“European Union and the Council of Europe working together to strengthen the Ombudsperson’s capacity to protect human rights”

LEGAL ANALYSIS
OF THE MAIN MODELS OF INSTITUTIONALISATION OF THE STATE SUPERVISION WITH REGARD TO PERSONAL DATA AND ACCESS TO PUBLIC INFORMATION IN UKRAINE

PREPARED BY
Volodymyr VENHER
Oleh ZAIARNYI

Kyiv, 2020

CONTENTS

ABBREVIATIONS

Convention 108, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Supervisory Authority, the state supervisory authority in the field of personal data and access to public information

Regulation (EU) 2016/679, 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

Ukraine–EU Association Agreement, Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part

CEA, the central executive authority

INTRODUCTION

Nowadays, the protection of human rights acquires new aspects and meets specific challenges. The area of creation, transfer, storage, use and protection of information is one of such new and non-traditional areas.

Two main blocs of legal regulation are evolving in parallel in this area. On the one hand, society seeks clear and democratic governance, which now increasingly requires that public authorities and the state in general profoundly implement the principles of publicity and transparency in their performance. It gave rise to the concept of "public information" and its widest possible circulation in various areas of life. On the other hand, the development of the "information society" does not, however, erase the classical challenges related to ensuring the secrecy of private life and the concept of privacy in general. The collection, processing and use of personal data are the key issues in this respect as they now demonstrate most vividly the practical manifestations of privacy. In fact, today privacy acquires new shapes, features and forms of expression. Its informative context is becoming increasingly relevant and threatening. Therefore, the international standards of access to public information prioritize the security of data transfer and personal data protection. This demonstrates rather clearly the tendency of a human-centred approach to the performance of a state when such performance is defined and limited in terms of the human rights content.

Therefore, the subject of this analysis is the study of human rights protection tools in the field of personal data and their translation into administrative and governance procedures which ensure access to public information. These areas of legal regulation should not only be seen from the perspective of the functioning of a state but at the same time instruments of influence on the state and its authorities (policy making, regulatory measures, supervision, etc.) should be provided.

The international obligations assumed by Ukraine require also that the aforementioned problem be dealt with by institutionalising the instruments for the state (administrative) supervision in the fields of personal data protection and access to public information.

The consolidation and provision of high standards related to human rights acknowledged by the Council of Europe is a priority of internal and foreign policy of Ukraine as the Council of Europe member state. Following the ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms[1] by the Verkhovna Rada on 17 July 1997, the fundamental rights enshrined in it became the reference points for building Ukraine as a democratic state with the rule of law.

The international obligations imposed on Ukraine are not limited to the implementation of the European human rights standards into its domestic law. These obligations of Ukraine cover, inter alia, the rights enshrined in Articles 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, i.e. the right to respect for private and family life and the privacy of correspondence, and the right to freely express opinions and to freely collect and disseminate information. Ukraine acknowledged its desire to guarantee the appropriate implementation of these human rights by enshrining them in the provisions of Articles 32 and 34 of the Constitution of Ukraine[2] with due regard to the peculiarities of the domestic formulation of their content.

These guarantees include, among other things, the need to ensure objective, fair and impartial state supervision with regard to personal data and access to public information. The unification of state supervision in both areas of law is rooted in the immediate link between the regulation of personal data transfer and public information.

---

[1] Convention for the Protection of Human Rights and Fundamental Freedoms of 4.XI.1950 URL: https://zakon.rada.gov.ua/laws/show/995_004 , accessed 1 April 2020.

[2] Constitution of Ukraine dated 28 June 1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр , accessed 1 April 2020.

Ukraine as the owner of national public registers functions in fact, through competent authorities, as the administrator of public information and the controller, and, when appropriate, the processor of personal data stored or processed in the relevant registers. On the other hand, personal data are a tool for the identification of the legal framework for the exercise by individuals of their right to freely receive and impart information provided for in Article 10 of the Convention. Indeed, the fundamental preconditions for the exercise of the right to access to official information containing personal data include the consent by personal data subjects to the processing of information relating to them, the public interest for such information, and possible negative consequences following such processing.

At the same time, as individual's rights provided for in Articles 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms are non-absolute rights of proportional nature as compared to the other human rights provided for in this Convention, effective instruments of supervision of those rights' observance and the prevention of abuse of rights for privacy, family life and free collection and dissemination of information by subjects possessing such rights should be implemented in the domestic legislative norms.

In light of the foregoing and with the aim of institutionalising state supervision, it is worth considering the two mentioned areas together and formulating proposals relating to supervision models with regard to both personal data transfer and public information spheres.

This legal analysis has been prepared in the framework of the Joint Project between the European Union and the Council of Europe "European Union and the Council of Europe working together to strengthen the Ombudsperson’s capacity to protect human rights" by the national consultants of the Project **Volodymyr Venher,** PhD in Law, associate professor at the Department of general legal theory and public law of the National University “Kyiv-Mohyla Academy”, Executive Director of the Research Centre for the Rule of Law; and **Oleh Zaiarnyi,** Doctor of Law, associate professor at the Administrative Law Department of the Faculty of Law of the Taras Shevchenko National University of Kyiv.

PRECONDITIONS FOR SELECTING A MODEL

a. Implementation of international standards of state supervision in the field of personal data.

The Convention 108 of the Council of Europe or the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, hereinafter, the Convention 108 is the key element in the system of the Council of Europe instruments for the legal protection of personal data. Article 1 of the Additional Protocol to the Convention 108 dated 8 November 2001 provides for the establishment of supervisory authorities with regard to personal data protection in the Council of Europe member states and the requirements for their functioning[1].

As Ukraine ratified the Convention 108[2] on 6 July 2010, and the relevant Additional protocol to it, later on, it affirmed assuming the direct commitment to implementing the Council of Europe standards relating to institutionalisation of state supervision in the field of personal data into the provisions of its national legislation.

Following the ratification of Ukraine on 27 June 2014 of the Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part[3], hereinafter, the Ukraine-EU Association Agreement, its obligation to institutionalise supervision in the field of personal data obtained a larger and multi-dimensional scope.

The provisions of the 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, hereinafter, the Regulation (EU) 2016/679[4], are mainly at the core of this obligation in terms of institutionalisation of the state supervision with regard to personal data. As Article 3 of the Regulation (EU) 2016/679 establishes a specific group of non-EU residents that can be participants to activities covered by this Regulation, this fact increases the need for an in-depth implementation of the European standards in this area of law in Ukraine.

These documents offer a clear pathway for developing the national legislation in this field. As Ukraine is a member state of the Council of Europe, Convention 108 identifies for it the binding framework for the establishment and development of supervision with regard to personal data. Furthermore, the standards provided for in the Regulation (EU) 2016/679, although not of strictly binding nature for Ukraine, do outline, however, the optimal option of exercising and institutionalising the state supervision in this field.

Following the ratification of Convention 108 and the Additional Protocol to it, Ukraine took certain measures to implement state supervision in the field of personal data. Specifically, the Decree of the President of Ukraine dated 6 April 2011, No. 390/2011, identified the State Service on Personal Data Protection as the state authority to supervise compliance with the legislation on protection of personal data.

---

[1] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Strasbourg, 8.XI.2001 URL: www.conventions.coe.int/treaty/en/Treaties/Html/181.htm. , accessed 2 April 2020.

[2] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28.01.1981, https://zakon.rada.gov.ua/laws/show/994_326 , accessed 1 April 2020.

[3] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part, 27 June 2014. URL: https://zakon.rada.gov.ua/laws/show/984_011 , accessed 1 April 2020.

[4] 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). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 , accessed 1 April 2020.

This central executive authority, hereinafter, "CEA", had functioned until 1 January 2014, when the amendments to the Law of Ukraine "On personal data protection" placed the execution of oversight and supervisory powers in the field of personal data protection on the Ukrainian Parliament Commissioner for Human Rights, leaving thus the majority of regulatory functions in this field outside of the legal framework.

In addition to that, this Law amended the Law of Ukraine "On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" dated 6 July 2010, No. 2438-VI. In accordance with these amendments, Ukraine declared that the Ukrainian Parliament Commissioner for Human Rights was the supervisory authority in the meaning of the Convention.

Although the relevant Law became effective 1 January 2014, on 16 September 2014 the Cabinet of Ministers dismantled the State Service on Personal Data Protection on the grounds of its Resolution "On the optimisation of the system of central executive authorities in Ukraine". It is worth mentioning that the Regulation "On the State Service on Personal Data Protection" was itself recognised as such that ceased to have effect only by the Decree of the President of Ukraine dated 20 June 2019, No. 419/2019, that is, five years after the relevant authority ceased to exist. Moreover, although the Law of Ukraine "On personal data protection" established by its Article 23 the subjects of supervision and oversight of the observance of personal data subjects' rights, it overlooked, however, the problem of division of supervision and oversight in the relevant area of law into specific types.

b. The establishment of state supervision in the field of access to public information in Ukraine.

The obligations regarding the institutionalisation of supervision of respect for the right of individuals to information, in particular, the right to have access to information, are mainly based on the provisions of the international "soft" law. In particular, the Joint Declaration of 2004 "International Mechanisms for Promoting Freedom of Expression"[1] declared the right to appeal any refusals to disclose information to "an independent body with full powers to investigate and resolve such complaints", which makes it possible to appeal to other mechanisms beyond courts. The Recommendation of the Council of Europe refers to the right to have recourse to "a court of law or another independent and impartial body established by law"[2].

Article 23(1) of the Law of Ukraine "On access to public information" adopted 13 January 2011, No. 2939-VI, provided for the following rule: "decisions, actions or inaction of information administrators may be appealed to the administrator's superior official, a higher authority or court".

Such approach to institutionalisation of state (administrative) supervision in the field of access to public information, embodied in the provisions of the Law of Ukraine "On access to public information", was the reason for the significant international criticism of this Law, in particular, its procedures for appealing decisions, actions or inactions of administrators of public information and the guarantees for the respect of the information requesters' rights[3].

[1]International Mechanisms for Promoting Freedom of Expression. Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 6 December 2004 https://www.osce.org/files/f/documents/6/f/38632.pdf

[2]Recommendation Rec (2002)2 of the Committee of Ministers to member states on access to official documents adopted on 21 February 2002. URL: http://zakon2.rada.gov.ua/laws/show/994_a33 , accessed 1 April 2020.

[3] T. Mendel Analytical Review of the Models of Supervisory Authorities in the Field of Access to Information / T. Mendel [electronic recourse]. Available at http://comin.kmu.gov.ua/control/uk/publish/article?art_id=115100&cat_id=108852

The provisions of this Law concerning institutionalisation of state (administrative) supervision in the field of public information became the subject of extensive and well-argued criticism from the international experts of the Council of Europe and other international organisations[1]. The following aspects relating to the implementation of the Law of Ukraine "On access to public information" provided grounds for such critical comments:

- the absence of direct references to state authority or a system of authorities empowered to exercise state (administrative) supervision and oversight in the field of access to public information;
- appeals against decisions, actions or inaction of information administrators addressed to officials or bodies of a higher level mean applying internal procedures for the control of administrators based on the principles of subordination and accountability of the respondents;
- the absence of strict safeguards guaranteeing the independence of subjects of state supervision with regard to access to public information.

The adoption on 27 March 2014 of the Law of Ukraine "On amending certain legislative acts of Ukraine in the context of the adoption of the Law of Ukraine "On information" and the Law of Ukraine "On access to public information" was an attempt to eliminate these and a number of other problems related to supervision in the field of access to public information at the legislative level.

The provisions of this Law significantly enlarged the content and the range of instruments relating to the parliamentary supervision provided for in Article 17 (1) of the Law of Ukraine "On access to public information" and exercised by the Parliament Commissioner for Human Rights. However, the provision of the Article 17 (3) of this Law envisaging that state supervision of the provision of access to information by information administrators should be carried out in accordance with the law, was not appropriately developed.

So far, as of today, the supervision of compliance with the norms of the national legislation on personal data protection and access to public information is established in Ukraine on the basis of its parliamentary model embodying some procedures and measures of impact traditionally inherent to state (administrative) supervision.

c. Practical challenges and problems

Such radical changes in the supervision in the fields of personal data and public information gave rise to a broad range of problems which adversely affected human rights respect in the field of information and led to non-compliance by Ukraine with a number of its international obligations in this respect. The problems, in particular, are as follows:

- a large number of registers, databases, information and telecommunication systems function in Ukraine as components of the national information infrastructure lacking at the same time documents, which would establish their legal rights, and special procedures for personal data processing procedures;
- the lack of a full-fledged, motivated, independent and impartial auditing of public registers, databases, information and telecommunication systems owned by the state or local communities;
- availability of only isolated annual reports on the level of cybersecurity of the national information infrastructure facilities;

[1] Kristina Brazevič, Agnė Limantė, Waltraud Kotschy. Developing guidelines for effective monitoring by the Office of the Ombudsperson of the state of compliance by relevant stakeholders with the legislation in the field of access to public information. Kyiv, 2018 URL: http://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjzgrjdnYnpAhXBXJoKHdnqDqAQFjAAegQIARAB&url=http%3A%2F%2Fwww.twinning-ombudsman.org%2Fwp-content%2Fuploads%2F2017%2F03%2FUKR_Activity-2.3.5-Annex-1.pdf&usg=AOvVaw2K_xhNsVZgpl5u4FX7iMlZ

- there are many cases in Ukraine where regulations on information exchanges (interaction) between public registers, information and telecommunication systems as well as the procedures for processing personal data are in the form of documents with restricted access;
- lack of clear, transparent and competitive grounds for identifying administrators of public registers and information and communication systems;
- insufficient application of administrative measures in the form of cessation of operations, administrative preventive measures and general instruments designed to prevent offences in the fields of protection of personal data and provision of access to public information, etc.

Along with other problems, the Annual Report of the Ukrainian Parliament Commissioner for Human Rights on the Observance and Protection of the Human Rights and Freedoms of Citizens of Ukraine of 2018[1] underlined also the presence in Ukraine of a persistent trend towards the transformation of typical violations of the right to information into more serious and specific violations of legislative provisions on personal data protection and access to public information.

These and the number of other factors seriously aggravate the problems related to the institutionalisation in Ukraine of the state supervision of compliance with the legislation on personal data protection and access to public information.

d. The limits of authority needed for an effective state supervision

The priorities of the state policy in this sphere arise in general from the challenges and problems mentioned above in the fields of personal data and public information. The results of the comprehensive analysis of these problems, as well as of the national legislation and the practice of its implementation allow for the identification of the following groups of powers to be institutionalised (i.e., assigned to a certain body or a number of state bodies) to appropriately ensure policy making and execution in the fields of personal data and public information:

1. *Powers relating to the legal and regulatory framework of personal data transfer and access to public information:*
   - the development, professional expertise and adoption of legislative and regulatory acts necessary to implement the state policy in the fields of personal data and access to public information;
   - submission, to the subjects authorised by law to initiate legal acts, of proposals on amending laws of Ukraine regulating relations in the fields of personal data and access to public information;
   - approval of draft regulatory acts affecting the rights of personal data subjects or requesters of public information with the exception of the draft laws of Ukraine;
   - development of standard procedures for personal data processing and regulations on personal databases;
   - approval of regulatory requirements for the automatic processing of personal data using information technologies which may pose heightened risks for personal and family privacy;
2. *Regulatory powers and the implementation of state policies:*
   - exercising of regulatory powers in the fields of personal data and public information in accordance with the national regulatory policy legislation;
   - provision of methodological support to controllers, recipients and processors of personal data and administrators of public information related to the organisation of their work;
   - assisting administrators of public information in the performance of their duties related to recording, official publishing and protection of public information,

[1] Annual Report of the Ukrainian Parliament Commissioner for Human Rights on the Observance and Protection of the Human Rights and Freedoms of Citizens of Ukraine, 2018. URL: https://dpsu.gov.ua/upload/file/report_2019.pdf

authorisation of procedures for publishing relevant information, proposed by its administrators, and approval of standard arrangements for such publishing;

- authorisation of drafts of local acts of entities of primarily state and communal ownership regulating internal processing and protection of personal data;
- provision of clarifications to the state and local self-government authorities, entities and individuals on how to apply the Ukrainian legislation on personal data protection and access to public information;
- provision of recommendations on how to process personal data in times of a state of emergency or emergencies;
- submission of notifications on the compulsory performance of duties by administrators of public information, resulting from requests for information submitted for their consideration;
- authorisation of draft decisions by the executive and local self-government authorities on establishing or renewing public registers and telecommunication systems where personal data are to be processed or stored;
- authorisation of terms of reference related to establishing or renewing public registers and telecommunication systems where personal data are to be processed or stored;
- training and informing civil servants of their performance as persons responsible for administrating public information or persons designated as controllers of personal data.
- raising public awareness of procedures for access to public information and the content of the right to access such information.

3. *Supervision powers:*
   - routine and extraordinary inspections of administrators of public information and controllers, processors and recipients of personal data with regard to their compliance with the rights of personal data subjects and public information requesters;
   - deciding whether a request for public information was appropriately considered by an administrator;
   - notifying administrators of public information of their violations of the provisions of the laws on information;
   - analysing risks for legitimate processing of personal data related to designing new public registers, databases or telecommunication systems.
4. *Powers related to administrative jurisdiction:*
   - issuing compliance orders to administrators of public information, controllers, recipients and processors of personal data on the elimination of violations found;
   - application of measures involving the administrative suspension of activities of administrators of public information, controllers, recipients and processors of personal data;
   - initiating and carrying out of administrative jurisdiction proceedings in the cases involving alleged administrative offences in accordance with Articles 188-39, 188-40, 212-3 of the Code of Ukraine on Administrative Offences;
   - the imposition of administrative penalties for committing relevant administrative offences;
   - appealing of unlawful decisions, actions or inactions by administrators of public information, controllers and processors of personal data suggesting violations of law;
   - submission to relevant law enforcement agencies of case-files suggesting offences violating human rights enshrined in Articles 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;
   - submission to courts of case-files related to full or partial prohibition of personal data processing by entities as a result of offences committed by them;
   - participation in the procedures of pre-trial settlement of conflicts in the area of

information, etc.

e. The methodological framework of the analysis

It should be concluded from the systematic analysis of the provisions of the Convention 108 and the Regulation (EU) 2016/679 that the institutionalisation of the state supervision in the fields of personal data and public information should provide for the establishment of a separate independent entity within the system of state authorities in Ukraine to exercise the appropriate comprehensive supervision in this area.

It should be taken into account that the above international documents recommend designating a single special body (authority) to exercise powers in this respect. However, no limitations are established as to exercising such powers by several bodies to perform systematically and in due coordination the relevant functional state duties.

It is obvious that the selected format and the institutional model of supervision in this area should be premised on the provisions of the national legislation and the practice of its application in the similar (contiguous) areas. For the purposes of this research and to designate this authority we will use the term "the State supervision authority in the fields of personal data and access to public information", hereinafter, the Supervisory Authority. We will use this term for the definition of both a standalone body and a system of bodies which would exercise the relevant state functions.

It should be mentioned also in connection with the scope of the mandate and the competence of the Supervisory Authority, that the experts have limited the subject of this research with the range of problems related to state supervision in the fields of personal data and access to public information. In light of the mentioned, the subject of this legal analysis does not cover the overview of procedures for personal data processing, access to public information and the characteristics of the functioning of databases, registers or portals containing such data, except if directly related to the issues of institutionalisation of the state supervision in the relevant areas of law.

The proposals and recommendations outlined in this document do not either cover the issues related to institutionalisation of the state supervision of compliance with the legislation on personal data protection and access to public information with regard to justice administration, pre-trial investigations of alleged crimes and execution of criminal convictions. These areas of the institutionalisation of the state supervision of compliance with the legislation on personal data protection and access to public information may become the subject of a whole separate legal research.

The key features of each model were defined based on the most important aspects of the constitutional and legal statuses of different state bodies and other authorities exercising effective power.

In this respect, importance should be attained also to, for example, the procedures for selection (nomination) of the head and members (in the case of collegial working procedures) of such body, procedures for its decision-making on procedural and rule-making issues, the arrangements for its interaction with judicial and quasi-judicial state bodies.

It is important in terms of the selection of a specific Supervisory Authority model to decide whether its decisions would be legally effective. This refers to the powers of the Supervisory Authority in the field of personal data to issue compliance orders to state authorities and private law entities, authorise draft laws and regulations possibly affecting human rights as provided for by Articles 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms and to approve procedures for the disclosure of public information, etc. These powers are essentially within the limits of the functional and substantial aspects of the work of the Supervisory Authority in the fields of personal data and access to public information.

This analysis together with the studies on the right to information by the international experts demonstrates that several models of supervisory authorities in the fields of personal data and access to public information exist in the Council of Europe member states. Each of these models, according to its content and legal nature, provides for different procedures for the Supervisory Authority establishment, guarantees of its performance, methods of interaction with the relevant parliamentary supervisory bodies, modes of a combination of regulatory and supervisory powers in its competence, etc.

In light of this and with due regard to the constitutional and legal principles of organisation of state power in Ukraine, this analysis presents three main models of state supervision in the fields of personal data and public information:

- a separate Supervisory Authority which does not belong to any of the branches of government in Ukraine;
- a separate Supervisory Authority as an independent central executive authority;
- a "collective" Supervisory Authority as a system of (several) supervisory bodies.

The modes and character of legislative definitions related to each of the national Supervisory Authority models affect directly the nature of the Authority, its integration with a specific branch of government, its goals and the extent to which the international standards for the right to information will be translated into law-making and law-application.

THE MODELS OF INSTITUTIONALISATION OF THE STATE SUPERVISION IN THE FIELDS OF PERSONAL DATA AND PUBLIC INFORMATION

Model 1: a separate state authority not belonging to any of the branches of government in Ukraine

This model entails the establishment of a new independent authority not directly subordinate to any of the branches of government and with an autonomous legal status.

This model is rather widespread in many countries of the world. As the systematic analysis of the provisions of domestic law in various countries demonstrate, independent supervisory authorities in the relevant areas act as inspections, commissions or commissioners, etc., empowered to protect the right to information (protect data). Those types of national supervisory authorities differ also among themselves by the structure of their competence, that is, by whether they are invested exclusively with supervisory or regulatory powers or with a combination of both.

In France, the independent National Commission on information technologies and freedoms (Commission Nationale de l'Informatique et des Libertés) functions as an autonomous administrative collective body the members of which represent various branches of government[1]. In the Federal Republic of Germany, the special Federal Commissioner for Data Protection and Freedom of Information functions as an official and a federal authority with the unity of command[2]. Poland uses a similar model, as the Personal Data Protection Office functions there as an autonomous authority with the unity of command, conferred with broad powers and a special status for its president and officials[3]

Without getting into the detailed analysis of specifics of each model in these and other countries, it should, however, be said that the implementation of a similar model in Ukraine will require the following:

a. The Constitution should be amended, and a separate special law should be adopted (or serious corrections should be made to the laws on personal data protection and access to public information). Such amendments should provide for the functioning of a new authority out of direct control from legislative, executive or judicial authorities. Such authority may be a (single-person) body with the unity of command (Prosecutor General, Head of the Security Service of Ukraine), a collegial body (the National Council of Television and Radio Broadcasting of Ukraine and the Central Electoral Commission), or a combination of both (Governor and the Council of the National Bank of Ukraine). The advantages and deficiencies of collegial governance or governance based on the unity of command may be the subject of a separate analysis. It should be mentioned here only that the constitutional law theory conventionally believes that collegial governance allows for a higher level of independence of an institution. Against this background, the best option for Ukraine seems to be the establishment of a collegial body with a status similar to that of the Anti-Monopoly Committee of Ukraine or the National Council of Television and Radio Broadcasting of Ukraine.
b. A special procedure should be provided for the appointment and dismissal of the head (and members) of such supervisory authority functioning at the highest level (with the participation of the President of Ukraine, the Verkhovna Rada of Ukraine and/or the other highest state authorities). The participation of national associations representing main

[1] Commission Nationale de l'Informatique et des Libertés // https://www.cnil.fr/en/node/287
[2] Federal Data Protection Act (Chapter 4) // https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0081
[3] Act on the Protection of Personal Data () // file:///C:/Users/User/Downloads/Act%20on%20the%20Protection%20of%20Personal%20Data.pdf

providers of information services in the procedures regulating the Supervisory Authority composition may not be excluded, similar to the procedures for the composition of national telecommunications regulatory bodies existing in some Council of Europe member states, in particular, the UK, Germany, Poland and others. Convention 108 (even as amended by the Protocol 223) does not contain any specific requirements for the composition of a supervisory authority. This being said, the Regulation (EU) 2016/679 provides that the supervisory authorities may be appointed by parliaments, governments, heads of State or other independent bodies under Member State law (article 53.1 of the Regulation). It is obvious that applicants to senior positions (head/members) in the Supervisory Authority should comply with the specially established requirements as to their professional competency and past performance and their nomination procedure should be regulated in detail by separate laws to provide for its fairness and impartiality.

c. The duration of the term of the Supervisory Authority should be defined with reasonable substantiation to additionally ensure its political independence. In particular, it is desirable that it not be equal to the terms of office of the President, the Verkhovna Rada and the Cabinet of Ministers, or other authorities of Ukraine. At least the times of commencement and termination of its powers should not depend on the election or termination of powers of these bodies or officials. As the terms of powers of the President and the Verkhovna Rada of Ukraine equal to 5 years, the terms of powers of the Supervisory Authority should be more than 5 years (for example, 6 or 7 years, however, a longer term may appear excessive). For example, such an approach was applied to the Central Electoral Commission and the terms of powers of its members are 7 years.
d. It should be adequately provided with financial and technical resources. The Supervisory Authority should be guaranteed the appropriate annual allocation of necessary funding for its functioning in a separate budget line of the State Budget of Ukraine. Such an approach has been already introduced in the Ukrainian context at the constitutional level with respect to the provision of funding and appropriate operational environment for courts and the work of judges (Article 130 of the Constitution amended on 2 June 2016). However, the implementation of this instrument has not always matched the expectations invested in it.
e. A special status should be established for the employees of this authority (officials of its administration or secretariat, etc.). This special status should provide for special procedures for their appointment, service career and termination, advanced training, social benefits during and after the termination of service, etc. This tool is particularly important for an independent authority. Indeed, the status of almost all public servants (civil servants in particular) is very precisely and in detail regulated by a number of regulations issued by the Government of Ukraine (for example, governmental resolutions establish terms of remuneration, procedures for competitions to fill vacancies, advanced training, etc.). Therefore, appropriate guarantees for the Supervisory Authority officials and support personnel should be provided to guarantee its full independence.
f. Appropriate broad powers should be defined and assigned to the Supervisory Authority enabling it to develop and implement state policies in the fields of personal data and public information. Such powers should be sufficient to provide for a functional authority model where its regulatory acts are supported by appropriate procedures for the supervision of their execution.
g. Parliamentary and the state (administrative) supervision in the fields of personal data protection and access to public information should be separated for the purposes of the establishment of an independent Supervisory Authority in these areas of law. If the Supervisory Authority is established, then, in the light of the purpose of the parliamentary supervision as established in Article 3 of the Law of Ukraine "On the Parliament Commissioner for Human Rights", Article 17 of the Law of Ukraine "On access to public information, Article 23 of the Law of Ukraine "On personal data protection", other

legislative acts, the Parliament Commissioner for Human Rights should retain powers related to the monitoring of observance of the rights to information in Ukraine and authorisation of draft law possibly affecting these rights of individuals. The above mentioned includes also other powers directly relating to the purpose of the parliamentary supervision by the Parliament Commissioner for Human Rights, in particular, non-judicial protection of human and citizen's right to information, preparing annual reports on observance of human rights and freedoms, recommendations to the Government, central executive authorities and local self-government authorities on how to improve their work in terms of observance of the right to information, interventions in response by the Commissioner within the scope of his or her competence, etc. Accordingly, If the Supervisory Authority is established in Ukraine, the parliamentary and state (administrative) supervision in the relevant fields should be divided mainly depending on the subject of supervision, authorities of its realisation and intervention measures to be applied within each of these two areas of supervision.

h. The system of units or officials dealing with personal data and public information should be established. Such a system should be adapted to international standards, in particular to the requirements of Convention 108 and the Regulation (EU) 2016/679. It seems advisable to establish a system of "state authorised representatives" and "representatives" coordinated by the Supervisory Authority. A similar model exists in Ukraine in the area of prevention of corruption. According to the Law of Ukraine "On prevention of corruption", public authorities shall establish (appoint) units (persons) authorised to prevent and disclose corruption, with special legal regulation of their status and performance. It will be extremely difficult to effectively organise the work of the Supervisory Authority as an independent body without the network of such "agents".
i. Special procedures should be established to ensure the transparency and openness of the Supervisory Authority, the involvement of civil society in its work, modes of parliamentary supervision, appeals in courts against its decisions, actions or inactions. As the Supervisory Authority would be a fully independent body, these procedures should take into account particularities inherent to this sphere of the regulation (for example, the risks of uncontrolled personal data leaks etc.) and at the same time ensure clear and understandable algorithms for the accountability of the Supervisory Authority. It should guarantee the high level of social trust to the Supervisory Authority, its works and measures to be taken.

The arguments in favour of such an approach:

+ An independent authority would be out of direct political, administrative, financial or other formal influence from other high authorities, political parties or individuals.
+ Separation of the Supervisory Authority from the system of executive authorities may provide fairer supervision of the executive authorities themselves and the Cabinet of Ministers in the first instance. After all, it is precisely the Cabinet of Ministers which would have had a certain administrative influence on the Supervisory Authority in the fields of personal data and access to public information if the latter were a part of the system of executive authorities.
+ The establishment of such new body will allow for lessening of the workload of the Parliament Commissioner for Human Rights and his or her Secretariat by ensuring for the Commissioner the opportunity to focus attention and administrative resources on other areas of parliamentary supervision of the observance of human rights.
+ If the functions of state (administrative) supervision and the implementation of state policies in the fields of personal data protection and access to public information are to be concentrated within a single authority, it will allow for the establishment of such political and legal model where regulatory acts issued by this authority would be underpinned by appropriate procedures for the supervision of their execution.

The arguments against such an approach (risks):

- If a single authority is simultaneously invested with powers of rule-making, regulatory policy, making and implementing public policies in the field of personal data, initiating and ensuring bringing perpetrators to justice, it would give rise to serious admonitions as to the observance of the constitutional principle of the separation of powers. After all, the principle of separation of powers not only requires their division into legislative, executive and judicial branches but provides also for the system of checks and balances. The establishment of a fully independent body simultaneously possessing rule-making, regulatory, implementational, supervisory and punitive functions would undoubtedly upset the already delicate equipoise of checks and balances within the system of authorities in Ukraine.
- The establishment of the Supervisory Authority as a separate state body would require substantial amendments to the information laws and an in-depth redistribution of powers among the newly established Supervisory Authority, the Parliament Commissioner for Human Rights, the Ministry of Justice, the Ministry of Internal Affairs and other central executive authorities. As the Supervisory Authority by its nature would be a regulatory authority, then the transfer of powers from the executive authorities to the newly established Supervisory Authority could invest the latter with a certain scope of "executive powers" which might eventually lead to its certain "competition" with the executive authorities in the field of the public information policy.
- The establishment of a new authority would require additional instruments for the safeguarding of its functional independence: comprehensive and wide powers in the field of regulatory policy; supervisory and oversight powers with regard to obtaining on-demand information from various public and private entities (businesses as well); the judicial review of acts issued by other authorities, with their presumable temporary suspension; possible expertise of draft laws prior to their consideration in the Verkhovna Rada; initiating and ensuring the bringing to justice of perpetrators of laws on personal data protection, etc. Such scope of powers invested to the Supervisory Authority would be disproportional to the purpose of its establishment within the Ukrainian legal and administrative system, as it would significantly transcend the scope of powers of any existing authorities. If applied in the Ukrainian political and legal realities, this could lead to excessive and disproportional interference in the human rights without appropriate external control, as there would be no instruments of supervision over the actions of Supervisory Authority except for the retrospective judicial control. It could lead to systematic abuses.
- The establishment of the Supervisory Authority as a constitutionally independent authority could facilitate the effective supervision of the transfer of personal data and public information, however, the Ukrainian political and legal realities demonstrate, unfortunately, that the institutional safeguards of authorities' independence by no mean always function in a proper way. In some cases, even the institutions possessing the highest "constitutional" status and guarantees function depending on political and social sentiments. Such state of affairs requires balancing the proportion between institutional independence, powers invested and possible risks relating to their implementation.
- The proposed functions of a new body along with its fully independent constitutional status would require significant human and material resources for its management. After all, constitutionally independent bodies may not permanently rely on the use of human, financial, technical, etc., resources of executive authorities. For example, The Security Service of Ukraine has own full-fledged structure - both the central offices and the extensive network of territorial bodies, the Central Electoral Commission has a network of the district, territorial and polling station electoral commissions functioning in times of elections and the National Council of Television and Radio Broadcasting of Ukraine has a rather "centralised" and relatively small functionality. At the same time, the purpose and

functions (the planned scope of powers) of the Supervisory Authority would definitely require the significant number of employees in the central office (the secretariat) and the establishment of territorial divisions. In the current context, it is, by all means, a substantial obstacle to the establishment and prompt start of the performance of such a body.

Model 2: the separate central executive authority

This model envisages the establishment of a separate central executive authority within the executive branch of government and with additional guarantees of institutional independence. Such guarantees should provide the Supervisory Authority with personnel, technical and financial resources, premises and infrastructure necessary for its efficient performance independently of other executive bodies.

This model is rather widespread in many countries of the world. In various countries, supervisory authorities are established as single-person authorities supported by special offices (secretariats) or independent collegial bodies. In some cases, such bodies are established under relevant ministries or other government agencies. In Austria, for instance, the Data Protection Council functions as a collegial body under the Ministry of Constitutional Affairs, Reforms, Deregulation and Justice and there exists also the Data Protection Authority, a separate body with the unity of command, in actual subordination to this Ministry[1]. The State Data Protection Inspectorate functions in Lithuania as a separate executive body with the unity of command, responsible before the Government and the Minister of Justice[2]. And in Norway, such authority functions as an independent agency under the Ministry of Local Government and Modernisation[3]. The mentioned types of supervisory authorities differ in their competences, that is, in whether they include exclusively supervisory or regulatory powers or a mixture of them.

Without getting into the detailed analysis of specifics of each model in these and other countries, it should, however, be said that the implementation of a similar model in Ukraine will require the following:

a. A separate special law should be adopted (or serious corrections should be made to the current laws on personal data protection and access to public information). Such amendments should provide for the functioning of new executive authority in the executive power system (such amendments should be developed with due regard to the Article 116 of the Constitution of Ukraine which defines that the Cabinet of Ministers establishes executive authorities under the law). Such authority could be both an authority with the unity of command (single-person authority) (the State Bureau of Investigations or the National Agency for Prevention of Corruption after the amendments of 2 October 2019) or a collegial authority (the National Securities and Stock Market Commission or the National Agency for Prevention of Corruption prior to the amendments of 2 October 2019). As already mentioned before, the constitutional law theory conventionally believes that collegial governance allows for a higher level of independence of an institution. Still, in Ukraine, the model of (single person) bodies with the unity of command significantly prevails among the executive authorities as hierarchy and subordination are the general features of the executive power. However, it seems that the establishment of a collegial body with a status similar to that of the National Securities and Stock Market Commission should be preferable for Ukraine, with due regard to the specificities of functions pertaining to the Supervisory Authority.

[1] Federal Act concerning the Protection of Personal Data (DSG) (Chapter 2 Bodies) // https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

[2] LAW ON LEGAL PROTECTION OF PERSONAL DATA (CHAPTER THREE SUPERVISORY AUTHORITIES) // https://vdai.lrv.lt/en/legislation

[3] The Norwegian Data Protection Authority (DPA) // https://www.datatilsynet.no/en/about-us/

b. Its place in the system of executive bodies should be defined. Several models of central executive authorities exist in Ukraine: the authorities with a special legal status, which, as a rule, is established by the Constitution, as, for instance, the State Property Fund of Ukraine; authorities with a special legal status established by ordinary laws (the State Bureau of Investigation, the Asset Recovery and Management Agency, etc.); ordinary authorities supervised by a member of the Cabinet of Ministers (the National Police of Ukraine supervised by the Minister of Internal Affairs or the State Tax Service of Ukraine supervised by the Minister of Finance). It is obvious that the special functions and powers of the Supervisory Authority require that it have additional institutional independence and special status and be directly subordinated to the Cabinet of Ministers. It does not seem advisable to amend the Constitution to this end. The special status for the Supervisory Authority may be appropriately established legislatively, for example, through amending the Law of Ukraine "On personal data protection". The method of securing the independence of a body within the executive system through its special status pays off in general, as, for instance, the performance of the State Bureau of Investigation or the National Agency for Prevention of Corruption demonstrates, given the absence (at least public) of evidence of their dependence from the Cabinet of Ministers.
c. A special procedure should be developed for the appointment and dismissal of the head (members) of the Supervisory Authority. This procedure should obviously be performed at the highest public level (with the involvement of the President, Verkhovna Rada or/and the other highest state authorities of Ukraine). Convention 108 (even as amended by the Protocol 223) does not contain any specific requirements for the composition of a supervisory authority. This being said, the Regulation (EU) 2016/679 provides that the supervisory authorities may be appointed by parliaments, governments, heads of State or other independent bodies under Member State law (article 53.1 of the Regulation). It should be mentioned here that, as with regard to the previous model, applicants to senior positions (head/members) in the Supervisory Authority should comply with the specially established requirements as to their professional competency and past performance and their nomination procedure should be regulated in detail by separate laws to provide for its fairness and impartiality and include competitions. It should be stressed that if the Supervisory Authority is established in the form of a collegial body, a part of its members could obtain this status by virtue of their positions, for example, one of its members could be ex officio the Minister of Justice. Such being the case, a reasonable and proportional representation of various stakeholders should be provided.
d. Guarantees should be established against the influence on the head/members of the Supervisory Authority through the procedures for their dismissal or disciplinary actions against them. Articles 52 and 53 of the Regulation (EU) 2016/679 provide a rather good framework for the provision of independence of the Supervisory Authority as an autonomous structure which may not be subject to any pressure arising out of personal attitudes to its head/members. The examples of such procedures have been elaborated in Ukraine and they are rather intensely applied with varying degrees of success. However, a special law providing for the status of the Supervisory Authority should envisage rigorous enough and exceptional conditions for the termination of powers of its director/members.
e. As with regard to Model 1, the duration of the term of the Supervisory Authority should be defined with reasonable substantiation to additionally ensure its political independence, primarily, from the Cabinet of Ministers. At least the times of commencement and termination of its powers should not depend on the formation of a government, the appointment of the Prime Minister or any minister, the termination of powers of these bodies or officials. It should be done so because the duration of the term of the Cabinet of Ministers of Ukraine depends on the duration of the term of the Verkhovna Rada and is 5 years at the most. With this in mind, it is advisable that the duration of the term of the Supervisory Authority be over 5 years.

f. It should be adequately provided with financial and technical resources. The provision of the financial, human and organisational independence of the Supervisory Authority is particularly important if it functions within the system of executive bodies. Therefore, the key elements of such independence are worth setting up at the level of a special law. It is advisable to do by amending the laws "On personal data protection", "On access to public information" and other special laws and legislative acts (for example, on civil service) in order to establish terms of remuneration, appointment, service career and its termination, advanced training, social benefits during and after the termination of service, etc. for the senior and other officials of the Supervisory Authority. As already mentioned before, these factors are not only important from the point of view of the Ukrainian social and political realities, but they are also prescribed by the international standards. Thus, the Regulation (EU) 2016/679 clearly sets out that the Supervisory Authority should be financially independent (Article 52.6 of the Regulation).

g. Appropriate broad powers should be defined and assigned to the Supervisory Authority enabling it to make and implement state policies in the fields of personal data and public information. Such powers should be sufficient to provide for a functional authority model where its regulatory acts are supported by appropriate procedures for the supervision of their execution. Such powers should be detached from the competence of other executive bodies and conferred to the Supervisory Authority. Some particular powers might and should be left to executive authorities, especially at the regional and subregional (district) levels, with real and effective supervision of their exercising.

h. Parliamentary and state (administrative) modes of supervision in the field of personal data protection should be separated. As already mentioned before, a clear-cut separation of parliamentary and administrative supervision in the field of personal data protection is a key element of each of the models of a Supervisory Authority. If the Supervisory Authority is established, then, in the light of the purpose for the parliamentary supervision as established in Article 3 of the Law of Ukraine "On the Parliament Commissioner for Human Rights", Article 17 of the Law of Ukraine "On access to public information, Article 23 of the Law of Ukraine "On personal data protection", other legislative acts, its scope of competence should exclude powers relating to the monitoring of observance of the right to information in Ukraine and the authorisation of draft law possibly affecting those rights of individuals. The above mentioned includes also other powers directly relating to the purpose of the parliamentary supervision by the Parliament Commissioner for Human Rights, in particular, non-judicial protection of human and citizen's right to information, preparing annual reports on observance of human rights and freedoms, recommendations to the Government, central executive authorities and local self-government authorities on how to improve their work in terms of observance of the right to information, interventions in response by the Commissioner within the scope of his or her competence, etc. Accordingly, If the Supervisory Authority is established in Ukraine, the parliamentary and state (administrative) supervision in the relevant fields should be divided mainly depending on the subject of supervision, authorities of its realisation and intervention measures to be applied within each of these two areas of supervision.

i. The system of units or officials dealing with personal data and public information should be established. Such a system should be adapted to international standards, in particular to the requirements of Convention 108 and the Regulation (EU) 2016/679. It is advisable to create a system of controllers and processors to be coordinated by the Supervisory Authority. A similar model exists in Ukraine in the area of prevention of corruption. According to the Law of Ukraine "On prevention of corruption", public authorities shall establish (appoint) units (persons) authorised to prevent and disclose corruption, with special legal regulation of their status and performance. It will be extremely difficult to effectively organise the work of the Supervisory Authority without the network of such "agents".

j. The procedures for the interaction of the Supervisory Authority with the Verkhovna Rada, the President and other authorities of Ukraine should be established. This element is important because the Supervisory Authority as an executive body subordinated to the Cabinet of Ministers should possess powers enabling it to interact directly with other bodies without special permission or control on the part of the Government. A relevant example here could be the interaction with the Verkhovna Rada in the form of expertise of draft laws in the fields of personal data and access to public information.
k. Algorithms should be established for the interaction of the Supervisory Authority with the Cabinet of Ministers of Ukraine and other executive authorities. The principles and general limits of such interaction should be established by law. Indeed, it will be an additional element of the independence of the Supervisory Authority from the Cabinet of Ministers in the first instance. As the Supervisory Authority would oversee the performance of the executive authorities, appropriate legal and organisational mechanisms should be provided to avoid conflicts of interests among institutions, managerial "corporate ethics" or other forms of partiality and biased approaches both from other bodies towards the Supervisory Authority and in the attitude of the Supervisory Authority towards the bodies under its supervision.
l. Special procedures should be established to ensure the transparency and openness of the Supervisory Authority, the involvement of civil society in its work, modes of parliamentary supervision, appeals in courts against its decisions, actions or inaction, etc. Such procedures should differ from ordinary procedures pertaining to executive bodies. After all, it should guarantee the high level of social trust to the Supervisory Authority, its work and measures to be taken.

The arguments in favour of such an approach:

- The position of the Supervisory Authority within the executive system would best of all correspond to the nature of powers conferred to it. After all, as already mentioned before, according to the model of powers provided for by the Convention 108 and the Regulation (EU) 2016/679, the Supervisory Authority would be primarily a supervisory and regulatory body. This fact should in no way call into question neither the nature of this new entity nor the system of checks and balances enshrined in the Constitution.
- The Supervisory Authority could be established either through the adoption of a new law or through amending certain provisions of the Law "On personal data protection" or the Law "On access to public information". This would enable the relatively prompt regulation of procedures for the performance of the Supervisory Authority, the start of its functioning and if needed the correction of certain technical aspects of its performance after the practical testing of the selected model.
- The establishment of such new body will allow for lessening of the workload of the Parliament Commissioner for Human Rights and his or her Secretariat by ensuring for the Commissioner the opportunity to focus attention and administrative resources on other areas of parliamentary supervision of the observance of human rights.
- If the functions of state (administrative) control and the implementation of state policies in the fields of personal data protection and access to public information are to be concentrated within a single authority, it will allow for the creation of such political and legal model where the regulatory acts issued by this authority would be underpinned by appropriate procedures for the supervision of their execution.
- There should be a possibility to use available resources of other executive authorities, in particular, at the lower or territorial level. Certain powers relating to the implementation of policies in the fields of personal data protection and public information can be left to the existing executive bodies with the provision of a clear algorithm of their supervision by the Supervisory Authority. For example, the territorial divisions of the Ministry of Justice could exercise expert review of local regulatory acts issued by local state

administrations for the purpose of their conformity to the legislation on personal data protection simultaneously with their registration. The Supervisory Authority should obviously develop the methodology, criteria and algorithms for such expertise, and, as a matter of fact, procedures for verification of its efficiency. In such a way, the functioning of the Supervisory Authority within the system of executive bodies lessens the need for it to build own administrative hierarchy line at all levels of administration.

The arguments against such an approach (risks):

- The functioning of the Supervisory Authority within the system of executive bodies means its subordination, at least formal, to the Cabinet of Ministers of Ukraine. It would pose a threat to its institutional and functional independence. A number of legal, organisational and financial guaranties, essentially separating the Supervisory Authority from among the other executive authorities, should be provided by law to safeguard such independence (which is highly important in the light of the performance by the Authority of its tasks and the requirements set forth by international standards).
- The establishment of the Supervisory Authority as a separate executive body would require substantial amendments to the information laws and an in-depth redistribution of powers among the newly established Authority, the Parliament Commissioner for Human Rights, the Ministry of Justice, the Ministry of Internal Affairs and other central executive authorities. As the Supervisory Authority would function within the system of executive bodies, this process would be to some extent easier than if an absolutely new and independent body were created, however, it would nevertheless require a long time and significant efforts.
- The Supervisory Authority would, as a part of the system of executive bodies, oversee the performance of other executive bodies. This could under certain circumstances trigger conflicts of interests among institutions, the development of a managerial "corporate ethics" or other forms of partiality and biased approaches on the part of the Supervisory Authority while exercising supervisory powers with regard to executive bodies under its supervision. In the first instance, such assertions hold relevance with regard to the central executive authorities which are the administrators of the largest national public registers and communication systems where the main bulk of confidential public information on individuals (citizens of Ukraine, foreign nationals and stateless persons legally residing on the territory of Ukraine) is processed. In order to avoid such situations, a number of organisational and legal mechanisms related to their prevention and application of countermeasures should be developed.

Model 3: a system (a number) of supervisory authorities.

This model entails preservation and the in-depth comprehensive development of the currently existing model of supervision in the fields of personal data and access to public information. In practice, it means interinstitutional cooperation and comprehensive regulation of performance of subjects in the public and non-public areas.

According to this approach, a number of bodies united by a clear algorithm of interaction, decision-making and reporting, should exercise relevant powers related to state supervision in the areas of personal data protection and access to public information. This model would not contradict either to international standards or common approaches with regard to personal data protection, as provided by the Convention 108 and the Regulation (EU) 2016/678. So, for example, Article 51.1 of the Regulation (EU) 2016/679 clearly affirms that there could be one or more independent public authorities to perform relevant supervisory functions. It should be underlined in this respect that the

independence criteria established for the supervisory authority, would apply to all bodies empowered to implement relevant functions.

The appropriate implementation of this model would be the most difficult task as it should provide not only for the development of the unified supervisory structure and a legislative framework for it but also for guaranteeing their synchronous, coordinated and efficient performance, which is a far more difficult issue. With this consideration in mind, it could be argued that the implementation of this model in Ukraine will require the following:

a. Organisational and functional auditing of the implementation of public policies in the fields of personal data and public information should be prepared and performed. Indeed, as it was already mentioned in the introductory part of this document, the history of legislative regulation and public administration in these areas is rather long and ambiguous. Its current mechanism in the form of the supervision by the Ukrainian Parliament Commissioner for Human Rights is hardly effective and fails to accomplish the main purpose of such supervision. However, the previous institutions and mechanisms could not be either regarded as efficient. Moreover, the current mechanism of supervision seems to be deficient and too general in nature. Therefore, full auditing of functions of various public authorities in the areas of personal data and public information should become a base for the development of a mechanism for the further improvements of the system of supervisory bodies.
b. A clearly functioning system of bodies to jointly perform the functions of the Supervisory Authority should be developed. Such a system should include bodies with a clear division of functions between them. Accordingly, each body would implement one of the components of state (administrative) supervision in the fields of personal data and access to public information. Special units could be established within the relevant bodies for this purpose. Only rough proposals can be made on what functions might be implemented by this or that body.[1] This being said, one of such bodies could be the principal one in terms of organisational, human and technical resources (for instance, it could be the Ministry of Justice, in view of its nature, purposes, objectives and current powers). However, it could be possible to present final recommendations and define the final model only after the auditing, referred to in the previous paragraph, is over.
c. Within such "collective" Supervisory Authority, the main coordinator should be identified as a body, responsible for the making and implementation of the state policies in the fields of personal data and public information. Such a responsible body could be: 1) the Parliament Commissioner for Human Rights (as it is now, but with significantly amended and reduced functions); 2) a holder of a specially established office under the Cabinet of Ministers, i.e., the

[1]The following division of powers among the existing ministries could be preliminarily proposed as a presumptive speculation only:

- The Ministry of Digital Transformation of Ukraine: regulatory functions with regard to administrators of public registers and telecommunication systems where personal data is processed; authorisation of terms of references relating to the creation or renewal of public registers or telecommunication systems where personal data will be processed; implementation of public policies with regard to access to public information; approval of procedures for automated personal data processing in the area of public administration, etc.
- The Ministry of Justice: the expertise and legal regulation (by statutory instruments) of the implementation of the amended Law of Ukraine "On personal data protection" and international standards;
- The Ministry for Development of Economy, Trade and Agriculture: exercising regulatory powers with regard to the non-public area, i.e., the application of the Law "On protection of personal data", international standards and procedures by business entities and legal persons of private law;
- The Ministry for Communities and Territories Development: coordination of the application of standards and procedures in the fields of personal data and public information by local self-government authorities of all levels, etc. The Ministry of Digital Transformation of Ukraine: elaboration of standards with regard to databases, registers, automated personal data processing and public information disclosure, authorisation of standards relating to information infrastructure, etc.;
- The Ministry of Internal Affairs: operational supervision and information collection with regard to personal data, for example, through a specially established or an already existing unit (the Department for Cyber Police of the National Police of Ukraine).

authorised representative of the Government on relevant matters (following the example of the Government Agent before the European Court of Human Rights); 3) one of the heads of the central executive authorities (for example, the Minister of the Cabinet of Ministers, the Minister of Justice or other). Such a coordinator should possess broad enough powers to be able to seamlessly organise the performance of the whole personal data protection system. A special coordination council under the Cabinet of Ministers could be established as a collegial body to reinforce the coordinator's administrative impact, where the abovementioned official could be, for instance, a chair.

d. The broad range of guarantees for the independence of authorities (and special units) in performing supervision with regard to personal data and public information should be made regular by law (for example, by amending the Law of Ukraine "On personal data protection" and the Law of Ukraine "On access to public information"). It is very important to emphasise that the tools for guaranteeing such independence should correspond to the international standards provided for this purpose in Convention 108 and the Regulation 2016/679. Such guarantees should apply to the assumption of offices (appointments), service career, remuneration, grounds for dismissal and disciplinary liability, etc. It would obviously be very difficult to implement this element. However, there is already a legacy in Ukraine relating to establishing special units or special officials, or administrators of public information or controllers of personal data in every public authority, each of them possessing a number of additional guarantees in comparison to other employees.
e. The powers of each body in the system of the "collective" Supervisory Authority should be defined and very clearly apportioned. The law should exhaustively identify all the powers and procedures for decision-making and interaction. Such legislative provisions should be directly expanded by resolutions of the Cabinet of Ministers and other statutory instruments regulating the status of all the bodies involved and the principles of their performance. It would be appropriate to use the powers of supervisory authorities provided for in the Regulation (EU) 2016/679 as a reference point, upon which to build the distribution of powers in our case (Articles 57 and 58 of this Regulations identify clearly enough the main groups of tasks and the powers to perform them). Ambiguines and lack of clarity may cause incomprehension and significantly compromise the effectiveness of the whole system.
j. The system of units or officials dealing with personal data and public information should be established. Such a system should be adapted to international standards, in particular to the requirements of Convention 108 and the Regulation (EU) 2016/679. It is advisable to create a system of controllers and processors to be coordinated by the "collective" Supervisory Authority. A similar model exists in Ukraine in the area of prevention of corruption. According to the Law of Ukraine "On prevention of corruption", public authorities shall establish (appoint) units (persons) authorised to prevent and disclose corruption, with special legal regulation of their status and performance. It will be extremely difficult to effectively organise the work of the "collective" Supervisory Authority without the network of such "agents".
f. Clear indicators of performance transparency, external supervision and accountability should be provided. The procedures for internal mutual supervision are extremely important in the system of structurally separated bodies (units). However, of more importance is the development of instruments relating to parliamentary, judicial and civil supervision. It is advisable to provide for such level of transparency and liability, which would be even stricter than, for example, the one provided by the Regulation (EU) 2016/679, taking into consideration the complexity of this area of regulation and the risk of large-scale violations. Of course, these issues should be defined proceeding from the final model (the number of bodies, the principles of their performance, etc.) of the system of bodies of the "collective" Supervisory Authority.

The arguments in favour of such an approach:

- It would enable the authorities to perform their tasks in the areas of law and administrative areas immanent to them and combine their efforts with regard to personal data protection and access to public information. Each body would act within its constitutional and legal status. Such an approach may be regarded as inclusive. Indeed, it would allow for making use to the fullest extent of professionals serving within the machinery of government and to achieve key relevant objectives in a decentralised way.
- The establishment of such system of bodies will allow for lessening of the workload of the Parliament Commissioner for Human Rights and his or her Secretariat by ensuring for the Commissioner the opportunity to focus attention and administrative resources on other areas of parliamentary supervision of the observance of human rights.
- As the already existing authorities would exercise supervision with respect to personal data and public information, this model would require relatively few material and administrative resources and therefore could be implemented within the essentially shorter times than the previous two models.
- This system of bodies (units) would be functionally divided between different institutions and it would naturally diminish the risks of their falling under the political, administrative, financial or any other influence from any person or authority. This argument is especially valid in the current political and legal realities of Ukraine. The division of powers between different bodies with regard to the issuance of subsidiary acts, general monitoring, oversight in the non-public area (legal persons of private law and business) and initiating of bringing perpetrators to justice would allow for the creation of an internal mini-model of checks and balances in the areas of personal data and public information. Unfortunately, it is today one of the most efficient tools for actually enabling institutions to function independently of administrative and political influence.

The arguments against such an approach (risks):

- The functioning of the system of bodies acting as the "collective" Supervisory Authority and the procedures for their interaction should be as comprehensive and inclusive as possible. It would require much attention and administrative efforts. The search for an optimal balance in the situation where any administrative initiative or decision is politicised will be complicated enough and may not lead to the desired result.
- There are significant problems with the identification of the "collective" Supervisory Authority to be entrusted with the coordination of the state (administrative) supervision in the fields of personal data and access to public information.
- It would be much more difficult to administrate the system of bodies (units) rather than the single body. This would require an efficient enough management and the application of modern management technologies. However, even that factor may be neutralised by the heterogeneity of administrative procedures, low management discipline and the lack of diligence in various authorities.
- Low-quality distribution of powers between various bodies in the system of the "collective" Supervisory Authority may with the lapse of time cause incomprehension, certain competition and even conflicts with regard to exercising any given powers. Sure enough, this will not be conducive to exercising effective supervision in the fields of personal data and public information.
- The mechanism for the interaction with the Parliament Commissioner for Human Rights as the authority for the parliamentary supervision in the fields of personal data and access to public information would be complicated. If such a model of the Supervisory Authority in the fields of personal information and access to public information is introduced, then there would be a need to amend laws and identify additional procedures, grounds and

instruments of its interaction with the parliamentary supervisory authority and the levels of such interaction.

CONCLUSIONS AND RECOMMENDATIONS

This research of the national legislation, the practices of its implementation and the international practices with regard to the institutionalisation of state supervision in the fields of personal data and access to public information allows for the following conclusions and recommendations:

1. Currently, the institutionalisation and development of state supervision in the fields of personal data and access to public information in Ukraine are of high necessity and may be implemented on the basis of the provision of the legislative framework for any of the following three models:

- a separate Supervisory Authority which does not belong to any of the branches of government in Ukraine;
- a separate Supervisory Authority as an independent central executive authority;
- a "collective" Supervisory Authority as a system of (several) supervisory bodies.

2. The international obligations of Ukraine arising from its ratification of the Convention 108 and the Ukraine-EU Association Agreement imply directly the institutionalisation of the state (administrative) supervision in the fields of personal data and access to public information on the basis of one of the proposed models. This constitutes a key guarantee of observance of the rights of personal data subjects and public information requesters in terms of prevention of violation of their rights, elimination of the violations found and the implementation of the European human rights standards into the practice of controllers and processors of personal data and administrators of public information.

3. The institutionalisation of the Supervisory Authority should be exercised so that its sufficient independence and autonomy are guaranteed. With this in mind, it seems advisable that the collegial decision-making and the inter-institutional mechanism for the selection (appointment) of the head and the members of the Authority should serve as a basis for its legal status as an independent authority.

4. In the process of establishing the optimal Supervisory Authority model, the following issues should be necessarily regulated by a separate law or several laws: the legal status of this authority; procedures for its establishment and the election of its head (members); independence guarantees, including financing and modes of supervision of other entities; the substance of its competence; the relationship between its regulatory and supervisory powers; the arrangements for the separation of its supervisory powers from the parliamentary and judicial supervision in the fields of personal data protection and access to public information; conferral of rule-making powers; the procedures for cooperation with the relevant Council of Europe bodies; the procedures for its internal organisation and structuring.

5. If the first or the second supervisory authority model is chosen out of those studied, their heads/members should comply with the specially established requirements as to their professional competency and past performance and their nomination procedure should be regulated in detail by separate laws to provide for the fairness and impartiality of their performance.

6. It is important to provide at the legislative level that the duration of the term of the head/members of the Supervisory Authority does not coincide with the beginning and duration of terms of the authorities directly involved in their election (nomination). Such duration of the term of the Supervisory authority should be defined with reasonable substantiation to additionally ensure its political independence.

7. In the same vein as Articles 52 and 53 of the Regulation (EU) 2016/679 provide for the standards of the independence of supervisory authorities as autonomous bodies, it seems advisable to introduce into the national legislation of Ukraine the system of guarantees for the head/members of such authority against unlawful influence on their performance, including the risks related to unsubstantiated dismissal or disciplinary liability.

8. Amending the current Laws "On access to public information" and "On personal data protection" seems to be the most reasonable legal basis for the performance of the Supervisory Authority. At the same time, amendments to the Constitution of Ukraine could be acceptable only in the absence of any other means to regulate the procedures for the institutionalization of the Supervisory Authority.

9. If any of the models being the subject of this legal analysis is selected for the institutionalisation of the Supervisory Authority, the law should provide for the broad, consistent and efficient interaction of this new authority with the institutions (members of the civil society) involved in the civil supervision of the observance of the law in the areas of personal data protection and access to public information. Such guarantees could be of financial, procedural or jurisdictional, etc., nature. However, they in any case should be permanent and real, and the state should provide for the high standards of their implementation.

THE LEGAL BASIS FOR THE ANALYSIS

1) 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). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058 , accessed 9 April 2020.
2) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136 , accessed 7 April 2020.
3) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Strasbourg, 8.XI.2001 URL: www.conventions.coe.int/treaty/en/Treaties/Html/181.htm , accessed 2 April 2020.
4) Human rights guidelines for Internet service providers developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA). URL: https://rm.coe.int/1680599368 , accessed 1 April 2020;
5) The Code of Ukraine on Administrative Offences dated 7 December 1984, last updated on 1 April 2020. URL: https://zakon.rada.gov.ua/laws/show/80731-10 , accessed 29 September 2019;
6) Convention for the Protection of Human Rights and Fundamental Freedoms of 4.XI.1950 URL: https://zakon.rada.gov.ua/laws/show/995_004 , accessed 1 April 2020;
7) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28.01.1981, https://zakon.rada.gov.ua/laws/show/994_326, accessed 1 April 2020.
8) Constitution of Ukraine dated 28 June 1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр , accessed 1 April 2020;
9) Recommendation No. R (81) 19 of the Committee of Ministers to member states on the access to information held by public authorities adopted on 25 November 1981. URL: https://cedem.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv/ , accessed 1 April 2020;
10) Recommendation Rec (2002)2 of the Committee of Ministers to member states on access to official documents adopted on 21 February 2002. URL: http://zakon2.rada.gov.ua/laws/show/994_a33 , accessed 1 April 2020;
11) Law of Ukraine "On access to public information" dated 13 January 2011, No. 2939-VI, last updated on 1 May 2015. URL: https://zakon.rada.gov.ua/laws/show/2939-17 , accessed 1 April 2020;
12) Law of Ukraine "On personal data protection" dated 1 June 2010, No. 2297-VI, last updated on 30 January 2018. URL: https://zakon.rada.gov.ua/laws/show/2297-17 , accessed 1 April 2020;
13) Law of Ukraine "On information", dated 2 October 1992, No. 2657-XII, last updated 16 July 2019. URL: https://zakon.rada.gov.ua/laws/show/2657-12 , accessed 1 April 2020;
14) Law of Ukraine "On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of

Personal Data regarding supervisory authorities and transborder data flows" dated 6 July 2010, No. 2438-VI; https://zakon.rada.gov.ua/laws/show/2438-17 , accessed 1 April 2020;
15) Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" dated 23 December 1997 No. 776/97-BP, last updated 4 November 2018. URL: https://zakon5.rada.gov.ua/laws/show/776/97-вр , accessed 1 April 2020;
16) 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). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 , accessed 1 April 2020.
17) Recommendation CM/Rec (2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (Adopted by the Committee of Ministers on 13 January 2016, at the 1244th meeting of the Ministers' Deputies). URL: http://nkrzi.gov.ua/images/upload/58/19/Recomendation_KM_RE_2016.doc , accessed 1 April 2020;
18) Recommendation CM/Rec (2016)5[1] of the Committee of Ministers to member States on Internet freedom (Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies) URL: https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)5 , accessed 1 April 2020.
19) Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part, 27 June 2014. URL: https://zakon.rada.gov.ua/laws/show/984_011 , accessed 1 April 2020.