016/679 adopted on

4 May 2020 by European Data Protection Board provide that the nature of the relationship between employer and employee does not mean that employers can never rely on consent as a lawful basis for processing. Although in exceptional circumstances, but freely given consent is still possible (see para. 21, 22, 23, p. 9)[7]. In addition, Article 52.2 of the Draft Law provides for the possibility to collect data of employees on the basis of consent. As such, Article 6 (3) (1) is in contradiction with this provision.

It is recommended to amend wording of Article 6 (3) (1) of the Draft Law eliminating prohibition of freely given consent if there is dependence or subordination between data controller and data subject as this provision will be in contradiction with Article 52 (2) of the Draft Law and with Guidelines 05/2020 on consent under Regulation 2016/679.

According to Article (6) (5) of the Draft Law, the consent of the personal data subject to the processing of his/her personal data is considered to be informed if, before or at the moment of giving such consent, the personal data subject is informed about the following:

1) the reason, purpose, type of the processing of his/her personal data;

2) personal data to be processed;

3) contact details of the controller: permanent location and means of communication to the extent allowing the personal data subject to identify such controller and processor and to communicate with them without delay;

4) the rights provided for by the legislation in the field of personal data protection and the ways of their enjoyment;

5) any other information necessary to ensure the fair and transparent processing of personal data.

According to Article 5 (2) of the Convention 108+, data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject. The before-mentioned Guidelines 05/2020 on consent under Regulation 2016/679 adopted on 4 May 2020 by European Data Protection Board provide that at least the following information is required to be provided to the data subject for obtaining valid consent:

i. the controller's identity;

ii. the purpose of each of the processing operations for which consent is sought;

iii. what (type of) data will be collected and used;

[7] Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, accessed February 17, 2023

iv. the existence of the right to withdraw consent;

v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) [of GDPR] where relevant;

vi. on the possible risks of data transfers due to absence of an adequacy decision and ofappropriate safeguards as described in Article 46 [of GDPR].

It should be noted that providing information, such as the rights provided for by the legislation in the field of personal data protection and the ways of their implementation, is not necessary for the informed consent.

It is suggested to amend Article (6) (5) of the Draft Law by setting up clear requirement to provide information on the existence of the right to withdraw consent, the use of the data for automated decision-making (where relevant), on the possible risks of data transfers due to absence of an adequacy decision and/or of appropriate safeguards in third countries (where relevant).

3.3. SECTION III SPECIAL REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA

Article 7. Special requirements for the processing of sensitive personal data

According to Article 7 (2) (8), provisions of paragraph one of this Article shall not apply if 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 social or health care services (including health care electronic system), 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 conditions and safeguards referred to in part two of this Article.

As the relevant safeguards are provided not in the same paragraph 2, but in paragraph 3, the editing of the Article 7 (2) (8) is needed giving reference to paragraph 3 instead of paragraph 2 of this Article. Also, Article 7 (3) needs to refer to Article 7 (2) (8), as these conditions (obligation of professional secrecy) only apply in such a case, in line with Article 9.3 of the GDPR.

Article 8. Processing of personal data relating to criminal prosecution, offences, criminal proceedings and convictions, as well as security measures related thereto

According to Article 8 (2) of the Draft Law, processing of personal data relating to criminal prosecution of persons, offences, criminal proceedings and convictions, as well as security measures related thereto shall be kept under control by the supervisory authority in the manner approved by it.

Article 2 (1) of the Draft Law provides definition of supervisory authority: 'supervisory authority' means an independent authorised body that exercises supervision and control over compliance with the requirements of this Law and whose powers are stipulated by this Law and the Law that defines the authority ensuring state control over compliance with the personal data protection legislation. Keeping a register of criminal convictions, setting up rules relating to the functioning of such register should not be the tasks of data protection supervisory authority. Following Article 10 of GDPR, any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 8 (2) of the Draft Law shall be brought in line with Article 10 of GDPR, by conferring the duty of keeping a comprehensive register of criminal convictions on an official authority, but not on the supervisory authority.

Article 9. Processing of biometric data by public authorities

Article 9 (1) (3) gives reference to paragraph two of Article 7 of this Law, which regulates processing of special categories of personal data in general. Article 9 sets up special conditions for processing of biometric data by public authorities, therefore the link to Article 7 is not clear (i.e., whether and to what extent paragraph two of Article 7 could be applicable to processing of biometric data by public authorities). On the other hand, the interconnection between paragraphs 1 and 2 of Article 9 is not clear.

It is suggested:

1) deleting or clarifying reference to paragraph two of Article 7 in Article 9 (1) (3);

2) clarifying the relation between paragraphs 1 and 2 of Article 9 of the Draft Law (e.g.: "Processing of biometric data by public authorities is lawful if it **meets conditions set up in paragraph 1 of this Article and** is carried out for the following purposes <…>").

Article 10. Video surveillance

According to Article 10 (5) of the Draft Law, the controller shall be obliged to place a warning that video surveillance is being carried out, in an accessible place, in the state language. The warning shall contain the name and contact details of the controller and the person carrying out video surveillance if such person is different from the controller. It is not clear who is "a person carrying out video surveillance", and why the datasubject's right to information is narrowed only to the personal data collected (i.e., warning that video surveillance is being carried out) and the name and contact details of the controller. As regards restrictions relating to transparency of processing, according to Article

11 (1) of the Convention 108+, no exception to the provisions of Article 8 paragraph 1, regulating transparency of processing, shall be allowed, unless such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society to protect public interests (such as public safety etc.). It should be noted that information regarding data processing by means of video surveillance could be made accessible to the data subject by other means, not only on the warning sign. Guidelines 3/2019 on processing of personal data through video devices adopted on 29 January 2020 by European Data Protection Board provide that: "In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, par. 22). Regarding video surveillance the most important information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer) [8]."

Article 10 (5) of the Draft Law should be amended refusing to restrict data subject's right to information only to the personal data collected and the name and contact details of the controller.

Article 11. Processing of personal data as a result of audio, video or photo recording of public events

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 12. Processing of personal data for the purpose of direct marketing, pre-election campaigning and/or political advertising

Article 12 (2) of the Draft Law sets up conditions under which processing of personal data for the purposes of direct marketing is possible without the consent of the personal data subject. One of these conditions is that "contact details of the personal data subject received as a result of entering into and execution of a contract to which the personal data subject is a party or in order to take steps required to enter into a contract at the request of the personal data subject". It should be noted that according to Article 13 (2) of the E-Privacy Directive, only contact details for electronic mail could be used without prior consent: "Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that

[8] Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf , accessed February 24, 2023, see para. 111, p. 26.

customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use."

It is recommended to reconsider Article 12 (2) of the Draft Law in the light of Article 13 (2) of the E-Privacy Directive, limiting its scope to electronic contact details for electronic mail.

Article 12 (2) of the Draft Law also sets up the condition that processing of personal data for the purposes of direct marketing is possible without the consent of the personal data subject, provided that "the extent of interference with the private life of the personal data subject shall be no more than required for performance of the initial contract." It should be noted that the scope of Article 13 (2) of the E-Privacy Directive is not limited to the performance of the initial contract, i.e. electronic contact details for electronic mail could be used for direct marketing of the similar products or services after execution of the initial contract.

It is recommended to reconsider Article 12 (2) of the Draft Law in the light of Article 13 (2) of the E-Privacy Directive, by refusing excessive limitations on the use of contact details (for electronic mail) for direct marketing purposes.

Article 13. Processing of personal data for purposes other than those for which they were collected

Article 13 (1) of the Draft Law sets the list of circumstances to be considered when determining whether the new purpose of processing is compatible with the primary one. Para. 49 of Explanatory Report explains that: "In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data is initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*, any link between those purposes andthe purposes of the intended further processing; the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to its further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations." Article 6 (4) (b) of GDPR describing the context of collection of data makes emphasis on the relationship between the data subject and data controller; Article 6 (4) (c) of GDPR underlines the nature of the personal data, in particular special categories of personal data and data related to criminal convictions and offences.

It is advised to supplement Article 13 (1) with the provisions relating to reasonable expectations of data subjects based on their relationship with the controller as well as nature of personal data

(referring explicitly to special categories of personal data and data related to criminal convictions and offences).

Article 13 (2) of the Draft Law, without specifying any additional safeguards, provides that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be considered as processing compatible with the primary purpose. Para. 50 of the Explanatory Report explains that the further processing of personal data, referred to in Article 5 (4), (b) of the Convention 180+ for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is *a priori* considered as compatible provided that other safeguards exist (such as, for instance,anonymisation of data or data pseudonymisation, except if retention of the identifiable form is necessary; rules of professional secrecy; provisions governing restricted access and communication of data for the above-mentioned purposes, notably in relation to statistics and public archives; and other technical and organizational data security measures) and thatthe operations, in principle, exclude any use of the information obtained for decisions or measures concerning a particular individual. Article 89 (1) of GDPR also provides for safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Article 13 (2) of the Draft Law should be reconsidered in the light of Article 5 (4) (b) of the Convention 108+ and Article 89 (1) of GDPR, namely as regards additional safeguards.

Article 13 (3) of the Draft Law says that if the new purpose is incompatible with the primary purpose, the processing of personal data for the new purpose shall be lawful in the specified cases (data subject has given consent or such processing is necessary to fulfil a legal obligation provided for by law). Recital 50 of GDPR provides that where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. This provision implies that it is not necessary to perform purpose compatibility test if processing for new purpose is based on data subject's consent or is necessary to fulfil a legal obligation provided for by law.

For the sake of clarity, it would be advisable to reformulate wording of Article 13 (3) of the Draft Law "If the new purpose is incompatible with the primary purpose, the processing of personal data for the new purpose shall be lawful in the following cases <…>" to "Paragraph 1

of this Article shall not apply and the processing of personal data for the new purpose shall be carried out based on: <…>" or similarly.

Article 14. Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 14 (2) of the Draft Law leave discretion to the controller which processes personal data for the purpose of scientific or historical research to restrict the rights of the data subjectprovided for in Articles 19 (Right of the data subject to access to personal data), 21 (Right of the personal data subject to be forgotten), 22 (Right to object to the processing of personaldata), 24 (Right to restriction of processing of personal data) of this Law to the extent thattheir implementation will prevent the achievement of these purposes and such restriction is necessary to achieve them. Firstly, it should be noted that restriction of the data subject's rights in this case should be foreseen by law (see Article 23 (1) and 89 (2) of GDPR, Article 11 (2) of the Convention 108+). Secondly, restrictions of the data subject's rights when processing personal data for statistical purposes are not foreseen in the Draft Law at all, although it would have practical value and taking into account Article 89 (2) of the GDPR which refers to it in the context of restrictions.

Article 14 (2) of the Draft Law should be amended without leaving discretion to the data controller to restrict data subject's rights. It is advisable to consider the possibility to foresee in the Draft Law restrictions of data subject's rights when processing personal data for statistical purposes.

Article 15. Processing of personal data for the purposes of journalistic or creative activities

According to Article 15 (2) of the Draft Law, paragraph 1 of this Article shall be applied only provided that the controller performing the personal data processing solely for the purposes of journalistic or creative activities reasonably believes that disclosure of information is made in the public interest, and the harm from disclosure of such information does not exceed the public interest in its obtaining. Following paragraph 3, for the purposes of this Article, 'journalistic activities' shall be understood as activities of journalists and mass media, their employees, as specified by the Law of Ukraine "On Information".

Paragraph 96 of the Explanatory Report underlines that: "In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly". The same paragraph, when referring to freedom of expression, explains that freedom of expression includes freedom of journalistic, academic, artistic or literary expression, and the right to receive and impart information. Taking this into account it

could be concluded that the scope of Article 15 of the Draft Law is too narrow.

It is advised to amend Article 15 of the Draft Law by extending its scope to "the freedom of expression, including freedom of journalistic, academic, artistic or literary expression, and the right to receive and impart information".

Article 16. Processing of personal data after the death of the personal data subject

The Article is not in contradiction with Convention 108+ and with the GDPR. Thus, it does not raise specific comments.

Article 17. Use of technology for tracking actions of personal data subjects in electronic communications and services

Article 17, and more specifically its paragraphs 2 and 3, addresses the conditions under which personal data can lawfully be processed, in particular with prior consent of data subjects unless other conditions apply, when being collected via various tracking technologies. We understand that this Article aims to integrate the requirements set out by Article 5 (3) of the E-Privacy Directive which in a nutshell regulates the use of cookies and other tracking technologies on a data subjects' terminal equipment. However, the latter provision sets requirements for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user and not the processing of personal data. In other words, it relates more specifically to the placing of tracking technologies on a data subject's device. The collection and processing of personal data resulting from it is a separate operation and which will in any case be regulated by the general data protection provisions (i.e. for the EU, the GDPR).

The wording of Article 17 needs to be reconsidered to be aligned with the one of Article 5 (3) of the E-Privacy Directive, by setting out conditions for the storing of information, or the gaining of access to information on the device of a data subject but not the processing of personal data in this context.

According to Article 17 (3) (2) of the Draft Law, the data subject shall be provided with an explanation that he/she has the right to choose to which technology he/she agrees if the processing is carried out based on consent. Following definition provided in Article 2 (f) of the E-Privacy Directive, "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC [GDPR], i.e. "a freely given specific and informed indication of the user's wishes". Article 5 (3) of the before-mentioned Directive stipulates that the storing of information, or the gaining of access to

information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC [GDPR], inter alia, about the purposes of the processing. This means that consent shall be given to, a purpose of processing, but not to use of technology. In order consent to be valid, the information about processing should be clear and comprehensive, which would not be the case by naming only the technology. On the other hand, requirement to provide user with the right to choose to which technology he/she agrees seems inappropriate or even excessive.

Taking into account Article 2 (f) of the E-Privacy Directive, it is recommended to reconsider Article 17 of the Draft Law as far as it provides for the right of the user (data subject) to choose to which technology he/she agrees by replacing this reference with the right to choose the purpose of processing.

Article 17 (4) (2) of the Draft Law obliges controllers or processors that perform processing of the personal data referred to in paragraph one of this Article to ensure unconditional automated possibility for the personal data subject to make any changes to his/her processed personal data. It should be noted that Article 9 (1) (e) of the Convention 108+ and Article 16 of the GDPR foresee the right to rectification of inaccurate personal data, but not unconditional right to make any changes.

Article 17 (4) (2) of the Draft Law, as far as it provides for unconditional right to make any changes to processed personal data, should be reconsidered in the light of the Article 9 (1) (e) of the Convention 108+ and Article 16 of the GDPR.

3.4. SECTION IV RIGHTS OF THE PERSONAL DATA SUBJECT

Article 18. Right to information

It should be noted that Articles 13 and 14 of GDPR do not require separately to provide data subject with the information on the processor(s) (processors are covered by the recipients of the personal data), as well as objectives and methods of the processing, the actions or set of actions that will be performed with regard to the personal data. On the other hand, this Article is lacking information on the legitimate interests pursued by the controller or by a third party as well as for international transfers reference to the appropriate safeguards used and the means by which a copy can be obtained. In addition, in case of direct collection of data (Article 13), the GDPR does not provide for a requirement to specify the categories of data processed. Furthermore, Article 14 (4) of the

GDPR requires that on case of further processing for a purpose other than the initial purpose, the data subject shall receive prior information on it from the controller.

It is recommended to reconsider Article 18 (1) subparagraphs 2, 4, 5 of the Draft Law in the light of Articles 13 and 14 of GDPR, i.e. as far as Article 18 provides for additional transparency requirements.

Article 18 of the Draft Law should be supplemented in particular with the information on the legitimate interests pursued by the controller or by a third party where the processing is based on Article 5 (1) subparagraph 6 of this Draft Law as well as for international transfers on the appropriate safeguards used and the means by which a copy can be obtained.

Regarding the exemptions to the information obligation as set out in Article 18 (4) of the Draft Law, it can be noted that it does not foresee the case where the provision of information is likely to render impossible or seriously impair the achievement of the objectives of the processing as provided by Article 14 (5) (b) of the GDPR. In addition, even in cases when the exemptions to the information obligation are applicable (i.e., processing proves impossible, would involve a disproportionate effort or is likely to render impossible or seriously impair the achievement of the objectives of the processing), Article 14 (5) (b) of the GDPR requires that the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including by making the information publicly available.

It is advised to supplement Article 18 (4) of the Draft Law with respect to the exemptions to the information obligations as well as applicable conditions in light of Article 14 (5) (b) of the GDPR.

Article 19. Right of the personal data subject to access to personal data

In comparison to Article 15 (4) of GDPR, Article 19 of the Draft Law is lacking provision that the right to obtain a copy of the personal data shall not adversely affect the rights and freedoms of others. **It is recommended to supplement Article 19 of the Draft Law with the provision that the right to receive a copy of the personal data referred to in paragraph 2 shall not adversely affect the rights and freedoms of others.**

Article 20. Right of the personal data subject to rectification of personal data

According to Article 20 (3), the controller shall be obliged to notify all recipients to whom the personal data have been disclosed of the satisfaction of the request for data rectification unless such notification involves a disproportionate effort for the controller. It should be noted that Article 19 of GDPR provides for broader obligations as regards notification obligations: 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.

The Draft Law shall be made in line with the Article 19 of GDPR by supplementing with the obligations to notify recipients not only about rectification, but also erasure of personal data or restriction of processing, as well as to inform the data subject about those recipients if the data subject requests it. In addition, it should refer to the impossibility to perform the notification in line with the same Article of the GDPR.

Article 21. Right of the personal data subject to be forgotten

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 22. Right to object to the processing of personal data

Article 22 of the Draft Law, regulating right to object to the processing of personal data, is not in line with the Convention 108+ and Article 21 of GDPR as far as the way it regulates personal data processing and objection for direct marketing purposes. According to para. 79 of the Explanatory Report an objection to data processing for marketing purposes should lead to unconditional erasing or removing of the personal data covered by the objection. It should be noted that Article 21 (2), (3) of GDPR also pays specific attention to the right to object as regards personal data processing for direct marketing purposes: data subject can exercise the right to object at any time, and the data controller is unconditionally obliged to cease personaldata processing for direct marketing purposes if such objection received.

Taking into account Article 21 (2) and (3) of GDPR, Article 22 of the Draft Law should be supplemented with additional provisions regulating more explicitly the right to object: where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the 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. In case of objection to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Article 23. Right to personal data portability

Provisions of Article 23 of the Draft Law, relating to the right to data portability, seem to be very complicated to apply in practice and are going beyond to those of the Article 20 of GDPR. For example, supervision of Article 23 (3) of the Draft Law rules regulating claiming compensation from the data subject for costs of the implementation of this right would be sophisticated also for the supervisory authority. On the other hand, such claim of compensation from the data subject is in contradiction with the provisions of Article 12 (5) of GDPR, which says that any communication and any actions taken under Articles regulating data subject rights shall be provided free of charge, except where requests from a data subject are manifestly unfounded or excessive.

Taking into account Article 12 (5) and Article 20 of GDPR, regulating respectively modalities for the exercise of the rights of the data subject and right to data portability, it is recommended to delete paragraph 3 of the Article 23 of the Draft Law.

Article 24. Right to restriction of processing of personal data

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended (subject to recommendations above under Article 20).

Article 25. Right to the protection against automated individual decision-making

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 26. Right of the personal data subject to the protection of his/her rights and compensation for damages

According to Article 26 (3) of the Draft Law, the controller shall be exempt from liability for damage caused to the personal data subject if the controller proves that the events that caused such damage were not his/her fault and he/she took all reasonable measures to prevent the violation of rights and the occurrence of damage.

Article 26 (4) of the Draft Law provides that in order to compensate for the damage caused to the personal data subject as a result of the processing of personal data by joint controllers, the personal data subject may lodge a complaint or a claim with one of such controllers. Following Article 26 (5)

of the Draft Law, the controller who has compensated the personal data subject for the damage caused by the actions of the personal data processor shall have the right to claim compensation from such processor by way of recourse.

It should be noted that Article 82 (4) of GDPR makes reference not only to controllers, but also to processors involved in the same processing ("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"). Article 82 (3) of GDPR provides that the processor shall be exempt from liability as well if the conditions of this paragraph are met. According to Article 82 (5) of GDPR, where a controller or processor has 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.

Article 26 (3) of the Draft Law does not provide that the processor shall be exempt from liability for damage caused to the personal data subject. Article 26 (4) of the Draft Law limits the possibilities of the data subject to claim damages only from the data controller involved in the processing. Article 26 (5) of the Draft Law does not provide that the processor who compensated all the damage could claim compensation from the controller involved in the same processing. Therefore, Article 26 (3), (4) and (5) of the Draft Law is not in line with the Article 82 (3), (4) and (5) of GDPR. Provisions of Article 26 (3), (4) and (5) of the Draft Law should be supplemented by adding the processor.

Article 27. Procedure for considering requirements of the personal data subject

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

3.5. SECTION V RESPONSIBILITIES OF THE CONTROLLER AND PROCESSOR

Article 28. General responsibilities of the controller and processor

The Article is in compliance with Convention 108+ and consistent with the GDPR. Thus, it does not need to be modified or amended.

Article 29. Data protection by design and by default

The Article is in compliance with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 30. Joint controllers

Article 30 (3) foresees that: „Provisions of a contract regulating the allocation of responsibilities for compliance with the requirements for the processing of personal data and affecting the rights of the personal data subjects shall be deemed the information of public interest and shall be provided in the manner determined by the Law of Ukraine "On Access to Public Information". The personal data subject may exercise his/her rights in respect of each controller regardless of the terms and conditions of the contract and review the content of such contract in the manner determined by the Law of Ukraine "On Access to Public Information".”

It should be noted that the contract concluded by the controllers acting in private sector might contain commercial secrets, therefore it would be unjustified to consider it as the information of public interest. Art. 26 (2) of GDPR provides that the essence of the arrangement concluded by joint controllers shall be made available to the data subject, but not to everyone as it might be assumed in case of the information if public interest.

Provisions of the Article 30 (3) of the Draft Law should be reconsidered in the light of protection of commercial secrets. As the Draft Law and the Law of Ukraine "On Access to Public Information" have different purposes and scope, the reference to the latter in the Draft Law is suggested to be reviewed. It is recommended to amend second sentence of the Article 30 (3) of the Draft Law („Provisions of a contract regulating the allocation of responsibilities for compliance with the requirements for the processing of personal data and affecting the rights of the personal data subjects shall be deemed the information of public interest and shall be provided in the manner determined by the Law of Ukraine "On Access to Public Information") providing that the essence of the arrangement shall be made available to the data subject instead of being the information of public interest.

Article 31. Personal data processor

Second paragraph of the Article 31 (8) of the Draft Law foresees that provisions of a contract between the controller and the processor under which the processing is carried out and which affect the rights of the personal data subjects shall be provided in the manner determined by the Law of Ukraine "On Access to Public Information".

As in the previous Article regulating joint controllers, it should be noted that the controller and/or processor could act in the private sector, and the contract concluded by them might contain commercial secrets. On the other hand, controllers and processors who are not bound under the Law of Ukraine "On Access to Public Information", are not obliged to share information with the public. Thus, when it comes to such entities, the contract will not constitute information of a public nature. On the other hand, it will be public information if the contract is concluded by the controller who is obliged by the mentioned law – in this case, however, a special provision on this issue is not required in the Draft Law, as it should be self-regulated by the Law "On Access to Public Information".

Provisions of the Article 31 (8) of the Draft Law should be reconsidered in the light of the protection of commercial secrets. As the Draft Law and the Law of Ukraine "On Access to Public Information" have different purposes and scope, the reference to the latter in the Draft Law should be reviewed. It is recommended to delete second paragraph of the Article 31 (8) of the Draft Law („Provisions of a contract between the controller and the processor under which the processing is carried out and which affect the rights of the personal data subjects shall be provided in the manner determined by the Law of Ukraine "On Access to Public Information").

Article 32. Personal data processing under the authority of the controller or processor

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 33. Representative of the controller or processor

This Article is not in contradiction with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 34. Recording of data processing activities

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 35. Security of processing of personal data

Article 35 (1) foresees that: "The controller and the processor shall be obliged to implement appropriate technical and organisational measures to ensure a level of security of personal data processing appropriate to the risk of the processing to the rights and freedoms of personal data subjects in compliance with the proportionality principle." It is not clear what the "proportionality principle" means in the context of this Article. It should be noted that according to Article 7 (1) of

the Convention 108+, "the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data". Paragraphs 62, 63 of the Explanatory Report specifies that when deciding on security measures, both of technical and organisational nature, for each processing, the following should be taken into account: the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage, and so forth; security measures should take into account the current state of the art of data-security methods and techniques in the field of data processing, and their cost should be commensurate with the seriousness and probability of the potential risks.

According to article 32 (1) of GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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.

It is not recommended to use "proportionality principle" in the context of technical and organisational measures aimed to ensure security of personal data. Taking into account provisions of article 32 (1) of GDPR, it is recommended to supplement this article with the main factors, such as state of the art, costs of implementation, nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Article 36. Cooperation of the controller and processor with the supervisory authority

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 37. Notification of a personal data breach to the supervisory authority

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 38. Communication of a personal data breach to the data subject

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be

modified or amended.

Article 39. Data protection impact assessment

This Article is compliant with Convention 108+ and with the GDPR. Thus, it does not need to be modified or amended.

Article 40. Prior consultations

This Article frames the condition under which a prior consultation is to be carried out by a controller with the supervisory authority when an impact assessment under Article 39 of the Draft Law indicates that the processing of personal data would result in a high risk for data subjects. It is in line with the Convention 108+ and with the GDPR subject to the comment below.

Article 40 (3) suggests that following such consultation the supervisory authority will issue a recommendation to the controller but that it may also adopt other decisions without however specifying what such measures could be. For instance, under the GDPR, in accordance with Articles 36 (2) and 58 (2) (a) the supervisory authority can issue a warning that the processing subject to the impact assessment is likely to infringe the GDPR.

If other measures, than a recommendation are envisaged to be issued by the supervisory authority, they should be referred more specifically in this Article for clarity and legal certainty for controllers. If such measures are to be specified by the law regulating the supervisory authority, then it is recommended to refer to this law in this Article.

Article 41. Data protection officer

The Article states the situations where the controller or the processor shall designate a data protection officer. One of these situations is described in Article 41 (1) (3) which provides that a data protection officer must be designated if the core activities of the controller or processor consist or relate to the processing on a large scale of personal data. Such scenario of mandatory designation of a data protection officer is broader than what is required by the corresponding Article of the GDPR (see Article 37). The latter requires indeed the designation of a data protection officer in cases of processing of personal data on a large scale but restricts it to controllers or processors who process on a large-scale special categories of personal data (Article 9) or data relating to criminal offenses (Article 10 GDPR). Thus, it does not require the designation of a data protection officer generally for all kind of processing data on a large scale.

In view to be aligned with Article 37 of the GDPR, Article 41 (1) (3) should be amended to set out that the designation of a data protection officer is necessary in case of data processing on a large scale only when the core activities of the controller or the processor consist of processing of special categories of data or to personal data relating to criminal convictions and offences.

Article 41 (7) provides for a list of persons who may not be designated as data protection officers. Among them the Article refers to the persons that have failed the "qualification examination" without further reference.

As the qualification examination is regulated by at least Article 42 of the Draft Law, it is advisable for the avoidance of any doubt to add a reference to it in this provision.

Article 42. Qualification examination for the position of data protection officer

This Article provides that a person may be appointed as data protection officer for a public authority if such person has passed the qualification examination and obtained a certificate issued by a personnel certification body. However, it is not clear from the Draft Law how the examination process, training and certification are to work in practice and how the certification body will intervene. It nevertheless results from the Article as well as the transitional provisions (section XI point 4) that these elements are to be defined by the supervisory authority.

For clarity, it is advisable to refer to the relevant provisions or act where the details of the framework applying to the qualification examination process can be found. In addition, consistency of Article 42.1 with Article 41 (7) (3) needs to be reviewed: the former suggests that the qualification examination only applies in case of public authorities while the latter also refers to controllers and processors.

Article 43. Codes of conduct relating to personal data protection

This Article sets out the framework for the adoption and approval of codes of conduct in a similar manner as under Article 40 of the GDPR.

According to Article 43 (1), codes of conduct are referred as a voluntary measure while it results from Article 43 (2) that certain types of organizations are mandatorily required to adopt codes of conduct. It can be wondered whether there might be a contradiction between the two Articles.

For legal certainty, the articulation between Articles 43 (1) and 43 (2) needs to be clarified to specify that the obligation for certain organizations to adopt a code of conduct comes in

addition to the voluntary adoption of codes of conduct by other organizations not subject to Article 43 (2).

The drafting of Article 43 (3) is unclear as to the content and objective to be achieved by a code of conduct taking into account Article 40 (2) of the GDPR. According to this provision of the GDPR, the purpose of a code of conduct is to specify the application of the GDPR with respect to a set of elements (scope of application, fair and transparent processing, etc.) which correspond to the ones listed in Article 43 (3) of the Draft Law.

To reflect more closely the requirement of Article 40 (3) of the GDPR, Article 43 (3) should state that the code of conduct shall specify the application of the Draft Law with respect to the elements listed in this Article.

Article 43 does not address the requirement to have in place mechanisms for monitoring the application of the code of conduct including by way of a monitoring body in line with Articles 40 (4) and 41 of the GDPR. In the absence of such mechanisms, the effectiveness of a code of conduct as a means of achieving compliance with data protection legislation is doubtful.

Article 43 needs to be supplemented with a requirement regarding mechanisms, including a body, for monitoring the application of the code of conduct taking into account Article 40.4 and 41 of the GDPR.

3.6. SECTION VI TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

Article 44. Grounds for transferring personal data to third countries or international organisations

The Article complies with Convention 108+ and the GDPR and does not need to be amended.

Article 45. Transfers of personal data to third countries or international organizations which ensure an appropriate level of protection

This Article relates to the possibility of transferring personal data to countries recognized as adequate, the modalities of doing so and the applicable consequences.

Article 45 (4) specifies that when a transfer is made to a country recognized as adequate, that no specific authorization is required from the supervisory authority. The Article also states that the same applies when a transfer is made "from" an adequate country. However, it can be questioned why the Draft Law would regulate data flows and transfers originating from third countries to

Ukraine, as this would generally be outside the scope of the Draft Law.

The reference to transfers "from" third countries in Article 45 (4) is unclear and clarifications from the drafters would be welcomed on why the Draft Law would regulate data flows and transfers originating from third countries to Ukraine.

Article 46. Transfers of personal data to third countries or international organisations subject to appropriate safeguards for personal data

The Article complies with Convention 108+ and the GDPR and does not need to be amended.

Article 47. Transfers of personal data to third countries subject to binding corporate rules

The Article complies with Convention 108+ and the GDPR subject to the following comments and recommendations.

Article 47 (1) sets out the scope of organizations that may use binding corporate rules. It however seems to provide two sets of definition for that purpose.

For clarity, it is recommended to combine or unify the definition of types of organization under this Article that may use binding corporate rules for transferring personal data.

Article 47 (4) states that the binding corporate rules may provide for other measures to ensure security of personal data processing. The content of this provision and the objective it aims to achieve are unclear and cannot be fully assessed taking also into account that the GDPR does not set such a requirement for binding corporate rules under Article 47.

It is necessary to clarify the provisions of Article 47 (4) to set out more specifically their purpose and objective in light of the rest of Article 47.

Article 48 Individual cases of the transfer of personal data to third countries or international organizations

Article 48 (1) (8) of the Draft Law provides that in the absence of an adequate level of protection and appropriate safeguards, a transfer of personal data to a third country or an international organization shall take place if such transfer is necessary for the exercise of the right to freedom of expression and "is proportionate under the specific circumstances". Article 14 (4) (d) of Convention 108+ provides that in such a case the transfer could take place if it constitutes a necessary and proportionate measure in a democratic society for freedom of expression. In light of this provision of Convention 108+, it is not clear what is meant by "is proportionate under the specific circumstances" under Article 48 (1 (8) of the Draft Law. "Specific circumstances" could

not necessarily be related to democratic society values.

Article 48 (1) (8) of the Draft Law should be aligned with Article 14 (4) (d) of Convention 108+, providing that a transfer of personal data to a third country or an international organization shall take place if such transfer is in a specific case necessary and proportionate measure in a democratic society for freedom of expression.

Article 49. Transfer of personal data to third countries for law enforcement purposes

This Article sets out the conditions for transferring personal data by law enforcement agencies of Ukraine to third countries for law enforcement and provides in essence that this can be done either if the third country provides an adequate level of protection (Article 49 (1)) or on the basis of a relevant international treaty (Article 49 (2)) It should be noted that the Law Enforcement Directive under its Article 35 (1) provides for additional conditions to be met for carrying out an international transfer for law enforcement purposes, in particular that the transfer is necessary for law enforcement purposes, the transfer is made to a competent authority for that purpose. In addition, it provides for the possibility to rely on derogations for transfers (Article 35 (1) (d)) and sets out requirements for onward transfers (Article 35 (1) (e)).

Article 49 should be reconsidered to be supplemented with additional conditions in order to frame international transfers for law enforcement purposes, taking into account article 35 of the Law Enforcement Directive.

3.7. SECTION VII PROCEDURE FOR ACCESS OF THIRD PARTIES TO PERSONAL DATA

Article 50 relates to the procedure for access of third parties to personal data in possession of the public information processor.

Article 50 (5) raises some questions as it is actually written unclearly. It would make more sense to combine both of the points and in favour of legal certainty it would be better to write that the request shall be rejected if any of the conditions from the previous paragraph are not met, especially if the requester has not provided the legal basis or legal purpose of obtaining personal data. When the request is only imperfect, for example it does not have all the required elements, the requester is usually asked to complete it within a certain period of time, so that, for grounds of principle of economy, both – applicant and the authority – are relived of the burden of re-examining a newly, perhaps again incomplete, filed request.

Also, with regards to Article 50 (7), we would like to point out that it seems that some regulation or policy setting limits on the costs of copying and printing already exists. If this is indeed the case, we suggest at least a descriptive reference to that regulation. It would also make sense for the controllers to commit themselves to setting the costs of copying and printing within the limits set out in this regulation.

If such a regulation does not exist yet, it would be reasonable to oblige the supervisory authority to adopt it within a certain period after the entry into force of this Draft Law.

Finally, it is also necessary to examine whether the restrictions set out in this Article (for example paragraph 6) also apply to cases where personal data are disclosed in documents (more than 5 pages) under the provisions of the Ukrainian Law "On Access to Public Information". If what is written about such costs should only apply to access to the personaldata under this Act, this should be explicitly emphasized.

3.8 SECTION VIII PROCESSING OF PERSONAL DATA BY THE EMPLOYER

Article 51. General issues relating to the processing of personal data by the employer

This Article defines the general framework applying to the processing of personal data by the employer. It does not raise specific issues in light of Convention 108+ or the GDPR.

Article 52. Processing of personal data by the employer

This Article addresses the more specific conditions of processing and transfer of personal data by the employer in the context of labour relations. We only comment on those provisions that raise issues and/or would need to be amended.

According to Article 52 (2) the employer may collect data on employees, job applicants, civil servants from other persons (sources), i.e. presumably third parties, on the basis of consent of the employee.

Since Article 51 (5) addresses the conditions for obtaining consent of employees, Article 52 (2) should make a reference to it, to ensure consistency and so that consent is obtained in an appropriate manner.

In addition, collection of personal data of employees from third parties may also be based on other legal bases than consent, depending on the purpose of processing of personal data and especially

where consent cannot be an appropriate legal basis because it cannot be lawfully obtained (i.e. when conditions for obtaining consent cannot be met). This would be generally the approach under the GDPR. For example, if the employer requests information on length of service or work experience, and such information is necessary in the process of concluding an employment relationship, its processing can be based on the measures necessary before concluding the employment contract and consent does not need to be obtained.

It is therefore recommended to amend Article 52 (2) to provide that the collection of personal data from other sources can also be based on other legal bases than consent as appropriate.

Article 52 (3) provides that personal data processed for labour relations shall be stored for the period necessary to achieve the legitimate purpose pursued. This Article reiterates in substance the limited retention principle provided otherwise under the Draft Law but does not set out how more specifically this principle is to be complied with in the context of labour relations which may raise difficulties in practice for its application. Such data could for instance be kept for the duration set out by relevant sectoral laws or for the duration necessary to manage disciplinary proceedings or litigation.

For the avoidance of any doubt, it is recommended to add that the requirement to store personal data for the period necessary to achieve the legitimate purpose pursued stands for personal data stored in a form which permits identification of data subjects in line with articles 5 (4) (e) of Convention 108+ and Article 5 (1) (e) of the GDPR. In addition, it is recommended to set out more specifically how long personal data of employees may be kept, for instance by referring to other laws that may provide for specific retention periods and/ or elements allowing to determine such retention period (e.g., statute of limitation for legal proceedings) to facilitate the application of this provision in practice and ensure proper compliance with the limited retention period principle under the cited provisions of Convention 108+ and the GDPR.

Article 52 (6) addresses the right - presumably by the person subject to an internal investigation by the employer and other concerned employees - to have access to the results of such internal investigation. It specifies that such access shall happen "no earlier than the end of the limitation period". We are wondering however what the "limitation period" corresponds to and whether this could be the statute of limitation of legal proceedings. If so, it is difficult to envisage how the possibility of access can be effective if it occurs at the end of such period and the concerned persons

can no more challenge the results.

Article 52 (6) needs to be clarified with respect to the timing in which persons can access the results of the investigation, including the reference to the limitation period, to ensure that such possibility of access is effective and that the persons are able if needed, to legally challenge the results or obtain their review.

Article 52 (8) which refers to the approval of a procedure for the processing of personal data by the employer is not completely clear and we are unsure about what it aims to achieve. If the procedure is the equivalent of an internal regulation, defining the mandatory rules as part of the labour relations including with respect to the processing of personal data of employees, it would be an appropriate mean, amongst others, to provide information to employees on the processing of their personal data in the spirit of Articles 13 and 14 of the GDPR.

Article 52 (9) is about the transfer of personal data collected by the employer for the purpose of labour relations to public authorities.

As is the intention of the GDPR it is recommended that Article 52 (9) states that personal data are transferred to public authorities if the processing is necessary to fulfil the legal obligations of the employer – see Article 6 (1) (c) of the GDPR.

Article 52 (11) appears to relate to requirements on access to public information and more specifical regarding the access to data of officials.

It is recommended to add to this provision the reference to the Ukrainian legal act on access to public information, so that Article 52 (11) is applied in line with the requirements of this act.

Article 53. Processing of personal data of employees by their representatives

This Article does not raise specific comments or need for amendment.

Article 54. Special requirements for the processing of personal data of employees or job applicants by the employer

Article 54 (1) refers to the possibility for the employer to collect health data of employees and job applicants which are also referred in more detail in Article 54 (2).

It is suggested to add a reference in Article 54 (1) to the fact that the processing is allowed

under the conditions set out under Article 54 (2) to establish clearly the conditions under which Article 54 (1) is to be applied.

Article 54 (2) lists the cases in which the employer may collect personal data on health of a job applicant or employee. Although these processing will be authorized by the Draft Law, it is necessary to ensure however that they will in any case be performed lawfully and in compliance with other provisions/requirements of the Draft Law (e.g. appropriate legal basis).

It is advisable to supplement Article 54 (2) with the requirement to carry out the processing cases listed in this provision in compliance with other conditions set out by the Draft Law.

Article 54 (3) refers to processing of genetic data of employees while Article 54 (4) further refers to the conditions for the processing of biometric data of employees. It is difficult to envisage the processing of genetic data in employment relationships and we are wondering whether the drafters had rather intended to refer to biometric data in Article 54 (3) as well.

The scope and consistency of Article 54 (3), notably with respect to Article 54 (4), needs to be reviewed to presumably refer to biometric data uniquely identifying a person instead of genetic data.

Article 55. Transparency of the processing of personal data for the purposes of labour relations

This Article governs the data protection rights of an employee. We only comment on those provisions that raise issues and/or would need to be amended.

Article 55 (1) addresses the employee's right to information (Article 18 of the Draft Law) including through the right of access (Article 19 of the Draft Law) but does not refer to other rights provided by the Draft Law.

It is advisable to refer to all data protection rights of the employee in this Article since emphasizing one or two rights may in practice lead to doubts as to whether the employees enjoy all data protection rights (Article 20 and seq. of the Draft Law) or only those rights, which are specifically mentioned in this Article.

Article 55 (3) relates to the employees' right to receive his/her personal data on his/her assessments and the right to appeal the accuracy of such data to the governance body and courts. The possibility

of an appeal or complaint before the supervisory authority is not mentioned.

For the avoidance of any doubt, Article 55 (3) should be completed with a reference to the employee's right to appeal or submit a complaint to the supervisory authority.

Article 55 (4) sets out a prohibition to make decisions that have a significant impact on the rights and obligations of the employee based on automatic data processing without taking into account the opinion of the employee.

For ensuring that this provision is implemented in compliance with the rules governing more generally automated decision making under the Draft Law (Article 25), it is highly recommended to add to this Article a reference to the provisions relating to automated decision making.

Article 55 (7) stipulates the exercise of the rights of the employee who is the subject of an internal investigation may be delayed until the investigation is completed. This limitation of rights and delay as provided by this Article appears rather broad in light of GDPR requirements requiring a controller to facilitate the exercise of rights by data subjects (Article 12 (2)) and may also raise issues under article 11 of Convention 108+ 11.1 which sets limits and conditions to the restrictions that may be provided to transparency requirements (i.e. the exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society). In addition, when data is indirectly collected on a data subject, which may be the case as part of an internal investigation, information notice on the processing of data shall be provided no later than 1 month to the data subject in accordance with Article 14 (3) (a) of the GDPR. At the same time, an exception is also envisaged under Article 14 (5) (b) which provides for the possibility to delay information, if it may seriously impair the achievement of the objectives of the processing.

Taking into account these elements, Article 55 (7) could be amended to specify that the exercise of the rights, including the right to information, can be withheld where these are likely to seriously impair the investigation (e.g. because of a risk of loss of evidence) but that the rights can be exercised as soon as the risk is eliminated.

3.8 SECTION IX PROCESSING OF PERSONAL DATA BY LAW ENFORCEMENT AGENCIES

Section IX relates to the processing of personal data by law enforcement agencies. As a preliminary remark, it should be recalled that Convention 108+ applies also to the processing of personal data

by competent authorities for law enforcement purposes. On the EU side, the GDPR does not apply to such processing of personal data which is governed instead by the Law Enforcement Directive. Thus, from the EU perspective, our comments under this section addressing processing for law enforcement purposes are made in light of the Law Enforcement Directive and not the GDPR. Please note however that contrary to Convention 108+, nor the GDPR, nor the Law Enforcement Directive apply to the processing of personal data for national security, state secrecy or national defence purposes (i.e., activities generally carried out by intelligence agencies) as such matters are outside the scope of the EU's competence and legislation. Bearing in mind these clarifications, this section raises several general comments as set out below.

Firstly, the provisions of this section which apply to the processing of personal data by law enforcement agencies also mention specifically "intelligence agencies" without defining them, while the definition of "law enforcement agency" under the Draft Law seems to encompass activities generally carried out by intelligence agencies. In this regard, while the title of Article 56 refers to both law enforcement agencies and intelligence agencies, the provisions of Article 56 irregularly refer to law enforcement agencies and intelligence agencies while the title of section IX does not refer to intelligence agencies and Article 57 and its content do not make explicit the specific authorities concerned by these provisions.

Secondly, the scope of activities referred under this section are focused on processing of data for "law enforcement purposes" (see, Article 56 (2), 56 (4), 57 (1)) but also refer sometimes specifically to processing for "intelligence purposes" (Article 56 (3)). Our understanding, taking into account the definition of law enforcement agency under the Draft Law, is that activities for intelligence purposes are included in the category of law enforcement purposes. The fact that the Draft Law addresses these two types of activities is welcomed but it must be underlined that they may be subject to different data protection law requirements under European standards on data protection.

Finally, the section does not define what is to be understood by "intelligence purposes". Processing for such purposes, in light notably of Convention 108+, could be, for national security, state secrecy or national defence activities. The definition of "personal data processing for the law enforcement purposes" under the Draft Law, appears to encompass some of such activities as it refers to "intelligence operations" and "ensuring national security". However, under the Law Enforcement Directive, such activities and more generally intelligence activities are not part of law enforcement purposes as not being regulated by EU legislation as explained above. As such, the applicable data

protection regime including possible exceptions will be different, depending on the purpose of processing (regardless of the type of agency conducting such processing) i.e., when processing data for law enforcement purposes or for intelligence activities although in any event Convention 108+ applies to both activities.

As the processing of personal of data in these fields, be it law enforcement purposes or intelligence activities, is likely to have a significant impact on the privacy and data protection rights of individuals, it is of utmost importance to set out clear and precise rules in this regard notably as to the scope and purposes for which data may be processed.

Taking into account the definitions provided under the Draft Law for "law enforcement agency" and "personal data processing for the law enforcement purposes" there is a need to clarify in this section which provisions apply to which agencies (law enforcement or intelligence) and for which purposes (law enforcement or intelligence purposes) so as to avoid confusion and ensure legal certainty and establish the applicable regime including possible exceptions in consideration of the purpose of the processing activity.

In addition, Article 56 (1) sets out the general requirement for law enforcement and intelligence agencies to abide by the Draft Law taking into account specific rules provided by Article 57 for the exercise of data subject rights in connection with the processing of personal data for law enforcement purposes. At the same time, Article 56 reiterates some of the data protection principles to be followed by law enforcement and intelligence agencies, namely the principles of lawfulness (Article 56 (2)) and purpose limitation (Article 56 (3)) but does not refer to other data protection principles applicable under the Draft Law. It also sets out one specific requirement for law enforcement and intelligence agencies to differentiate information about different categories of personal data subjects and to process it in separate databases (Article 56 (5)). Such drafting of the provisions may give the wrong impression that only those rules that are referred in this section are applicable to law enforcement and intelligence agencies, while the intention resulting from Article 56 (1) is that the whole Draft Law applies to them with certain specificities set out in this section.

For clarity and legal certainty, it should be added to section IX or its Articles that these provisions apply in addition to all of the other provisions of the Draft Law except as otherwise provided (e.g. for the exercise of data subject rights referred in Article 57). For the same reasons, it is also highly recommended to complement this section with additional provisions to take into account certain specificities of the processing of personal data by law

enforcement agencies where the corresponding provisions of the Draft Law may not be fully relevant (e.g. processing of sensitive data (see Article 10 of the Law Enforcement Directive), automated decision making (see Article 11 of the Law Enforcement Directive), distinction between personal data and quality of personal data (see Article 7 of the Law Enforcement Directive), or to impose specific obligations (logging of actions performed (see Article 25 of the Law Enforcement Directive) and restrictions including for intelligence agencies but always taking into account requirements of Article 11 (1) and (3) of Convention 108+.

Article 56. Requirements for processing of personal data by law enforcement and intelligence agencies

Article 56 (1) provides that law enforcement and intelligence agencies shall abide by the Law "*with account*" the provisions of Article 57 which sets out specific rules on the exercise of data subject rights. Similarly, Article 56 (4) mentions that processing of personal data for law enforcement purposes shall be carried out "*with account*" of the principles defined by the Law. *"With account*" may be interpreted as not equalling firm obligations while it must be ensured that the stated rules are duly complied with as any obligation under the Draft Law, by law enforcement and intelligence agencies.

It is recommended to delete from Articles 56 (1) and 56 (4) the references to "taking into account" and "with account" so as to reflect clear obligations for law enforcement and intelligence agencies. Article 56 (4) should also make explicit which principles are to be complied with as it is unclear under the current drafting.

Article 56 (2) provides for the lawfulness principle as required by Convention 108+ and in a consistent way with the corresponding provision of the Law Enforcement Directive (Article 8).

To be fully aligned, at least with respect to law enforcement agencies, it should be specified either in the Draft Law or other legal provisions, the objectives of their processing, the personal data to be processed.

Article 56 (3) provides for the purpose limitation principle as required by Convention 108+. It takes into account broadly the corresponding provisions of the Law Enforcement Directive (Articles, 4 (1) (b) and 4 (2) (a) and (b)) but requires further clarification in this regard.

In addition to stating that personal data cannot be further used unless specifically permitted by law, the provision should however also provide in this case, for the requirement to ensure

that such processing is necessary and proportionate to that further purpose. Taking the possible impact for individuals subject to such data processing, setting such limits are necessary to avoid any unwarranted use of their personal data and to ensure compliance with the purpose limitation principle. In addition, the provision should explicitly mention that personal data is not processed in a manner which is incompatible with the initial purpose. These amendments would bring in line the provision with Articles, 4 (1) (b) and 4 (2) (a) of the Law Enforcement Directive. Also, the drafters of the Draft Law may wish to consider including in the Draft Law purposes of use that would be compatible.

Article 56 (5) provides for the requirement for law enforcement and intelligence agencies to differentiate information about different categories of personal data subjects and to process it in separate databases, similarly to what is provided by Article 6 of the Law Enforcement Directive.

Regarding the last indent of this Article, it is advisable to clarify who are "other participants of criminal proceedings", in line with Article 6 (d) of the Law Enforcement Directive (i.e. persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of suspected or convicted persons).

Article 57. Specifics of exercise of rights of personal data subjects in connection with processing of personal data for law enforcement purposes

This Article governs the limitations that may be imposed to the data protection rights of individuals when processing their personal data for law enforcement purposes and the conditions for imposing such limitations.

More specifically, Article 57 (1) provides for the existence of this limitation regarding the rights referred in Articles 18 (right to information), 19 (right of access) and 21 to 24 (right to be forgotten, to object, to portability, to restriction) and lists the objectives for which the rights may be limited in accordance with the law.

However, Article 57 (1) does not refer to the right to rectification (Article 20 of the Draft Law) which needs to be added, unless no limitations are envisaged for this right. In addition, the right to portability (Article 23 of the Draft Law) does not appear relevant in the context of processing for law enforcement purposes and reference to the corresponding Article should be deleted for the avoidance of any doubt. Regarding the conditions under which the rights may be limited, the general reference to the fact that it will be done in the manner

provided for by the law does not appear sufficient and needs to be complemented with the requirements set out in this respect by Article 11 (1) of Convention 108+ which requires more specifically that the limitation must also respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society.

Article 57 (2) further sets out in a general manner how the decisions to limit the exercise of the rights shall be taken on a case-by-case basis. It provides for a balance to be made between the necessity to achieve the goal of the law enforcement activity and the necessity to ensure the rights of the data subject which appears generally in line with the requirements in this regard under article 11 (1) of Convention 108+ and the Law Enforcement Directive.

There is a need however to make a link between, this provision and Article 56 (1), by making a reference to it as, the latter sets out the overarching and indispensable conditions, including admissible purpose for limitation, to be complied with by the competent authorities for imposing restrictions to the rights of individuals. In addition, it should be specified further either in the Draft Law or other legal provisions how the limitations may be imposed for each specific right since they will not necessarily be imposed and applied in the same manner (e.g. right of access not limited in the same manner as right to information). In the absence of such clarifications, it is unsure whether the limitations could still be considered as meeting the requirements of article 11(1) of Convention 108+, in particular as to the condition that the restriction is "provided by law".

Articles 57 (3) and 57 (4) do not raise specific comments.

As a final remark for this section, we would like to note that the following documents adopted by the Council of Europe can be a helpful guidance when considering the above recommendations and their implementation:

- Recommendation (87) 15 regulating the use of personal data in the police sector of 17 September 1987;
- Practical guide on the use of personal data in the police sector, 15 February 2018.

3.9 SECTION X LIABILITY FOR VIOLATION OF LEGISLATION ON PERSONAL DATA PROTECTION

This section sets out the general conditions and the rules for the imposition of fines in case of violation of the Draft Law.

Article 58. Liability for violation of legislation on personal data protection

Article 58 (1) in addition to referring to liability to be triggered on the basis of the Law also refers in a general manner to "other laws of Ukraine".

For legal certainty for controllers and data processors, the provision should clarify the other applicable Ukrainian laws which may be the basis for triggering liability in case of violations in the field of personal data protection and especially whether these other laws may also sanction violations of the Draft Law.

Article 58 (2) refers in general terms to "*measures*" that may be applied by the supervisory authority in case of violations in the area of personal data protection but does not specify the nature or content of these measures and whether there may be other measures than fines as specified by this section. The Explanatory Note to the Draft Law, as well as the Draft Law of Ukraine "On National Commission in the Field of Data Protection and Access to Public Information" № 6177 as 18.10.2021[9] (Draft Law on National Commission) seem to suggest that there may indeed be other measures such as administrative sanctions but without full certainty. In certain cases, measures other than fines (e.g., ban of a processing) are necessary to ensure for effective, proportionate and dissuasive sanctions as expected under Convention 108+ (see § 100 of the Explanatory report, Article 12 of Convention 108+) as well as the GDPR (see Article 83 (1)).

The measures that may be imposed by the supervisory authority in case of violations of the Draft Law need to be set out in more detail, especially to clarify whether there may be other types of sanctions than fines (e.g., warning, order to stop the processing etc. as provided by Article 58 (2) of the GDPR) for legal clarity and also for setting out an effective and appropriate sanctions and remedies framework in line with Convention 108+ and the GDPR.

Article 58 (4) refers to rights and remedies available to the data subject regardless of the liability that may be imposed on a party in accordance with the Draft Law.

For the avoidance of any doubt, the Article should also refer to the right for the data subject to lodge a complaint with the supervisory authority in such a case.

[9] Draft Law of Ukraine "On the National Commission in the Field of Data Protection and Access to Public Information" № 6177 as of 18.10.2021 available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992

Article 59. Liability of controllers and processors for violations of legislation on personal data protection

Article 59 provides for amounts and thresholds for the fines that may be imposed by the supervisory authority in case of a violation of the Draft Law. More particularly, it follows in this regard a similar approach as under the GDPR (Article 83) by setting different thresholds of fines (expressed in fixed amounts or percentages of annual turnover including maximum limits for total amounts) depending on the provisions infringed and whether the violation has been committed by a natural person or legal entity. It also takes into account whether the infringement has led to a violation of rights of a data subject or the repeated nature of the violation. As such, the provision appears to overall set an effective, proportionate and dissuasive framework for imposing fines in line with Convention 108+ (see § 100 of the Explanatory report, Article 12 of Convention 108+) as well as the GDPR (see Article 83 (1)) provisions in this regard. Some specific provisions nevertheless raise questions as set out below and would require amendments.

Articles 59 (1) and 59 (2) which set the lower threshold of fines, provide for different thresholds depending on whether the infringement has led or not to a violation of rights of a data subject. Such distinction referring to the existence or not of a violation of rights of data subjects is not made for Article 59 (3) which provides for the higher threshold of fines. In any event, nor Convention 108+ nor the GDPR make specifically such distinction and it can be questioned whether setting different thresholds depending on whether there has been or not a violation of rights is necessarily relevant for setting different thresholds and imposing fines. Even though the imposition of a sanction needs to take due account among other factors of the existence of a concrete violation of data subject rights, an infringement of data protection legislation will in most of the cases also lead to some extent to a violation of data protection or privacy rights of data subjects without always being qualified as a "right" in the meaning of Articles 19 to 24 of the Draft Law (e.g., it could be an intrusion to privacy, the impossibility to withdraw consent, or only a material damage, etc.).

Unless the drafters of the law intend to achieve a specific purpose, it would be recommended to remove the distinction of thresholds depending on whether there has been or not a violation of rights of data subjects as provided in Article 59 (1) and 59 (2), and thus to only keep Article 59 (2), at least for consistency with Article 59 (3). Instead, to enhance the provisions, it is suggested to complement Article 59 with additional provisions setting out that fines shall be imposed taking into account the circumstances of each individual case and to specify the factors to be taken into account by the supervisory authority in this regard, similarly to what is set out under Article 83 (2) of the GDPR. To that end, it is advisable to

at least move into the Article the circumstances that are listed in the Explanatory Note to the Draft law regarding the imposition of fines (i.e. "*nature, severity and duration of the violation and its consequences, the actions taken to meet the requirements of the Draft Law as well as any actions to prevent the negative effect arising out of the violation or to reduce their impact*").

Article 59 (4) which refers to rules for imposing fines for violations of "*other provisions*" of the Draft Law than those listed under Articles 59 (1) to 59 (3) is unclear as to its scope.

It is recommended to clarify more specifically what other provisions can be concerned under this Article 59 (4) as the relevance of this provision appears otherwise unclear.

Article 60. Limitation periods for application of liability under this Law

This Article provides for a statute of limitations of 3 years for the liability that may be imposed for violations of the Draft Law. In other words, a data controller or data processor's liability will not be triggered if a period of 3 years has elapsed after the discovery or commitment of violation under the Draft Law. Nor Convention 108+, nor the GDPR address the topic of statute of limitations for the imposition of fines or other types of sanctions in case of violation of data protection legislation. At the same time, a statute of limitations of 3 years, which is a relatively short period, could significantly weaken the effectiveness of the Draft Law and more specifically the dissuasive nature of the framework for triggering the liability of data controllers or data processors provided by Article 59. Data controllers or processors could precisely try to find ways to dissimulate their violations as knowing that they can avoid liability after a period of 3 years. In addition, Guidelines 04/2022 on the calculation of administrative fines under the GDPR adopted by the European Data Protection Board on 12 May 2022 provide that infringements committed a long time ago might still be of interest when assessing the "track record" of a controller or processor as part of a sanction procedure, and that as such fixed limitation periods are not to be set (while recognizing that certain EU national laws currently provide for such limitation periods). It thus appears that limitation periods may to some extent prevent a supervisory authority to act in an efficient manner when assessing the infringements committed by a controller or processor.

For these reasons, it is recommended either to delete this Article 60 or at least to considerably extend the limitation period beyond 3 years, so that the supervisory authority is able to effectively intervene and take account of relevant infringements by a controller or processor within an appropriate duration of time as part of sanctions procedures.

3.10 SECTION XI. FINAL AND TRANSITIONAL PROVISIONS

This section sets out the provisions relating to formal aspects of the Draft Law (i.e., the taking of effect of the Law, rules for the transitional period) and also provides for a set of amendments to other acts of legislation of Ukraine in specific areas or sectors (Labour Code, Burial and Funeral Business, E-commerce, Health care electronic system, Electronic Communications). These amendments to other acts either aim to introduce a mere requirement to comply with the Draft Law where relevant or provide for certain specific obligations in the referred acts of legislation. In this regard, the formal aspects (points 1 to 4 of this section) and the introduction of the requirement to comply with the Draft Law into specific Ukrainian legislative acts (point 5.1 to 5.4 of this section) do not raise specific comments or specific views. With respect to the provisions introducing particular obligations in certain areas or sectors as referenced in this section (point 5), as Convention 108+[10] and the GDPR do not set out specific rules for the processing of personal data in such areas or sectors, we only provide comments if relevant and from a general standpoint on the basis of these texts. However, concerning electronic communications and issues relating to privacy and confidentiality when processing of personal data in this context, our comments are made in light the E-Privacy Directive. Please finally note that our comments are provided as far as possible on the basis of only the excerpts of law set out in this section without knowledge or access to the full acts of legislation at stake.

Point 5.5 of the Transitional provisions refers to Article 11 of the Law of Ukraine "On the State Financial Guarantees of Public Health Care" (Bulletin of Verkhovna Rada of Ukraine 2018, No.5, p.31) – Article 11. Health care electronic system

This Article seems to relate to the operation of an electronic health care system. More specifically, para 5.2. of the Transitional provisions provides that Article 11 of the mentioned Law provides that access to patient data contained in the health care electronic system shall be granted to a doctor with whom the patient has signed declaration or other medical personnel bound by obligations in accordance with Article 40 of the Law of Ukraine "Fundamentals of the Health Care Legislation of Ukraine".

We would assume, in this respect, that the other medical personnel is bound by medical secrecy or other confidentiality obligations as provided by the referenced Ukrainian law but for the avoidance of any doubt this should be explicitly stated in this Article to ensure that appropriate safeguards are indeed in place for the access to patient data which qualify as

[10] Nevertheless, the Council of Europe has adopted Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 February 1995, which to a certain extent still appears relevant. Our opinion is thus also enlightened by the provisions of this Recommendation.

special category data under Article 6 (1) of Convention 108+ and Article 9 (1) of the GDPR. It could further be foreseen whether additional appropriate safeguards should be specified in the law, in line with Article 6 (1) and 6 (2) of Convention 108+, to address any possible risks to the processing of patient data, including for instance in terms of security (e.g. by setting out in the Draft Law security requirements for the operation and access to the electronic healthcare system and patient data).

Article 11 (4) provides that an authorized body shall publish "*data accumulated in the health care electronic system on the official website*" under conditions to be defined by the Cabinet of Ministers of Ukraine and subject to the supervisory authority's approval. It is also stated that data – presumably the same set as referred in the previous sentence – shall be fully depersonalized before publication in accordance with the Law of Ukraine "On Personal Data Protection".

This Article does not raise specific comments and recommendations.

Point 5.6) On the Law of Ukraine "On Electronic Communications" (Official Bulletin of Ukraine, official edition 2021, No. 6, p.10, Article 306, act code 102665/2021)

As a preliminary and general comment, we note that the Articles set out under this point use certain key concepts such as "traffic data", "location data", "additional service", "user", "end user", "consumer" but without providing definitions for them which may raise questions on their applicability.

For clarity and legal certainty, it is highly recommended to include definitions for the concepts referred above to ensure the appropriate application of the provisions set out under this point taking into account corresponding definitions set out for these terms under the E-Privacy Directive and also the Council of Europe Convention on Cybercrime including its amending protocols (so called "Budapest Convention").

In addition, from a general perspective, it is not explicit who may sanction or otherwise trigger liability of concerned organizations for violations of the provisions set out under this point. Under Article 15a of the E-Privacy Directive, enforcement and other forms of liability of such provisions is required with effective, proportionate and dissuasive sanctioning framework. Such enforcement could be carried out by the supervisory authority.

It is necessary to complement the provisions relating to the Law on "Electronic Communications" to specify how the provisions set out below will enforced, taking into account requirements of Article 15a of the E-Privacy Directive.

Article 31. Security of electronic communications

Article 31 (1) complies with the requirement set out by Article 4 (1) of the E-Privacy Directive.

Article 31 (2) which relates to the risks to be assessed for implementing appropriate security measures provides for a definition of such risks and mentions in this regard that they shall be understood as any actions including amongst others "*services or goods*".

Unless there may be a translation error, this reference to "services and goods" should be deleted as it does not appear to make sense in this context. In addition, to ensure an effective and complete protection for the privacy of the individuals, the provision should be more explicit as to the list of risks by specifying that it may be a risk for the content of a communication/correspondence but also any related data to such communication/correspondence (i.e., traffic data).

Article 31 (3) lists the general rules to ensure security of communications, in the same manner as Article 4 of the E-Privacy Directive as amended in 2009. Nevertheless, Article 31 (3) (2) which provides for the obligation to prevent specific threats against personal data which correspond to the scope of definition of a personal data breach, does not reflect that these threats/acts may be unlawful or accidental as provided by Article 4 of the E-Privacy Directive as well as in line with the definition of a personal data breach under the GDPR and the Draft Law itself.

For consistency with the Draft Law's definition of personal data breach in line with the E-Privacy Directive, as well as to ensure that the full scope of risks to be prevented against personal data are covered, Article 31 (3) (2) would need to refer to the accidental or unlawful nature of security threats/acts upon personal data.

Article 31 (3) (3) which provides for the implementation of organization and other security measures is unclear as to the "*approval*" mentioned for such measures (by whom? how?) as well as with respect to the reference to "*legislation on protection of information and personal data*".

It is recommended to clarify this provision on what is meant or expected for the approval of

the security measures and to refer to the name of the Draft Law instead of "legislation on protection of information and personal data" for the avoidance of any doubt.

Article 31[1]. Notification to consumers and end users about the risk for security of the electronic communication networks and/or services

We understand that this provision relates to obligations of electronic communication networks and/or services providers to notify consumers and users of electronic communication services about the occurrence of a risk of security affecting such services. As the obligation refers to risks for security, it thus seems to be distinct from the personal data breach notification obligations as provided by Articles 37 and 38 of the Draft Law.

As the risk of security of electronic communication networks and /or services, as defined under Article 31 (2), can in practice also lead to a personal data breach in the meaning of the Draft Law, it should be clarified in the text that the notification obligations provided under Article 31[1] are without prejudice and thus apply in addition to personal data breach notification obligations under Articles 37 and 38 of the Draft Law, to ensure legal certainty for providers of electronic communications networks and services. In addition, in order to ensure appropriate information of consumers and users, including to enable them to assess any privacy and data protection risks, the provision should also specify the content of the notification to be made to the individuals, in particular the nature of the risk and possible consequences for the individuals.

Article 31[2]: Secrecy of private communications

This Article provides for the obligations aiming at ensuring the secrecy of private communications as well as possible limits, in the same spirit as Article 5 of the E-Privacy Directive.

As a preliminary point for this Article, we note that Article 5 of the E-Privacy Directive which sets out the principle of confidentiality of communications, does not make a distinction between "private" and other communications and provides for a requirement of confidentiality for any type of communication. The same goes as well for the definition of "communication" under Article 2 (d) of the E-Privacy Directive.

To the extent that the concept of "private communications" may introduce confusion as to

the type of communications that are protected or not in accordance with Article 31[2], it is advised to replace it with "communications" only, in line with the E-Privacy Directive.

Article 31[2] (1) sets the general requirement to ensure the secrecy of private communications. While the Article is focused on "private communications", it also refers to correspondence, telephone conversations, telegraph or other correspondence but does not make apparent whether these communications are also to be included in the category of "private communications".

The Article should be further clarified to determine whether "correspondence, telephone conversations, telegraph or other correspondence" is also to be included in the category of private communications and thus benefit from the same protections. In addition, it should add to the elements covered by secrecy of private communications, the identity of the sender/recipient, the title of the communication and any attachment if relevant, as the secrecy for the individuals cannot be ensured if these elements are not covered by its benefit.

Article 31[2] (2) which states the obligation for electronic communication networks and/or services and other persons involved in the operation of the electronic communication to protect the secrecy of private communications even after termination of their operation does not raise specific comments as it would meet the general requirement for ensuring confidentiality of communications as set out by Article 5 of the E-Privacy Directive.

Article 31[2] (3) relates to the possibility for electronic communication networks and/or services providers to obtain, use and transfer information on private communication to other persons to the extent necessary to provide the electronic communication services. The Article is drafted in a wide manner and raises the risk of unwarranted use and transfer of such private communications in contradiction with the requirement of confidentiality of communications under Article 5 of the E-Privacy Directive.

Taking into account Article 5 (1) of the E-Privacy Directive, the Article needs first to specify the operations which may be considered as necessary to provide the electronic communication services and, secondly to state that other persons to which private communications may be provided must be subject to strict confidentiality obligations and ensure the confidentiality of such communications.

Article 31[2] (4) provides for the prohibition to interfere with private communications and sets out rules allowing in certain cases for exceptions to this prohibition following overall the same

approach as under the E-Privacy Directive (Article 5 (1) and recital 22). At the same time, the types of interferences listed in this Article (monitoring, recording, storage, and transfer of information) could be further expanded to ensure a comprehensive and effective protection of private communications.

To that end, the Article should be completed by adding a reference to "tapping" and "any other type of interception" in line with Article 5 (1) of the E-Privacy Directive.

In addition, this provision sets out in a general manner that interferences may be permitted when necessary to provide electronic communication services but without specifying what type of activities this may more specifically authorise. According to Article 15 (1) of the E-Privacy Directive and its recital 22, only limited technical operations (technical storage which is necessary for the conveyance of a communication and for the duration necessary thereof) appear admissible and in any event subject to ensuring confidentiality of communications.

To restrict interferences, necessary to provide electronic communication services, in line with Article 15 (1) of the E-Privacy Directive, the provision should further specify what the necessary operations may be and recall that even in such cases the secrecy needs to be guaranteed.

Further, the provision provides in a broad manner, that interferences may be permitted by law without further specifying the objectives for which this may happen and more generally the conditions or particular rules applying in such a case. However, according to Article 5 (1) of the E-Privacy Directive, confidentiality of communications may be derogated only under strict and specific conditions as further specified by Article 15 (1) of the same Directive. According to this latter provision, the restriction must constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system – all of which needs to be specified under national law. It is to be noted that this also mirrors the approach and conditions under Convention 108+ (Article 11) and GDPR (Article 23) when restrictions are applied to certain data protection provisions or rights and the latter provisions should also be taken into in our view when dealing with interference to the secrecy of private communication which as they involve personal data. Concretely, to be aligned with European standards including more generally article 8 (2) of the European Convention on Human Rights setting out conditions in case of interferences into private

life notably in the field of communication [11], the national law must in particular set out the purposes for which the interference may occur in line with the limited objectives provided by Articles 15 (1) of the E-Privacy Directive and 23 of the GDPR (e.g. investigation, detection and prosecution of criminal offenses), by whom it may be performed (i.e. relevant controllers/competent authorities), the form it will take (including any prior judicial or administrative authorization) which data may be collected or accessed, their retention period as well as the safeguards (e.g. supervision) and rights for the individuals.

Article 31[2] (4) thus needs to be further completed to detail more specifically the applicable framework of interferences to the secrecy of private communications by competent authorities taking into account applicable requirements of the E-Privacy Directive (Article 15 (1)), GDPR (Article 23), Convention 108+ (Article 11) and Article 8 (2) of the European Convention for Human Rights (as referred above). More specifically, there is a need to specify the purposes for which interferences may be carried out, in which form, by whom, which data will be accessed or preserved and for how long and the safeguards and rights of individuals in this context. Principle 2.5 of Recommendation No. R (95) 4 can also serve as a useful guidance in this regard.

The purpose of Article 31[2] (5) is uncertain, and its meaning may have been lost with the translation. We understand to some extent that it provides for an obligation for the electronic communication network or services provider to notify the consumer or user when entering into the service contract or prior to it of the fact that the provider obtains information about private communications, records or stores them however it is unclear why such actions may be carried out by the provider (other than for providing the service). In addition, it sets out that the information about private communication must be removed as soon as technically feasible and where the information is no longer necessary to provide the service. Presumably, this provision might relate to some extent to the processing of traffic data which is further regulated by Article 119[1] or the processing of location data under Article 119[2.]

It is unclear what specific scenario or obligations this provision aims to cover and its scope and possible link with Articles 119[1] and 119[2] addressed further should be clarified. We are unable to comment on it further.

[11] On this topic, the drafters are also invited to consider relevant case law from the European Court of Human Rights under article 8 in the field of interception of means of communications (see, to that end ECHR Personal Data Protection Factsheet, March 2023 edition).

Article 31^2 (6) allows the recording of private communications and related data when carrying out entrepreneurial activities for the purpose of providing proof of effected payment for the and the conditions under which this can be done. The provision follows in substance Article 5 (2) of the E-Privacy Directive but needs to be specified to be fully aligned with the latter.

This Article should be completed by specifying that the recorded communication needs to be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged in line with Article 5 (2) and recital 23 of the E-Privacy Directive.

Article 31^2 (7) refers to a notification about the recording of communication, but it is unclear to which recording of communication this refers to.

If Article 31^2 (7) aims to specify a notification obligation about the recording of communications provided under Article 31^2 (6), then this should be explicitly mentioned in the provision so as to have a clear link between the two Articles. Otherwise, the content of Article 31^2 (7) would need to be further clarified on its scope.

Article 31^2 (8) provides for the possibility for authorized representatives of the electronic communication network provider to process personal data of consumers or users provided that they are bound by a non-disclosure obligation with respect to confidential information that became known to them in connection with their professional activity. The exact objective of this provision is unclear. Indeed, it can reasonably be assumed that the employees of the electronic communication network provider would in any case need to process certain personal data of consumers or users, e.g. for providing the service or for billing purposes, and this does not specifically need to be regulated by the law as the general provisions of the Draft Law would in any case apply to such processing of personal data unless, the provision aims to address a particular scenario or obligation. In this regard, it can be wondered why there is a specific reference to confidential information of consumers and users together with the requirement for the authorized representative to be bound by non-disclosure obligation. Presumably, this provision might relate to some extent to the processing of traffic data which is further regulated by Article 119^1 or the processing of location data under Article $119^{2.}$

Article 31^2 (8) would need to be reviewed to clarify its scope and possible link with Articles 119^1 and 119^2 addressed further.

Article 31^3. Procedure for provision of information upon request on provision of access to personal data of consumer and/or end user of the electronic communication services and storage of information about such requests

This Article seems to regulate the provision by electronic communications networks and service providers of personal data and private communications of consumers or users upon requests from competent authorities. The scope of such requests and the authorities is however uncertain and cannot be fully assessed as Article 31^3 (1) refers in this regard to an Article of the Draft Law or separate legislation which are not included in the text submitted for the review.

To the extent that the provision to competent authorities of private communications of consumers or users but also of personal data, upon request, as referred under Article 31^3 (2) would amount to an interference, our comments would be the same as those set out on the same topic for Article 31^2 (4) (please see above). Incidentally, it should also be clarified how the two provisions, i.e. Article 31^3 (2) and Article 31^2 (4) are to be articulated since they relate in the end to the same matter. Article 31^3 (2) could for instance refer to Article 31^2 (4) for detailing the conditions under which access to private communications or consumers and users' personal data could be granted.

Article 31^3 (3) is about the records to be kept by electronic communication networks and/or services providers about requests they receive from competent authorities and reflects Article 15 (1) (b) of the E-Privacy Directive in this regard.

Article 117. Number catalogues (phone directories)

This Article sets out the rules for the inclusion of personal data of consumers and end users into phone directories and the rights of consumers and users in this regard. This results mainly from Articles 117 (1) and 117 (2), the content of which is very similar to the one of Article 12 of the E-Privacy Directive addressing the same issue and do not raise comments. Article 117 (3) which provides for the right of consumers and end users to prohibit the use of their personal data for calls with commercial and research purposes reflects principle 7.8 of Recommendation No. R (95) 4 and does not require amendments.

Article 117 (4) sets out notably that information about verification, rectification or erasure of personal data as referred in Article 117 (2) (which grants consumers and users such rights) shall not be included into the phone directory. However, this provision is not clear and may even be

contradicting to some extent Article 117 (2) if understood as prohibiting the inclusion of rectifications, erasures of personal data requested by consumers and end users. We would assume that this is not the purpose of this Article.

The prohibition set out by Article 117 (4) would need to be made clearer in particular to avoid any contradiction with the data protection rights guaranteed to consumers and users under Article 117 (2).

Article 119. Protection of information about the consumer, the end user and the provided electronic communication services

The Article provides a limited list of purposes for which electronic networks and/or services providers may collect and store necessary personal data of consumers or end users (Article 119 (1). It also sets out that information to be provided about the electronic communication services received by end users "may" be provided in the manner defined by the "this Law in compliance with the requirements of the Law of Ukraine "On Personal Data Protection"". The use of the term "may" could imply that the provision of information in such a manner is only an option while any information of end users on the processing of their personal data as part of electronic communication services needs to be provided in accordance with the Ukrainian data protection legislation, i.e., the Draft Law.

It is recommended to replace the term "may" with a clear obligation to provide end users with information on the processing of their personal data in accordance with the Draft Law. In addition, as the purposes of processing set out by this Article are closely linked to the topics addressed in subsequent Articles (119[1], 119[2], 119[3], 119[4], 119[5]) notably on the processing of traffic data, or on location data of end users, it is suggested to include in Article 119 a reference to the fact that the processing must be carried out under the conditions described in these subsequent Articles.

Article 119[1]. Traffic data

This Article sets out the conditions for the processing of traffic data of consumers or end users by the electronic communication network or services provider which shall be, as a rule, deleted or depersonalized as soon as they are no longer necessary for the purpose of provision of the electronic communications services unless an exception provided by this Article applies. The

Article mirrors for the most part the same conditions as under Article 6 of the E-Privacy Directive but raises comments and recommendations set out below.

Among exceptions to the further storage of traffic data, Article 119[1] (1) (1) provides for the possibility to do it in accordance with the law, referred in a broad manner and without further conditions. We would assume that such possibility aims to cover the retention of certain traffic data for the purpose of communication to competent authorities for criminal investigation, judicial procedure, or public security purposes for instance. Similarly, as for interferences to the secrecy of private communications, traffic data may be accessed and retained as an exception in line with Article 6 of the E-Privacy Directive, only under strict and specific conditions specified by Article 15 (1) of this Directive[12]. Our comments and recommendations will thus be the same in this case as well. In a nutshell, as explained above the restriction must constitute a necessary, appropriate and proportionate measure within a democratic society for specified and limited objectives, respect the essence of fundamental rights and freedoms and must be set out under national law. This corresponds also to the requirements under Convention 108+ (Article 11) and GDPR (Article 23).

Article 119[1] must be complemented to detail more specifically the applicable framework of access of traffic data by competent authorities taking into account applicable requirements of the E-Privacy Directive, GDPR and Convention 108+ set out above. To comply with Article 15 (1) (b) of the E-Privacy Directive, the Article needs to provide for the requirement for the service providers to establish internal procedures for responding to requests for access to users' personal data and the obligation to provide the competent authorities, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Another exception set out by Article 119[1] (1) (4) relates to the storage of traffic data for calculation of payment for the electronic communication services which is further regulated by Article 119[1] (3).

For the avoidance of any doubt as to the conditions applying in such a case, it is suggested to

[12] Please note however, that this provision of the E-Privacy Directive refers to another EU Directive on the retention of traffic data (2006/24/EC) of 15 March 2006 on the retention of data generated or processed in connection with the provision of services by electronic communications services or networks providers but which was declared invalid by the CJEU in 2014 (Case C-293/12 et C-594/12, Digital Rights Ireland, 8 April 2014) and is no more applicable. The applicable rules on the matter to be taken into account thus result from CJEU case law, including the cited Digital Rights Ireland Case, but also Case C-203/15 Tele 2 Sverige/Watson 21 December 2016, Case C-511/18, La Quadrature du Net, 6 October 2020.

mention in Article 119[1] (1) (4) that such use will be carried out under the conditions set out under 119[1] (3).

Article 119[1] (1) (5) refers to the provision of marketing or other additional electronic communication services which is further regulated by Article 119[1] (2).
For the avoidance of any doubt as to the conditions applying in such a case, it is suggested to mention in Article 119[1] (1) (5) that such use will be carried out under the conditions set out under 119[1] (2).

Article 119[1].2 provides for the specific conditions to be complied with for using traffic data for the purpose of providing marketing or additional services, subject to the consent of the consumer, mirroring in substance the requirements provided by Article 6 (3) of the E-Privacy Directive.

The provision should also make clear that consent in such a case is to be understood and obtained under the same requirements as set out by the Draft Law to ensure that it is obtained in a manner that complies with the applicable data protection requirements. Also, the Article should explicitly mention the consumers or end user's right to withdraw consent in line with Article 6 of the E-Privacy Directive.

Article 119[1] (3) provides for the specific conditions to be complied with for using traffic data notably for the calculation of payment for the services, for the purpose of providing marketing or additional services, subject to the consent of the consumer, mirroring in substance the requirements provided by Article 6 (2) of the E-Privacy Directive.

To further circumscribe such uses in line with Article 6 (2) of the E-Privacy Directive and ensure compliance with the principles of purpose limitation, data minimization and limited retention provided by Convention 108+ (Article 5 (4)) and the GDPR (Articles 5 (1) (a) to (c)), the Article should be completed by specifying that the processing for calculating and managing the payment is permissible only up to the end of the period during which the bill may lawfully challenged or payment pursued. As we also note that these provisions do not address the issue of itemized billing while provisions in this regard would be expected under Article 7 of the E-Privacy Directive, it is recommended to add rules regulating this topic in line with the E-Privacy Directive.

Article 119[1] (4) requires that the processing of traffic data be only done by authorized representatives of the electronic communication networks and/or services and for specified purposes. This provision reflects the one of Article 6 (5) of the E-Privacy Directive and does not raise comments.

Article 119[2]. Data on location of consumer and/or end user

This Article sets out the conditions for the processing of location data of consumers or end users by the electronic communication network or services provider. It reflects in most part the same conditions as under Article 9 of the E-Privacy Directive subject to following comments and recommendations detailed below.

Article 119[2] (1) provides that in addition and to the extent necessary for providing "*additional services*" to the consumer or end user, the location data can be processed on the basis of the law, or where such data is depersonalised, and the consumer or end user has granted consent. The provision nevertheless raises several issues.

Except for the case when the processing is in accordance with the law (see our comments below), the provision seems to set cumulative conditions for the provision of additional services to consumers and to end users requiring that personal data be depersonalized, and that consent of these individuals is also obtained. It can be noted that such cumulative conditions are not required under Article 6 (1) of the E-Privacy Directive since either consent of the individual is obtained for providing the value-added service or location data is made anonymous before being further used. Also, it appears difficult to envisage how the additional services could be provided if location data is depersonalized – assuming that it has the same meaning as made anonymous.

It is recommended to review the drafting of this provision in line with Article 6 (1) of the E-Privacy Directive, so as to provide that either consent is required for the processing of location data for the provision of additional services or, location data is anonymized.

Regarding the reference under this provision to the processing of location data in accordance with

the law, we would assume that this aims to cover the situations of retention of location data for the purpose of communication to competent authorities for criminal investigation, judicial procedure, or public security purposes for instance. Similarly, as for other exceptions of processing permitted by the law as examined above (secrecy of private communications, retention of traffic data), this exception can only apply for determined objectives and needs to be further specified by the law in accordance with Article 15 (1) of this Directive. As such our comments and recommendations are the same as stated above for secrecy of private communications and retention of traffic data.

The Article must be complemented to detail more specifically the applicable framework of access to location data by competent authorities taking into account applicable requirements of the E-Privacy Directive, GDPR and Convention 108+ set out above. More specifically, there is a need to specify the purposes for which such data can be collected, accessed and preserved, in which form, by whom and for how long as well as the appropriate safeguards and rights of individuals in this context. In addition, to comply with Article 15 (1) (b) of the E-Privacy Directive, the Article needs to provide for the requirement for the service providers to establish internal procedures for responding to requests for access to users' personal data and the obligation to provide the competent authorities, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Article 119^2 (2) sets out the information notice requirements to the consumer or end user prior to obtaining his/her consent (as referred in the Article 119^2 (1)) to the processing of his/her personal data. The provision thus sets out a requirement very similar to Article 9 (1) of the E-Privacy Directive. It is unclear however why the provision refers to consent for the processing of "personal data" while Article 119^2 (1) address consent for the processing of "location data". Similarly, the information notice elements to be provided do not refer to location data but to personal data while Article 119^2 in line with Article 6 of the E-Privacy Directive is focused on location data.

It appears necessary to review and complete the wording of Article 119^2 (2) by replacing "personal data" with "location data" including when referring to the possibility to withdraw consent and the type of data processed. Furthermore, it is suggested to make a link with Article 119^2 (1), since Article 119^2 (2) further specifies the requirement set out in Article 119^2 (1). The provision should also state that consent in such a case is to be understood and

obtained under the same requirements as set out by the Draft Law to ensure that it is obtained in a manner that complies with the applicable data protection requirements.

Article 119[2] (3) is about the consumers' and end users' right to withdraw consent with respect to each connection or each instance of data transfer. It reflects the requirement set out by Article 9 (2) of the E-Privacy Directive and does not raise comments.

Article 119[2] (4) provides that the processing of location data under this Article may be done by persons authorized by the electronic communication networks and/or services provider for the specified purposes set out in the Article. While the Article is drafted in the same spirit as Article 9 (3) of the E-Privacy Directive, it nevertheless seems to set, with the use of the term 'may", a more flexible possibility of processing by authorized persons than under the E-Privacy Directive which refers to "restricted" persons. In addition, the purposes for which the processing of location data under this Article is allowed (issuing of invoices, managing traffic, answering consumer and/or end user requests, establishing cases of fraud, providing marketing services or other additional services) do not match with the purpose set out under Article 9 (3) of the E-Privacy Directive (providing value added services).

The Article should set out more restrictively that the processing of location data is only allowed by authorized persons for specified purposes. In addition, to be aligned with Article 9 (3) of the E-Privacy Directive, the purposes for which location data may be processed in this context need to be amended by referring only to additional services or value added services as under Article 9 (3) of the E-Privacy Directive.

Article 119[3]. Provision of data on location of the consumer and/or end user

Article 119[3] (1) aims to address the situations where the electronic communication networks and/or service providers may be required to communicate the location of an end user to authorised bodies or other persons as defined by applicable Ukrainian law relating to the "System of Emergency Assistance to the Population under Single Phone Number 112" in order to protect the vital interests of concerned persons as specified in this provision.. According to an unofficial English translation of the said law, we understand that such authorized bodies cover a range of emergency response services (including for instance the police, medical emergency assistance services, civil protection

service, emergency gas service, fire and rescue units). The possibility to provide the location of individuals in circumstances as provided in this Article is also set out by Article 10 (b) of the E-Privacy Directive and, Article 119[3] (1) would as such be consistent with it.

Article 119[3] (2) states the obligation for the electronic communication networks and/or service providers to act quickly in response to "substantiated requests" without making explicit however from whom these requests may originate and what their form must be in particular to be considered as substantiated. In addition, the same provision provides that the electronic communication networks and/or services provider is liable to comply with "the law" – without mentioning which law is referred to in this case - during provision of the data.

The provision needs to be clarified regarding the substantiated requests that are referred so as to specify from whom they may originate as well as under which conditions they are considered to be substantiated. In addition, the last sentence of this Article needs to be reconsidered as the obligation it aims to set out is not certain.

Article 119[4]. Tracking malicious or undesirable calls to subscribers and

This Article regulates the conditions for tracking malicious or undesirable calls in order to allow a subscriber which would be subject to such calls to obtain the identity of the author of these calls. It is to be noted that the E-Privacy Directive under Article 10 (a) only provides, as an exception to the elimination of the presentation of a calling line identification, for a general obligation for providers of electronic communications services to have in place transparent procedures relating to requests from subscribers for tracing malicious or nuisance calls and the storage and provision of the data containing the identification of the calling subscriber. It does not specify how the said procedure must function and other associated conditions as it is for national legislations to define these aspects. As such, formally, Article 119[4] appears to achieve this objective and is in line with Article 10 (a) of the E-Privacy Directive.

We nevertheless would like to highlight on the substance, that the Article may raise some issues with respect to the privacy of the subscriber to be identified following a request received in accordance with these provisions. More specifically, as the provision only sets as a condition for the requesting subscriber to prove the necessity to obtain the identity of the caller to protect his/her

rights in courts without further conditions or criteria as to what is considered as an acceptable evidence to be submitted in such a case (e.g. high number of calls received, malicious content of communications, and any other element substantiating a an actual legitimate interest in obtaining the identification), the risk would be that anyone pretending that it is a victim of malicious calls on the basis even of 2 or 3 calls, and arguing that they need it for judicial proceedings may easily obtain the identity of another subscriber in an unwarranted manner.

It is thus highly recommended to set out additional conditions to frame more restrictively the framework for identification of authors of malicious calls to prevent that such a procedure is used in an abusive manner and/or allows undue breach of the privacy of subscribers.

As a further point we note that the provision indirectly refers to the identification or restriction of the calling line of a subscriber but does not specify the applicable rules in this regard. The E-Privacy Directive specifically addresses this topic and set outs conditions for its implementation under Article 8.

It is recommended to add a specific provision regulating the presentation and restriction of calling and connected line identification in line with Article 8 of the E-Privacy Directive.

Article 119^5 Undesired calls and messages to subscriber

This Article regulates the conditions for undesired calls and messages in order to allow a subscriber which would be subject to such calls or messages to obtain the identity of their author. The E-Privacy Directive, as for malicious calls examined above provides, for such obligation for providers of electronic communications services to have in place transparent procedures relating to requests from subscribers for tracing malicious or nuisance calls and the storage and provision of the data containing the identification of the calling subscriber. It does not specify how the said procedure must function and other associated conditions as it is for national legislations to define these aspects. As such, formally, Article 119^5 appears to achieve this objective and is in line with Article 10 (a) of the E-Privacy Directive.

We nevertheless would like to highlight, on the substance, similarly as for malicious calls, that the Article may raise some issues with respect to the privacy of the subscriber to be identified

following a request received in accordance with these provisions. More specifically, as the provision only requires the requesting subscriber to commit to use the identity of the caller to protect his/her rights in courts without further conditions or criteria notably as to the acceptable evidence to be submitted in such a case by the requesting subscriber (e.g. high number of calls received, content of communications indicating the nuisance nature, and any other element substantiating a an actual legitimate interest in obtaining the identification), the provision runs the risk to be used in an abusive manner. Indeed, the risk would be that anyone pretending that it is a victim of malicious calls on the basis of even 2 or 3 calls and arguing that they need it for judicial proceedings may easily obtain the identity of another subscriber in an unwarranted manner.

It is thus highly recommended to set out additional conditions to frame more restrictively the framework for identification of authors of nuisance calls or messages to prevent that such procedure is used in an abusive manner and allow to unduly breach the privacy of subscribers.

As a final comment on the provisions relating to electronic communications, we note that they do not address the issue of automatic call forwarding as provided by Article 11 of the E-Privacy Directive. According to this provision, subscribers shall have the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

The drafters of the Draft Law should consider including a similar provision as Article 11 of the E-Privacy Directive.

4. CONCLUSIONS

The Draft Law provides an enhanced version of provisions setting a comprehensive data protection legal framework. Compared to the previous version, it covers additional and key topics such as, the liability regime for violations of the Draft Law, and addresses specific processing activities including with respect to processing of data for law enforcement purposes and, in particular sectors, notably electronic communications.

The general approach under the Draft Law is rather close to the one resulting from European standards. In this regard, it can be noted that several provisions are in line with Convention 108+

and the GDPR as well as other relevant standards and do not need to be amended. For other provisions, it is recommended to review, clarify or amend them in view of being aligned with European standards and in particular Convention 108+ and the GDPR.

In addition, the following points should deserve particular attention:

- The provisions governing the processing of personal data as part of electronic communications provide for the framework guaranteeing the secrecy of communications which includes the possibility for interferences permitted by law. The conditions applying to such interferences which are not further specified under the Draft Law, need to be regulated more specifically either in the Draft Law or another Ukrainian legislative act, taking into account applicable requirements on this topic under European standards. The same would apply regarding the access by competent authorities to location data of individuals, which is only addressed in a general manner under the Draft Law.

- As part of the articles relating to processing of personal data by providers of electronic communications networks or services, the Draft Law includes provisions regulating the conditions of processing of traffic data of users of such services. It addresses in a general manner the possibility for competent authorities to access such data but does not regulate the conditions under which such retention may occur. The topic of retention of traffic data should be subject to a specific legal framework and appropriate safeguards under relevant Ukrainian legal acts to the extent it constitutes an interference into the data protection and rights of data subjects. This should take into account applicable European standards in this field including Convention 108+ and on the EU side relevant case law of the CJEU on this matter.

- As part of the process for the finalization and adoption of the Draft Law, it is highly recommended to examine this Draft Law together with the law regulating the supervisory authority as the two acts are very closely linked and cannot be implemented one without the other in line with Convention 108+ and the GDPR. The existence and functioning of a supervisory authority are a key component of an effective data protection framework.

Finally, we would like to note that personal data processing can, beyond the general data protection

law, also be regulated by other laws regulating specific issues (elections, political campaigns, employment, electronic communications, etc.). Therefore, systematic amendments regarding legislative process could significantly contribute to the better quality of the legal acts regulating personal data processing in different areas and at the same time to the higher level of personal data protection in Ukraine, avoiding potential conflicts of laws. As regards lawfulness of the processing, the basis for the processing referred to in GDPR art. 6 (1) point (c) – compliance with the legal obligation and (e) - performance of a task carried out in the public interest, shall be laid down by law. The said law should define the purpose of the processing, as well as may contain specific provisions to adapt the application of rules of GDPR (types of data to be processed, the data subjects concerned, etc.). Therefore, we would advise to set up the obligation for the state institutions involved in the legislative process to include into the pieces of legislation regulating personal data processing, the purpose of the processing at stake and, as the case may be, other related information. This obligation could be set up in the Draft Law or in other legal acts of Ukraine regulating legislative process.
