ARTICLE 19

Ukraine: Data Protection Act and related legislation

July 2012

Legal analysis

Executive Summary

ARTICLE 19 has analysed the provisions of the Ukraine Data Protection Act, Law on Information, and Law on Access to Public Information, to assess their compatibility with international standards relating to the rights of freedom of expression and information. ARTICLE 19 finds the Data Protection Act and related legislation to be lacking significant provisions, which would ensure that the rights to privacy and freedom of expression and information are appropriately balanced.

Recommendations:

1. The Data Protection Act and the Law on Information should be amended to ensure that there is clear exemption for freedom of expression in all cases relating to communicating information to the public - ideas, or opinions of general interest - or for literary or artistic expression.

2. Clarify the relationship between the three laws by creating and setting out a clear exemption for personal data in the Law on Access to Public Information, and by amending provisions in the other laws which contradict this.

3. Create a common list of exemptions for personal data which clearly exclude information collected about public officials or others acting in an official capacity relating to their duties or to matters which may affect their obligations, and to those influencing public policy, and to information relating to expenditures of public funds or use of public resources.

4. Ensure that the public interest test in the Law on Access to Public Information Act applies to personal information, to allow for its release where the release of the information is in the public interest.

5. Harmonise provisions on subject access in the Data Protection Act and the Law on Access to Public Information to ensure that external enforcement through an independent body is available for denials of access to individuals seeking to access or correct their own records.

6. Amend the Data Protection Act and other laws to ensure the independence of the data protection body from the state. This should be an independent regulatory body for the protection of personal data, which is administratively and financially independent of any public authority and is given adequate resources to conduct its activities.

7. Create or appoint an independent body for oversight and appeals for the Law on Access to Public Information. This can be the Ombudsman or another independent body. It must have adequate resources to effectively oversee and enforce the right to information.

Table of Contents

About the ARTICLE 19 Law Programme

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications, which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Law Programme publishes a number of legal analyses each year, commenting on legislative proposals, as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available online at http://www.article19.org/resources.php/legal/.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org or call us at +44 20 7324 2500.

International Media Support

This publication was made in the framework of the IMS Media and Democracy Programme for Eastern Europe and the Caucasus

I. Introduction

In 2010, Ukraine adopted the Law No. 2297-VI "On Personal Data Protection" (hereafter referred to as "the Data Protection Act"), as part of its obligation to adopt legislation in compliance with its obligations under European law, to protect the personal information of its citizens as an aspect of their privacy rights. In 2011, it adopted the Law No 2939-VI on "Access to Public Information", as well as amendments to the existing Law on Information.

Currently, the Government of Ukraine is reviewing the Data Protection Act and related legislation. This analysis is intended to provide input into the process to ensure that the legal framework adequately complies with international standards on freedom of expression and access to information. It does not fully assess the compatibility of the Act with Ukraine's obligations to protect personal data except as it may relate to the other rights.

The right of privacy and the rights of freedom of expression and freedom of information are co-equal human rights. ARTICLE 19 believes that data protection and freedom of expression and freedom of information are complimentary rights designed to empower the citizen to protect their rights and to improve the transparency of public and private bodies that hold and wield power in society. ARTICLE 19 supports the adoption of well-designed data protection acts, which protect individuals' rights while ensuring government transparency and freedom of expression. Nearly all the countries in Europe have now adopted both data protection and right to information laws.

In this analysis, ARTICLE 19 sets out its concerns about the legal framework and its compatibility with Ukraine's international obligations under international human rights law to protect freedom of expression and information, as well as, the right to privacy.

II. International Freedom of Expression and Privacy Standards

The right to freedom of expression is a fundamental human right. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy, particularly in countries transitioning to democracy. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

At the same time, the right to privacy is recognised in most international human rights treaties including the Universal Declaration of Human Rights[1], the European Convention on Human Rights[2], the

[1] UDHR, Art 12.

[2] Article 8.

American Declaration of the Rights and Duties of Man[3], and the American Convention on Human Rights.[4] Under these treaties, privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies and other individuals. It is often summarised as "the right to be left alone", but it encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognised as a core right that underpins human dignity and other values, such as freedom of association and freedom of speech. It is also understood to be essential to provide private breathing space for individuals to be able to realise their other rights, including freedom of expression.

Privacy and freedom of expression are intertwined rights in human rights law. They appear together in international instruments, national constitutions and laws. Together they ensure the accountability of the state and other powerful actors to citizens. This section lays out the two rights in international law and their interrelations.

A. Universal Declaration of Human Rights

The Universal Declaration of Human Rights (UDHR) protects both freedom of expression and privacy rights.[5] The UDHR, as a UN General Assembly Resolution, is not directly binding on states. Nonetheless, parts of it are widely regarded as having acquired legal force as customary international law since its adoption in 1948.[6]

Article 19 of the UDHR guarantees the right to freedom of expression in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.

Article 12 guarantees the right to privacy:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

B. International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) elaborates upon and gives legal force to many of the rights articulated in the UDHR. The ICCPR binds its 167 member states to respect its provisions and implement its framework at the national level.[7] Ukraine has acceded to the ICCPR, and as a State Party must ensure that any attempts to limit expression and privacy are compliant with the ICCPR.

---

[3] Articles 5, 9 and 10.

[4] Article 11.

[5] UN General Assembly Resolution 217A(III), adopted 10 December 1948.

[6] See, e.g., De Schutter, International Human Rights Law, Cambridge University Press, 2010.

[7] Article 2 ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

Article 19 of the ICCPR guarantees the right to freedom of expression in its first two paragraphs:

> 1. Everyone shall have the right to freedom of opinion.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

Article 17 of the ICCPR protects the right to privacy, and states that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

The United Nations Human Rights Committee (HR Committee), as the monitoring body for the ICCPR, has issued commentary on both provisions. In June 2011, it issued General Comment No. 34 in relation to Article 19.[8] The General Comment constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 of the ICCPR, and provides a progressive and detailed elucidation of international law relating to freedom of expression and access to information.[9]

While the right to freedom of expression is fundamental, it is not guaranteed in absolute terms. Article 19(3) of the ICCPR permits limitations on the right that are necessary and proportionate to protect the rights or reputation of others, for the protection of national security or public order, or public health and morals including privacy. Nonetheless, restrictions on the right to freedom of expression must be strictly and narrowly tailored to achieve one of these objectives, and must not jeopardise/jeopardize the right itself. Determining whether a restriction is narrowly tailored is often articulated as a three-part test, requiring that restrictions are prescribed by law, pursue a legitimate aim and conform to the strict tests of necessity and proportionality.[10]

A similar regime exists for privacy. International law requires that restrictions on privacy are based on the same permissible limitation requirements as are found for the protection of freedom of expression. In General Comment 16 on the Right to Privacy, the HR Committee stated that:

> The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.... Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.[11]

According to the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

> [A]rticle 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17,

[8] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 21 June 2011.

[9] ARTICLE 19 statement on HR Committee Comment No. 34, available at http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression.

[10] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[11] United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), CCPR/C/GC/16, 4 August 1988.

> and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[12]

It is also generally recognised that the right to privacy creates positive obligations for states to ensure that they adopt laws to protect all persons against attacks. The UN HR Committee in General Comment No 16 stated that:

> In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[13]

C. European Convention on Human Rights

Ukraine has also signed and ratified the European Convention on Human Rights (ECHR). The Convention and the associated case law of the European Court of Human Rights set out extensive protections for both privacy and freedom of expression.

Article 10 states that:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The European Court of Human Rights has described it as a core human right especial to democracy:

> Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment. Subject to paragraph 2, it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society". As set forth in Article 10, this freedom is subject to exceptions, which must, however, be construed strictly, and the need for any restrictions must be established convincingly.[14]

Equally, the Convention recognises and protects the right to privacy. Article 8 of the ECHR states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

---

[12] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

[13] General Comment 16, Ibid.

[14] Plon (Societe) v France (Application No. 58148/00), [2004] ECHR 200 (18 May 2004) (European Court of Human Rights).

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Court has also provided for strong recognition of privacy in its case law. It has described it as a broad concept that includes "the right to establish and develop relationships with other human beings".[15] In addition, the Court has stated:

> As to respect for the individual's private life, the Court reiterates the fundamental importance of its protection in order to ensure the development of every human being's personality. That protection extends beyond the private family circle to include a social dimension.[16]

Under the ECHR, restrictions on privacy must meet the same criteria as for freedom of expression – they can only be imposed if they are "in accordance with the law" and "necessary in a democratic society", and if the interference is legitimate and proportionate.[17]

D. Privacy and Data Protection

The most relevant aspect of the right to privacy engaged here relates to the collection, use and dissemination of personal information known as "data protection". With the mass adoption of information and communications technologies, the right to privacy has evolved to address issues relating to the collection, use and dissemination of personal information in information systems. New information technologies have driven the collection of personal information by governments and private bodies into unprecedented vast databases. New communication technologies create and collect substantial records about individuals in the process of providing communications and share information with little limits. All of this has led to concerns about abuses including misuse of information for unlawful purposes and identity theft.

This aspect of data protection has been incorporated by major human rights bodies and national courts into their applications of protections for privacy. The German Federal Constitutional Court in a seminal case in 1983 defined it as "the authority for the individual to determine himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others".[18]

The UN Human Rights Committee in General Comment 16 stated that:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[19]

---

[15] Niemietz v. Germany, judgment of 16 December 1992, Series A no. 251 B.

[16] Biriuk v. Lithuania (Application no. 23373/03), 25 November 2008.

[17] Niemietz v. Germany, ibid.

[18] Federal Constitutional Court decision of December 15, 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

[19] General Comment 16, ibid, §10.

The European Court of Human Rights has found that Article 8 provides for strong protections for personal data. The ECtHR noted in a recent case that:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article.[20]

The rights of data protection have also been adopted in administrative and legal procedures across the globe.[21] This includes the UN General Assembly Resolution on guidelines for the data protection of personal information held in computer databases, which was adopted in 1981.[22]

In Europe, the framework for data protection is made up of two major instruments: the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in 1981, which applies to all CoE member states that have ratified it (currently 44),[23] and the European Union Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data adopted in 1995, which applies to all EU Member States, accession countries, and indirectly to all other nations in relation to personal data that originates from EU Member States.[24] Both set up comprehensive systems of regulation for the processing of personal information by both government bodies and private parties.

At the national level, the right of data protection has been long standing in Europe. The first national law on data protection was adopted in Sweden in 1973 – the same nation that first adopted freedom of information. It was followed by Germany in 1977, and many other nations shortly after. Today, nearly every nation in Europe has adopted a comprehensive data protection law based on the CoE Convention and the EU Directive.[25]

E. The Relationship of Privacy and Freedom of Expression

Privacy and freedom of expression are both recognised human rights. As two equal human rights, it is essential that governments and courts balance the two in a fair manner without giving precedence to

---

[20] S. and Marper v. The United Kingdom, Application No. 30562/04, [2008] ECHR 1581 (4 December 2008). See also Leander v. Sweden, 26 March 1987, § 48, Series A no. 116, 9 EHRR 433; Amann v. Switzerland [GC], no. 27798/95, § 69, ECHR 2000-II, 30 EHRR 843; P.G. and J.H. v. the United Kingdom, no. 44787/98, § 59-60, ECHR 2001 IX, BAILII: [2001] ECHR 550.

[21] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); Canadian Standards Association (CSA) International, Model Code for the Protection of Personal Information, 1996; APEC Privacy Framework, 2005; The Madrid Privacy Declaration, Global Privacy Standards for a Global World, 3 November 2009.

[22] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.

[23] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, ETS 108, 1981.

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[25] See Surveillance Monitor 2011: Assessment of surveillance across Europe (Privacy International, Electronic Privacy Information Center, and the Center for Media and Communications Studies, 2011).

one over the other. International human rights law does not recognise a hierarchy of rights, in which one trumps the other.

As the Vienna Declaration and Programme of Action, adopted by the World Conference on Human Rights in 1993, states:

> All human rights are universal, indivisible and interdependent and interrelated. The international community must treat human rights globally in a fair and equal manner, on the same footing, and with the same emphasis. While the significance of national and regional particularities and various historical, cultural and religious backgrounds must be borne in mind, it is the duty of States, regardless of their political, economic and cultural systems, to promote and protect all human rights and fundamental freedoms.[26]

The UN High Commissioner for Human Rights has stated that:

> [A]ll human rights are equally important. The 1948 Universal Declaration of Human Rights makes it clear that human rights of all kinds—economic, political, civil, cultural and social—are of equal validity and importance… Human rights are also indivisible and interdependent. The principle of their indivisibility recognizes that no human right is inherently inferior to any other.[27]

This approach of balancing competing rights has been taken up by the European Court of Human Rights in cases involving privacy and freedom of expression:

> [W]hen verifying whether the authorities struck a fair balance between two protected values guaranteed by the Convention which may come into conflict with each other in this type of case, freedom of expression protected by Article 10 and the right to respect for private life enshrined in Article 8, the Court must balance the public interest in the publication of [information] and the need to protect private life.[28]

It is also important to note that the rights are mutually supportive. Freedom of expression and freedom of information allow individuals to investigate and challenge abuses to human rights including violations of privacy. Privacy allows individuals to work in a space unhindered by authority. As a practical matter, limits on privacy affect the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and other sources.[29]

The European Commission in a recent impact assessment on the revised data protection regime noted that:

> Privacy and the protection of personal data are fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. They play a key role for the exercise of fundamental rights in a broader sense. Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. Freedom of thought, freedom of expression, freedom of assembly and association, but also the freedom to conduct a business will not be exercised fully by all citizens in an environment where the individual feels that each of her or his moves, acts, expressions and transaction is subject to

[26] Vienna Declaration and Programme of Action, U.N. Doc A/CONF.157/23 (12 July 1993).

[27] Office of the United Nations High Commissioner for Human Rights, Frequently Asked Questions On A Human Rights-Based Approach To Development Cooperation, 2006.

[28] Von Hannover v Germany, (2005) 40 EHRR 1; See also Chauvy and Others v France (Application no. 64915/01), 29 June 2004.

[29] See e.g. IFEX Alert, Thirty IFEX members call on governments to respect fundamental human rights of free expression and privacy of communications, 5 June 2009. http://www.ifex.org/international/2009/06/05/ja_gm/

> scrutiny by others trying to control him or her. Exercise of these freedoms is crucial to maintain all fundamental rights.[30]

As described by the UN Special Rapporteur in his 2009 report on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

> In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed. Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively.[31]

Thus, its is both counterproductive and in violation of international law to consider the two run in a zero-sum manner, trying to eliminate one on the behalf of another. The two must be considered together with the recognition that they are often mutually supporting.

III. Analysis of the Data Protection Act and Associated Legislation

A. Overview of Legal Framework

There are numerous overlapping pieces of legislation in Ukraine relating to data protection. Law No 2297-VI, "On Personal Data Protection" ("Data Protection Act"), was adopted on 1 June 2010 and went into force on 1 January 2011. Its provisions are further supplemented by Article 32 of the Constitution of Ukraine, Law No 2657-XII "On Information", and the Civil Code.

The Data Protection Act generally follows the model as set out by Council of Europe Convention 108 and the EU Data Protection Directive 95/46, albeit in a somewhat complex and inconsistent manner. Broadly, this includes: a broad definition of personal information; principles on how personal information can be processed with additional limits on the processing of "sensitive information" such as racial and ethnic data; a right of access and correction for individuals with respect to their own records; a requirement to register databases; limits on how information is collected and used, as well as under what circumstances this can be done; the creation of an oversight body; and the establishment of penalties for violations of the law.

The protections are supplemented by an additional law approved on 2 June 2011 that amends the Code of Administrative Offenses to revise two provisions to provide for criminal and civil penalties for violations of data protection.[32]

[30] European Commission, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation 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 (General Data Protection Regulation) And Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, 25 January 2012.

[31] Ibid.

[32] Law of Ukraine No 3454-VI of 2 June 2011, amending certain legislative acts of Ukraine to upgrade the penalties of legislation on protection of personal data.

On 13 January 2011, Law No 2939-VI, "On Access to Public Information", was adopted. It is a general "right to information" law that creates a framework for facilitating access to information held by public bodies. The framework consists of: a right for persons to be able to demand information from public bodies (including their own records, with a right of correction); procedures for access; exemptions to the right; appeal mechanisms for denials; structures in bodies for the release of information both in response to requests and on a routine basis; partial protection of whistleblowers who release information of public interest; the creation of registers of documents; and penalties for non-compliance with the law.

Finally, Law No 2658-XII, "On Information", originally adopted in 1992 and amended in 2011 (and at numerous other times previously), sets out the broad information framework for Ukraine. Its provisions strongly overlap with both the Data Protection Act and the Law on Access to Public Information. It defines its purpose as "regulat[ing] the relations regarding the creation, obtaining, storage, use, dissemination, security, and protection of information" with provisions on rights to information, freedom of expression and protection of privacy. It also sets out journalists' rights and those of the mass media.

B. Limited Legal Protections for Freedom of Expression in Data Protection Act

An initial concern is the failure to fully recognise freedom of expression as a right to be balanced against the protection of personal data, as is typically found in other similar laws in European countries and in major international conventions on data protection. The limited exemption is troubling and in violation of international requirements for limitations to freedom of expression. It raises concerns that without better clarity, data protection may be unlawfully used to justify the suppression of expression by citizens, other than those officially designated as journalists.

Under the Data Protection Act, there is a limited exemption for the processing of personal data, which only applies to individuals acting in specific professional capacities, rather than recognising the right itself as one held by all persons. Article 1 provides that the law does not apply to journalists "with regard to execution of his/her professional duties" or to "professional creative employees for purposes of creative activity".[33]

There is no mention of non-journalists employed by media organisations or media organisations in general, or broader free expression reasons. This will substantially affect the provision of information by persons who are not officially employed journalists, such as freelance journalists, book writers, and bloggers as well as non-professional creative employees exercising their free expression rights such as artists and writers who are also employed in some other capacity and engage in artistic pursuits in their spare time.

All of these persons are required to follow to obligations of the act, including the bureaucratic requirements of registration, and to demands that they do not process personal information without consent.

Furthermore, the DPA and other laws would appear to all subject to potential criminal liability for dissemination of personal information all of those persons exercising their free expression rights and displaying personal information of any form, no matter the sensitivity of the information, who are not

[33] We note that other laws such as the Law on Print Media and the Law on Broadcasting definitions of journalists which are only limited to those either directly employed or assigned to

"journalists" or "creative employees". Under Article 182 of the Code of Administrative Offenses,[34] "unlawful collection, storage, use, destruction, or dissemination of confidential information about a person" is punishable by fines, prison sentences or restrictions on liberty. This may or may not be relieved by Article 29(1) of the Law of Information, which states that restricted information can be disseminated if it is in the public interest, and Article 30(3) which allows that "parties to information relations" (presumably this would include any persons providing information to the public) are exempt "from liability for disseminating restricted access information, if a court finds such information of public necessity".

The situation is further complicated by overlapping provisions in the framework Law on Information. It contains a number of provisions which are not consistent with the DPA: Article 2 delineates "freedom of expression of views and beliefs" (only a subset of what is protected under international law relating to freedom of expression) as well as protection of personal data and "guaranteed right to information" as "main principles of information relations". However, Article 11(2) prohibits the processing of personal information without consent, except when a law allows it "in the interests of national security, protection of economic well-being and human rights". However, Section III on "Activities of Journalists, Mass Media and their Employees" sets out the rights of journalists and mass media, with Article 24(1) prohibiting censorship of a broader category of persons than just journalists - "journalist, a mass medium, a founder (co-founder), publisher, manager, or disseminator".

This tangled structure governing the relationship between data protection and freedom of expression is in sharp contrast to the legal framework set out in EU legislation, which clearly addresses these issues to ensure that both interests are considered appropriately. Under the European Union Directive on Data Protection 95/46[35], there are several recognitions of the importance of freedom of expression and the right to information. The most significant is Article 9 on "Processing of personal data and freedom of expression", which requires that all EU Member States adopt exemptions to data protection rules in cases of all persons who are engaged in journalistic, literary or creative pursuits, rather than only persons who are officially recognised as a journalist or "creative employee". It states that:

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

In addition, Recital 37 provides further detail on the scope of the balancing:

> Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of [expression] and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for

[34] Law of Ukraine No 3454-VI of 2 June 2011, amending certain legislative acts of Ukraine to upgrade the penalties of legislation on protection of personal data.

[35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

> this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities.

The European Court of Justice in evaluating this provision has ruled that states must develop a "fair balance" between the two rights based on the principle of proportionality.[36] As noted by the ECJ in a 2008 case:[37]

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary.

Most pertinently relating to the existing provisions, the Court also noted that the exemptions in the Directive apply beyond just the official media: "the exemptions and derogations provided for in Article 9 of the directive apply not only to media undertakings but also to every person engaged in journalism."[38] It also noted that publication for profit did not automatically exempt the activity from being journalistic.[39] Finally, it also stated that the medium used to convey the information was irrelevant.[40] Overall, it stated that the journalistic exemption applied "if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes."[41]

Similarly, Article 9 (2) of CoE's Convention 108 also provides for derogation of data protection principles for human rights purposes, which has been interpreted by the CoE to include freedom of expression.[42]

The free expression exemption has been widely adopted by countries across Europe, even beyond the EU Member States. For example, the Russian Data Protection Act, Article 2(6), states that consent for processing is not necessary if "Personal data are processed to fulfil a purpose of journalistic, scientific, literary or other creative activities – unless the rights and freedoms of the personal data subject are infringed on".[43]

> The Polish Data Protection Act similarly exempts freedom of expression-related activities. Article 3 states that:[T]he Act shall also not apply to press journalistic activity within the meaning of [The Press Law] and literary and artistic activity, unless the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject.[44]

---

[36] Case C-101/01, Bodil Lindqvist, 6 November 2003, p. 87-90.

[37] C-73/07, Satakunnan Markkinapörssi and Satamedia (Grand Chamber), 16 December 2008.

[38] Ibid, p 58.

[39] Ibid, p 59.

[40] Ibid, p 60.

[41] Ibid, p 61.

[42] See Data protection and the media, study prepared by the Committee of Experts on Data Protection (CJ- PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Council of Europe, Strasbourg, 1991.

[43] Federal Law of the Russian Federation of 27 July 2006, N 152 – FZ "On Personal Data" (unofficial translation).

[44] Act of August 29, 1997 on the Protection of Personal Data, Journal of Laws of October 29, 1997, No. 133,

The UK Data Protection Act 1998, Article 32, on "Journalism, literature and art" sets out a comprehensive regime on balancing data protection and freedom of expression:

> (1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if—
>
> (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
>
> (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
>
> (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.
>
> ...
>
> (3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which—
>
> (a) is relevant to the publication in question, and
>
> (b) is designated by the [Secretary of State] by order for the purposes of this subsection.
>
> (4) Where at any time ("the relevant time") in any proceedings against a data controller under section 7(9), 10(4), 12(8) or 14 or by virtue of section 13 the data controller claims, or it appears to the court, that any personal data to which the proceedings relate are being processed—
>
> (a) only for the special purposes, and
>
> (b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time twenty-four hours immediately before the relevant time, had not previously been published by the data controller,
>
> the court shall stay the proceedings until either of the conditions in subsection (5) is met.
>
> (5) Those conditions are—
>
> (a) that a determination of the Commissioner under section 45 with respect to the data in question takes effect, or
>
> (b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.
>
> (6) For the purposes of this Act "publish", in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

The breadth of protected freedom of expression-related activities will be extended in both of the revised frameworks of the European Union and the Council of Europe currently being considered. Under a revised draft for a new EU Regulation on Data Protection, Article 80 now states that:

> Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.[45]

Recital 121 of the revised framework sets out in more detail the interests of freedom of expression that must be considered:

---

item 883 (as amended).

[45] Proposal for a Regulation 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 (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012.

> The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

Specific protections for freedom of expression are also being incorporated in the revisions to the Council of Europe Convention 108 on Data Protection. In the draft currently being considered, Article 9 states that member states should incorporate an exemption when it is necessary to "protect the data subject or the rights and freedoms of others, notably freedom of expression and information".[46] The draft further notes that: "The Explanatory Report will specify that this provision concerns data processing carried out solely for communicating information to the public, ideas, or opinions of general interest, or for literary or artistic expression." Furthermore, revised Article 12 provides for an even broader derogation of data protection for freedom of expression, stating that: "Each Party may foresee in its domestic law derogations to the provisions set out in this Chapter, providing they constitute a measure necessary in a democratic society to [protect] freedom of expression and information."[47]

Thus, in its consideration of the Data Protection Act, the government of Ukraine should take a forward looking view based on the developing EU and CoE frameworks to ensure that the legislation does not require further amendment to ensure compatibility and to maximize freedom of expression protections.

Recommendation

- The Data Protection Act and the Law on Information should be amended to ensure that there is clear exemption for freedom of expression in all cases relating to communicating information to the public, ideas, or opinions of general interest, or for literary or artistic expression.

C. Failure to Balance Data Protection and Public Access to Information

Another problematic issue is the lack of clarity between the Data Protection Act and the newly adopted Law on Access to Public Information, relating to the disclosure of personal information of third parties held by public bodies.

---

[46] Council of Europe, The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108] (T-PD), Final document on the modernisation of Convention 108, T-PD (2012)04Mos, 15 June 2012.

[47] Ibid.

Like freedom of expression, the right to information and the right to privacy are both fundamental human rights that are intertwined and need to be properly balanced.[48] The Council of Europe affirmed in a 1986 Resolution that they are "not mutually distinct but form part of the overall information policy in society".[49] Laszló Majténi, the first Parliamentary Commissioner for Data Protection and Freedom of Information in the Republic of Hungary, has described that the two rights have a common purpose "to continue maintaining the non-transparency of citizens in a world that has undergone the information revolution while rendering transparent the state."[50]

A specific recognition of the importance of government transparency has also been incorporated into European law. Recital 72 of the EU Data Protection Directive states that "Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive".

Thus, to meet international standards on balancing the two rights, the legislation must clearly set out the circumstances in which information may be withheld on privacy grounds, and create mechanisms for balancing. This is not adequately achieved in the Ukrainian legislation.

Firstly, it is not clearly delineated in the Law on Access to Public Information under which circumstances personal information may be withheld. There is no specific exemption for personal privacy. Instead, the law uses a broader exemption which applies to a variety of different types of information as set out in other (unnamed) laws. Under Article 6, access to "public information" can be limited when it is "confidential" which is protected by law. 6(2) states that the law must be:

> exclusively in the interest of national security, territorial integrity and civil order with the purpose of prevention of unrests or crimes, protection of public health, protection of reputation and rights of other people, prevention of the disclosure of information received confidentially, promotion of the authority and impartiality of justice.

Article 7(1) defines confidential information as "information, access to which is limited by a person or legal entity, apart from the subjects of public authority, and that can be disseminated at their wish and under their conditions." 7(2) restricts bodies from disclosing the confidential information unless they have consent or "only in the interests of national security, economic wellbeing, and human rights." This is apparently intended to refer to personal information protected under the Data Protection Act. However, it also may include the Law on Information or any other related legislation and it not exclusively and clearly related to personal information.

The reference in 7(2) to human rights may include freedom of expression and information but it is not expressly set out and we understand that courts have already been treating this provision restrictively.

A better approach would be to include in the legislation an exemption for personal information, and to clearly define the circumstances under which it can be withheld, rather to obliquely refer to other laws. The Council of Europe Convention on Access to Official Documents states that:

---

[48] For a more detailed analysis of the balancing of the two rights and legislative frameworks, see Banisar, The Right to Information and Privacy: Balancing Rights and Managing Conflicts (March 10, 2011). World Bank Institute Governance Working Paper. Available at SSRN: http://ssrn.com/abstract=1786473.

[49] Council of Europe Recommendation 1037 On Data Protection and Freedom of Information (1986).

[50] Dr. Laszlo Majtenyi, Freedom of Information, the Hungarian Model (2002), http://www.lda.brandenburg.de/sixcms/media.php/2232/maitenyi.pdf

> Each Party may limit the right of access to official documents. Limitations shall be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting: [...] privacy and other legitimate private interests.[51]

This has been incorporated into most right to information laws globally. For example, under the US Freedom of Information Act, records can be withheld if they constitute "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy".[52] This ensures that the information has both some level of sensitivity and would cause harm if released. The Slovenian Access to Public Information Act limits access when the information is "[p]ersonal data the disclosure of which would constitute an infringement of the protection of personal data in accordance with the Act governing the protection of personal data", which again provides some clarity about the type of information which should be protected and the harm that needs to be met.[53]

This should be further qualified with a requirement providing for the release of information in cases where the public interest in the release is greater than the interest in the protection of the information. Article 6(2)(3) already provides for such a test. However, it should be redrafted to ensure that it reflects and applies to the new specific exemption.

Secondly, in defining personal information, it is also important to clearly describe the types of information which are protected and those that are not protected as a means of ensuring transparency. This can be done by providing a better definition of personal information, which should be consistent across all legislation.

This is only done partially and inadequately in a piecemeal and overlapping fashion in all three of the laws. The Law on Access to Public Information has no definition of personal information while Article 2 of the Data Protection Act takes a broad definition of personal information as "information or aggregate information about a natural person who is identified or may be identified". However, the more archaic Law of Information also states that "any information about the ethnicity, education, marital status, religious convictions, health condition, as well as the address, date, and place of birth of an individual shall be deemed confidential."[54] It is unclear why it is necessary to have multiple definitions.

There are also narrow exclusions in the laws to the types of personal information that can be protected. The protections placed on personal data are somewhat limited by Article 5(4) of the Data Protection Act, which provides for an exemption for the personal data of a person "who claims for or holds an elective post or position of a state official of the first category". However, information about such persons can still be "assigned as such pursuant to the law". Under Article 6(5) of the Law on Access to Public Information, information about expenditures of budget funds and property including the names of those who received them cannot be withheld, and Article 6(6) provides that asset disclosure statements of elected officials and those running for office, and state and local officials above a certain category, are not put into the category of limited access.

It would be better for all of the laws to use a common definition of personal information to define categories of information that are not considered personal information. These should include all official records which list the official activities of public officials and others acting in a public capacity and those attempting to influence them, as well as information relating to expenditures of public funds and

[51] Council of Europe Convention on Access to Official Documents, CETS 205 (2009), Article 3.

[52] Freedom of Information Act, 5 USC 552 b(6).

[53] Access to Public Information Act (ZDIJZ) §6(1)(3).

[54] Law on Information §11(2).

other uses of public resources. In Ireland, the Freedom of Information Act sets out 12 categories of information that constitute examples of personal information.[55] It then sets out 3 broad areas of information that cannot be considered personal information:

> (I) in a case where the individual holds or held office as a director, or occupies or occupied a position as a member of the staff of a public body, the name of the individual or information relating to the office or position or its functions or the terms upon and subject to which the individual holds or held that office or occupies or occupied that position or anything written or recorded in any form by the individual in the course of and for the purpose of the performance of the functions aforesaid,
> (II) in a case where the individual is or was providing a service for a public body under a contract for services with the body, the name of the individual or information relating to the service or the terms of the contract or anything written or recorded in any form by the individual in the course of and for the purposes of the provision of the service, or
> (III) the views or opinions of the individual in relation to a public body, the staff of a public body or the business or the performance of the functions of a public body.

In Slovenia, information must be released "if the considered is information related to the use of public funds or information related to the execution of public functions or employment relationship of the civil servant".[56] In Germany, the Federal Right to Information Law, Section 5, on "Protection of personal data", sets out in detail information relating to information collected in official circumstances:[57]

> (3) The applicant's interest in accessing information shall generally outweigh the third party's interests warranting exclusion of access to the information where the information is limited to the third party's name, title, university degree, designation of profession and function, official address and official telecommunications number and the third party has submitted a statement in proceedings in the capacity of a consultant or expert or in a comparable capacity.
> (4) Names, titles, university degrees, designations of professions and functions, official addresses and official telecommunications numbers of desk officers shall not be excluded from the scope of access to information where they are an expression and consequence of official activities and no exceptional circumstances apply.

Recommendations:

- Clarify the relationship of the three laws by creating and setting out a clear exemption for personal data in the Law on Access to Public Information, and by amending provisions in the other laws which contradict this.

- Create a common list of exemptions for personal data which clearly exclude information collected about public officials or others acting in an official capacity relating to their duties or to matters which may affect their obligations, and to those influencing public policy, and to information relating to expenditures of public funds or use of public resources.

- Ensure that the public interest test in the Law on Access to Public Information Act applies to personal information, to allow for its release where the release of the information is in the public interest.

[55] Freedom of Information Act, 1997, §2(1).

[56] Article 6(3).

[57] Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act) of 5 September 2005.

D. Subject Access

Both the Data Protection Act and the Right of Access to Public Information Act provide a right to individuals to obtain information relating to themselves, commonly known as "subject access". Under the Data Protection Act, individuals have a right to demand information about themselves that is held by both public and private bodies. Under the Law on Access to Public Information, individuals may only demand information from public bodies and others funded by public bodies or delegated power from public bodies.

The texts of the two provisions are virtually identical, which may lead to some confusion by individuals under which law to demand their information under and by officials deciding on which law to apply when a request is made.

Significantly, the two Acts have substantially different means of external appeal for enforcing the right. Under the Data Protection Act, the Data Protection Commission has the authority to investigate claims of denials of rights and to enforce those rights. Under the Access to Public Information Act, appeals for denials are made to a court under the Code of Administrative Courts. Experience from the UK shows that this is likely to be a significant barrier to individuals' access to their own records and their ability to control and correct their files, as court procedures are complex and expensive compared to appeals to independent commissions with a mandate to provide assistance to the individual. If an individual makes a request without specifying which legislation to apply or chooses the wrong one, their ability to have an external review may be limited.

The two provisions should be harmonised to ensure that an adequate means of appeal to an external body is available to those who demand access to records held by public bodies. This could be through an administrative regulation ensuring that all requests are funnelled through the Data Protection Act or by extending the authority of the Ombudsman or Data Protection Commission to hear information requests (more on this issue in following section).

Recommendation:

- Harmonise provisions on subject access in the Data Protection Act and the Law on Access to Public Information to ensure that external enforcement through an independent body is available for denials of access to individuals seeking to access or correct their own records.

E. Oversight Mechanisms

1. Independence of the Data Protection Authority

Article 23 of the Data Protection Act sets up the "Authorised State Body on Personal Data" (Data Protection Commission) as the central executive body to enforce the provisions of the Act. The Article sets out the powers of the Commission including oversight of the implementation of state policy, maintaining the register of databases, conducting investigations, receiving complaints and appeals, and dealing with foreign bodies. This is intended to meet Ukraine's international obligations.

However, the Act is notably silent on important aspects of the Commission including its financing and independence and in 2010, the Government of Ukraine announced that the designated authority under the Directive is the Ministry of Justice. This is inconsistent with Ukraine's international obligations under the Council of Europe's Convention 108, as supplemented by Convention 181, as well as the EU Directive's requirements for countries that are recipients of personal data that originate in EU Member States.

International law clearly requires that the body is functionally and administratively independent from all public authorities. CoE Convention 181,[58] an amendment to the main CoE data protection convention, signed by Ukraine in 2005 and ratified in 2010, states that "The supervisory authorities shall exercise their functions in complete independence".[59] As noted by the explanatory memorandum to the Convention, "Supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence".[60]

Similarly, the EU Data Protection Directive 95/46, Article 28(1), requires each Member State to set up oversight authorities, which "shall act with complete independence in exercising the functions entrusted to them".[61] Furthermore, EU Directive 2002/21/EC on electronic communications networks emphasises the autonomy of national regulatory bodies including that they should be "in possession of all the necessary resources, in terms of staffing, expertise, and financial means, for the performance of their tasks".[62]

In a recent case at the European Court of Justice, the Court noted that "In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure".[63] The Court found that Commissions are "an essential component of the protection of individuals with regard to the processing of personal data",[64] which "must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or [subparts], and not of the influence only of the supervised bodies."[65]

The Court found that independence should be defined as:

> meaning that the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.[66]

This was more recently emphasised by the Advocate General in a July 2012 case reviewing the law of Austria, which places the national commission as part of the Federal Chancellery, a situation similar to that currently in Ukraine.[67] In that case, the Advocate General wrote that the law did not meet the requirements of the Directive because:

---

[58] 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, E.T.S. 181, Strasbourg, 8 September 2001.

[59] Article 1(3).

[60] Explanatory Report to ETS 181.

[61] EU Directive §28, recital 62.

[62] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[63] Case C-518/07 Commission v Germany. p. 18.

[64] Ibid, p.23.

[65] Ibid, p. 25.

[66] Ibid, p. 30.

[67] Case C-614/10 European Commission v Republic of Austria, Opinion of Advocate General Mazak, 3 July 2012.

> It follows that if a person or entity exercises influence over the office and the staff of the supervisory authority, which is unquestionably the case here, that person or entity consequently exercises influence over the authority as such, a situation which is not compatible with the requirement that the supervisory authority be independent.[68]

The requirements of independence are being further strengthened in the proposed revisions of the EU Directive on Data Protection and the Council of Europe Convention 108. Under Article 12bis (4) of the draft revised CoE Convention countries must ensure that "The supervisory authorities shall accomplish their duties and exercise their powers in complete independence. They shall neither seek nor accept instructions from anyone." Article 12bis (5) requires that countries "ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to accomplish their mission and exercise their powers autonomously and effectively."

The revised EU Directive on Data Protection adopts similar language, requiring that countries "ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it,"[69] and that countries "ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers".[70]

Independent commissions are already found in most other countries in the region. For example, the Lithuanian Data Protection Act states that "When discharging its functions established by this Law and making decisions related to the discharge of the functions established by this Law, the State Data Protection Inspectorate shall be independent. Its rights may be restricted only by law."[71] In Poland, the Inspector General is appointed by the Parliament with the consent of the Senate.[72]

2. Lack of Oversight Body for Act on Public Information

The Law on Access to Public Information also fails to provide for an independent oversight body. This is a significant omission. The existence of an oversight body is essential to ensuring the functioning of right to information laws.[73] Like the data protection commissions, the bodies play an important role both in promoting and implementing the right, as well as hearing and deciding appeals. Experience across those countries which have adopted a freedom of information law shows that the establishment of a body to monitor and supervise implementation tends to greatly improve implementation of the law. Because of their specialised mandate and smaller workload, oversight bodies can handle complaints far more quickly than the courts, an important advantage given that information is a 'perishable commodity' and delay may make the requested information irrelevant. If needed they can examine files in closed sessions to verify whether the information-holder's concerns about their disclosure are justified, and directly issue an order for disclosure in appropriate cases. The law should specify that plaintiffs before the body need not be represented by a lawyer, further reducing the costs of an appeal.

---

[68] Ibid, p. 40.

[69] §40(1).

[70] 40(5).

[71] Law of the Republic of Lithuania on Legal Protection of Personal Data, Article 37(2).

[72] The Act of 29 August 1997 on the Protection of Personal Data (unified text: Journal of Laws of 2002 No. 101 item 926 with amendments), § 8(2).

[73] For a detailed review of different oversight models, see Neuman, Enforcement Models: Content and Context (World Bank Institute, 2009).

As importantly, the bodies can play a significant role in educating public officials and members of the public about the existence and implications of the law, and advising the government on ways to improve implementation. It can organise and run training programmes for public officials, or advise public bodies in putting together their own programmes, and by issuing annual reports raise concerns regarding the implementation of the law and providing a focus point for periodic debate.

A significant majority of countries in Europe have adopted some form of external body. In some countries, a free standing entity, such as the Slovenian Information Commission (now merged with the data protection commission), Commission d'accès aux documents administratifs (CADA) in both France[74] and Belgium[75] and the Portuguese Comissão de Acesso aos Documentos Administrativos have been created.[76] These bodies are independent and are able to both receive complaints and to review more generally the activities of the state in implementing the laws.

In many other countries, including Spain, Greece, Bosnia, Croatia, Sweden, Norway and Denmark, the Ombudsman has been designated to hear complaints about denials of access to information. However, a significant disadvantage is the bodies' decisions to order the release of information are not binding on public authorities. They may also be limited in their ability to conduct promotions and systemic investigations of the implementation of the law. This issue has been addressed differently in Ireland, where the Information Commission has also been appointed the Information Commissioner and is giving more powers for that role.

Finally, in the past decade, it has become more common across Europe to merge the information oversight body with the Data Protection Authority.[77] As noted above, both the EU Data Protection Directive and CoE Convention require the creation of an independent authority to supervise the enforcement of the data protection law and all countries in Europe have adopted one in some form.

There is still some debate on the merits of having a single body for data protection and freedom of information. It largely is based on the situation in each country, including the relative recognition of the rights and the perceived expertise of the institution to be able to appropriately enforce and eventually balance both rights. In some countries, such as the UK, the existing Data Protection Commission was extended in a joint commission but relatively less resources were provided for freedom of information, resulting in poor implementation and long delays.

On the positive side, there is also an important economic argument to only having a single body. All the administrative costs such as human resources, technical infrastructure, and administrative support are not duplicated.

Having a single body can also reduce and better manage the possible conflicts between the rights of information and data protection. In practice, many requests for information under RTI will also relate to personal information, and having this dual expertise will allow for better balancing the two. The UK Data Protection Registrar commented during the legislative process that:

> Working within one institution should allow more focused and effective consideration than working across institutional boundaries. Any tension will be contained within the institution. Making the actual decision about where the balance should lie between data protection and freedom of information in a particular

[74] http://www.cada.fr/

[75] http://www.cada.cfwb.be/

[76] http://www.cada.pt/

[77] Estonia, Germany, Hungary, Latvia, Malta, Serbia, Slovenia, Switzerland, and the United Kingdom.

> case will not be less difficult because there is one commissioner. However, with experience and understanding of both issues in-house the decision process itself should be eased.[78]

It is also easier for the public to have a single point of contact for public bodies in order to better exercise their rights. The Slovenian Commissioner has found that it resulted in greater awareness of both rights:

> The merged body also insures for its greater visibility as well as unification of the entire legal practice of the field. It will also increase the awareness of all other government bodies while carrying out the stated legislative provisions to the benefit of all applicants.[79]

Recommendations:

- Amend the Data Protection Act and other laws to ensure the independence of the data protection body from the state. This should be independent regulatory body for the protection of personal data, which is administratively and financially independent of any public authority and is given adequate resources to conduct its activities.

- Create or appoint an independent body for oversight and appeals for the Law on Access to Public Information. This can be the Ombudsman or another independent body. It must have adequate resources to effectively oversee and enforce the right to information.

[78] Elizabeth France, UK DP Registrar, Testimony before UK Parliament,June 1999.

[79] Nataša Pirc Musar, New Principles of the Amended Act on Access to Public Information in Slovenia: Commissioner or Ombudsman, 2006.