sciendo

Data Protection in Ukraine and in the Czech Republic, a few Remarks on the Data Protection Authority

Olha Shpakovych[*]
Oleksandr Shevchuk[**]
Petra Melotíková[***]

Summary: Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) establishes the obligation for states to designate a supervisory authority to oversee compliance with the rules set out therein. The obligation to designate a supervisory authority is also enshrined in other legislation at the international level and at the constitutional level. The article focuses on the aspect of embedding it in legislation and its status as an independent administrative authority.

Keywords: GDPR, personal data, supervisory authority, Office for Personal Data Protection

Citation: SHPAKOVYCH, O., SHEVCHUK, O., MELOTÍKOVÁ, P. Data Protection in Ukraine and in the Czech Republic, a few Remarks on the Data Protection Authority. *European Studies – the Review of European law, Economics and Politics.* 2023, vol. 10, no. 2, pp. 221–245, DOI: 10.2478/eustu-2023-0019.

Acknowledgement: This paper was written with the support of the project "CODE – COoperation and DEvelopment" (reg. no. 23-PKVV-UM-6) financed by the Ministry of Foreign Affairs of the Czech Republic within the framework of development cooperation abroad.

[*] Doctor of Jur. Sciences (Dr.hab), Professor of the chair of comparative and Europen law of the Taras Shevchenko National University of Kyiv, Educational and Scientific Institute of International Relations.

[**] PhD in Law assistant of the chair of international law of the Taras Shevchenko National University of Kyiv, Educational and Scientific Institute of International Relations.

[***] Senior lecturer, Palacky University Olomouc, The Faculty of Law. Contact: petra.melotikova@upol.cz.

1. Introduction

In the 21st century, the rapid development of information technologies and the constant growth of the scale of personal data transfer and processing are placing particular emphasis on the personal data protection and the right to privacy.

Cross-border data transfer and processing have brought tangible benefits to everyday life: search engines facilitate access to vast amounts of information, social media services enable people around the world to communicate, express their opinions and mobilize support on social, environmental and political issues, and companies and consumers receive benefit from effective marketing tools in sectors such as insurance, healthcare, etc. However, the boost of information technologies over the past two decades has posed new challenges for the personal data protection.

Our society is becoming ever more digitised. The pace of technological developments and how personal data are being processed affects each of us every day and in all sorts of ways in the light of these changes. Indeed, every person should have at their disposal mechanisms to protect their private information. In order to enable individuals to control their information and protect it from misuse, data protection laws at the institutional level should regulate the activities of private and public companies regarding the security of personal data protection during its transmission and processing.

The Internet has made it easier to access information, by visiting a website or purchasing goods and services from a website, organizations collect vast amounts of data about individuals. Companies collect name and address information to track web browser behaviour, location, and other information that enables companies to identify a person. Such data is then used by companies for a variety of purposes, ranging from sales and customer relationship management to marketing campaigns. The availability of data collection means that thousands of companies not only collect personal data, but also store it in secure locations, share it with third parties, or move that data across borders to support their business. Furthermore, their business models rely on selling access to this data to advertisers.

The protection of personal data is now commonly understood as an integral part of the right to the protection of personal privacy. The public law protection of personal data is linked to the common practice in democratic states, where there is a separate independent authority with oversight of this 'sub-area' of privacy protection, which has the ability to apply remedies or carry out checks on entities processing personal data. The concept of an independent supervisory authority is not to be found in the Council of Europe *resolutions* on data

protection,[1] this approach is more related to the tendencies in modern public administration, which instead of being closed is guided by the principle of openness of public administration and is put in the context of the rapid development of technology towards the end of the second millennium, but also the restructuring of the relationship between the public and private sectors.

The aim of this article is therefore to highlight the rationale for the existence of an independent supervisory authority, to point out how its independent status is enshrined in effective legislation both in Ukraine and in the Czech Republic, and to discuss the key aspects and guarantees of its independence.

2. Data Protection System in the Czech Republic

2.1. Introductory remarks

At the level of the constitutional order, the foundations of the protection of personal data are enshrined in Article 7(1) of Act No. 2/1993 Coll., the Charter of Fundamental Rights and Freedoms; according to this provision, "the inviolability of the person and his privacy is guaranteed. It may be restricted only in cases provided for by law". Article 10 of the Charter, which is a kind of basis for the protection of privacy in a broad sense, provides that "(1) Everyone has the right to have his human dignity, personal honour, reputation and name preserved. (2) Everyone has the right to protection from unwarranted interference with his private and family life. (3) Everyone has the right to protection against the unauthorized collection, disclosure or other misuse of personal data."

The Council of Europe, which has always been proactive on data protection, also plays an important role in data protection. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108"), came into force on 1 October 1985, the Czech Republic signed Convention 108 on 8 September 2000, and after the ratification process it entered into force for the Czech Republic on 1 November 2001. This document has succeeded in defining, first of all, the basic concepts in the field of personal data protection – personal data, data subject, automated data set, automated processing and data controller. To date, it has already been supplemented by Additional Protocols.

The Czech Republic as a member state of European Union is interested in all of the steps that lead to more effective data protection policy. In the field of

[1] Resolution (73) 22 on the protection of privacy of individuals vis-a-vis electronic databanks in the private sector or e.g. Resolution (74) 29 on the protection of privacy of individuals vis-a-vis electronic databanks in the public sector.

primary EU law, the basis for the protection of personal data is, firstly, Article 16 of the Treaty on the Functioning of the European Union (TFEU), which constitutes a primary right and guarantees the right of everyone to the protection of personal data concerning them. Furthermore, Article 8 of the EU Charter of Fundamental Rights, which in particular enshrines the obligation to process personal data fairly, purposefully and with the consent of the data subject, while guaranteeing access to the data collected, including rectification, is at the level of a fundamental right in EU law. Furthermore, Article 7 of the EU Charter of Fundamental Rights guarantees respect for private and family life. Originally a purely political declaration, it became legally binding on 1 December 2009, when the Lisbon Treaty entered into force, Article 6(1) incorporating the EU Charter of Fundamental Rights by reference into primary EU law. The adoption of Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), which became effective on 25 May 2018. GDPR is a solution to ensure a more uniform standard of protection of personal data across the European Union, providing a general basis that is already further developed at the European level and in individual national arrangements supplemented and expanded by specific legislation such as "anti-money laundering rules."[2]

Furthermore, the Czech Republic has adopted the Adaptation Act No. 110/2019 Coll. As Machová points out, "it completes the entire legal framework and contains both permitted derogations and special adaptations to the GDPR."[3]

2.2. On the existence of independent supervisory authorities in general

Although the existence of independent supervisory authorities is now often taken as an unexamined fact, this concept was not always common. As Pouperova points out in her detailed analysis of their status,[4] their emergence is linked to the political situation in the United States, when in 1889 the Interstate Commerce Commission, not subordinate to the President, was created, designated as an

[2] KASL, F. Internet věcí a ochrana dat v evropském kontextu. *Revue pro právo a technologie*. 2016, no. 13, p. 126.

[3] MACHOVÁ, M. Zákon o zpracování osobních údajů – prováděcí úprava k GDPR z pohledu českého zákonodárce. *E-pravo*. 27. 6. 2019. [online] Available at: https://www.epravo.cz/top/clanky/zakon-o-zpracovani-osobnich-udaju-provadeci-uprava-k-GDPR-z-pohledu-ceskeho-zakonodarce-109542.html.

[4] For more on the establishment of the first independent supervisory bodies, see. POUPEROVÁ, O. Nezávislé správní úřady. *Správní parvo.* 2014, vol. 47, no. 4, pp. 209–226.

independent administrative agency, and even then there was an effort to remove a certain type of oversight from the direct influence of the chief executive.

The requirement for the independence of certain supervisory authorities is today most often justified by (a) the need to regulate a particular atypical area of the economy, or (b) the desire for a sensitive approach to potentially conflicting issues that are likely to cause uproar and concern in broad sections of society. This demand for independence is thus a reflection of the desire to deal apolitically with a certain range of issues which will therefore not fall under the direct influence of political groups and the top executive.

This independence is built on several complementary pillars. Thus, we can most often speak of personal independence (related to the appointment of the head and members of the body, including the conditions of remuneration and the conditions of removal from office), functional independence (consisting in independence from the government, but also in the absence of the element of a superior body) and financial independence (related to the ability of the supervisory body to dispose of financial resources or have sufficient material security for the exercise of its powers), some authors are inclined to the even broader concept of political and functional independence,[5] or political and economic independence.[6]

2.3. Legal regulation connected with supervisory authorities

The basis for the independent status of the supervisory authority can be found in the Convention 108, which entered into force on 1 October 1985 and has been binding on the Czech Republic since 1 November 2001. In its Article 13 'Cooperation between the Contracting Parties', the Convention enshrines the obligation of each Contracting Party to Convention 108 to designate one or more authorities ('authorities') to provide mutual assistance between the Contracting States. Such an authority is then to provide information on its State's law and administrative practice in the protection of personal data and "shall take...appropriate measures to provide specific information on certain automated processing...". Further, under Article 14 of Convention 108, the obligation to assist a person of another State was enshrined in the sense that the authority was to be obliged to receive a request for assistance to be transmitted to the competent authority in the applicant's country, and it could only do so at the request of the person and not on its own initiative or without the person's consent. The refusal of such a request is

[5] HANDRLICA, J. Nezávislé regulačné orgány (?) *Justičná revue.* 2008, vol. 60, no. 2, pp. 165–187.

[6] The concept of mere economic independence was the original concept promoted by the EU. POUPEROVÁ, O. Nezávislé správní úřady. *Správní parvo*. 2014, vol. 47, no. 4, pp. 209–226.

possible only on three enumerated grounds set out in Article 16 of Convention No. 108. The implementation of Convention No 108 in the Czech Republic was achieved by the adoption of the now ineffective Act No 101/2000 Coll., on the Protection of Personal Data.[7] Convention No 108 was further supplemented by an Additional Protocol, which contained clarifications on the functioning of supervisory authorities.[8] As reported by Nonnemann[9] on the changes to the legal regulation of supervisory authorities, it *introduces in particular the obligation for supervisory authorities to approve instruments for the transfer of personal data to third countries, to have the possibility to participate in the legislative process and to comment on any draft legislation relating to the processing of personal data*.

Convention 108 has been subjected to detailed scrutiny by a Council of Europe working group in recent years and the Council of Europe has finally presented a new text which is open for signature by Member States, but the new version does not significantly shift the meaning of the independence of the supervisory authority, but the proposed changes relate mainly to the scope of its competence.[10] In May 2018, the Council of Europe adopted CETS Protocol No. 223, thus amending Convention 108. The modernised Convention 108+ takes into account most of the challenges posed by the development of information and communication technologies and strengthens the requirements for its implementation.

Another key provision for the position of the supervisory authority in the field of personal data protection is the wording of Article 8 of the Charter of Fundamental Rights of the European Union[11] , which enshrines, inter alia, the right to the protection of personal data, their fair, efficient processing and "... compliance with these rules shall be supervised by an independent authority".

---

[7] The Treaty was signed on 8 September 2000 and, following the ratification process, entered into force on 1 November 2001.

[8] It entered into force for the Czech Republic on 1 July 2004.

[9] NONNEMANN, F. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. *Epravo.cz*, 30. 9. 2022. [online] Available at: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html.

[10] The new text of Convention 108 can be found here: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf. There are several proposed changes to the competence of supervisory authorities which cannot be described as partial and insignificant, such as the obligation for States to ensure that the supervisory authority can rule on breaches of the rules on the processing of personal data, or the possibility to comment on the text of all legislation relating to the protection of personal data.

[11] Charter of Fundamental Rights of the European Union 2012/C 326/02. The provisions of Article 8 built on Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Article 8 of the European Convention, which was in force at the time.

Similarly, under the later version of Article 16 of the Treaty on the Functioning of the European Union[12] , the protection of personal data is guaranteed and the European Parliament and the Council are required to adopt rules on the protection of natural persons with regard to processing by the institutions, bodies, offices and agencies of the Union, and it is further provided that "compliance with the rules shall be subject to control by independent authorities ('independent authorities')."

It is interesting to observe the shift in the view of the status of such authorities, where the element of "independence" was not initially included in Convention 108 and it was left to the will of the States as to which authority would be involved or to which authority the duty in question would be entrusted.

Act No. 1/1993 Coll., the Constitution of the Czech Republic, does not directly establish a similar independent authority, while Act No. 2/1993 Coll., the Charter of Fundamental Rights and Freedoms, contains in the provisions of Article 7, Article 10(3) and Article 13 the establishment of rights related to the protection of personal data, but it also does not contain an obligation to designate an *independent supervisory or contact authority*.[13]

Therefore, the key legislation for more precisely anchoring the position and competence of the supervisory authority is the regulation represented by Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[14], where the GDPR is directly applicable legislation in accordance with the provisions of Article 10, the Constitution of the Czech Republic.[15] The wording of Article 4(21) GDPR in combination with

[12] Treaty on the Functioning of The European Union.

[13] For the sake of completeness, let us add that the interference with a person's privacy is, from a private law point of view, dealt with in more detail in Act No. 89/2016 Coll., the Civil Code, the provisions of Sections 81-90.

[14] Regulation 2016/659 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, hereinafter referred to as "GDPR." The GDPR builds on the protection of personal data represented by a number of Council of Europe resolutions, Convention 108 and, within the European Union, develops ideas from Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Compared to this Directive, the main advantage of the GDPR lies in its direct applicability in the Member States. In particular, the GDPR develops the idea of independence in relation to supervisory authorities, modifies certain offences and sets a uniform rate of fines, introduces the idea of full unification of supervision and newly (leaving aside the partial modification in Convention 108) introduces a single point of contact for data subjects.

[15] The previous legislation in the field of the European Union's competence was in particular Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which

Article 51 GDPR shows us that the perception of the position, scope and powers of supervisory authorities is different from, or much more precise than, the Resolutions and Convention 108. Indeed, Article 4(21) GDPR explicitly refers to the supervisory authority as "an independent public authority established by a Member State." Chapter VI of the GDPR then sets out the basic points relating to the status of supervisory authorities in the Member States, enshrining the basic guarantees of their independence and the limits of cooperation between supervisory authorities. [16]

This independence is further elaborated in Article 52 GDPR. Its wording combines a number of guarantees of independence in the personal, functional and financial sense and also emphasises economic independence in the sense of independence of members from other economic operators. As regards the functional independence of the decision-making of the members of the Authority in matters of its specified competence, the GDPR tells us in particular in Article 52(1) that the supervisory authority "... shall act with complete independence" and in (2) that "... the members of each supervisory authority shall, in the performance of their tasks and the exercise of their powers under this Regulation, remain independent of outside influence, direct or indirect, and shall not seek or receive instructions from anyone." The personnel component of independence is particularly relevant to Article 52(5), whereby the supervisory authority should be able to "... select and have its own staff subject to the sole direction of a member or members of that supervisory authority." The emphasis on financial independence (in conjunction with economic independence) is represented by Art. 52(3), where the members "shall not engage in any gainful or unprofitable employment incompatible with that function", (4), where the supervisory authority is to be "provided with the human, technical and financial resources, premises and infrastructure it will need for the effective performance of its tasks and the exercise of its powers", and (6), where the supervisory authority is to have ".. .a separate public annual budget,

already clarifies the concept of supervisory authority and provides in Article 28 for the Member States to entrust "...one or more public authorities... with the supervision of compliance with the provisions adopted by the Member States pursuant to this Directive. These authorities shall carry out their tasks...in complete independence." It also set out the minimum remit of supervisory authorities, and emphasised the obligation to cooperate with supervisory authorities in other Member States. However, after many years, the form of the "directive" proved inadequate, and the GDPR, a regulation with direct applicability to the territory of the Member States, was then drafted.

[16] Article 57 of the GDPR broadly sets out the powers of supervisory authorities, including, among others, cooperation with supervisory authorities, raising public awareness of the handling of personal data. In order to exercise its competence, the supervisory authority is endowed with a number of powers, which the GDPR divides into investigative, remedial, authorising and advisory powers (Article 58 GDPR), this list is intended as a minimum range of powers that may be extended in individual legal arrangements according to local circumstances.

which may be part of the overall ... State budget." Article 53 GDPR then sets out a set of conditions that a member of the supervisory authority must fulfil, including both basic, moral and professional conditions[17] and is thus another of the guarantees of the independent status of the staff of the supervisory authority, whereby the member must be appointed in a transparent manner, have the professional qualifications to perform the duties and exercise the powers, and there is a limited possibility of termination of his or her term of office. In this respect, the GDPR therefore distinguishes 'ordinary' staff of the Authority from 'members' and places higher demands on them or their independence.

Given the considerable breadth of the issue and taking into account the established practice in a given country, the GDPR also foresees in Article 60 that a State may, at its discretion, set up several supervisory authorities, presumably with the assumption of different competences or taking into account the specificity of certain personal data (the question of a special supervisory authority for e.g. an area related to classified information or business secrets). For the latter case, the GDPR then provides for the obligation of the State to designate one lead supervisory authority and sets out the procedure for the other supervisory authorities concerned to proceed with their decisions.[18]

Finally, the protection of personal data is also guaranteed by the implementing law to the GDPR, Act No. 110/2019 Coll., on the processing of personal data (hereinafter as Act on Personal Data).[19] Section 2 of the Act on Personal Data sets out its scope of competence,[20] and the key wording for the position of the

[17] For example, PATTYNOVÁ, J. et al. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář.* 2. edition. Praha: Leges, 2019, p. 375.

[18] As a certain guarantee of uniformity of decision-making and in order to respect the principle of lawfulness and uniformity, the GDPR enshrines in Article 68 the creation of the European Data Protection Board. Its position is conceived as fully independent and, of course, given the nature of decision-making in the European Union, each Member State is represented on the Board by one member – the head of the supervisory authority of the Member State, and the European Data Protection Supervisor or their designated representatives. In view of the scope of the subject matter, we will not deal with this topic in detail in this article.

[19] The Act transposed, inter alia, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data and repealing Council Framework Decision 2008/977/JHA.

[20] In the Czech society, as in other countries, the competence of the OPDP is also enshrined in a number of special legal regulations, especially in relation to the internal administration, and these special regulations are not entirely related to the above-mentioned issue of the status of the OPDP as a supervisory authority; they can be systematically divided into three areas. The first and essential area for the OIOA is the protection of personal data as provided primarily in the GDPR and the Act on the OA. The second category represents the areas where the OPDP is obliged to participate in co-operative actions with regard to the obligation so enshrined for it

supervisory authority is point, which states that it regulates "the position and competence of the Office for Personal Data Protection (hereinafter OPDP)," which is thus the supervisory authority for the Czech Republic in accordance with the GDPR. According to Article 50 of Act on Personal Data, it is the "central administrative authority for the protection of personal data" (it is referred to as a "central administrative authority" in Article 2 of Act No. 2/1969 Coll., the Competence Act). The Competence Act enshrines a number of guarantees of independence in line with the trend and binding wording of the GDPR. Article 51(1) of Act on Personal Data provides that the competence of the OPDP may only be interfered with by law, and it also explicitly refers to an *independent procedure,* where the OPDP "shall act independently and shall be guided only by the law and directly applicable regulations of the European Union".

Furthermore, the provision of Article 51(2) Act on Personal Data states that its activities are paid for from a separate chapter of the State budget (one of the guarantees of financial independence). With regard to functional and personal independence, we must emphasise the wording of Article 51(3) of the Act on the Civil Service, which explicitly states that 'the Deputy Minister of the Interior for the Civil Service is not a superior official to the President of the OPDP. No appeal shall be admissible against the decision of the President of the OPDP in a civil service matter or against the decision of the disciplinary committee of first instance established in the OPDP." This is consistent with the approach set out in GDPR, whereby some authors, given the wording of Article 52 of the GDPR, lacked in the original draft of the Act on Personal Data.[21] For the Chairperson and Vice-Chairpersons of the OPDP, almost identical conditions for their appointment apply, as set out in Article 52(3) of the Act on Personal Data[22] – the guarantee of personal independence is certainly the enshrinement of the possibility of their

in specific laws, although it should be added that in these cases the co-operation is also closely related to the protection of personal data, e.g. for the receipt of a notification on the creation of an information database on the creditworthiness and trustworthiness of a consumer pursuant to Section 20z(12) of Act No. 634/1992 Coll., on Consumer Protection. The third area is the range of matters related to electronic communication, e.g. the competence in the area of supervision of the dissemination of commercial communications pursuant to Act No 480/2004 Coll., on certain information society services.

[21] Cf. NULÍČEK, M. et al: *GDRP Obecné nařízení o ochraně osobních údajů*. 2. editon. Praha: Wolters Kluwer, 2018, p. 441.

[22] "Only a citizen of the Czech Republic who (a) is fully capable of exercising his/her legal capacity may be appointed as the Chairman of the OPDP,

(b) he or she has reached the age of 40 years, (c) he or she is of good repute, fulfils the conditions laid down in other legislation and possesses the knowledge, experience and moral character required for the proper performance of his or her duties, and (d) he or she has obtained a university degree by completing a master's degree programme in law or computer science, has the necessary level of knowledge of English, German or French and has at least 5 years'

removal only if they no longer meet any of the conditions for appointment.[23] But here the question arises whether, in the event of e.g. political pressure for the resignation of the chairman, the condition in Article 52(3)(c), i.e. what "...moral qualities" the chairman should possess, is not too broadly conceived and whether it can thus provide a guarantee of independence and adequate exercise of the powers conferred on him.[24] Only the Chairperson and Vice-Chairperson of the OCCP are subject to the GDPR's provisions on independence and the staffing and appointment of "members" of the supervisory authority.

We can summarize that the independence of the OPDP is therefore could be seen in its *functional independence*, which means that the OPDP is not subordinate to any other authority and carries out the tasks assigned to it on the basis of by law, and at the same time only within the limits of that legislation. *The material independence* is reflected in the fact that the budget of the OPDP forms a separate chapter of the State budget and is approved by the Chamber of Deputies. *Personnel independence* is connected with the fact that the Director of the OPDP is not subordinate to the Minister.

2.4. On the independent position of the Office for Personal Data Protection

If the existence of independent supervisory authorities in certain segments of the economy cannot be accepted without reservations, the question of whether the existence of an independent administrative authority is possible in the Czech legal environment comes to the forefront of the discussion, and this question is not fully resolved in the professional community. It can be stated that the Czech supervisory authority for personal data protection is most commonly referred to as an *independent administrative authority*, although some authors have reservations about this designation.[25] Hendrych agrees that the key competence in the field of personal data protection is provided by an independent

experience in the field of personal data protection or human rights and fundamental freedoms; a different course of study may be admissible if he or she has more than 10 years' experience."

[23] The Court of Justice of the European Union has also commented on the question of the termination of the mandate on several occasions, see, for example, the judgment in European Commission v. Hungary, C-288/12, paragraphs 53 and 54, where even the termination of the mandate due to the reorganisation of the Office is not admissible and is incompatible with the requirement of the independence of the Office.

[24] Cf. PATTYNOVÁ, J. et al. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář.* 2. edition. Praha: Leges, 2019, pp. 680–681.

[25] The question of whether an administrative authority can be independent is debated, even though the immanent characteristic of an administrative authority is supposed to be the opposite of independence, and in terms of hierarchy, the government is the head of the authority in accordance

OPDP, which has powers *typical of a central administrative authority*.[26] If we follow Sládeček's breakdown[27] into *absolutely independent* and relatively independent administrative authorities, the OPDP falls into the former category. From the diction of the provisions of Article 50 of the Act on Personal Data it follows that it is a "central administrative authority", from Section 2 of the Act No. 2/1969 Coll., the Competence Act, it follows that it is a "central authority of the state administration." Thus, as an *administrative authority, it* should not be independent but subordinate to the Government as the supreme executive. However, Article 51(1) of the Act on Personal Data adds that its activities may "be interfered with only on the basis of the law, it shall act independently in the exercise of its powers and shall be governed only by the laws and directly applicable regulations of the European Union." Is this independence enshrined in the legislation not therefore in breach of Article 79(1) of Act No. 1/1993 Coll. the Constitution (as well as the relationship of the OPDP to the Government as the supreme executive body enshrined in Article 67(1) of Act No. 1/1993 Coll., the Constitution) Pouperova judges,[28] also with regard to selected provisions of the Constitutional Court's ruling,[29] that the concept of independent administrative authorities will be constitutionally compliant only if fundamental rights are protected or with regard to the obligation to establish a supervisory authority enshrined in EU law. To find constitutional compliance, Sládeček then proposes as a solution the adoption of a new wording of Article 79(2) which reads: "... the OPDP are administrative authorities established by law, which are not subordinate to the government. The law may provide that certain other administrative authorities may be partially or wholly exempted from subordination to the Government." [30]

with Article 67 of the Constitution. For more details see. POUPEROVÁ, O. Nezávislé správní úřady. *Správní parvo.* 2014, vol. 47, no. 4, p. 215.

[26] HENDRYCH, D. *Právnický slovník*. 3. editon. Praha: C. H. Beck, 2009, p. 985.

[27] SLÁDEČEK, V. *Obecné správní právo*. 4. edition. Praha: Leges, 2019, p. 287. Sládeček thus divides relatively independent administrative authorities, i.e. mainly other central administrative authorities, which are granted independent status by special laws, and fully independent administrative authorities, whose independence directly results from special legislation.

[28] POUPEROVÁ, O. Zřizování nezávislých správních úřadů jako způsob řešení nestabilní politiky. *Právna politika a legislatíva – Vplyv politky,normotvorby a súdnej judikatúry na výkon verejnej správy.* Bratislava: Wolters Kluwer, 2020, p. 194.

[29] Constitutional Court ruling Pl. ÚS 21/14 of 30 June 2015.

[30] SLÁDEČEK, V. *Obecné správní právo*. 4. editon. Praha: Leges, 2019, p. 294.

3. Data Protection System of Ukraine

3.1. Introductory remarks

Currently, technological development is significantly ahead of legislation in Ukraine. At the same time, outdated legislation slows down and creates obstacles in the implementation of innovative solutions both in the private sector (for example, IT) and in the public sector (e-democracy, digitization of administrative services).

Legal frameworks of the European Union (EU) and the Council of Europe that safeguard the protection of privacy and personal data is at the forefront of data protection worldwide. The EU's data protection standards are based on Council of Europe Modernised Convention 108+ and GDPR. The General Data Protection Regulation (GDPR) is considered as the most effective and clearly compiled legal act which regulates privacy and security law in the European Union (EU).

Ukraine is a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). In May 2018, the Council of Europe adopted CETS Protocol No. 223, thus amending Convention 108. Thus, Ukraine faced the issue of ratifying the specified Protocol and bringing the legislation into compliance with the requirements of the updated Convention 108+.

The topic of personal data protection is of particular importance for Ukraine. The Association Agreement between Ukraine and the European Union requires bringing the legislation of Ukraine in line with European standards, which also applies to personal data protection. One of the key tasks of Ukraine is harmonisation of Ukrainian legislation to European standards in the field of personal data protection through the implementation of the Regulation (EU) 2016/679 GDPR in accordance with paragraph 11 of the Action Plan No. 1106 for the implementation of the Association Agreement approved by the Cabinet of Ministers of Ukraine dated October 25, 2017.

The main issues of the reform of national data protection legislation are: clarification of the duties and responsibilities of data controllers and data processors; improvement of the concept of data protection by design and data protection by default; appointment of a person responsible for personal data protection; development of the notification system regarding personal data breaches; and establishment of the independent supervisory authority in the area of personal data protection.

3.2. Development of Personal Data Protection

An important step in the development of personal data protection was the adoption of the Constitution of Ukraine in 1996. Article 32 of the Constitution states that "no one may be interfered with in his personal and family life, except in cases provided for by the Constitution of Ukraine. The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except as provided by law, and only in the interests of national security, economic welfare and human rights." These provisions became the basis for the further development of data protection in Ukraine.

In June 2010, the Verkhovna Rada of Ukraine has passed the Law "On Protection of Personal Data", which has become a fundamental act of the national legislation on personal data protection. The entry into force of this Law became an important precondition for the ratification of the Council of Europe Convention No. 108 and the Additional Protocol thereto in Ukraine. Following the ratification of the Council of Europe Convention No. 108, Ukraine undertakes to adhere to the principles and standards of the Council of Europe on the processing and transfer of personal data.

On April 6, 2011, the Regulations on the State Service for Personal Data Protection were approved by the Decree of the President of Ukraine. The main functions of the State Service for Personal Data Protection included the implementation of state policy in the field of personal data protection, as well as the supervision and control over the compliance with laws on personal data protection. The Cabinet of Ministers of Ukraine coordinated the activities of the State Service for Personal Data Protection through the Ministry of Justice of Ukraine.

In order to improve the institutional mechanism of personal data protection, the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Improving the Personal Data Protection System" No. 383-VII was adopted on July 3, 2013 which liquidated the State Service for Personal Data Protection and delegated the powers to exercise the regulatory oversight to the Commissioner for Human Rights of the Verkhovna Rada of Ukraine. The Department for Personal Data Protection was established within the structure of the Commissioner. These changes are aimed at bringing Ukrainian laws in line with the European Union standards by establishing an independent supervisory authority for personal data protection.

It should be noted that up to time at the Ukrainian parliament was registered two draft laws № 8153[31] and № 6177[32]. These draft laws play an important role in the process of Ukraine's integration into the EU Digital Single Market.

[31] Draft Law of Ukraine "On Personal Data Protection"

[32] Draft Law of Ukraine "On the National Commission for Personal Data Protection and Access to Public Information"

According to Ms. Liliia Oleksiuk, Non-Staff Consultant of the Verkhovna Rada Committee on Digital Transformation, draft law № 8153 "On Personal Data Protection" aims to renew the outdated national legislation in this area. The draft law has been developed closely to GDPR, which is applied in all 27 countries of the European Union. But for the successful integration, Ukraine is also required to create an independent regulator in the field of personal data protection in addition to updating the respective legal framework. This issue is regulated by draft law № 6177 "On the National Commission for Personal Data Protection and Access to Public Information".[33]

3.3. International legal obligations of Ukraine in the area of personal data protection

The key component of Ukraine's cooperation with the European Union and its member states is the process of our country's regulatory approximation to the EU acquis.

Consideration of this issue becomes especially important in the context of the need to adapt the Ukrainian laws to the laws of the European Union in accordance with Ukraine's obligations under the Association Agreement.

Section III of the Association Agreement provides for cooperation in the field of justice, freedom and security. According to the Article 15 of the Association Agreement, "Ukraine and the European Union have agreed to cooperate in order to ensure an adequate level of personal data protection in accordance with the highest European and international standards, including relevant Council of Europe documents."

In addition, according to the Article 129 of the Association Agreement, "Ukraine and the European Union shall take appropriate special measures to protect the right to privacy and fundamental rights and freedoms, for example in connection with the transfer of personal information."

Paragraph 11 of the action plan No. 1106 on the implementation of the Association Agreement provides for the task of improving the personal data protection legislation in order to bring it into line with the Regulation 2016/679.

In November 2019, the Cabinet of Ministers of Ukraine adopted a resolution № 1005 amending the Action Plan № 1106 on Implementation of the Association Agreement between Ukraine and the EU. For the moment, Ukraine shall improve legislation on personal data protection to bring into line with the Regulation (EU) 2016/679 (General Data Protection Regulation) till May 25, 2020.

[33] EBA Ukraine. Interview with Liliia Oleksiuk. GDPR implementation in Ukraine is expected for 2023–2024. [online]. Available at: https://eba.com.ua/en/vprovadzhennya-gdpr-ochikuyetsya-v-2023-2024-rokah/.

In accordance with the Strategy for the Integration of Ukraine into the Single Digital Market of the European Union ("Road Map"), which was recently agreed with the EU, the legislative consolidation of the right to the protection of personal data among the basic rights and freedoms of natural persons, as well as the provision on the free movement of personal data, bringing the compliance with the EU law of the principles of personal data processing and terminology should take place by December 2023.

According to the representative of the Ombudsman of Ukraine for Information Rights Yuliia Derkachenko, it is the reform of the legislation on personal data protection and the creation of a new supervisory authority that is an essential step for Ukraine on the way to joining the Modernized Convention 108 +. "After the reform in the field of personal data protection begins in Ukraine, our country will be able to start the process of joining the Modernized Convention 108 + and finally sign the relevant protocol. Therefore, the implementation of this reform will enable our state to fulfill both international obligations in the field of personal data protection, and in general to be at a high level in implementing international standards."[34]

3.4. Reform of the data protection legislation of Ukraine in line with the Regulation (EU) 2016/679, CoE Convention No. 108 and best comparative practices

The main problem in the field of personal data protection in Ukraine is the lack of an effective national system of personal data protection, establishment of the independent supervisory authority in the area of personal data protection, a proper organisational and legal mechanism for regulating relations and responsibility for committing offences in this area.

The adoption by the Verkhovna Rada of Ukraine of the Law "On Protection of Personal Data" in June 2010 was a significant step towards Ukraine's fulfilment of its international obligations in the field of personal data protection. At the same time, its adoption was only a part of the process, as sometimes nationally adopted principles do not meet international standards, for example, it is important to strengthen the institutional capacity of the Verkhovna Rada Commissioner for Human Rights to monitor the compliance with personal data protection provisions. In particular, an important step is the adaptation of terminology to the standards of the European Union, clarification of the rights of the personal data subjects, special attention should be paid to the cross-border transfer of personal

[34] LEOSHKO, V. Personal data protection is a core value. ‚Voice of Ukraine' 4. 7. 2023. [online] Available at: http://www.golos.com.ua/article/371967

data. Thus, verification of the compliance of national legislation with international standards is an important part of Ukraine's fulfilment of international obligations on personal data protection and bringing the Law into line with EU and the Council of Europe personal data protection standards.

It is important to pay attention to the following points based on our comparative legal analysis of the compliance of the Law of Ukraine "On Personal Data Protection" with Ukraine's obligations in the field of European integration and GDPR and Council of Europe Convention No. 108 in order to bring Ukrainian legislation in the field of personal data to European standards:

- To create an effective institutional mechanism for personal data protection in Ukraine: an independent supervisory authority responsible for developing guidelines, monitoring and control over the compliance with legislation in the field of personal data protection.
- To bring the terminology of the Law of Ukraine "On Personal Data Protection" in line with GDPR.
- To implement EU legal standards on personal data protection defined by the GDPR.
- To detail the content of the principles of personal data protection in accordance with GDPR.
- To introduce a requirement for companies to appoint a data protection officer.
- To adopt the rules of internal policy of companies and ensure the use of instruments that meet, in particular, the principles of data protection by design and data protection by default.
- To introduce and improve a number of rights of subjects in relation to their personal data, including the right to: erasure (the "right to be forgotten"), the right to data portability.
- To develop and improve codes of conduct and system of certification.
- To improve the procedure for notification of data leakage, namely to implement a chain system of notification of personal data violations:
- To define in detail and clearly the powers, duties, responsibilities of the controller and data processor.
- To introduce control over the transfer of personal data outside Ukraine. Establishing criteria for recognising the appropriate level of protection

Reform of the data protection legislative framework of Ukraine aimed at bringing it in compliance with the requirements of the GDPR is one of the obligations of Ukraine taken under the Association Agreement between Ukraine and EU. Ukraine has also ratified the Convention 108, and is consequently expected to ratify the Amending Protocol modernising the Convention.

It should be noted that in February 2020 there was established the joint working group on reforming the legislation around processing and protection of

personal data to work out the Draft Law of Ukraine "On personal data protection" №8153 and Draft Law of Ukraine "On the National Commission for Personal Data Protection and Access to Public Information" №6177.

Up to time the Draft Law of Ukraine "On personal data protection" №8153 and Draft Law of Ukraine "On the National Commission for Personal Data Protection and Access to Public Information" №6177 were registered in Ukrainian Parliament and submitted to the assessment to international data protection experts of the Council of Europe.

The opinion on Draft Law No. 8153 prepared by experts of the Council of Europe notes that the document contains an expanded version of the provisions establishing a comprehensive data protection legal framework highlighting the following: "The general approach envisaged by the Draft Law is quite close to the one based on European standards." [35]

Andriy Nikolaev, the key expert on personal data protection of the EU4DigitalUA Project (FIIAPP), noted that the new version of the Law of Ukraine "On personal data protection" is designed to ratify European documents and update the legislation of Ukraine to the requirements of the present time, make it suitable for the technology of personal data processing that exists today. The adoption of the new Law of Ukraine "On personal data protection", which will meet European requirements, is an inevitable and essential step towards European integration".[36]

3.5. Institutional mechanism in the area of personal data protection

The Convention 108 is the key element in the system of the Council of Europe instruments for the legal protection of personal data.

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.

Modernised Council of Europe Convention 108+ requires a country to have one or more authorities responsible for ensuring compliance with the Convention's provisions, commonly called Data Protection Authorities (DPAs). These

[35] Council of Europe Office in Ukraine. Protection of Ukrainians' personal data is on time – an expert discussion of the opinion provided by the Council of Europe on the Draft Law No. 8153 of 25.10.2022 on "Personal Data Protection". [online] Available at: https://www.coe.int/en/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection-

[36] NIKOLAJEV, A. The right to privacy: why Ukraine needs a new law on personal data protection. European Pravda, 15. 12. 2022. [online] Available at: https://www.eurointegration.com.ua/experts/2022/12/15/7152519/

supervisory authorities must be completely independent, able to investigate, hear claims, ensure cases come before judicial authorities, allow appeals from their decisions to the courts, and satisfy various other requirements for a DPA (art 15).[37]

The issue of ensuring independence is one of the key issues in the creation of a new supervisory authority in the field of personal data protection.

The issue of non-compliance with the requirements for the independence of the supervisory authority has been the main reason for liquidation of the State Service of Ukraine for Personal Data Protection and the transfer of its powers to the Verkhovna Rada Commissioner for Human Rights.

It should be noted that the existence and effective operation of an independent supervisory authority is one of the criteria for a decision of the European Commission to recognize the appropriate level of personal data protection.

In addition, the creation of supervisory authorities with full independence in the performance of their functions is an essential element of protecting individuals when processing personal data.

When creating a supervisory authority, the following criteria for independence and transparency should be provided for:

1. To establish by law that any state bodies and/or officials do not have the right to interfere in or influence the activities of the body in any way, to provide any orders, instructions, etc.to the supervisory body, its management and employees, and the latter do not have the right to carry out such orders, instructions, etc.

The decision of the Supervisory Authority in the field of personal data protection may only be overturned by the court.

2. At the level of the law, to prescribe a transparent mechanism for selecting and appointing the head of the body, or members of the body, if the body is collegial.

It should be noted that paragraph 121 of the Preamble of the GDPR provides that such appointment may be made by parliament, the government or the head of state on the basis of a proposal made by the government, a member of the government, parliament or an independent body vested with such powers in accordance with the law of the member state. The same provisions are enshrined in the first part of Article 53 of the GDPR.

It is advisable to legally define transparent rules for the selection of candidates for a position, as well as requirements for the formation, composition and activities of the competition commission for such selection.

[37] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. [online] Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

3. To establish a long term for which the head of the supervisory authority (and/or members — in the case of a collegial body) is elected.
4. At the legislative level, to exclude the possibility of removing the head of a supervisory body from office at the discretion of the appointing body or for political reasons.

An exclusive list of cases when the powers of the chairman (members) of the body are terminated (including ahead of schedule) should be provided for in the law.

5. To restrict the right of the head of the body (members of the body) and employees of the body to hold other positions in public administration to engage in other activities that are not compatible with the performance of the functions assigned to them and the exercise of the powers granted.
6. To legally limit the possibility of holding the position of head of a supervisory authority for more than one or two cadences.
7. To establish requirements for the independence and integrity of candidates for the position of head and/or members of the body.
8. To provide by law that the expenses for financing the Supervisory Authority in the state budget of Ukraine are determined by a separate line at the level that ensures the proper performance of powers, and the body is the main manager of the state budget of Ukraine allocated for its financing.

It is advisable to fix at the level of the law the minimum amount of official salaries, allowances and bonuses of the chairman (members) of the body and employees of the body with reference to the minimum wage/subsistence minimum, etc. The level of certain official salaries, allowances and bonuses should be adequate in relation to market salaries and sufficient to minimize corruption risks.

9. To grant the supervisory authority the right to independently determine its internal structure and implement personnel policy.
10. To give the supervisory authority the power of the regulator in the field of personal data protection, namely: to adopt relevant regulations and provide explanations of legislation.
11. To grant the authority to carry out inspections and investigations, as well as directly apply sanctions (impose fines).

Taking into account the broad powers required for the work of the body and serious guarantees of the independence of both the body itself and its management, it is important, at the legislative level, to ensure transparency of its work and minimize the risks of abuse.

According to Ms. Dijana Šinkūnienė, Director of the State Data Protection Inspectorate of the State Data Protection Inspectorate of Lithuania: to ensure stable functioning of a supervisory authority, it is crucial to identify its structure

and status as well as regulate the aspects relating to its independence by law or another legal act adopted by the parliament:[38]

- Appointment of the supervisory authority head / members;
- Qualifications and eligibility requirements for appointment of the supervisory authority head
- members;
- Term of office of the supervisory authority head / members;
- Grounds for dismissal of the supervisory authority head / members;
- Dismissal procedures for the supervisory authority head / members;
- Personnel policy (e.g., right to hire its own staff, etc.);
- Salary of the supervisory authority head / members.

Dijana Šinkūnienė also emphasized the importance of the implementation of international standards of personal data protection and their introduction into the legislation of Ukraine.[39]

In the view of Volodymyr Venher and Oleh Zaiarnyi: with due regard to the constitutional and legal principles of organisation of state power in Ukraine, there are three main models of state supervision in the fields of personal data and public information:[40]

- 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.

According to Ms. Liliia Oleksiuk, Non-Staff Consultant of the Verkhovna Rada Committee on Digital Transformation, Draft Law №6177 provides for the establishment of a central executive body with a special status aimed at implementing policies in the field of personal data protection and access to public information, as well as control over compliance with the law. The staff of the National Commission will be formed based on open competition. Candidates

[38] ŠINKŪNIENĖ, D., OLEKSIUK, L., SHEVCHUK, O. *Analysis of the European models of the independent oversight authority in the field of data protection and access to public information*. Strasbourg: Council of Europe Publishing, 2021. [online] Available at: https://rm.coe.int/analysis-report-2021-eng-2web/1680a6e81d.

[39] Council of Europe Office in Ukraine. Round table on challenges and future of data protection. [online] Available at: https://www.coe.int/en/web/kyiv/-/round-table-on-challenges-and-future-of-data-protection.

[40] VENHER, V.; ZAIARNYI, O. *Legal Analysis of the main models of institutionalization of the state supervision with regard to personal data and access to public information in Ukraine*. Council of Europe, 2020. [online] Available at: https://rm.coe.int/legal-analysis-on-institutialisation-of-the-data-protection-independen/16809ee579.

need 5 years of experience in data protection and access to public information, so having legal education alone will not be enough for application. As explained by Ms. Oleksiuk, this requirement should guarantee the authority's competence in data protection and prevent it from becoming a tool of pressure on the business. The Chair of the National Commission is elected from among its members, and no public authority shall influence this decision. The members of the Commission may hold office for no more than two consecutive terms. In general, it is noted that the draft law №6177 was developed with the consideration of Convention 108 and the GDPR and therefore it is in line with the principles of transparency and independence.[41]

Lilit Daneghian, Deputy Head of Co-operation Programmes Division in Department for the Implementation of Human Rights, Justice and Legal Co-operation Standards, said: "Modernisation of the data protection legislation creates wide-range benefits and positive impact both for the individuals and businesses. Allow me also to stress its contextual importance from the standpoint of the war dimension. Informational confidentiality and data protection in times of war becomes an obvious need for Ukraine." Ms Daneghian also noted that the Council of Europe is at the origin and the heart of promoting the responsible use of technology ensuring respect for privacy. "I would like to reiterate the Council of Europe's commitment to further support Ukraine's efforts towards a rules-based market economy where the privacy is highly respected," she added.[42]

4. Conclusion

The position of the Office for Personal Data Protection is fully in line with the requirements arising for the Czech Republic from international obligations. Although the drive to create independent administrative authorities dates back to the mid-20th century, it is the massive adoption of Convention 108 and its application in the laws of a number of states that marks the real breakthrough, with the GDPR confirming and refining the requirements for all accessible elements of achieving independent status for such an authority. It can be concluded that the provisions

[41] EBA Ukraine. GDPR implementation in Ukraine is expected for 2023-2024. [online] Available at: https://eba.com.ua/en/vprovadzhennya-gdpr-ochikuyetsya-v-2023-2024-rokah/

[42] Council of Europe Office in Ukraine. Protection of Ukrainians' personal data is on time – an expert discussion of the opinion provided by the Council of Europe on the Draft Law No. 8153 of 25.10.2022 on "Personal Data Protection". [online] Available at: https://www.coe.int/en/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection-.

of both Convention 108 and the GDPR regarding supervisory authorities are not in competition with each other, they are complementary and in many aspects they are driving each other to further develop the content of the aforementioned documents, also in view of the permanent rapid changes in the field of data protection. As indicated, Convention 108 is open to further amendments, while the text of the GDPR leaves room for Member States to adjust further scope and rules to enshrine the independence of supervisory authorities according to national needs. Last but not least, the role of the OIA is also important in terms of continuity of its existence. The ÚOOÚ was established on the basis of Act No. 101/2000 Coll., on the protection of personal data, i.e. since 1 June 2000 it has been working to protect personal data, the form of processing and distribution of which has changed considerably over 22 years and the ÚOOÚ is still facing new challenges. It is worth highlighting the fact that this supervisory authority has shown signs of independence since its inception, as required by international instruments, and its independence has never been significantly challenged. The position of the OIPO as an independent administrative supervisory authority for the protection of personal data is the result of a long-standing development in the field of personal data protection and is the logical outcome of the need to establish a fundamental form of supervision over an area which is an integral part of the privacy of every natural person and where its violation results in a significant interference with the rights of individuals. While the *element of independence is* problematic in terms of constitutional compliance, it is nonetheless currently an obligation under EU law and there is a broader political and social consensus on it.

On the other hand, the situation in Ukraine is a bit different. Thus, analysing the risks, gaps, problems and weaknesses in the implementation of personal data protection mechanisms in Ukraine, it could be concluded that the existing domestic system of personal data protection requires establishment effective institutional mechanism for personal data protection in Ukraine and further improvement of legal standards and principles of personal data protection and reforming regulations, by introducing higher standards and effective mechanisms for the personal data protection into the national law and approximating it gradually to the standards of personal data protection of the European Union in accordance with GDPR and Council of Europe Modernised Convention 108+.

It is important to emphasize that for the full operation of the personal data protection system (legal and institutional mechanism), it is significant to adopt both the draft laws: Draft Law of Ukraine "On Personal Data Protection" and Draft Law of Ukraine "On the National Commission for Personal Data Protection and Access to Public Information". The adoption of the draft laws will make it possible to bring the personal data protection system in line with the GDPR and

the Modernized Convention 108+. The adoption of draft laws will ensure proper and effective control and monitoring of compliance with the legislation on personal data protection in both the private and public spheres and will strengthen the protection of the rights of each personal data subject.

List of references

Council of Europe Office in Ukraine. Protection of Ukrainians' personal data is on time – an expert discussion of the opinion provided by the Council of Europe on the Draft Law No. 8153 of 25.10.2022 on "Personal Data Protection". [online] Available at: https://www.coe.int/en/web/kyiv/-/protection-of-ukrainians-personal-data-is-on-time-an-expert-discussion-of-the-opinion-provided-by-the-council-of-europe-on-the-draft-law-no.-8153-of-25.10.2022-on-personal-data-protection-

Council of Europe Office in Ukraine. Round table on challenges and future of data protection. [online] Available at: https://www.coe.int/en/web/kyiv/-/round-table-on-challenges-and-future-of-data-protection

EBA Ukraine. Interview with Liliia Oleksiuk. GDPR implementation in Ukraine is expected for 2023–2024. [online] Available at: https://eba.com.ua/en/vprovadzhennya-gdpr-ochikuyetsya-v-2023-2024-rokah/

HANDRLICA, J. Nezávislé regulačné orgány (?) *Justičná revue.* 2008, vol. 60, no. 2, pp. 165–187.

HENDRYCH, D. *Právnický slovník*. 3. editon. Praha: C. H. Beck, 2009.

KASL, F. Internet věcí a ochrana dat v evropském kontextu. *Revue pro právo a technologie.* 2016, no. 13, p. 126.

LEOSHKO, V. Personal data protection is a core value. ‚Voice of Ukraine' 04.07.2023. [online] Available at: http://www.golos.com.ua/article/371967

MACHOVÁ, M. Zákon o zpracování osobních údajů – prováděcí úprava k GDPR z pohledu českého zákonodárce. *E-pravo.* 27. 6. 2019. [online] Available at: https://www.epravo.cz/top/clanky/zakon-o-zpracovani-osobnich-udaju-provadeci-uprava-k-GDPR-z-pohledu-ceskeho-zakonodarce-109542.html

NIKOLAJEV, A. The right to privacy: why Ukraine needs a new law on personal data protection. European Pravda. 15. 12. 2022. [online] Available at: https://www.eurointegration.com.ua/experts/2022/12/15/7152519/

NONNEMANN, F. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. *Epravo.cz* 30. 9. 2022. [online]. Available at: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html

NULÍČEK, M. et al: *GDRP Obecné nařízení o ochraně osobních údajů*. 2. editon. Praha: Wolters Kluwer, 2018, p. 441.

PATTYNOVÁ, J. et al. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář.* 2. edition. Praha: Leges, 2019.

POUPEROVÁ, O. Nezávislé správní úřady. *Správní právo*, 2014, vol. 47, no. 4, pp. 209–226.

POUPEROVÁ, O. Zřizování nezávislých správních úřadů jako způsob řešení nestabilní politiky. *Právna politika a legislatíva – Vplyv politk, ,normotvorby a súdnej judikatúry na výkon verejnej správy.* Bratislava: Wolters Kluwer, 2020.

ŠINKŪNIENĖ, D., OLEKSIUK, L., SHEVCHUK, O. *Analysis of the European models of the independent oversight authority in the field of data protection and access to public information*. Strasbourg: Council of Europe Publishing, 2021. [online] Available at: https://rm.coe.int/analysis-report-2021-eng-2web/1680a6e81d

SLÁDEČEK, V. *Obecné správní právo*. 4. edition. Praha: Leges, 2019.

VENHER, V.; ZAIARNYI, O. *Legal Analysis of the main models of institutionalization of the state supervision with regard to personal data and access to public information in Ukraine*. Council of Europe, 2020. [online] Available at: https://rm.coe.int/legal-analysis-on-institutialisation-of-the-data-protection-independen/16809ee579