Partnership for Good Governance

Partnership for Good Governance
Enhance the Right to Data Protection in Eastern Partnership countries

Training Manual on the Role and Missions of Data Protection Authorities

EXECUTIVE SUMMARY

The aim of this Training Manual is to give a general description of the role and mission of data protection authorities with a specific focus on the experiences of the countries covered by the Partnership for Good Governance (PGG), i.e. Armenia, Azerbaijan, Georgia, Moldova, Ukraine and Belarus.

It is intended to help newly established data protection authorities or new members of these authorities to better understand the features and specificities of data protection authorities.

A specific focus is made on the challenges posed by the establishment of the authority (reasons for the creation of a data protection authority, requirements of independence, definition of a strategy and of a working programme, definition of a structure and an organisational chart, etc).

The consultative role of the data protection authority is then closely described. This role is becoming increasingly diverse and the data protection authority may be involved on various aspects: notification and authorisation procedures; opinions on draft legislations; definition of models and sectoral guidelines; development of accountability tools; establishment of relations with research and innovation circles, etc.

This Training Manual then turns to the supervisory powers of a data protection authority. It describes the *ex post* powers of the authority: the handling of complaints of individuals; the inspections of data controllers; the adoption of sanctions; the ability to bring a case to the attention of judicial authorities, etc.

The need for a communication strategy and awareness raising campaigns is also addressed.

Finally, the cooperation and international activities of the authorities is described.

TABLE OF CONTENT

INTRODUCTION

The rapid and constant evolution of information and communication technologies is extremely beneficial for individuals and should be encouraged. At the same time, individuals may also be confronted with the challenges posed by a continuous stream of data that may take various forms: big data, internet of things, cloud computing, mass surveillance, video surveillance, profiling, credit scoring, behavioural advertising, direct marketing, geolocation through RFID chips or Wi-Fi connections, biometric identification, etc.

This technological revolution brings the questions of privacy and protection of personal data at the centre of our social and political systems.

Data protection authorities whose role, missions and powers are described in this Manual, play an increasingly strategic role to protect the fundamental rights and liberties of individuals in the digital era.

1. The protection of the right to privacy at the international level

1. United Nations

Article 12 of the Universal Declaration of Human Rights, proclaimed by the **United Nations** General Assembly in Paris on 10 December 1948 (Resolution 217 A), provides that "*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*".

This Declaration is a milestone document in the history of human rights and has been translated into over 500 languages. Privacy underpins human dignity and other key values such as freedom of association and freedom of expression. It has become one of the most fundamental human rights issues of the modern age.

Article 17 of the International Covenant on Civil and Political Rights, adopted by United Nations General Assembly Resolution 2200A (XXI) of 16 December 1966 also protects the right to privacy.

Article 16 of the Convention on the Rights of the Child, adopted by the General Assembly Resolution 44/25 of 20 November 1989, states that "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation*".

Other international human rights instruments contain similar provisions. While the right to privacy under international human rights law is not absolute, any interference must be prescribed by law and subject to a careful and critical assessment of its necessity, legitimacy and proportionality with regard to the legitimate aim pursued.

2. Council of Europe

At the level of the **Council of Europe**, Article 8 of the European Convention on Human Rights (ECHR) provides that "*Everyone has the right to **respect for his private and family life**, his home and his correspondence*".

Pursuant to an extensive case-law of the European Court of Human Rights[1], the right to private life encompasses the importance of personal dignity and autonomy and the interaction of a person with others, both in private or in public. It comprises the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of its own personality.

Respect for one's private life includes also for instance the respect of the right to image, the right to personal autonomy, the respect for sexual life, the respect for private and confidential information, the right not to be subject to unlawful state surveillance, the right to control the information about one's private life, etc.

2. The historical development of a specific right to the protection of personal data at national level

1.

In the early 1970s, several countries began adopting broad laws intended to protect individual privacy with the development of information technology. The surveillance potential of information technologies led to the development of specific rules governing the collection and handling of personal information to prevent abuses.

The genesis of legislation in this area can be traced to the first data protection legislations adopted in the Land of Hessen in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (with, in 1974 a law for federal agencies only), or by Germany (1977), France and Luxembourg (1978).

Data protection was also incorporated as a fundamental right in several Constitutions (notably Article 35 of the 1976 Constitution of Portugal; Article 18 of the 1978 Constitution of Spain).

2.

For example, in France, the French Government announced in 1974 a plan, known as SAFARI ("Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus"), designed to identify each citizen with a specific number and, using that unique identifier, to interconnect all government records.

This plan led to great controversy in the public opinion after the publication of an article in the newspaper "*Le Monde*" on 24 March 1974. It underlined the dangers inherent to certain uses of

[1] http://www.echr.coe.int/Pages/home.aspx?p=home&c=fre

information technology and aroused fears that the entire French population would soon be recorded in files without any proper democratic control. This fear led the government to set up a commission mandated to recommend concrete measures intended to guarantee that any developments in information technology would remain respectful of privacy, individual rights and public liberties.

After broad debates and public consultation, it was decided to set up an independent administrative supervisory authority, the "Commission on Information Technology and Liberties" ("Commission Nationale de l'Informatique et des Libertés" or CNIL), to monitor the implementation of the French law on the protection of individuals with regard to the processing of personal data, adopted on January 6, 1978[2].

3.

A large number of countries around the world, on all continents, have adopted data protection legislations. In 2017, 115 data protection authorities are members of the International Conference of Data Protection and Privacy Commissioners[3].

3. The development of the right to the protection of personal data at European and international level

1. Council of Europe

The rapid increase of flows of personal data between organisations and across borders created new risks for the protection of the private sphere of individuals at an international level. At the same time, national legislations in the field of the protection of individuals with regard to the processing of personal data were in most cases non existing. A uniform model of protection had not yet been developed.

In the face of this trend, the representatives of governments at the **Council of Europe** decided to establish a framework of specific principles and norms to prevent unfair collection and processing of personal data[4].

A first step in this direction was taken in 1973 and 1974, with the adoption of Resolutions (73) 22 and (74) 29 which established principles for the protection of personal data in automated data banks in the private sector and in the public sector.

Finally, the Convention for the "Protection of Individuals with regard to Automatic Processing of Personal Data" ("**Convention 108"**) of the Council of Europe was open for signature on 28 January 1981 after four years of negotiations. It is the first binding international instrument which protects the individual against abuses which may accompany the processing of personal data and which seeks to provide a framework for international flows of personal data.

[2] https://www.cnil.fr/en/cnils-facts-and-numbers
[3] https://icdppc.org/the-conference-and-executive-committee/history-of-the-conference/
[4] http://www.coe.int/en/web/data-protection/background

These **principles** set out in Convention 108 concern in particular fair and lawful automatic processing of data and the storage for specified legitimate purposes. They concern also the quality of the data, which must be adequate, relevant and not excessive. Moreover, individuals shall be fully informed about the processing of their personal data and should have a right of access, rectification and deletion.

In addition to providing guarantees in relation to the processing of personal data, it outlaws the processing of **"sensitive" data** (data relating to a person's race, politics, health, religion, sexual life, criminal record, etc.) in the absence of proper legal safeguards.

The Convention provides for the free flow of personal data between states Parties to the Convention unless protection of personal data in the other Party is not "equivalent" or if the data are transferred to a third state which is not Party to the Convention.

The Convention establishes a **Consultative Committee**, consisting of representatives of Parties to the Convention complemented by observers from other states (members or non-members) and non-state actors, international organisations, etc.

An additional protocol to Convention 108 regarding supervisory authorities and transborder data flows was opened to signature in 2001, reinforcing the mission and powers of supervisory authorities and prohibiting the transfer of personal data to states or organisations that do not provide for an adequate level of protection.

In November 2017, 51 states are parties to Convention 108, including countries that are not members of the Council of Europe, such as Mauritius, Senegal, Tunisia or Uruguay[5] (others such as Burkina Faso, Morocco, Cap Verde and Argentina having been invited to accede), reinforcing the potential of Convention 108 to constitute a global standard of data protection rules.

In 2010, on the one hand to better address challenges resulting from the use of new information and communication technologies, and on the other hand to strengthen the implementation of Convention 108, the **process of modernisation of Convention 108 has been engaged** and is currently in its final stage.

One should also mention the **increasing role of the case-law of the European Court of Human Rights** in the field of the protection of personal data. The Court recalls 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*" (cf. ECtHR, *M.S. v. Sweden*, 27 August 1997, n°74/1996/693/885).

An extensive case-law of the European Court of Human Rights has been developed on the protection of personal data[6].

[5] http://www.coe.int/en/web/data-protection/parties

[6] Cf. *Handbook on European data protection law*, published by the Council of Europe and the EU Fundamental Rights Agency: https://rm.coe.int/16806b294a ; Cf. also European Court of Human Rights Factsheet on personal data protection : http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

2. OECD

At the level of the **Organisation for Economic Co-operation and Development (OECD)**, several initiatives have been taken in the late 70s. OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislations and would at the same time prevent interruptions in international flows of data.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts. The Recommendation was adopted and became applicable on 23 September 1980.

The basic principles of national application contained in the Guidelines are the following ones, which are very close to those of Convention 108: collection limitation principle; data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle (right of access, etc.), accountability principle[7].

These Guidelines were updated in 2013. Two themes run through the updated Guidelines:

- a focus on the practical implementation of privacy protection through an approach grounded in risk management, and;
- the need to address the global dimension of privacy through improved interoperability[8].

3. United Nations

At the level of the United Nations, one may mention the Guidelines for the Regulation of Computerised Personal Data Files, adopted unanimously by the General Assembly's Resolution 45/95 of 14 December 1990.

The Guidelines lay out ten principles to provide minimum guarantees of privacy protection for personal data: lawfulness and fairness; accuracy; purpose-specification; interested-person access; non-discrimination; power to make exceptions in specific cases to the first 5 principles; principle of security; supervision by an authority and sanctions; free circulation of data between countries when those countries have "comparable safeguards for the protection of privacy"; applicability of the principles "to all public and private computerised files"[9].

In April 2015, following Edward Snowden's revelations on massive surveillance and a related Resolution of the General Assembly, the United Nations Human Rights Council adopted Resolution 28/16 deciding to appoint for the first time and for a period of three years a Special Rapporteur on the right to privacy[10].

[7] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[8] http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm
[9] http://www.un.org/documents/ga/res/45/a45r095.htm
[10] Cf. http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

4. European Union

In the framework of **the European Union**, articles 7 and 8 of the Charter of Fundamental Rights provide that everyone has the right to respect for her or his private and family life, home and communications and that everyone has the right to the protection of her or his personal data.
Before the Charter, in 1995, conscious both of the shortcomings of laws, and the many differences in the level of protection in each of its member states, the European Union passed a Europe-wide directive.

The **Directive 95/46/EC** of the European Parliament and of the Council of 24 October 1995 was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries[11].

Data controllers must respect the privacy and data protection rights of those whose personal data is entrusted to them. They must for instance:

- collect and process personal data in a fair and open manner, for a legitimate purpose, in a proportionate manner, with accurate and kept up to date data; etc.;
- ensure that there is a legitimate basis to process personal data;
- refrain, with exceptions, from collecting special categories of data that are considered as sensitive;
- ensure the security of personal data;
- inform the individuals about the processing and ensure the right of access to data or the right to object to the processing of data;
- respect certain obligations regarding the processing of personal data;
- respond to complaints regarding breaches of data protection rules;
- collaborate with national data protection supervisory authorities; etc.

This Data Protection Directive has been complemented by other legal instruments.

One may mention in particular the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), known as the e-Privacy Directive[12]. This Directive contains in particular specific requirements concerning the confidentiality of electronic communications, the security of networks and services, data breach notifications, traffic and location data, spam, public directories or calling-line identification[13].

There are also specific rules for the protection of personal data in police and judicial cooperation in criminal matters adopted through the Council Framework Decision 2008/977/JHA of 27

[11] http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046
[12] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058
[13] https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive

November 2008[14]. The protection of personal data collected by the European Union's institutions and bodies is ensured by the Regulation 45/2001[15].

5. General Data Protection Regulation or "GDPR"

In January 2012, the European Commission proposed a **comprehensive reform of data protection rules in the EU**. On 4 May 2016, after several years of negotiations, the official texts of the new Regulation and the new Directive have been published in the EU Official Journal in all the official languages.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation or "GDPR"**) will become fully applicable as of 25 May 2018[16].

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data entered into force on 5 May 2016 and EU member states have to transpose it into their national law by 6 May 2018[17].

The objective of this new set of rules is to give back to individuals control over of their personal data, to simplify the regulatory environment for business and to harmonise data protection legislations throughout European countries.

The E-Privacy Directive and Regulation 45/2001 are also currently under review.

4. The enhancement of the right to the protection of personal data in the 'Partnership for Good Governance (PGG) countries

In April 2014, the European Union and the Council of Europe agreed in a statement of Intent that targeted cooperation activities with Armenia, Azerbaijan, Georgia, Moldova, Ukraine and Belarus - the EU's Eastern Partnership countries - would be implemented under a specific framework of co-operation currently referred to as PGG.

One of the overall objectives of this PGG Programme is to "enhance the right to data protection".

[14] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0977
[15] http://ec.europa.eu/justice/policies/privacy/docs/application/286_en.pdf
[16] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[17] http://eur-lex.europa.eu/legal-c
content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

1. The Republic of Armenia

The Republic of Armenia signed Convention 108 on 8 April 2011 and ratified the instrument on 9 May 2012.

At the same date, it ratified the Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows.

The Constitution of Armenia contains a provision related to the protection of privacy (article 34).

The Law on Personal Data Protection was adopted by the Parliament on 18 May 2015 and came into force on 1 July 2015. It sets up a legal framework for the processing of personal data by the public and private sectors.

The Personal Data Protection Agency of Armenia was established in 2015 based on the Law on Personal Data Protection.

It is an administrative body acting under the Ministry of Justice of the Republic of Armenia responsible for the oversight over the legality of personal data processing.

The Agency controls and supervises the implementation of the personal data protection legislation and legitimacy of personal data processing[18].

The Agency is composed of 7 persons (including the Head of the Agency), for a total estimated population of 3 million persons.

2. The Republic of Azerbaijan

The Republic of Azerbaijan signed and ratified Convention 108 on 3 May 2010.

Article 32 of the Constitution deals with the protection of privacy.

Moreover, a Law of Azerbaijan Republic "on data, data processing and data protection" has been enacted[19].

This law defines the state policy on information systems, types, ways and forms of collecting, as well as on the use and protection of information.

Chapter 5 of this law regulates issues related to the protection of data. According to Article 17, purposes of data protection consist of the following elements:
• to take preventive measures against destruction, loss and falsification of data;
• to provide safety of state, public and citizens;
• to take preventive measures against unauthorised acts connected with destruction, modification, copying and isolation of data;

[18] http://www.moj.am/
[19] https://rm.coe.int/16806aef9d

• to protect confidentiality of data that constitutes the state secret;
• to ensure rights of physical persons and legal entities in information processes and at elaboration, production and use of information systems, technology and means for their support.

On 11 May 2010, the Republic of Azerbaijan adopted a law "On personal data" to regulate the collection, processing and protection of personal data as well as issues related to the cross-border transfer of personal data to define the rights and obligations of public bodies and local authorities, individuals and legal entities operating in this field. Article 4 of this law determines basic principles of the collection, processing and protection of personal data.

The Cabinet of Ministers of the Republic of Azerbaijan approves "The requirements for the protection of personal data" for applying the "Law on personal data". The requirements for the protection of personal data are implemented by the following authorities: Ministry of Communications and High Technologies; State Security Service; Ministry of Internal Affairs; Ministry of Justice; Special state Protection Service.

No independent specific data protection authority has been set up.

3. The Republic of Belarus

The Republic of Belarus is not a member of the Council of Europe and is not a Party to Convention 108.

The Constitution of the Republic of Belarus is the fundamental document for the protection of personal data. In accordance with Article 28 of the Constitution, everyone has the right to protection against unlawful interference in their personal lives, including on their correspondence, telephone and other communications, honour and dignity.

Article 34 of the Constitution establishes the obligation of the government authorities, public associations and officials to grant citizens of the Republic of Belarus the opportunity to review materials affecting their rights and legitimate interests.

This article also stipulates that the use of information may be restricted by legislation in order to protect the honour, dignity and family life of citizens and for them to fully exercise their rights.

The norms of the Constitution are further developed in the law of the Republic of Belarus of 10 November 2008 "On Information, Informatisation and the Protection of Information".

Article 1 of this law defines the concept of personal data, which refers to an individual's basic and additional personal data that must be entered in the population register in accordance with the legislation of the Republic of Belarus as well as other data used to identify such an individual.

Article 18 also stipulates that the collection, processing, storage and use of personal data must be carried out with the written consent of this individual, unless otherwise specified by the legislative acts of the Republic of Belarus.

The procedure used to obtain, transfer, collect, process, accumulate, store, provide and use information about an individual's private life and personal data is specified by the legislative acts of the Republic of Belarus.

According to Article 34 of the law, information users are entitled to review their personal data.

In addition, given the absence of a comprehensive law on the protection of personal data, the legal regulation of the protection of personal data in the Republic of Belarus is administered at the level of secondary laws, the most important of which is the 21 July 2008 "On the Population Register".

This law describes the concept of personal data for the purposes of its enforcement and defines the list of personal data included in the population register as well as the procedure for working with such information.

Currently, there is no independent data protection authority in Belarus.

However, a special law on Personal Data should be developed and might be adopted in late 2018 – early 2019.

4. Georgia

Georgia signed Convention 108 on 21 November 2001 and ratified it on 14 December 2005.

On 10 January 2014, the Additional Protocol to Convention 108 regarding Supervisory Authorities and Trans-Border Data Flows was also ratified.

In **Georgia,** the **Constitution of 1995** protects the individual's right to privacy and secrecy of communications as well as information contained in official records pertaining to health, finances or other private matters of an individual (cf. articles 20 and 41).

The legislative framework related more specifically to data protection is mainly defined by **the Law of Georgia on Personal Data Protection** (cf. Law of Georgia No 6325 of 25 May 2012). This legislation defines the rules and procedures to process personal data in Georgia and creates the Office of the Personal Data Protection Inspector of Georgia.

The law foresees basic principles that shall be followed while processing the personal data and lays down the specific grounds for the legitimacy of data processing. There are separate grounds for the processing of general personal data and sensitive data. In addition, the law provides for specific regulations on biometric data, video surveillance and direct marketing. A separate Chapter of the law on Protection of Personal Data Law deals with the obligations of data controllers including, *inter alia*, the obligation to provide information to the data subject, ensure data security and maintain filing system catalogues. The rights of the data subject are also provided in a specific Chapter of the law. Under the current regulations the data subject has a right to request information or request to supplement, correct, block, destroy, delete or erase personal data as well as the right to lodge an objection or an appeal.

The law applies to the public as well as to the private sector. Its scope and the mandate of the Inspector cover all types of data processing with the following exceptions: (i) data processing for personal purposes, (ii) data processing for the purposes of court proceedings, as far as it may damage the proceeding itself; (iii) processing of data for the purposes of state security (including economic security), defense, Intelligence and counterintelligence activities, (iv) processing of the personal information regarded as the state secret except the information processed for the crime prevention, crime investigation, operative-investigational purposes and for the protection of the public order[20].

The office of the Inspector is composed of 43 persons for a total estimated population of 10.3 million persons.

5. The Republic of Moldova

The **Republic of Moldova** ratified Convention 108 on 28 February 2008 and the Additional Protocol to the Convention on 28 September 2011.

Article 28 of the 1994 Constitution protects privacy and the protection of personal data.

The first law on personal data protection was Law N°. 17-XVI of 15/02/2007, which was abrogated and replaced by Law n°. 133 of 08/07/2011, which constitutes currently the central legal document on personal data protection in the Republic of Moldova. It is worth mentioning two other important documents in this regard: (1) the Law No. 182-XVI of 10/07/2008 regarding the approval of the National Centre for Personal Data Protection Regulation, structure, staff-limit and its financial arrangements and (2) the Law N°. 229 of 10/10/2013 on the approval of the National Development Strategy of the personal data protection domain for the years 2013-2018 and the Action Plan for its implementation.

The National Centre[21] for Personal Data Protection of the Republic of Moldova (NCPDP) was established in 2008, obtaining the status of an autonomous public authority, independent of other public authorities, natural persons and legal entities as provided by Convention 108.

Currently, the NCPDP is the only authority empowered to carry out the supervision over the respect of the rights and fundamental freedoms of natural person with respect to the processing of personal data, notably the right to intimate, family and private life, enshrined in Article 28 of the Constitution of the Republic of Moldova.

A new draft law to enhance the current legal framework is also under preparation.

The Centre is composed of 16 persons (including the Director) for an estimated population of 2.9 million persons.

[20] https://personaldata.ge/en/home
[21] http://www.datepersonale.md/en/start/

It is worth mentioning that the current internal organisation of the Data Protection Authority will be considerably modified as a new law is currently assessed in Parliament. The planned increase of the staff-limit is from 21 to 45 staff members.

6. Ukraine

On 6 July 2010, **Ukraine** ratified Convention 108 and its Additional Protocol. On 1 January 2011 the Law of Ukraine on Protection of Personal Data came into force.

Article 32 of the 1996 Constitution protects privacy and personal data.

The Law of Ukraine on Personal Data Processing was adopted on 1 June 2010. It was since amended nine times (on 23rd February 2012, on 20th November 2012, on 16th May 2013, on 3rd July 2013, on 27th March 2014, on 13th May 2014, on 9th April 2015, on 3rd September 2015 and on 6th December 2016).

According to the amendments introduced by the Law of Ukraine "On amendments to certain legislative acts of Ukraine concerning the improvement of the protection of personal data" the function of control over observance of the legislation on protection of personal data is assigned to the Ukrainian Parliament Commissioner for Human Rights[22].

The Secretariat of the Ukrainian Parliament Commissioner for Human Rights includes a separate structural unit – a Department for Personal Data Protection.

The Department is composed of 15 persons for an estimated population of 42.5 million persons.

5. Scope of this Training manual

The aim of this Training Manual is to give a general description of the role and mission of data protection authorities.

It is intended to help newly established data protection authorities or new members of these authorities to better understand the features and specificities of data protection authorities.

A specific focus is made on the challenges posed by the establishment of the authority (reasons for the creation of a data protection authority, requirements of independence, definition of a strategy and of a working programme, definition of a structure and an organisational chart, etc).

The consultative role of the data protection authority is then closely described. This role is becoming increasingly diverse and the data protection authority may be involved on various aspects: notification and authorisation procedures; opinions on draft legislations; definition of models and sectoral guidelines; development of accountability tools (data protection officers, registers, privacy impact assessment, certification, codes of conduct, etc); establishment of relations with research and innovation circles, etc.

[22] http://www1.ombudsman.gov.ua/en/

This Training Manual then turns to the supervisory powers of a data protection authority. It will describe the *ex post* powers of the authority: the handling of complaints of individuals; the inspections of data controllers; the adoption of sanctions; the ability to bring a case to the attention of judiciary authorities.

The need for a communication strategy and awareness raising campaigns is also addressed.

Finally, the cooperation and international activities of the authorities is described.

If possible, and when resources are available in English, this Training Manual tries to provide examples deriving from the experiences of the concerned countries, i.e. Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. As Azerbaijan and Belarus have not established data protection authorities at the time of the preparation of this Training Manual, few references will be made to the experience of these two countries.

When resources from the experiences of the concerned countries are not available in English, this Training Manual will also provide examples from other countries.

The overall objective is also to share **good practices** that have been developed by various data protection authorities. This Manual may offer a toolbox for newly established authorities or more experiences authorities seeking information on a specific topic.

It should be recalled at the same time that the role and missions of data protection authorities depend in the first place on national legislations. It is the national legislation that will define the scope and extent of the competences of a data protection authority.

Some missions described in this Manual may not be in the scope of competence of a specific data protection authority.

It should be kept in mind that the missions described in this Manual reflect the possible missions of data protection authorities in general and do not reflect the actual missions and competences of each specific data protection authorities in the concerned countries.

PART 1: THE ESTABLISHMENT OF THE DATA PROTECTION AUTHORITY

Nearly all member states of the Council of Europe have adopted specific national data protection legislations, defining principles to protect human rights with regard to the processing of personal data.

Since the principles laid out in the law are general and broad in their nature (proportionality, purpose limitation, quality of data, security, etc.), while the risks are diverse and depend on the specific circumstances of each case, there is a need for an **external oversight from an impartial and qualified authority to reach a fair balance between conflicting interests**, i.e. the need for controllers to process personal data and the need to protect the privacy of individuals.

There is then a need to establish a specific authority with missions and powers to fully implement broad data protection principles, to draw recommendations on categories of personal data processing or even to authorise particular risky data processing to draw guidelines, to respond to complaints from individuals, and to monitor the activities of data controllers and the evolution of information and communication technologies.

Moreover, considering the volume of data processed, the number of possible individuals affected and the rapidly evolving technological landscape, this need may be met in a more responsive and detailed way by an independent and impartial authority than through the adoption of a regulatory framework or through a judiciary response.

A data protection authority may bring the necessary flexibility and reactivity to the challenges posed by the digital era.

As the supervisory authority also needs to monitor the processing activity of the public bodies, this authority should also be fully independent and impartial.

1. The obligation to establish a data protection authority and the existing models

1. Additional Protocol to Convention 108

The **Additional Protocol to Convention 108** states that Parties shall provide for one or more authorities to be responsible for ensuring compliance with the measures in their domestic law giving effect to the principles of the Convention and in its Protocol.

The Additional Protocol does not prescribe a specific model of data protection authority but provides that:

- supervisory authorities shall have the powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities' violations of provisions of domestic law;
- each supervisory authority shall hear claims lodged by any person concerning the protection of her or his rights and fundamental freedoms with regard to the processing of personal data within its competence;
- the supervisory authorities shall exercise their functions in complete independence;
- decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

2. National level

At national level, there are several models for privacy protection. In some countries, several models are used simultaneously.

The regulatory model adopted by European countries, Australia, New Zealand or Canada is the setting up of a *public body* enforcing a comprehensive data protection law.

Some countries such as the United States have avoided general data protection legislation in favour of specific *sectorial laws* governing, for example, video rental records, the protection of the privacy of children or financial privacy.

In other countries, sector laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as police files or consumer credit records.

Some countries also encourage various forms of self-regulation, in which companies and industry bodies establish codes of practice.

The EU Fundamental Rights Agency released a report on the role of data protection authorities. The report states that, in Europe, some states have designated one Data Protection Authority of general competence and several other sector-specific supervisory bodies (for instance, in health, post or telecommunications). Some of those states organised along federal lines or with significant powers held at the regional level are endowed, in turn, with one national supervisory body and several sub-state agencies entrusted with the same function at the regional or federal level. Furthermore, whereas in many countries, prior to the establishment of Data Protection Authorities, the duty to monitor the respect for privacy rights was entrusted to Ombudsman institutions, in some member states, the Ombudsman still maintains a relevant function in protecting personal data.[23]

[23] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

3. Models

Regarding the composition of data protection authorities, two main models are observed in European countries: a collegial model and a single commissioner model.

The collegial model

The collegial model is widespread but not the most common model. For instance, Austria, Belgium, Bulgaria, France, Italy, Greece, Luxembourg, Netherlands, or Portugal have a collegial data protection authority. The collegial model may also be found in Burkina Faso, Quebec, Mexico, Monaco, Morocco, Tunisia, Senegal or Uruguay.

The pluralism and qualification of members of a collegial body depend on the appointment of members who represent diverse backgrounds and constituencies and on the ability of the members to handle human rights and technological matters.

In the European Union, the number of members varies from three in Luxembourg and Netherlands, to four in Italy, to over ten in Portugal and Greece, up to 17 in France.

For instance, the French data protection authority, the CNIL, is composed of 4 parliamentarians; 2 members of the French Economic, Social and Environmental Council, 6 representatives of high jurisdictions and 5 qualified public figures appointed by the President of the National Assembly, the President of the Senate and the French Council of Ministers. The chairperson of CNIL is elected by and amongst its members.

In Belgium, the Parliament selects members from those nominated by the government. The government is obliged to nominate twice as many individuals as the number of members to be selected.

The single commissioner model

The "single commissioner" model is applied in numerous countries, sometimes using different procedures involving for instance an *ad hoc* independent jury before the appointment is made by the government or the Parliament.

Increasingly the designation is made by the Parliament itself. In Germany, the federal data protection authority was at first designated by the government, but he or she is elected now by the Parliament. In the German Länder, commissioners are also selected by provincial Parliaments.

The Commissioner is often assisted by one or two deputy commissioners.

Concerning the European Union Institutions, a specific selection procedure has been set up for the European Data Protection Supervisor and Assistant European Data Protection Supervisor:
- a public call for candidates results in the most competent applicants being shortlisted by an inter-institutional selection board;

- following interviews with the shortlisted candidates, the selection board presents the European Commission with their recommendations for its review and submission to the European Parliament and the Council.
- Hearings to evaluate the experiences, skills and independence of the candidates take place in the European Parliament;
- a joint decision of the Parliament and Council is reached following their deliberations.

4. In the PGG Countries

In the PGG Countries, Armenia, Georgia, Moldova and Ukraine have opted for the regulatory model as further described in the Manual.

Finally, one should mention that some data protection authorities also have a competence, vested by national legislation, in the field of freedom of information and access to public documents.

On this point, there is no single model in Europe, as some countries created a specific authority in the field of freedom of information whereas other countries have conferred to a single authority the competence to act both in the field of freedom of information and the protection of personal data.

2. The independence of data protection authorities

One of the major requirements for the establishment of the authority is the independence necessary to fulfil the missions.

Independence shall first and foremost be guaranteed by the applicable legal framework.

The guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of the managing members of data protection authorities. The budget devoted to the supervisory authority and the control over financial resources represents a second relevant element in ensuring the autonomy, independence and efficiency of the supervisory authorities.

1. Additional Protocol to Convention 108

The Additional Protocol to Convention 108 states that authorities shall exercise their functions in complete independence.

In the consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016[24]), it is clearly indicated in the proposed Article 12 bis that:

"*4. The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.*

[24] Cf. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c

5. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers".

The draft explanatory report[25] states that:

"*111. This Article aims at ensuring the effective protection of individuals by requiring the Parties to provide for one or more independent and impartial public supervisory authorities that contribute to the protection of the individuals' rights and freedoms with regard to the processing of their personal data. Such authorities may be a single commissioner or a collegiate body. In order for data protection supervisory authorities to be able to provide for an appropriate remedy, they need to have effective powers and functions and enjoy genuine independence in the fulfilment of their duties. They are an essential component of the data protection supervisory system in a democratic society. Other appropriate mechanisms for independent and effective review and supervision of processing activities, in so far as Article 9 paragraph 3 applies, may be provided for by the Parties.*

123. Paragraph 4 clarifies that supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the duration of exercise and conditions of cessation of their functions; the availability of sufficient resources to the authority; the possibility to hire its own staff ; or the adoption of decisions without being subject to external interference, whether direct or indirect.

124. The prohibition on seeking or accepting instructions covers the performance of the duties as a supervisory authority. This does not prevent supervisory authorities from seeking specialised advice where it is deemed necessary as long as the supervisory authorities exercise their own independent judgment".

2. **European Union**

In the **European Union**, the requirement for data protection authorities to be independent is laid down in particular by Article 16(2) of the Treaty on the Functioning of the European Union (TFEU) and Article 8(3) of the Charter of Fundamental Rights.

The Court of Justice of the European Union, has consistently emphasised that control by an independent authority is an essential component of the right to data protection and has laid down the criteria for such independence.

In particular, in its Grand Chamber Judgment (*European Commission v. Federal Republic of Germany*, 9 March 2010, Case C518/07[26]), the European Court of Justice found in particular that:

[25] https://rm.coe.int/16806b6ec2

[26] http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1137278

- 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;

- there is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. On the contrary, the concept of 'independence' is complemented by the adjective 'complete', which implies a decision-making power independent **of any direct or indirect external influence on the supervisory authority**;

- The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities 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 the Länder], and not of the influence only of the supervised bodies;

- the mere risk that the state scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks.

The Court has also emphasised the crucial role of independent supervisory authorities in relation to control of international transfers to non-EU countries.

In another case concerning Austria (cf. Judgment of the Court (Grand Chamber), 16 October 2012, *European Commission v Republic of Austria*, C614/10[27]), the European Court of Justice considered that the requirement of independence was not met concerning the Austrian data protection authority in the light of the following elements:

- the managing member of the data protection authority is a federal official subject to supervision;
- the office of the data protection authority is integrated with the departments of the Federal Chancellery; and
- the Federal Chancellor has an unconditional right to information covering all aspects of the work of the data protection authority.

27 http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=303091

2. General Data Protection Regulation (GDPR

The General Data Protection Regulation (GDPR) also emphasises the importance of independence.

Article 52 of the GDPR states that:

"*1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.*

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member state shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member state shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member state shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.; Chapter VI of the GDPR provides detailed rules for the establishment and functioning of independent supervisory authorities, including provisions on the resources necessary for the effective performance of their tasks and powers".

4. Armenia

In **Armenia**, the Personal Data Protection Agency is an administrative body acting under the authority of the Ministry of Justice of the Republic of Armenia responsible for oversight over legality of personal data processing.

5. Georgia

In **Georgia**, the Personal Data Protection Inspector is elected by the Parliament of Georgia. The Inspector is not subordinated to any other public official or body. Any influence on the Inspector or interference in her or his activities is prohibited and punished by the Law. The Inspector enjoys guarantees and immunities.

Concerning the election process, the Candidates to the Inspector's post are elected by a special commission which includes representatives of government as well as civil society organisations.

The candidates are then presented to the Prime Minister who selects at least two persons to the Parliament for the election. Accordingly, the civil society and the executive power are involved, together with Parliament, in the election process.

6. Republic of Moldova

In the **Republic of Moldova**, according to article 22(1) of the Law n°. 133 of 08/07/2011 on personal data protection, the National Centre for Personal Data Protection is led by a Director, appointed by the Parliament, with the majority of votes of the elected members of parliament, on proposal of the Chairman of the Parliament, a parliamentary fraction or at least 15 members of parliament, for a 5-year mandate, renewable once.

7. Ukraine

In **Ukraine,** the data protection authority was first under the authority of the government and this competence has later been conferred to the Human Rights Commissioner elected by the Parliament. Its status is defined by Article 101 of the Constitution of Ukraine, the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" and regarding data protection by the Law of Ukraine "On Protection of Personal Data".

According to Article 4 of the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights", the Commissioner performs her or his duties independently of other state bodies and officials. For the effective realisation of powers in the field of data protection, the Department for Personal Data Protection was established within the Secretariat of the Commissioner.

8. Resources and means of the authority

Concerning the **resources and means of the authority**, which is a condition for a full independence and efficiency, data protection authorities need to receive the resources necessary for their functioning. In most states, the financial resources are allocated from the state's budget on a specific line, and often from the budget allocated to the Ministry of Justice.

In few states, however, the supervisory authorities can significantly increase their financial resources through the revenues obtained from the notifications by controllers of their data processing operations and/or the monetary sanctions imposed as a penalty for the infringement of data protection legislation (e.g. Luxembourg, Malta).

In the United Kingdom, notification fees are the only source of income for the data protection work of the supervisory authority.

In many countries, the lack of adequate level of funding of supervisory authorities is highlighted as a problem[28].

[28] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

The allocation of the necessary budget to the institution is necessary to ensure the material independence of the authority and its efficiency.

The authority should in particular be able to recruit highly specialised employees.

Quite often, the necessary human resources are not available and authorities should be in a position to train new staff members to new competences involving technical, managerial and legal knowledge.

The Authority should also benefit from sufficient facilities and obtain modern IT equipment, solid software and hardware equipment necessary for performing the basic functions: hosting a website for information at national and international level, keeping a register of personal data collections and processing operations, computers for the employees, technical means to receive and instruct complaints and undertake inspections, to test new technologies, to cooperate with other data protection authorities, travel abroad to meetings, etc.

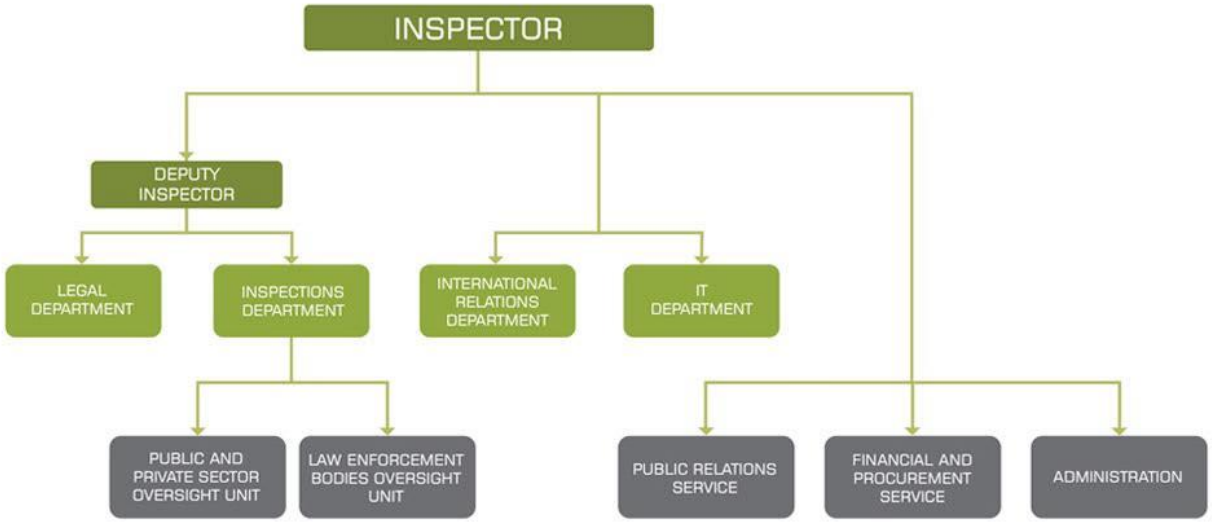
3. The structure of the data protection authority

The choice of a structure is a key decision for the establishment of a data protection authority.

The choice of the structure will largely depend on the local context, on the means and the experience of the organisation or on the specific challenges posed at national level.

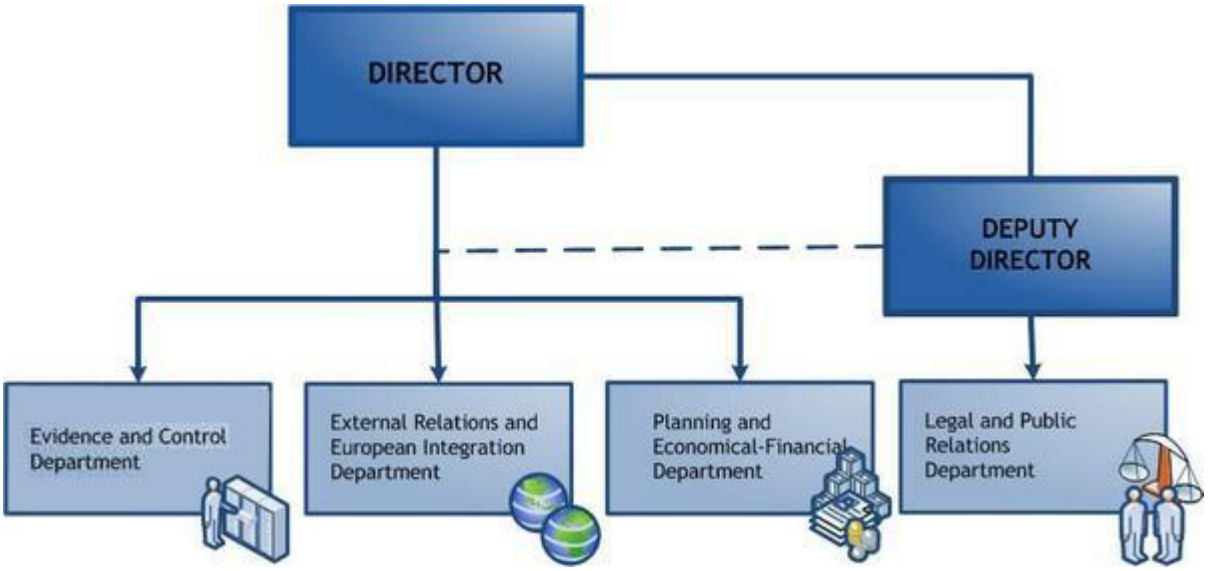
Some examples of existing structures of data protection authorities are given below.

Example 1: **Georgian Data Protection Authority, June 2017**

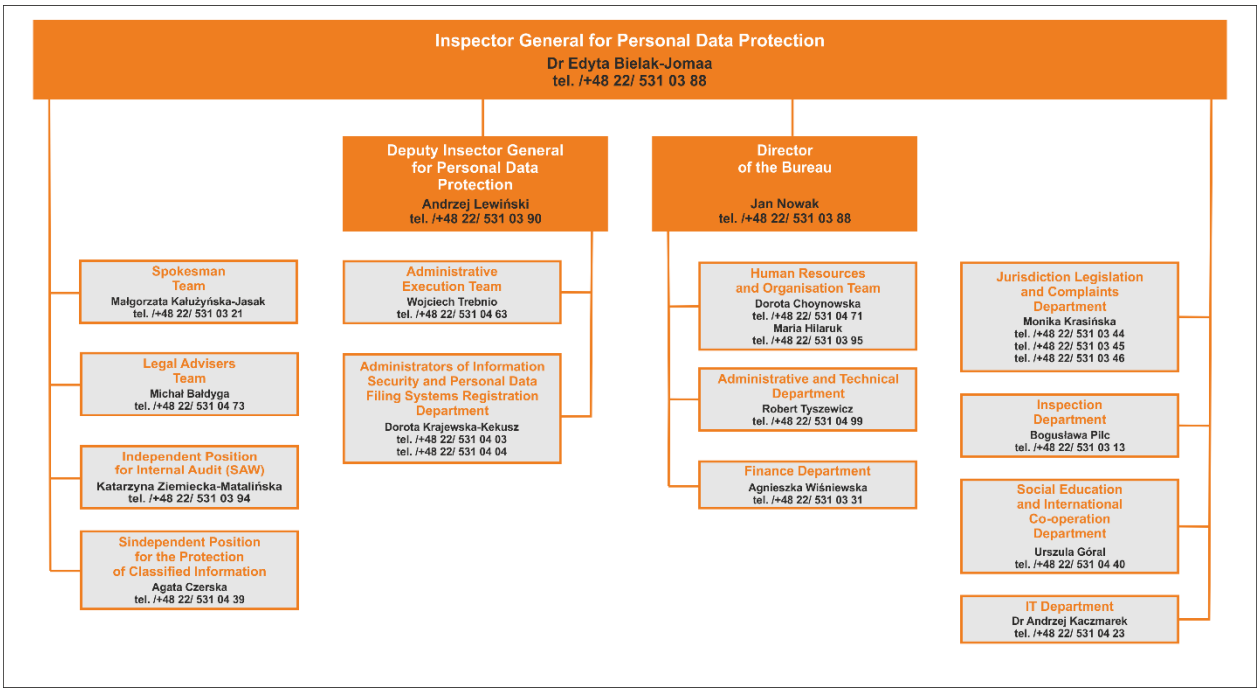


The inspections department is responsible for the investigations on the legitimacy of the data processing. If a violation of the law is revealed, the decision on the sanctions is made by the Inspector in order to separate the investigation power and the power of sanctions. The legal department is responsible for dealing with individuals' complaints.

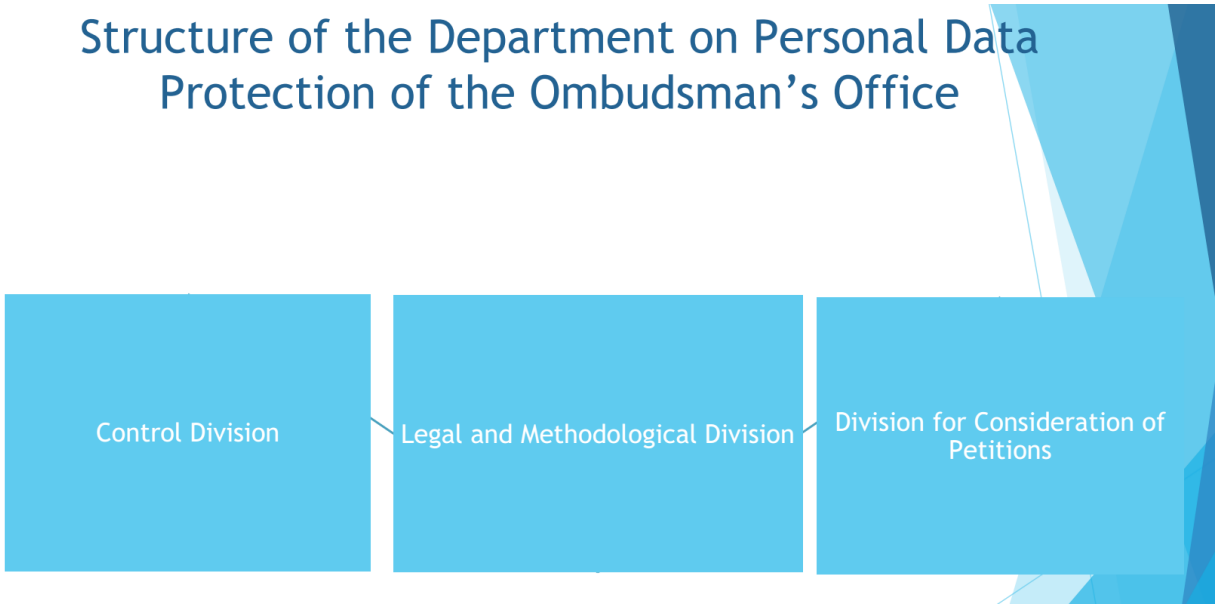
Example 2: Data protection Authority of the Republic of Moldova, June 2017



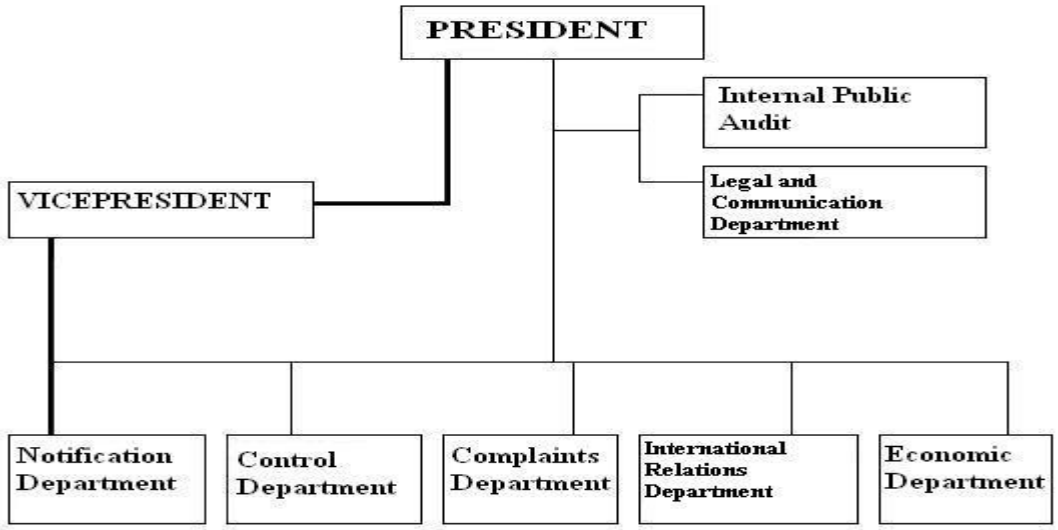
Example 3: Polish Data Protection Authority, June 2017



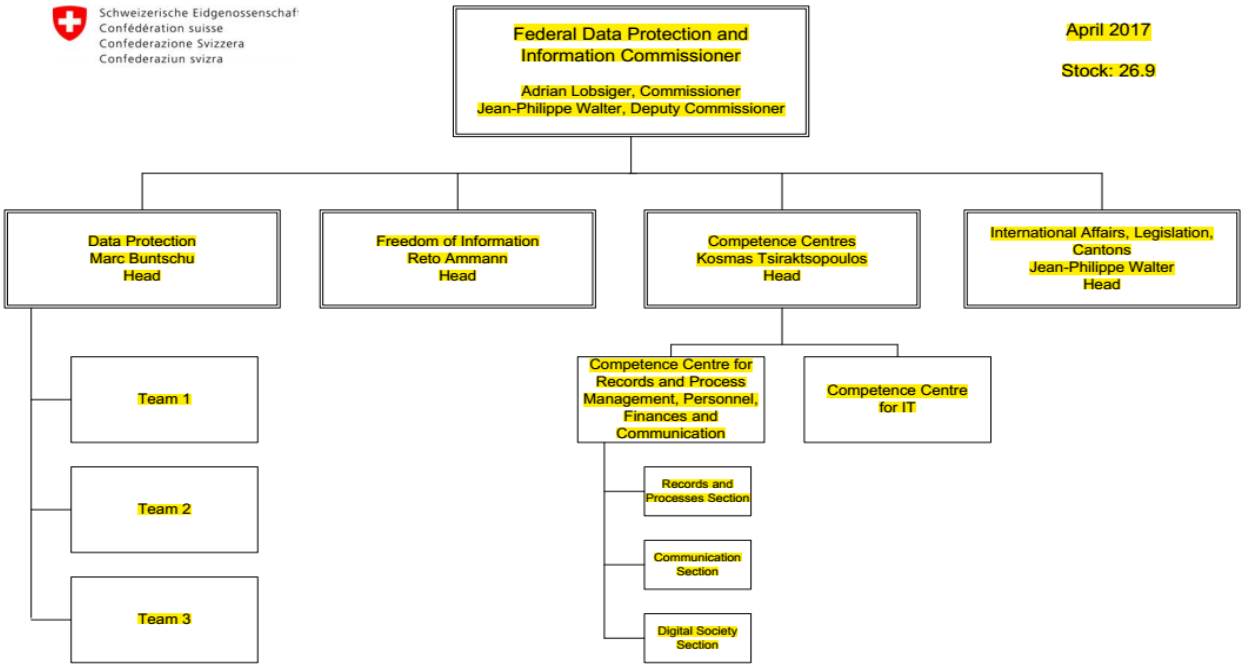
Example 4: Ukrainian Department on Personal Data Protection of the Commission for human rights



Example 5: Romanian Data Protection Authority, June 2017



Example 6: Swiss Data Protection Authority, April 2017



4. The definition of the strategy and the priorities of the institution

1. Priorities

The general mission of a data protection authority is to implement general data protection principles and ensure an efficient protection of individuals with regard to the processing of personal data, while enabling the free flow of information.

With limited human and financial means, and with a rapidly evolving technological context, data protection authorities must **define some priorities and identify key challenges, they will be addressing**.

The overall objective is to establish a virtuous circle for a sustainable data protection framework.

During the establishment phase of an authority, the first priority is in general to install the new facilities and premises of the institution.

The authority will also need to engage in human resources activities. The profiles of the members of the management need to be defined. Other members of the staff should be recruited in a second phase, focusing on various competences and profiles (management, legal and IT advisors, administration and support staff, etc.).

The staff members need to be trained and should be offered some career evolution opportunities.

2. Strategy

In terms of strategy, depending on their powers and the national debates that took place during the adoption of the data protection legislation, some data protection authorities have opted for a preventive and proactive role, emphasising their *ex-ante* role in ensuring the protection of personal data. Some other authorities have given priority to the *ex-post* enforcement and control.

The nature of the powers entrusted to the supervisory bodies may therefore, vary accordingly, with a preference for 'soft' preventive instruments in the first cases and for 'harder' measures in the second cases[29].

3. Implementation of the data protection legislation

When it comes to the implementation of the data protection legislation, data protection authorities usually do not have the means to target at the same time all sectors of activity.

Many data protection authorities make the choice to focus on some specific fields and sectors.

The analyses of the strengths, weaknesses and specific threats in a country should be analysed.

The attention and efforts of a data protection authority may focus on areas that present the highest risks of non-compliance or where the impact on privacy and data protection are the greatest.

Based on findings of the authorities, priorities should be identified.

In the first years, many authorities give priority to awareness raising activities for individuals, controllers (by sector of activity), and processors. One of the first challenge of an authority is to be identified and recognised in its country.

The strategy should also be constantly upgraded, revised and complemented.

4. Awareness

Once people become aware of personal data processing and data protection, polls may be used to identify what are the most pressing problems in one country:

This method was used for instance in Armenia.

Exemple : Poll undertaken in Armenia

Which is the most pressing problem in the field of protection of personal data in Armenia?

- Cameras in public and private places	34%
- Mobile advertising with text messages	16%
- Personal data protection in employment relations	17%
- Protection of data on people's health conditions	16%
- Protection of personal data of minors	17%

Still in Armenia, the Agency focused its activities during the first year of operations on three priority fields, namely: use of video surveillance data, dissemination of unsolicited electronic messages and protection of children. The Agency developed and adopted Video Surveillance Guidelines which are not mandatory but are recommended for use by all entities that carry out video surveillance processing.

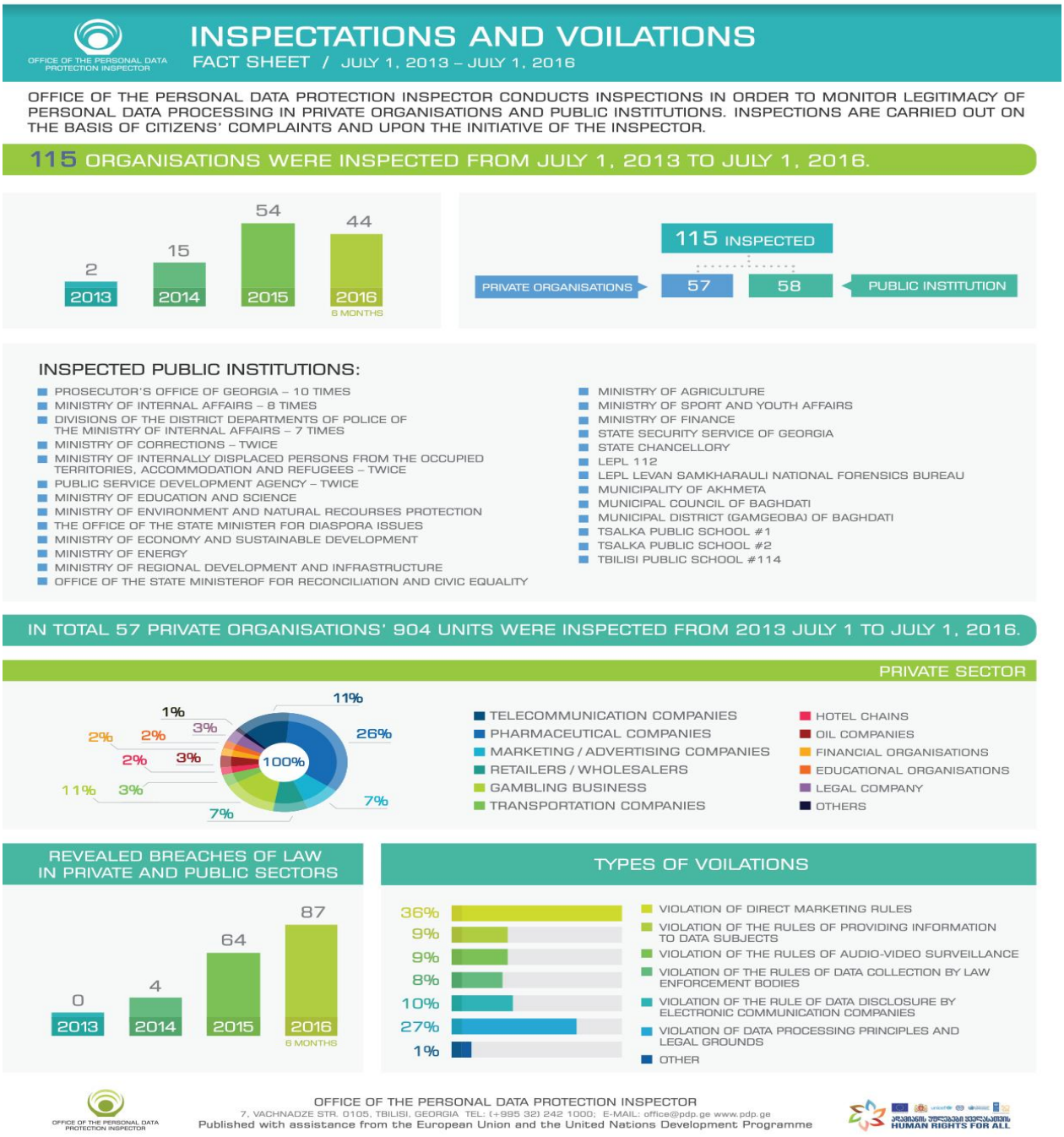
The nature of the complaints received by the data protection authorities may also contribute to help identifying key issues.

5. Georgia

In **Georgia**, a 2017-2021 institutional development strategy and a 2017-2018 action plan for the Office of the Personal Data Protection Inspector have been prepared. In this process the mission, vision, values, strategic goals and respective objectives were defined.

The analysis of the inspections undertaken by the Georgian data protection authority during its first three years of activity show that the main areas of non-compliance in the private sector concern direct marketing companies, electronic communication services, audio or video surveillance, etc.

According to the strategy, in 2017-2020 the main goals of the Office is to activate work in major areas and increase effectiveness of the Agency through organisational development, also to promote public awareness and further develop strategic partnerships[30].



[30] https://personaldata.ge/en/personalur-monatsemta-datsvis-inspeqtoris-aparatma-2017-2021-tslis-strategia-partniorebsa-da-samoqalaqo-sazogadoebas-tsarudgina/667

6. Moldova

The Data Protection Authority of **Moldova** also published its list of priorities and strategy[31]. The need to reinforce the capacities of the institution and to promote the concept of privacy is identified as a priority.

On the 10 October 2013, the Parliament adopted the National Development Strategy of the personal data protection domain for the years 2013-2018 and the Action Plan for its implementation.

A state of play of the implementation of this Strategy and the action Plan is for instance given in the 2016 annual report of the institution.

It describes in particular the objectives of the institution. The General Objective is to ensure an adequate level of personal data protection in the Republic of Moldova.

This General Objective is divided in specific objectives as follows:

- **Specific objective 1**. To inform all personal data controllers about their responsibilities, as well as about the need to protect the processed personal data, taking into account the most recent techniques in relation to the risks deriving from the personal data processing and nature of protected data:
  - Involvement of professional organisations of judges, bailiffs, lawyers, notaries, banks, press, trade-unions, IT, etc. to promote the registration in the Register of personal data controllers, as well as to develop the codes of professional conduct which would include provisions related to personal data protection or completing the codes with such rules;
  - Covering in the media the cases with special resonance and the violations admitted by the public and private law entities when processing personal data;
  - Provision of assistance to public and private institutions, which are established as personal data controllers so as to ensure the observance of the organisational and technical procedures for personal data protection;
  - Provision of assistance to personal data controllers to develop the confidentiality statements, as a contractual clause or being inserted in the job description, mentioning about the civil, contravention, or criminal liability for violation of such statement for the persons who participate in the personal data processing process;
  - Revision of the categories and amount of personal data processed by controllers;
  - Provision of methodological assistance to subdivisions / persons responsible for personal data protection established within the personal data controllers;
  - Tackling the principles of personal data protection, starting with the development of information systems and record-keeping systems meant for automated processing of personal data (privacy by design);
  - Coverage in the media, promotion, and monitoring the observance of the obligation to notify and register the personal data controllers, databases, information systems and IT systems storing and processing personal data,

[31] http://www.datepersonale.md/en/pdp/

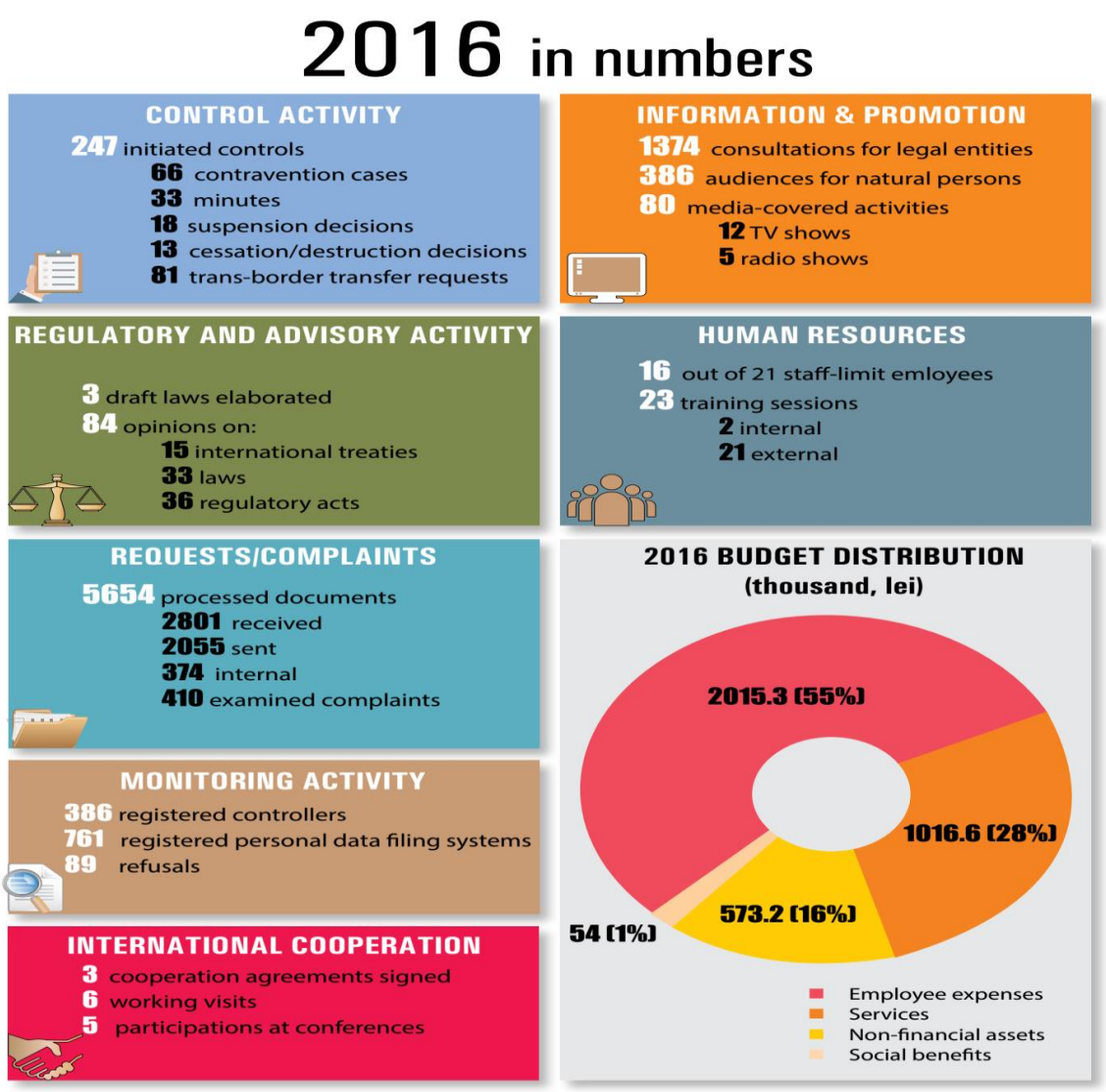
automatically or manually, as well as the observance of the principle of transparency in the activity of data processing.

- **Specific Objective 2.** To raise awareness of the public at large about the rights they have in relation to processing of personal data:
  - Active involvement of the representatives of civil society, authorities from education and mass-media field in raising awareness of the persons about the concepts of "private life", "personal data", the benefits resulting from personal data protection, the negative consequences which may occur when the regime of personal data processing confidentiality and security is not respected, as well as the role of personal data protection in the economic, social, and cultural development of the country;
  - Organization of training courses for journalists related to the need to ensure a balance between the right to freedom of expression and the right to private life;
  - Organization of conferences focused on the need to observe the principles of personal data protection;
  - Organization and implementation of national events dedicated to the Personal Data Protection Day.

- **Specific Objective 3**. To build the administrative and institutional capacities of the National Centre for Personal Data Protection of the Republic of Moldova:
  - Analysis of how the decisions issued by the Centre during the controls undertaken to identify the problems and emerged deficiencies are executed;
  - Analysis of claims and complaints submitted to the Centre so as to identify the problem and the necessary actions to be undertaken to improve the situation in relation to persons' protection as related to personal data processing, as well as the protection of the right to intimate, family, and private life;
  - Revision and endorsement of the sector normative framework in line with the principles of personal data protection;
  - Continuous training, exchange of experience with similar European institutions, participation in seminars, trainings, study visits, workshops, and international conferences;
  - Ensuring the participation in international forums of the national authorities supervising personal data protection, to promote the image of the Centre and that of the country, and active participation in the development of the normative framework regulating the area of personal data protection;
  - Ensuring the information of the public about the problems identified during the control of how the legislation is respected in relation to personal data protection.

In Moldova, the overview of the activity of the National Centre for Personal Data Protection also reflects the strategy and the organisation of the institution.

The following elements are an extract of the 2016 annual report of the institution[32]:



7. European Union

Taking the example of the European Union, the European Data Protection Supervisor (EDPS), which was established in 2001, adopted its Strategy 2015-2019[33].

It identified three strategic objectives and a number of actions to fulfil them:

- "*Data protection goes digital*": the EDPS aims to be an epicentre for creative ideas and innovative solutions, customising existing data protection principles to fit the global digital arena. Accountability is a key element and the EDPS tries to promote technologies that enhance privacy, transparency, user control and accountability in big data processing.

[32] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf
[33] https://edps.europa.eu/press-publications/publications/strategy_en

- "*Forge global partnerships*": the EDPS needs to invest in global partnerships with privacy and data protection authorities, fellow experts, non-EU countries, and international organisations to work towards a social consensus on data protection;
- "*Opening a new chapter for EU data protection*": the EDPS aims to be a more proactive partner to finalise a new EU data protection legal framework.

At the same time, the European Data Protection Supervisor establishes each year its priorities for its policy and consultation work for the coming year.

The annual plan is based on the work programme of the European Commission and the European Data Protection Supervisor adopts a selective approach, taking in particular into account the work programme of the Article 29 Working Party.

8. Consultative Committee of Convention 108

At international level, the **Consultative Committee of Convention 108** in its work programme for 2018-2019[34], identified the following key areas of work:

- Follow-up to the modernisation of Convention 108;
- Promotion of the Convention;
- Delivery of principle-based guidance on challenges to privacy and data protection (genomics and genetics, ICANN policies, artificial intelligence, articulation of data protection with freedom of expression).

[34] https://rm.coe.int/t-pd-2017-wp2018-2019-working-programm-2018-2019-en/168072ab2e

PART 2: THE ADVISORY ROLE OF THE DATA PROTECTION AUTHORITY

Data protection authorities need to foster the implementation of data protection requirements. The advisory role of data protection authorities is of utmost importance to fulfil this objective.

Article 12 bis of the proposal for a Modernised Convention 108 provides that **supervisory authorities shall be consulted on proposals for any legislative or administrative measures** which provide for the processing of personal data. In addition, supervisory authorities should also be asked to give their opinion when other measures concerning personal data processing are in preparation, such as for instance **codes of conduct or technical norms**[35].

Data controllers need to be aware of their obligations and data subjects need to be informed about their rights.

Various tools may be used, depending on the competences conferred to the data protection authorities by national law:

- official opinions on the parliament's or government's draft legislation that will impact data protection or create new files;
- review of notifications / authorisations of personal data processing;
- answers to the requests for advice from data controllers or data protection officers;
- development of accountability tools by data controllers;
- recommendations allowing the data protection authority to establish its "doctrine" in different fields; etc.

Depending on the mandate given by national legislation, the data protection authority is in general in charge of advising **private and public** organisations.

1. Examples of advisory missions of data protection authorities

1. Georgia

In **Georgia**, the advisory role of the Personal Data Protection Inspector and its Office entails for instance the following functions:

- **Provide consultations to public and private institutions, and individuals.** The office of the Inspector is open for consultations in order to establish correct practice of the personal data protection and to assist data controllers and data processors to follow the appropriate regulations. The Office also assists individuals in protecting their rights.

- **Elaborate and Issue Guidelines and Recommendations.** The Office of the Inspector prepares thematic and sector specific guidelines and recommendations for data controllers and data processors to assist in the process of the implementation of the provisions of the law in practice.

[35] http://www.coe.int/en/web/data-protection/modernisation-convention108

2. Moldova

In **Moldova**, the National Centre for Personal Data Protection:

- supervises the observance of the legislation on information protection, in particular the right to information, access, correction, appeal or removal of data;
- offers necessary instructions for adjusting the personal data processing in accordance with the law's principles, without affecting the field of competence of other bodies;
- presents information to personal data subjects on their rights regarding their personal data processing;
- requires necessary information for the performance of its duties and receives free of charge this information from legal entities and natural persons;
- obtains from the personal data holders the necessary support and information for carrying out the Centre's attributions[36].

In its 2016 Annual Report, the Centre gives details about its activity in this field. The Centre issued 84 opinions on draft regulations, draft laws and draft versions of international treaties on matters related to the protection of rights and liberties of natural persons and to personal data processing.

The examined documents are composed of 15 draft versions of international treaties, 36 draft regulations (Government decisions, decisions of the central public authorities etc.) and 33 draft laws (laws and decisions of the Parliament).

The Centre recalls that most of these documents raised objections which induced the formulation of appropriate proposals, as it was considered necessary to complete and review the respective texts in the light of personal data protection regulations.

As some of these drafts were presenting a considerable degree of intrusion in private life, notably weakening fundamental human rights, the Centre submitted several recommendations and objections in order to review these documents in the light of national and European/international standards, some even receiving a negative opinion from the start or in a later instance (if the recommendations and objections were not taken into account by the authors), as for example:

• Draft law on the Archive Fund of the Republic of Moldova (the Centre's proposals were repeatedly not taken into consideration by the authors);
• Draft law on the moratorium on state control (the Centre not supporting the draft, considering that the implementation of this law would lead to serious harm to both personal data subject's rights and to the rights and obligations of public authorities in exercising their competences);
• Draft law modifying and supplementing the law on currency regulation (submitted to the Centre without taking into consideration the previous made proposals and objections);
• Draft Government decision on the Management System of Documents and Authorities Registrations APC (SIGEDIA), towards which the Centre formulated objections in the context of the serious deficiencies detected [37].

[36] http://www.datepersonale.md/en/general/
[37] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

3. **Ukraine**

In **Ukraine**, according to Article 23 of the Law of Ukraine on Protection of Personal Data, the Commissioner has the following competences in the sphere of protection of personal data:

- to receive proposals, complaints and other appeals of individuals and legal entities concerning the protection of personal data and make decisions following their consideration;
- to approve normative legal acts concerning the protection of personal data in cases envisaged by the Data Protection Law;
- to provide recommendations on practical application of the legislation on protection of personal data, to explain the rights and obligations of the relevant persons upon request of subjects of personal data, possessors and controllers of personal data, units or persons responsible for the organisation of the protection of personal data, other persons;
- to submit proposals to the President of Ukraine, the Cabinet of Ministers of Ukraine, other state bodies, bodies of local self-government and their officials about the adoption or amendment to normative legal acts on the protection of personal data;
- to provide the conclusions concerning the draft codes of conduct in the sphere of protection of personal data and changes thereto upon requests of professional, self-government and other public associations or legal entities.

2. Opinions of data protection authorities concerning draft legislations and regulations

Some data protection authorities have the competence to give formal opinions on the draft legislation and its conformity with data protection requirements.

This competence and the procedure is detailed in national legislation.

Some authorities have created procedures for this advisory role.

Exemple: Methodology of the European Data Protection Supervisor (EDPS) for its advisory role

The EDPS has issued a Policy Paper in 2014 on its advisory role and proposed new legislation[38].

Each year, the EDPS publishes a list of priorities for its policy and consultation work for the coming year.

To be most effective, the EDPS provides input **at an early stage of the legislative process**. In accordance with a well-established practice, the EDPS is consulted by the European Commission before it adopts a proposal for new legislation that is likely to have an impact on individuals' right to the protection of their personal data.

Informal comments, that are not published, may be provided at an early stage.

[38] https://edps.europa.eu/sites/edp/files/publication/14-06-04_pp_edpsadvisor_en.pdf

Formal Opinions relate to proposals for legislation and are addressed to all three EU institutions (Commission, Council and Parliament) involved in the legislative process, with the aim of flagging the main data protection concerns together with recommendations. These Opinions are made public and are available on the EDPS website as well as in the Official Journal of the EU.

The EDPS also **monitors new technologies or other societal changes** that may have an impact on data protection. Where appropriate an Opinion is issued at the initiative of the authority[39].

One might also mention that the EDPS has developed a **"Necessity toolkit"** on assessing the necessity of measures that limit the fundamental right to the protection of personal data[40].

3. Role concerning notifications and authorisations

1. **European Union's Directive 95/46/CE**

Articles 18 to 20 of **the European Union's Directive 95/46/CE** refer to the obligation to notify the supervisory authority and the prior checking of processing operations likely to present specific risks to the rights and freedoms of data subject.

Directive 95/46/CE also provides that simplification of or even exemption from notification may for instance be adopted:

- for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects;
- where the controller appoints a personal data protection officer;
- for processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

Article 19 of the Directive provides that the notification shall include at least:

- the name and address of the controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.

Finally, Article 20 provides that member states shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and that supervisory authorities shall check that these processing operations are examined prior to the start thereof.

[39] https://edps.europa.eu/data-protection/our-role-advisor_en
[40] https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

2. In some EU member states

Because data processing practices may be very diverse, a large discretion is left to the states or to the authorities in deciding possible exemptions to such obligation (and any other form of simplification).

For example, some member states of the European Union have made extensive use of the possibility for exemptions from the notification requirement by increasing the accountability of the data controller - in particular through the appointment of a Data Protection Officer (DPO) – while others make very limited exemptions.

In **France** for instance, data controllers are obliged to notify their processing operations and their characteristics, except when exempted by law or by the French data protection authority.

The French data protection authority has developed a whole set of simplified norms, unique authorisations and exemptions that detail its "doctrine" in a specific sector. Exemptions are also granted if the controller has appointed a data protection officer[41], except for cases requiring an authorisation according to the law.

For instance, the EU Fundamental Rights Agency recalls that **Greece's** legislation initially introduced a system of universal notification, thus avoiding the possibility of exceptions and simplifications to registration and notification procedures offered by the Directive. A subsequent amendment of the law introduced the possibility of exemptions, which led to a drastic decrease in notification numbers[42].

In Germany, non-public bodies have a duty to notify automated data processing operations prior to their implementation to the supervisory authority or the competent Commissioner for Data Protection. Public bodies of the Federation have to announce such operations to the national authority. Obligatory registration does not apply if the controller has appointed an internal data protection officer. According to the Fundamental Rights Agency, it appears that a significant number of private companies that are by law obliged to appoint data protection officers do not comply with this obligation and that those companies that do comply with the general obligation to appoint data protection officers very often do not facilitate the efficient and effective work of those appointed[43].

3. From an "ex-ante" control by the DPA to an "ex-post" control

In the European Union, with the forthcoming GDPR, the general approach is to move **from an "ex-ante" control by the DPA to an "ex-post" control.** At the same time, the GDPR establishes new means to prevent possible abuses.

[41] Cf. https://www.cnil.fr/fr/deliberations (in French only)
[42] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities
[43] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

At the whole, notification and authorisation obligations will be substantially reduced under the GDPR.

On the other side the new Regulation adds or maintains some notification obligations to the supervisory authority for instance in the following cases:

- notification of data breaches of security without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (article 33);
- where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (article 36);
- to issue an opinion and approve draft codes of conduct (article 40-5);
- to accredit certification bodies (article 43);
- for certain categories of transfers outside the European Union (article 46-3 and 47); etc.

4. Ukraine

Each data protection authority has developed its own notification forms, taking into account the national requirements.

One may for instance mention that the **Ukrainian** data protection authority has developed various notification forms.

One form is attached to this manual in **Appendix 1.**

In **Ukraine**, a specific Order has also been approved by Decree of the Ukrainian Parliament Commissioner for Human Rights on 8 January 2014, № 1/02-14. This Order deals with the notification conditions for the processing of personal data, which is of particular risk to the rights and freedoms of subjects of personal data.

In particular, the holder of personal data shall inform the Commissioner on exercising of any kinds of processing of personal data, which is of particular risk to the rights and freedoms of subjects of personal data, except if:

- the sole purpose of the processing is to keep the registry in order to provide information to the public, when such registry is defined by law and open to the public;
- the processing is carried out by civil society associations, political parties and/or organisations, trade unions, employers' associations, religious organisations, civil society organisations of ideological orientation providing that the processing of personal data relates only to the members of these associations and is not transmitted without their consent;
- the processing is necessary for the realisation of the rights and duties of the holder of personal data in the employment relationships according to the law.

5. Georgia

Some countries have also introduced a **public register of controllers**. The aim of the public register is to enable individuals to obtain all the necessary information about processing operations.

With this information they are given an overview of the concrete use of personal data and should they wish to, they can exercise their rights, for example the right to access and the right to rectification.

This public registry is in principle accessible to all and nobody has to demonstrate a specific interest to access it.

In **Georgia**, Article 19 of the Law on Personal Data Protection obliges data controllers to keep a filing system catalogue for each filing system. It establishes the types of information to be included in the catalogue and requires a data processing organisation to notify the Office of the Personal Data Protection Inspector before creating a new filing system, adding new data categories or/and amending the information.

The information included in the register is public and the Inspector ensures its publication according to the appropriate rules. In 2015, the Office of the Personal Data Protection Inspector developed an electronic register of the filing system catalogues. In 2014-2015 the Office digitalised about 5,000 filing system catalogues provided by private or public data controllers. In addition, in 2016 the Personal Data Protection Inspector issued the Order Approving the Rule for Notification of the Personal Data Protection Inspector about Maintenance of Filing System Catalogues and Publication of Filing System Catalogues, according to which filing system catalogues can be submitted only in electronic form through the electronic register of filing system catalogues.

The Order simplified provision of electronic system catalogues to the Office of the Personal Data Protection Inspector, as well as the update of submitted filing system catalogues by data controllers. The electronic register of filing system catalogues also allows interested individuals to receive information about the categories of data processed by public and private organisations[44].

6. Moldova

In **Moldova**, according to the provisions of Article 23 of the Law no. 133 of 08/07/2011 on personal data protection, controllers and processors, have the obligation to notify to the Centre their personal data processing operations within a specific purpose.

During 2016, its Evidence and Control Department examined 850 notifications in order to register controllers and automatic and/or manual personal data filing systems in the Register of evidence of personal data controllers.

[44] https://catalog.pdp.ge/

Therefore, during this period were registered 386 controllers and 761 personal data filing systems. In examining the authorisation and registration notifications brought to the Centre, in accordance with Article 24 of the Law on personal data protection, 612 prior checks were performed. Furthermore, 89 refusals to register and authorise personal data processing operations were issued.

From the total written requests in 36 cases personal data trans-border transfers were authorised and in 25 cases they were refused, the Centre indicating the considerations that led to these decisions[45].

4. The importance of sector guidelines and recommendations

Data protection authorities need to provide guidance to data controllers, data processors and data subjects on the implementation of broad general data protection principles in specific sectors.

In that respect, one of the main tasks of data protection authorities is to develop sectoral guidelines establishing the "doctrine" of the supervisory authority.

It may be a good practice to hear the various stakeholders on a specific matter before adopting such guidelines..

1. Armenia

For instance, the Agency for Protection of Personal Data of the Ministry of Justice of the Republic of **Armenia** published a guide on the protection of personal data in labour relations.

The purpose of the latter is to ensure a high level of protection of personal data in labour relations, protect the rights of employees (data subjects), inform employers (data developers) on the main issues of personal data protection and ensure a uniform interpretation of legislation[46].

The authority has also issued for instance a Guide on the Protection of Personal Data of Children.

The purpose of the Guide is to ensure an integrated interpretation of the legislation on personal data protection, to raise awareness of children, parents and data controllers about their rights and responsibilities and to increase the level of protection about the processing of children's personal data.

The principles of protection of children with regard to personal data processing, the rights of children in the sphere of protection of personal data and the responsibilities of data controllers and processors, the peculiarities of the processing of personal data within educational institutions, on the Internet and in the mass media and the liability envisaged for violation of the right of protection of personal data of children have been introduced[47].

[45] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf
[46] http://www.moj.am/en/article/1760
[47] http://www.moj.am/en/article/1718

2. Georgia

The Data Protection Authority of **Georgia** published the following guidelines, available in English, on its website:

- Recommendations on Processing of Biometric Data;
- Recommendations for Conducting Video Surveillance;
- Recommendations on Personal Data Processing for Direct Marketing Purposes;
- Recommendations Regarding Personal Data Protection in Labor Relations[48].

The Inspector also published (for the moment in Georgian only) recommendations on the processing of data related to health, recommendations for schools and parents of the school children, recommendations for Internet service providers and users, etc.

3. Moldova

The National Centre for Data Protection of the Republic of **Moldova** also issued several recommendations on specific issues. One may for instance mention the following instructions, available in English on the website of the institution:
- Instructions on the processing of personal data in the election process.
- Instructions on the processing of personal data in the police sector
- Instructions on personal data processing in the education sector [49].

It also issued several recommendations and videos on the protection of personal data of children[50].

Through the upcoming EU-funded Twinning project, several guidelines and recommendations are also planned in the following sectors: financial-banking; IT and electronic communications; mass-media; healthcare; law enforcement and video surveillance and some existing ones will be revised as for example the one regarding electoral process.

4.

More generally, one should also refer to the numerous opinions, recommendations, resolutions and guidelines developed by:

- the Consultative Committee of Convention 108[51];
- the Article 29 Working Party of the European Union (nearly 250 opinions)[52;]
- the International Conference of Data Protection and Privacy Commissioners[53];
- all the data protection authorities at national level[54].

[48] https://personaldata.ge/en/publications/recommendations
[49] http://www.datepersonale.md/en/decizii/instructiuni/
[50] http://www.datepersonale.md/en/copii-protectie/
[51] http://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[52] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 ; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
[53] https://icdppc.org/document-archive/
[54] http://ec.europa.eu/justice/data-protection/bodies/index_en.htm

This extensive set of publicly available tools may offer guidance for other supervisory authorities but also for controllers, processors or individuals.

5. The increasing role of accountability and data protection officers

1.

There is an increasing trend to shift from an *ex-ante* supervision to an *ex-post* supervision.

If the data protection regulation system was in some countries previously largely based on notifications and authorisations, there is a clear increase in the development of the accountability principle.

The GDPR integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

The overall idea is to integrate a "data protection culture" within organisations processing personal data.

With that respect, tools should be developed to demonstrate this compliance. In some cases, certain tools are compulsory and have to be implemented by controllers.

In any case, even if there is no legal obligation, the development of programs and tools by controllers or processors may be encouraged by data protection authorities.

The objective is to develop a compliance "toolbox" by using the different means of action: adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; the data protection officers who form a privileged network of experts; the development of certifications and, for instance binding corporate rules that frame transfers of personal data within multinational companies; the creation of "conformity packages" by the DPA that are sector-based reference models covering an entire sector or professional branch; etc

2.

In an accountability-based approach, **data protection officers** are at the heart of the legal framework and should facilitate compliance with data protection requirements.

With that respect, data protection officers have become absolutely essential actors within public and private organisations which deal with personal data.

Under the GDPR, it is mandatory for certain controllers and processors to designate a data protection officer (DPO).

This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

The Article 29 Working Party already adopted Guidelines on data protection officers.

In particular, the Article 29 Working Party argues that: "*the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out data protection impact assessments and audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).*

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)).

Data protection compliance is a responsibility of the controller or the processor. The controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively."[55].

The training of DPOs and the establishment of networks of DPOs should also be encouraged.

3.

Moreover, **privacy impact assessments** will play an increasing role to foster compliance.
Article 35 of the GDPR introduces in EU law the concept of a Data Protection Impact Assessment (DPIA).

A DPIA is a process designed to describe the processing, assess the legitimacy and the legal basis of each purposes, the necessity and proportionality of a processing with regard to the data processed and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance.

Keeping in line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons".

On this question, the Article 29 Working Party also already developed specific guidelines[56].

[55] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
[56] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

4.

Increasingly, some data protection authorities have the power to deliver **certifications** for products or procedures that deal with data protection.

Usually, the certification allows a controller to distinguish itself from others by the quality of their services. For the users, it is a trust indicator on ICT products, services and procedures that allows users to identify and favour organisations that guarantee a high level of protection of personal data.

Finally, the GDPR encourages the drawing up of **codes of conduct** to be approved by the data protection authority. Such codes of conduct intend to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

These codes of conduct may be elaborated by associations and other bodies representing categories of controllers or processors or categories of data subjects. They should contain efficient mechanisms to monitor compliance with its provisions by the controllers or processors which undertake to apply it. Such mechanisms do not prevent data subjects from complaining to the data protection authority or to the judicial authorities.

6. Innovation and research

1.

Data protection authorities should also be encouraged to establish as soon as possible, strong relations with high level **research and innovation experts,** IT industry and services, with public authorities, with representatives of the private sector and of NGOs.

Supervisory authorities need to be fully aware of the new technological developments and accompany these developments as soon as possible.

2.

For instance, the French data protection authority, the CNIL has a **laboratory** within its walls that is dedicated to the testing and experimentation of cutting-edge products and applications. This laboratory is testing products, apps and services at their beta stages in order to evaluate their potential impact on the private lives of data subjects. With keeping "privacy by design" in mind, the CNIL strives to integrate data protection requirements within technological architectures, IT developments and new services.

In order to reinforce its mission to elaborate and reflect on potential prospects, the CNIL set up in 2012 a **Prospective Committee** that brings together external experts. It strives to consolidate two objectives: the taking into consideration, at a very early stage, of new subjects like tendencies, technologies or upcoming uses for data; and, the assessment of case studies and analyses brought about by innovative tools and projects.

Finally, the CNIL also created a **thesis award** in the field of data protection recognising the value of academic works and inciting the development of research regarding data protection and privacy rights in universities. This award touches many different disciplines such as: social sciences, law, political science, economy as well as technical fields[57].

3.

To give another example, the European Data Protection Supervisor (EDPS) identified Big data and data mining as a possible threat for both the right to privacy and data protection, but also other fundamental rights including freedom of expression and non-discrimination.

Big data is a long-term strategic concern for data protection authorities but also for other enforcement agencies in the areas of competition and consumer protection.

Considering this, the EDPS proposed the establishment of a **Digital Clearinghouse** to bring together agencies from the areas of competition, consumer and data protection willing to share information and discuss how best to enforce rules in the interests of the individual.

With this initiative, the EDPS intends to encourage a worldwide debate on the implications of big data and the need for reflection by legislators and regulators[58].

[57] https://www.cnil.fr/en/cnils-missions
[58] https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en

PART 3: THE SUPERVISORY ROLE OF DATA PROTECTION AUTHORITIES

Data protection authorities shall have the powers to monitor the compliance with data protection legislations.

To that end, data protection authorities usually have "*ex-post*" supervisory powers that enable them to receive and instruct complaints of individuals, undertake inspection of data controllers or processors, adopt sanctions and / or refer cases to the judicial authorities.

1. The handling of complaints

1. International standards

Article 1 of the Additional Protocol to Convention 108 provides that supervisory authorities shall "*have, in particular powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.*

Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence".

Article 12 bis of the consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016[59]) also states that "*each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress*".

According to Article 57 of the GDPR, each supervisory authority shall handle complaints lodged by a data subject, or by a body, organisation or association and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.

Each supervisory authority shall facilitate the submission of complaints by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

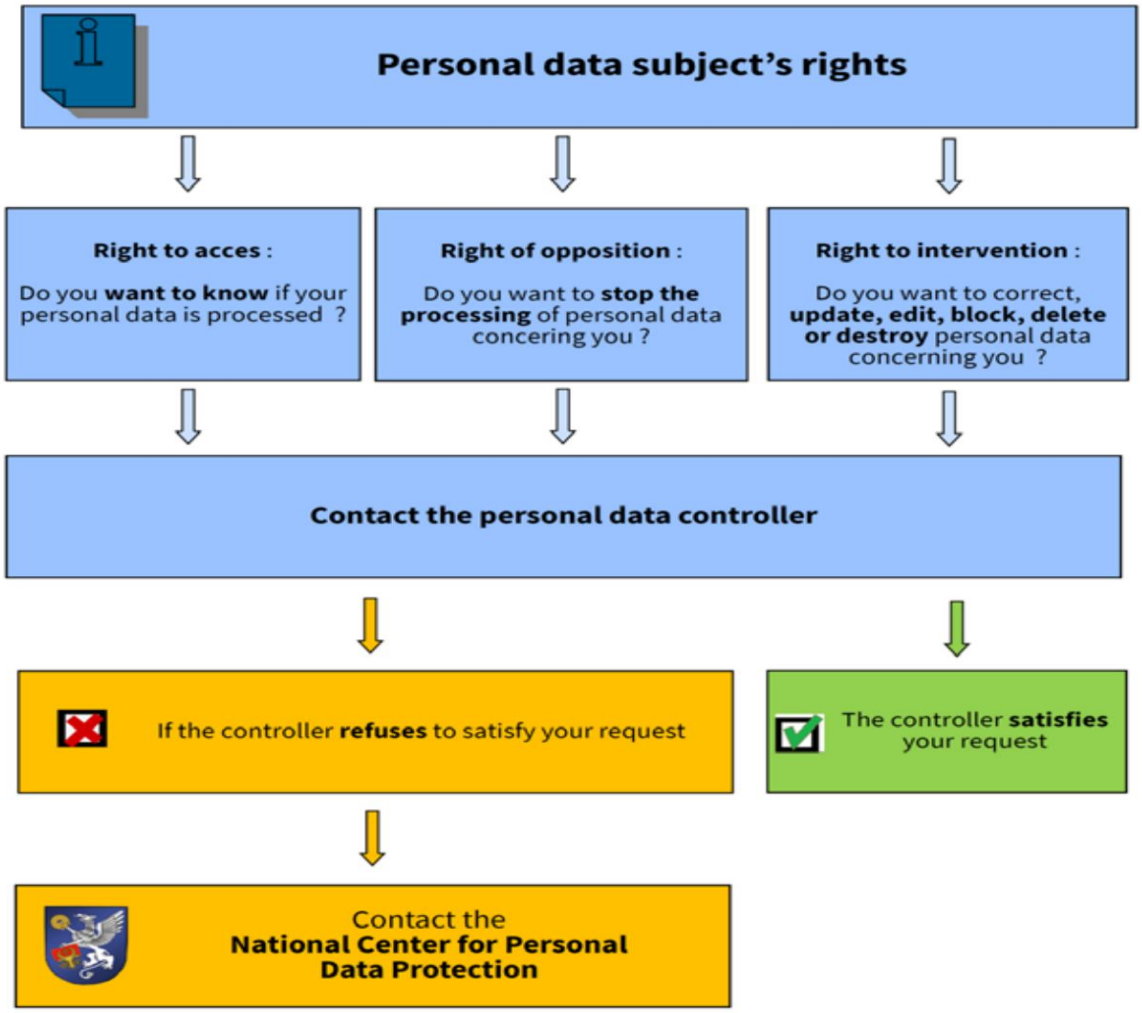
The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

[59] Cf. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c

The possibility for individuals to file a complaint is a key element for an efficient architecture enabling the protection of individual with regard to the processing of personal data. This helps to guarantee the right to an appropriate remedy. Complaints may for instance be filed if excessive amounts of personal data are being collected; if an individual is refused to access her or his personal data; if data has been processed illegally; etc.

2. Moldova

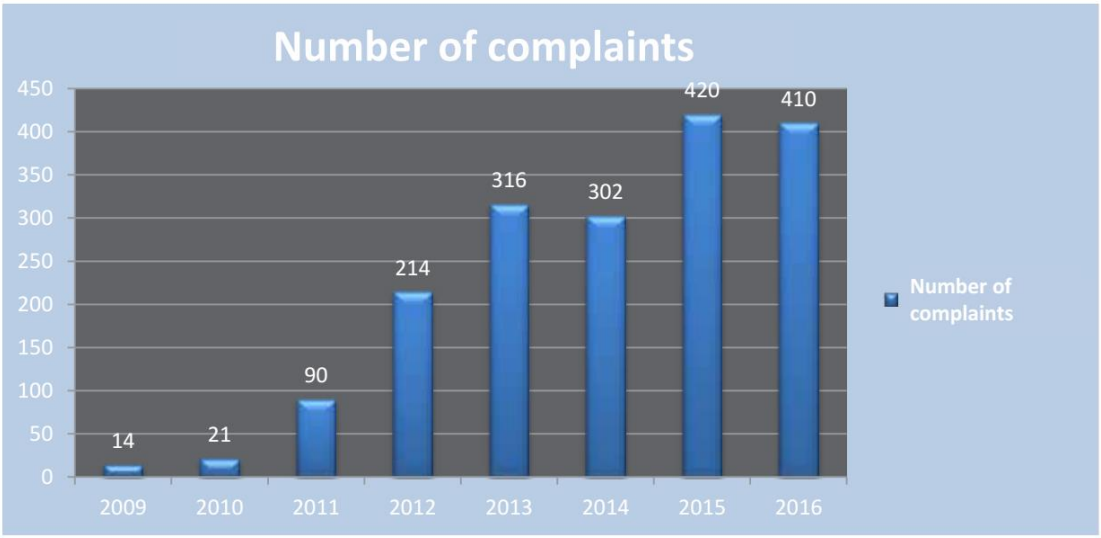
In **Moldova**, the National Centre for Personal Data Protection issued in its 2016 annual report, a description of the personal data subject's rights realisation procedure:



The number of complaints received is an important indicator of the level of awareness of individuals about their rights, as underlined by the data protection authority in its annual report[60].

[60] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

The evolution of the number of complaints submitted to the National Center for Personal Data Protection of the Republic of Moldova during 2009-2016



The considerable increase of the number of complaints received during 2015 (by 37% compared to 2014) demonstrates that data subjects have in comparison to previous years better understood the attributions of the NCPDP, and have more trust in the efficiency of the actions taken by the national supervisory authority for personal data protection in defending their fundamental rights and freedoms.

The complaints received by the NCPDP were dealing with a large range of issues related to personal data processing in the financial-banking sector, health sector, public services, video surveillance of public and/or private spaces, personal data processing conditions for controllers and recipients, the aspects related to personal data disclosure and the failure to respect security and confidentiality measures.

In 2016, in 171 cases, the NCPDP initiated personal data processing lawfulness controls based on complaints. In 113 cases, personal data subjects contacted the NCPDP to signal infringement of legal provisions related to the conditions in which personal data was disclosed to third parties without obtaining prior consent of the data subjects or without taking enough into consideration the right to information of the respective persons, personal data processing without a legal basis or disproportionate with the pursued purpose, disclosure of personal data in an unrestricted manner on the internet or on a mass-media or a company's website and blogs or using file sharing networks.

In 2015, one might notice a significant increase in the documents received from public and private legal persons. In particular, a significant percentage of these documents came from institutions as the Ministry of Internal Affairs, Ministry of Healthcare, Ministry of Information Technology and Communications, Ministry of Justice, state Chancellery, but also from stakeholders from the finance-banking, tourism, trade, services sphere field - entities directly involved in personal data processing.

3. Georgia

In **Georgia**, the Office examines the lawfulness of data processing in public and private institutions. The Inspector is empowered to inspect data controllers and data processors on the basis of the applications received and by its own initiative. The Inspector is authorised to access any information from the data controllers, including information regarded as state, commercial or professional secrets.

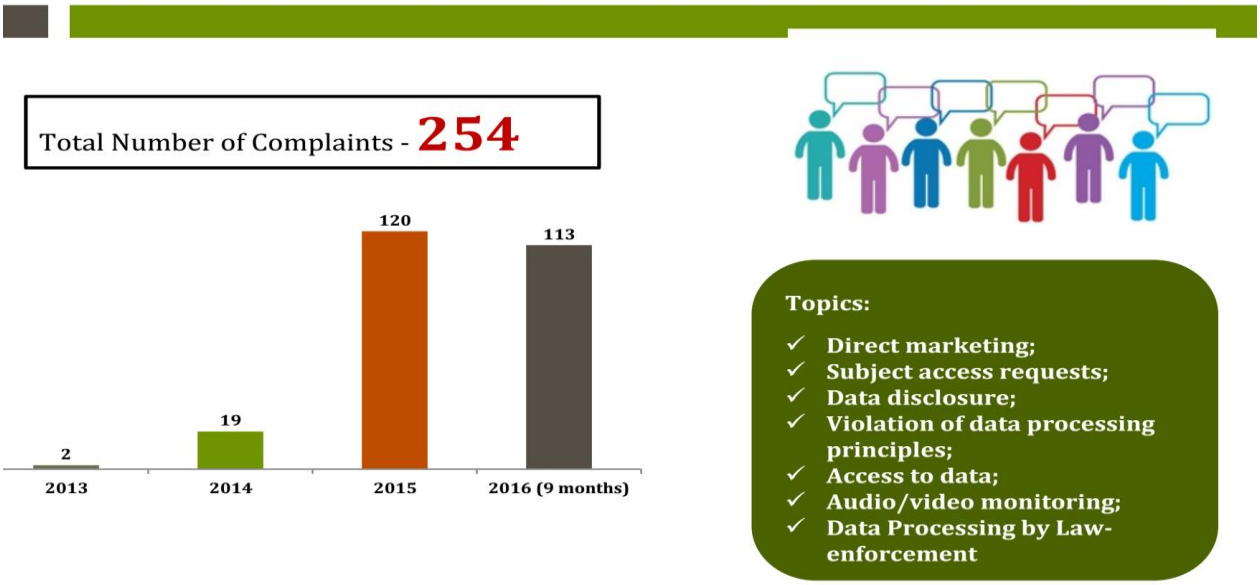
It deals with the individuals' complaints and is authorised to take measures prescribed by the law. While reviewing the complaint, the Inspector analyses provided facts and circumstances. If deemed necessary, the Inspector requests additional information and inspects the data controller and/or data processor. The timeframe for the dealing with the complaints is two months. This term can be prolonged for a one-month period with the reasoned decision of the Inspector.

If the unlawful data processing is revealed, the Inspector is entitled to:

- Request eradication of infringement and related discrepancies within the requested timeframe and in the recommended way;
- Request temporary or permanent termination of the data processing;
- Request obstruction, erasure, destruction and/or depersonalisation of data;
- Request termination of trans-border data flow;
- Provide recommendations to the data controller and/or data processor in case of minor violations;
- Address the Court if the data controller or data processor fails to fulfil the request of the Inspector;
- Draft a protocol if an administrative offence is revealed and impose administrative responsibility on the data controller/data processor;
- Address the law-enforcement bodies if the elements of a crime are revealed.

In Georgia, in 2016[61], the number of consultations provided to individuals, public and private organisations increased three times; the number of individuals' complaints and inspections was also increased two times; 221 facts of violations were revealed; fines were imposed on 63 organisations; while 35 organisations were warned[62].

[61] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf
[62] https://rm.coe.int/16806eead9



4. Ukraine

In **Ukraine**, on the official website of the Ukrainian Parliament Commissioner for Human Rights, people can find information how to file a complaint to the Commissioner.

Complaints to the Ukrainian Parliament Commissioner for Human Rights shall be submitted in writing and may also be sent via email. They shall mention various information, including details about the plaintiff and the essence of the request.

Ukrainian citizens, regardless of their place of (temporary) residence, foreigners and stateless persons residing on the territory of Ukraine, or persons acting on their behalf may lodge a complaint within one year after disclosure of the acts of violation of human rights and freedoms. In exceptional cases, this period may be extended by the Commissioner but should not exceed two years[63].

The Commissioner also provides extensive information about inadmissibility criteria[64].

638 complaints concerning data protection were filed in 2015 and 1,306 for the year 2016[65].

Complaints usually concern transfers of personal data to third parties; legal grounds for processing of personal data; access of the data subject to her or his personal data; compliance with the personal data protection legislation on the Internet.

[63] http://www.ombudsman.gov.ua/en/page/applicant/admissibility-criteria-for-petitions-to-the-commissioner/
[64] http://www.ombudsman.gov.ua/en/page/applicant/inadmissible-petitions/
[65] https://rm.coe.int/16806eeae1

5. United Kingdom

The supervisory authority may also provide, as a matter of good practices, template letters for individuals, for instance to access their personal data or to raise concerns to controllers or processors.

For instance, the Information Commissioner's Office in the United Kingdom publishes such templates on its website[66].

The Information Commissioner's Office also publishes a list of concrete cases, describing the methodology used when handling a case[67].

Examples are given in Appendix.

6. European Union

For the **European Union**, the EDPS gives advice on how individuals may exercise their rights or file a complaint.

Individuals who believe their rights have been infringed may complete a complaint form online[68].

In principle, the controller or its data protection officer should be contacted before a complaint is addressed to the EDPS.

A complaint must be made within two years of the date the individual becomes aware of the facts on which your complaint is based.

The EDPS handles the complaint confidentially. However, the concerned institution may be informed for the investigation. A request to remain anonymous may be lodged by the petitioner. If this request is not satisfied, the person may be able to decide to withdraw or proceed with the complaint.

To investigate a complaint, the EDPS is entitled to obtain all personal data and all information necessary for the enquiries from the EU institution concerned. It may also access the premises of any EU institution should an on-site investigation be needed. Complaints may also be decided on the Supervisor's initiative.

7. France

In France, the CNIL offers on its website an online complaint service for handling of complaints such as: the erasure of personal data on the internet, the objection to receiving publicity by mail, and the updating of the accuracy of personal data[69].

[66] https://ico.org.uk/for-the-public/raising-concerns/
[67] https://ico.org.uk/action-weve-taken/case-stories/case-story-10/
[68] https://edps.europa.eu/node/75
[69] https://www.cnil.fr/fr/plaintes

The solution, in some cases, may be found by a simple informal mediation operated at the initiative of the CNIL with the controller.

On behalf of data subjects, the CNIL can access national security, defense, and public security files that contain their data—especially surveillance and judicial police files. This type of access is called an **indirect access**. When requesting the CNIL to consult these files, one must write a letter to the CNIL indicating precisely their address and their telephone number as well as including a photocopy of their identity card.

2. The procedure to undertake inspections

1. European standards

According to the Additional Protocol to Convention 108 and to the proposed modernised text, supervisory authorities shall have powers of investigation and intervention.

Data protection authorities shall in particular have the possibility to ask the controller and processor for information concerning the processing of personal data and to obtain it.

According to the draft explanatory report to the modernisation proposals, the supervisory authority's power of intervention "*may take various forms in the Parties' law. For example, the authority could be empowered to oblige the controller to rectify, delete or destroy inaccurate or illegally processed data on its own account or if the data subject is not able to exercise these rights personally.*

The power to take action against controllers who are unwilling to communicate the required information within a reasonable time would also be a particularly effective demonstration of the power of intervention"[70].

Under the GDPR, each supervisory authority shall monitor and enforce the application of the legislation. It shall conduct investigations on the application of the Regulation, including based on information received from another supervisory authority or other public authority.

According to Article 58 of the GDPR, "*each supervisory authority shall have all of the following investigative powers:*

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all

[70] https://rm.coe.int/16806b6ec2

information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member state procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.[71] *"*

2. Moldova

In Moldova, the conformity control of personal data processing operations is performed exclusively by the National Centre for Personal Data Protection, except for the cases provided in article 2(4) of the Law no.133 of 08/07/2011 on personal data protection.

The control of the lawfulness of personal data processing can be initiated based on the data subject's complaint, by notification/ex-officio or in the context of requests for authorising trans-border transfers.

Article 74 of the Contravention Code of the Republic of Moldova is stating that if the inquired person refuses to allow access to the National Centre for Personal Data Protection to information, a fine ranging from 100 to 500 euros can be imposed.

[71] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

In 2016, a significant increase of the total number of controls initiated based on personal data subject's complaints was recorded. Simultaneously, a substantial decrease of the number of controls initiated on trans-border personal data transfers was recorded. Therefore, during this period **247** controls were initiated and examined, of which **186** were initiated based on the complaints of data subjects, notification/ex-officio, **61** based on requests for authorising trans-border transfers .

In 2016, **controls of lawfulness of the processing took place mainly *ex officio,*** following the written procedure to obtain necessary information to examine the invoked circumstances and to find a solution to the cases. In this context, it is worth mentioning that in order to clarify the circumstances and objectively examine the cases investigated by the NCDP, its employees, in most of the cases, had to travel to the spot. However, considering the small number of employees and the multiple overlapping activities during this period, in most cases, the evidence was gathered through sending inquiries/requests. The employees of the NCDP are therefore obliged to use the declared information without being able to verify its veracity. This situation can be overcome by substantially increasing the number of employees of the competent subdivision of the Centre[72].

Comparative data of the control activity undertaken by the Center from 2014 to 2016

Comparison period	Controls initiated on the basis of :		Acts issued as a reaction to controls			
	Complaints/ notification	Requests for trans-border transfers	Decisions on suspension of personal data processing	Decisions on cessation of personal data processing	Decision on destruction/ erasure of personal data processed in the breach of law	Cases of contraventions founded/ minutes issued
2014	140	34	1	3	1	56/34
2015	149	469	4	8	-	43/24
2016	186	61	18	11	2	66/33

3. Georgia

In **Georgia**, the Personal Data Protection Inspector inspects the lawfulness of data processing on its own initiative or based on a complaint.

Inspection involves:

- Establishing the existence of the grounds and principles for the legitimate data processing;
- Examining the compliance of the organisational and technical data security measures with the requirements of the legislation;
- Examining the compliance of the filing system, filing system catalogue and records of the disclosure of personal data with the established legal requirements;
- Examining the legitimacy of the trans-border data flow;
- Examining the compliance with other requirements of the legislation.

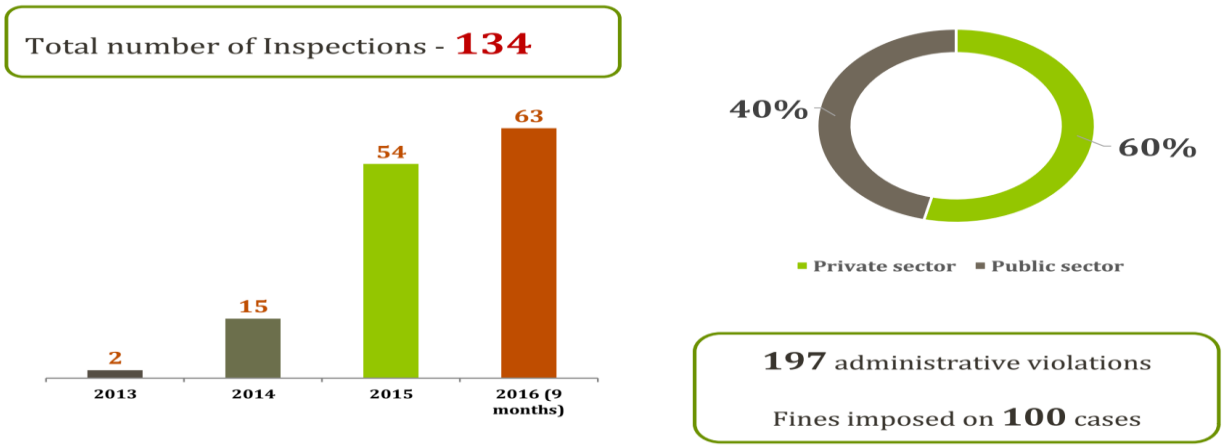
[72] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

During the Inspection, the Inspector is entitled to request the documents from any natural and legal person, including information involving commercial and professional secrets, and materials reflecting the operative-investigational activities and crime investigation that are classified as the state secret and are necessary to perform inspection.

Data controllers and data processors are obliged to provide the Inspector with the necessary information and documents immediately or within 10 days.

The Inspector is entitled to inspect any organisation and to get familiar with any information and documentation regardless of its content and storage form[73].

In 2016, the data processing in the following institutions was examined as a result of submitted complaints and conducted inspection[7475] :



4. Ukraine

In **Ukraine**, with the purpose of monitoring the observance of legislation on personal data protection, the employees of the Department for Personal Data Protection of the Secretariat of the Ombudsman carry out scheduled and unscheduled inspections of personal data controllers (state, enterprises, other institutions and organisations, irrespective of the form of their ownership). The number of inspections increases every year. 62 inspections were conducted in 2015, while in 2014 there were 53 inspections.

76 inspections have been conducted in 2016.

A specific procedure has been adopted to undertake inspections. This procedure is attached in Appendix to this Manual.

[73] https://personaldata.ge/en/about-us/what-we-do
[74] https://rm.coe.int/16806eead9
[75] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf

5. France

In **France**, the ex-post inspections allow the CNIL to verify the concrete implementation of the law. A programme of interventions[76] is established considering the current events and the high-level issues (new technologies, problematic current events and revelations) for which the CNIL is called upon to act.

Regarding inspections or complaints, in order to separate the regulatory power from the sanction power (as required under fair trial requirements), the CNIL set up a restricted committee (composed of 5 members and a Chair other than the CNIL's Chair) which can render various types of sanctions (warning, monetary sanctions, withdrawal of authorisation, injunction, etc)[77].

More information available at: https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil

https://www.cnil.fr/fr/controles-en-ligne-mode-demploi

The Irish data protection authority also published for instance a Guide to Audit Process giving details on inspections procedures[78].

3. The sanctions and the role of judicial authorities

1. Convention 108

The Additional Protocol to **Convention 108** provides that data protection authorities shall have the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law, giving effect to the principles of Convention 108.

Pursuant to Article 12 bis of the proposed modernised Convention 108, supervisory authorities shall have powers to issue decisions with respect to violations of the provisions of the Convention and shall have the power to impose administrative sanctions.

They shall at the same time have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of the Convention.

2. European Union

In **the European Union**, the GDPR confers strong powers to data protection authorities.

They shall have the power to bring infringements of the Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings.

[76] https://www.cnil.fr/fr/programme-des-controles-2016-quelles-thematiques-prioritaires
[77] https://www.cnil.fr/en/cnils-missions
[78] https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf

More importantly, they have the power to impose an administrative fine up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Pursuant to Article 83 of the GDPR, due regard shall be given to various factors when imposing a fine such as for instance:

- the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor considering technical and organisational measures implemented by them;
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- adherence to approved codes of conduct or approved certification mechanisms; etc.

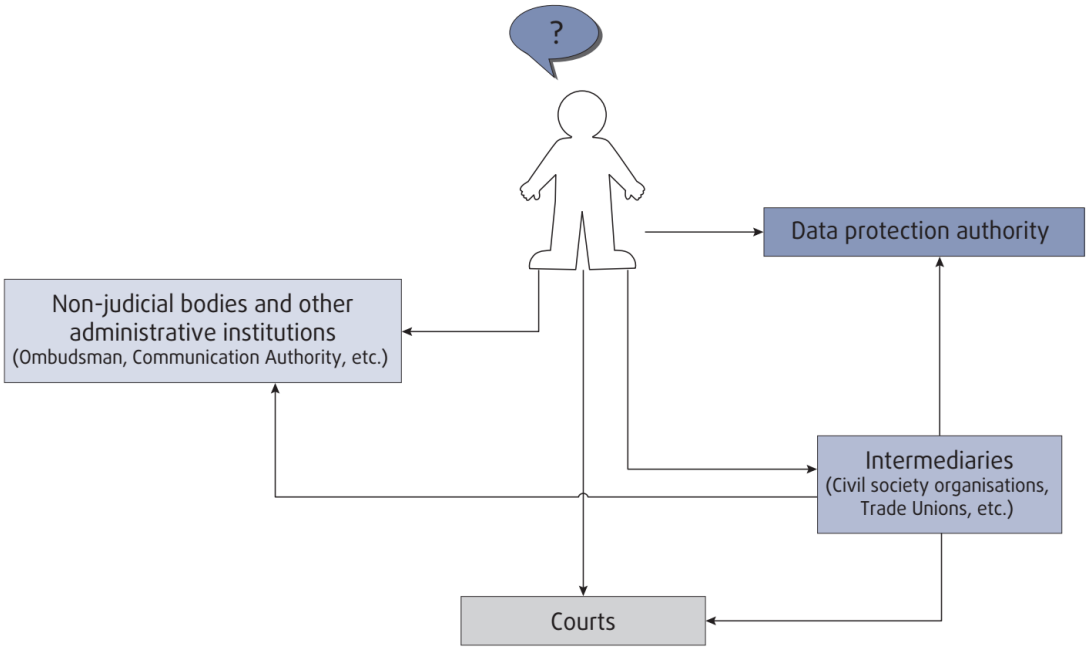
Sanctions and the need to transfer cases to judicial authorities are often the last recourse used by data protection authorities to ensure compliance. In many cases, there is no need to impose a sanction because the controller will immediately comply with recommendations or warnings issued by the supervisory authority.

In any case, individuals shall have the right to a remedy and to obtain compensation for a violation of their right to the protection of their personal date.

The EU Fundamental Rights Agency released in 2014 a publication on the access to data protection remedies in EU Member states[79]. The report contains for instance the following figure highlighting the fundamental role of data protection authorities:

[79] http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

Figure: Selected paths to access remedies in the area of data protection



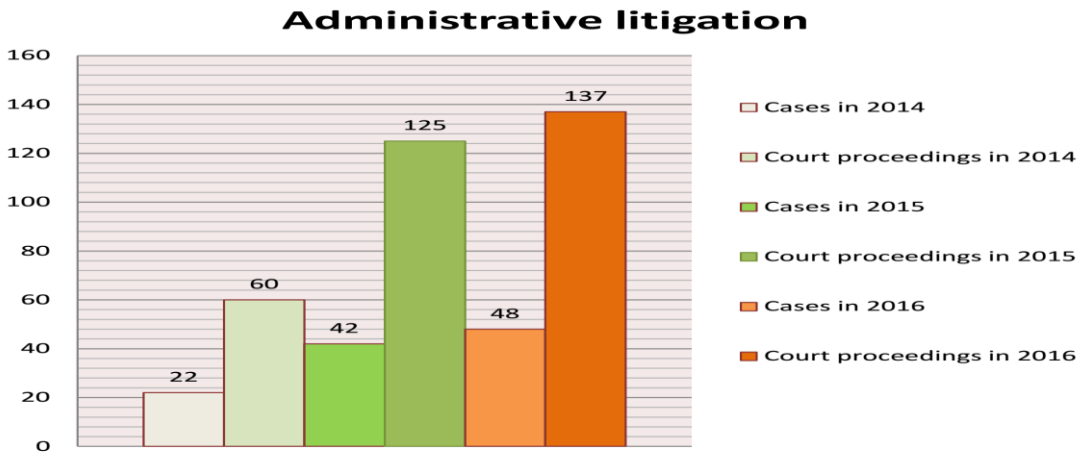
3. Moldova

In **Moldova**, during 2016, the Centre's interests were represented in 48 cases before administrative litigation instances, of which: - in 5 as accessory intervention; - in 2 as a petitioner; - in 41 as a defendant; At the same time, the examination of 10 court cases was finalised. In order to ensure the representation of the national supervisory Authority in judicial instances of administrative litigation, the employees of the Legal and Public Relations Department of the Centre participated in 137 court hearings during 2016[80].

Furthermore, in 2016, 66 contraventions were recorded, and 33 minutes were established related to contraventions, all being sent to the competent courts. Therefore, we can notice an increase of the number of minutes related to contraventions compared to 2015, when 24 minutes were drawn.

[80] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

Comparative dynamics of the number of cases and court proceedings in administrative litigation (2014-2016)



4. Georgia

In **Georgia**, if a data controller/data processor violated the requirements of the Law, the Inspector is authorised to use enforcement measures. In particular, the Inspector is entitled to:

- Request eradication of infringement and related discrepancies within the requested timeframe and in the recommended way;
- Request temporary or permanent termination of the data processing;
- Request obstruction, erasure, destruction and/or depersonalisation of data;
- Request termination of trans-border data flow;
- Provide written recommendations and instructions to data controller and data processor in case of minor violations;
- Address the Court if the data controller or data processor fails to fulfil request of the Inspector;
- Impose administrative responsibility upon the data controller and data processor if the administrative offence is revealed.

In 2016, 221 facts of violations were revealed; fine was imposed on 63 organisations; while 35 organisations were warned.

In the field of direct marketing, forty-eight data subjects applied to the Inspector with a request to examine violations of the direct marketing rules. Violations of the direct marketing rules established in the law were found in 30 cases. In 27 cases the Inspector imposed a fine, in 3 cases a sanction was not used because of the expiration of the statute of limitations provided in the law.

A great number of violations concerned the lack of a mechanism which would allow a person to opt-out from offers made through telephone calls or SMSs. The lack of information of individuals was also a major area of non-compliance[81].

[81] https://personaldata.ge/manage/res/images/2017/angarishi/2016%20Eng.pdf

PART 4: EDUCATION AND AWARENESS RAISING ACTIVITIES

1. European Union

Data protection authorities have a general duty to inform individuals about their rights and controllers and processors about their obligations.

The EU Fundamental Rights Agency recalls that, in February 2008, two Flash Eurobarometer surveys were published: "Data Protection in the European Union: Citizens' perceptions"[82] ; "Data Protection in the European Union: Data controllers' perceptions"[83].

A majority of respondents across EU said that they were very or fairly concerned about how their personal data is handled.

The most important findings from these surveys were that a majority of people who answered showed concern about data protection issues and that national Data Protection Authorities were relatively unknown to most of them.

While most respondents seemed to be aware of their rights regarding the use of personal data and the existence of relevant legislation, on average only 28% of the respondents in the EU were aware of the existence of a national data protection authority.

The most often-quoted reason for contacting the national data protection authority was asking for guidance (60% of respondents who were in regular contact with the data protection authority gave this reason) or making a notification (56%)[84].

2. Convention 108

The proposed modernised Convention 108 clearly states that data protection authorities shall promote:

- public awareness of their functions and powers as well as their activities;
- public awareness of the rights of data subjects and the exercise of such rights;
- awareness of controllers and processors of their responsibilities under the Convention;

Specific attention shall be given to the data protection rights of children and other vulnerable individuals.

Authorities tend to develop awareness raising campaigns targeting the public at large by means of the press, the authority's website, social networks and target workshops.

The authorities participate also in conferences, seminars, and workshops in order to inform and be informed, including with regard to ICT evolutions.

[82] http://ec.europa.eu/public_opinion/fl ash/fl_225_en.pdf
[83] http://ec.europa.eu/public_opinion/fl ash/fl_226_en.pdf
[84] http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities

In that respect, the use of websites and social networks is becoming increasingly important.

The annual report and its presentation to the press or to the competent authorities is a major tool that is used by data protection authorities.

3. Georgia

In **Georgia**, the Office of the Personal Data Protection Inspector regularly provides trainings on the personal data protection issues for the representatives of public and private bodies. Trainings are provided not only for data controllers, but also for any person who is interested in data protection. Any individual can register for the training through the web-page, trainings are held monthly and are free of charge.

Memorandums of Understanding were signed with several training centres of the public agencies and the personal data protection issues are included in the curriculum of the different training programs.

The Office of the Personal Data Protection Inspector provides regular trainings and informational meetings on personal data protection related issues to raise awareness of the data controllers and to establish a uniform practice.

The requirements of data protection legislation, practical examples and best practices of other countries are discussed during the trainings. The interactive form of the meetings provides for the opportunity to raise and discuss most challenging and acute issues for the audience.

The Office fruitfully cooperates with different training centres and educational institutions such as the Training Centre of Justice, the Police Academy and other public and private organisations.

The Office elaborated a basic training manual on data protection as well as thematic and sector specific materials for public and private institutions.

The Office of the inspector also organised winter schools for law faculty students from different universities of Georgia. Public lectures are carried out by the Office on a regular basis. Data protection weekends were also held for lecturers of law and journalists' faculties.

4. Moldova

In **Moldova**, according to the objectives set by the National Strategy of the Personal Data Protection Field for the years 2013-2018, the Centre increases public awareness on the importance of protection of individuals with regard to the processing of personal data and informs all controllers on their responsibilities.

The Centre has established and implemented other means to contribute to promoting a culture of personal data protection, such as conferences, debates, workshops, video spots, communication with users through newspapers, radio, television, social networks, web sites, etc.[85].

[85] http://www.datepersonale.md/file/Raport/Raport%202016DateENG.pdf

5. Ukraine

In **Ukraine** for instance, the Department of the Commissioner organised "School of personal data protection" and other seminars where participants had the opportunity to acquire knowledge of the legislation of Ukraine on data protection.

The "School of personal data protection" is a three-day course during which participants attend lectures held by employees of the Department for Personal Data Protection of the Secretariat of the Ombudsman. During colloquiums participants may test the knowledge they have gained.

Moreover, the manual «*Personal data protection: legal regulation and practical aspects*» has been published under the joint project of the European Union and the Council of Europe «Strengthening information society in Ukraine».

In addition, different booklets in the field of personal data protection have been printed, including «*What personal data subjects should know*» and «*What data controllers and processors should know*».

6. Digital Education Working Group

One might also mention more specifically the activity of the **Digital Education Working Group (DEWG) of the International Conference of Data protection and privacy Commissioners** undertaken over several years. The DEWG has created tools for authorities to make their efforts in digital education available to peers and helped instill a culture of sharing experience in that space[86].

[86] https://icdppc.org/document-archive/working-group-reports/

PART 5: THE INTERNATIONAL COOPERATION ACTIVITIES

Increasingly, the challenges faced by data protection authorities contain an international dimension.

International cooperation has become an absolute necessity for supervisory authorities whether through bilateral cooperation amongst authorities or through multilateral cooperation.

1. Co-operation

The international cooperation may first of all be encouraged through direct **bilateral co-operation** between two authorities.

For instance, a co-operation agreement has been signed on 10 October 2016 between the Office of the Personal Data Protection Inspector of Georgia and the National Centre for Data Protection of the Republic of Moldova.

Study visits and exchanges of staff members may also be organised between data protection authorities in order to facilitate co-operation and the exchange of relevant information.

2. Convention 108

The Additional Protocol to Convention 108 clearly states that "*the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information*".

Convention 108 establishes a **Consultative Committee,** consisting of representatives of Parties to the Convention complemented by observers from other states and international organisations, non-state actors, which is responsible for interpreting the provisions and for improving the implementation of the Convention.

It is also responsible for drafting reports, guidelines and guiding principles on a large variety of topics[87].

The proposal for a **modernised Convention 108** also encourages the cooperation among supervisory authorities in particular by:
a. providing mutual assistance by exchanging relevant and useful information and cooperating with
each other;
b. co-ordinating their investigations or interventions, or conducting joint actions;
c. providing information and documentation on their law and administrative practice relating to data protection.

[87] http://www.coe.int/en/web/data-protection/-consultative-committee-t-pd

3. European Union

At the level of the **European Union**, the **Article 29 Working Party** is an independent European working party that deals with issues relating to the protection of privacy and personal data. The data protection authorities of the 28 EU member states are members of the Working Party. Apart from the EU member states, the European Data Protection Supervisor also participates in the Working Group's activities. The member states of the European Economic Area (Iceland, Liechtenstein and Norway) have the status of observer in this group, as well as a number of candidate member states.

The Article 29 Working Party's missions comprise all issues related to the application of national provisions that were adopted in implementation of Directive 95/46/EC ("Data Protection" directive) and Directive 2002/58/EC ("Electronic communications" directive).

The Article 29 Working Party regularly issues opinions, publishes working documents and resolutions on different topics related to the protection of privacy and personal data. Almost 250 documents have been adopted by the Working Party[88].

The Article 29 Working Party draws up a two-yearly work plan, and its yearly activity report is also public and available online.

The Article 29 Working Party holds a two-day plenary session in Brussels five times every year.

With the forthcoming **GDPR**, strong rules for cooperation between authorities and mutual assistance are applicable. Joint operations of supervisory authorities are allowed. Moreover, a consistency mechanism is foreseen, and the Article 29 Working Party will be replaced by the **European Data Protection Board**, which will have in some transborder cases the power to issue binding opinions[89].

4. International Conference of Data Protection and Privacy Commissioners

Each year the **International Conference of Data Protection and Privacy Commissioners** meets in a different city hosted a data protection or privacy authority. The conference first met in Bonn, Germany, in 1979 and then crossed the Atlantic for its second meeting in Ottawa, Canada.

The Conference is an entity representing the collective accredited members, which are public authorities that meet the criteria for membership set out in the Conferences rules and procedures. There are currently 119 data protection and privacy authorities accredited as members of the Conference.

The Conference seeks:

- To be an outstanding global forum for privacy and data protection authorities;

[88] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[89] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

- To disseminate knowledge, and provide practical assistance, to help authorities more effectively to perform their mandates;
- To provide leadership at international level in data protection and privacy;
- To connect and support efforts at domestic and regional level, and in other international forums, to enable authorities better to protect and promote privacy and data protection.

International Standards on the Protection of Personal Data and Privacy have been adopted in 2009 during the Conference held in Madrid[90].

The Global Cross Border Enforcement Co-operation Arrangement was adopted in Mauritius on the occasion of the 36th Conference (2014).

5. International Working Group on Data Protection in Telecommunications

The **International Working Group on Data Protection in Telecommunications ("Berlin Group")** was established in 1983 at the International Conference of privacy and data protection commissioners.

The working group brings together telecommunication experts – legal and technical experts – of the data protection authorities and other actors in the telecommunications sector. The meetings are held twice a year, one in Berlin, and one on invitation by a member of the group. Since its establishment, the Berlin Group has adopted many documents and resolutions aiming to increase attention to data protection in telecommunications sectors and on the internet[91].

6. European Conference on Data Protection

The data protection authorities of the EU member states and of some of the Council of Europe member states meet annually at the **European Conference on Data Protection** ("Spring Conference").

The conference participants debate on numerous subjects related to data protection during plenary meetings, they exchange working methods and may adopt resolutions on various topics.

Two working parties established at the conference are dedicated to more specific topics:

- the "Working Party on Police and Justice";
- the "Case Handling Workshops": international workshops for data protection authority employees, which take place twice a year and are intended to exchange information and experience on concrete cases.

7. Central and Eastern Europe personal data protection authorities

At the end of 2001, during an international Conference organised by the Council of Europe, an international co-operation between **Central and Eastern Europe personal data protection authorities (CEEDPA)** was initiated.

[90] https://icdppc.org/

[91] https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Meetings of Central and Eastern Europe personal data protection authorities, aimed at supporting exchange of information and experience, raising awareness of personal data protection, as well as further harmonisation of the national provisions with the law, have taken the form of regular conferences organised in particular countries[92].

The 19th Meeting of the Central and Eastern Europe Data Protection Authorities took place on 17-18 May 2017 in Tbilisi, Georgia.

8. Working Party on Security and Privacy in the Digital Economy

At the level of the **Organisation for Economic Co-operation and Development (OECD), the Working Party on Security and Privacy in the Digital Economy (SPDE)**[93], formerly, the Working Party on Information Security and Privacy (WPISP), develops public policy analysis and recommendations to help governments and other stakeholders ensure that digital security and privacy protection foster the development of the digital economy.

One may mention that recommendations have been adopted for example in the following fields[94]:
- 2016: Recommendation of the Council on health data governance;
- 2015: Recommendation of the Council concerning Digital Security Risk Management;
- 2013: Recommendation of the Council concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data;
- 2012: Recommendation of the Council on the Protection of Children Online;
- 2011: Recommendation of the Council on Principles for Internet Policy Making.

In June 2007, OECD governments also adopted a **Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy**. The Recommendation called for member countries to foster the establishment of an informal network of Privacy Enforcement Authorities.

The **Global Privacy Enforcement Network (GPEN)** was created to strengthen personal privacy protections in a global context. GPEN connects privacy enforcement authorities from around the world to promote and support co-operation in cross-border enforcement of laws protecting privacy.

It primarily seeks to promote cooperation by:
- exchanging information about relevant issues, trends and experiences;
- encouraging training opportunities and sharing of enforcement know-how, expertise and good practice;
- promoting dialogue with organisations having a role in privacy enforcement;
- creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral co-operation[95].

[92] www.ceecprivacy.org
[93] http://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm
[94] http://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm
[95] https://www.privacyenforcement.net/public/activities

9. International Organisation for Standardisation

The **International Organisation for Standardisation (ISO)** is an independent and non-governmental international organisation with a membership of 163 national standards bodies[96].

It brings together experts to share knowledge and develop voluntary and consensus-based international standards. These standards intend to give specifications for products, services and systems, to ensure quality and safety while facilitating international trade.

ISO standards have been developed in the field of Privacy. One may for instance mention the following standards:

- ISO/IEC 29100 Information technology - Security techniques - Privacy framework;
- ISO/IEC 29101 Information technology - Security techniques - Privacy architecture framework;
- ISO/CEI 27001 Information technology - Security techniques - Management systems for information security - Requirements;
- ISO/CEI 27002 Information technology - Security techniques – Code of practice for information security management;
- ISO/IEC 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 29134 Information technology - Security techniques - Guidelines for privacy impact assessment; etc.

10. French-speaking association of data protection authorities

The **French-speaking association of data protection authorities** ("Association francophone des autorités de protection des données personnelles" or AFAPDP) was founded in 2007, and unites data protection authorities of 18 countries that are members of the "Organisation Internationale de la Francophonie" (OIF)[97].

This organisation has the task of promoting cooperation and training initiatives between French-speaking countries in the field of data protection. It wants to offer room for guidance and exchange to newly established data protection authorities and is a source of expertise for countries which do not yet have a DP legislation.

Every year, the AFAPDP organises a meeting for all of its members and organises a yearly collective seminar, intended as a forum for information exchange and the discussion of current topics.

[96] https://www.iso.org/fr/home.html
[97] http://www.afapdp.org/

11. Ibero-American Network of Data Protection

The **Ibero-American Network of Data Protection (RIPD)** is born following the agreement reached at the Ibero-American Symposium on Data Protection (EIPD) held in Guatemala in June 2003, with the attendance of 12 Ibero-American countries.

The RIPD was established as a forum for the promotion of the right to data protection in the ibero-american community.

The RIPD is aimed at promoting the legal and institutional development of the protection of data in the ibero-american countries.

The network is also working on co-operation through the exchange of information, experience and knowledge in the development of common instruments and involving coordinated/joint activities [98].

12. Asia-Pacific Economic Cooperation

The **Asia-Pacific Economic Cooperation (APEC)** is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. APEC brings together 21 members.

It aims at facilitating the cross-border commerce as well as the development of e-commerce within the zone.

The "**APEC Privacy Framework**" adopted in 2004 promotes a flexible approach to information privacy protection across APEC member economies. The framework establishes a common set of privacy principles and provides technical assistance to those economies that have yet to address privacy from a regulatory or policy perspective[99].

[98] http://www.redipd.org/index-ides-idphp.php
[99] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Appendix 1: Form developed by the Ukrainian Parliament Commissioner for Human Rights for personal data processing that poses a special risk to the rights and freedoms of personal data subjects

Approved by
Decree of the Ukrainian
Parliament Commissioner for
Human Rights
_____ January 2014 № _____

Application for personal data processing that poses a special risk to the rights and freedoms of personal data subjects *

*** The application is filled in block letters**

1 Full name / Name of the Controller of personal data

USREOU / Registration number of the taxpayer's registration card												
Passport number and its series												

Issuing authority and date of issue

Location (for legal entites)/ Place of residence (for individuals)	

2.The personal data processing:

□ racial origin	□ ethnic origin	□ national origin	
□ political beliefs	□ religious beliefs	□ ideological beliefs	
□ membership in political parties and / or organisations	□ membership in trade unions	□ membership in religious organisations	□ membership in public organisations of ideological orientation
□ state of health	□ sex life	□ biometric data	□ genetic data
□ administrative liability	□ criminal liability	□ application of measures during pre-	□ measures taken in accordance with the

		trial investigation	Law of Ukraine "On operative-search activities"
□ committing against persons of certain types of violence	□ location and / or types of movement of persons		

3. Category or categories of subjects whose personal data are processed:

4. The purpose of personal data processing with reference to the legal acts, regulations, constitutive or other documents that regulate activity of the controller of personal data:

5. Name / Full name of the Processor of personal data *

USREOU / Registration number of the taxpayer's registration card												
Passport number and series												

Passport details and date of issue

Location (for legal entites)/ Place of residence (for individuals)	

*** Filled for each administrator of personal data**

6. Information regarding third parties to which personal data is transferred to*

☐ The personal data transferred to third parties	☐ Personal data are not transferred to third parties

7. Information on transborder transfer of personal data

☐ not done	☐ done

7.1 Name of the country (countries) in which personal data are transferred:

7.2 Information concerning a foreign entity (entities) relations in which the personal data are transferred:

7.3 The purpose of the transborder transfer of personal data

7.4 The legal basis for transborder transfer of personal data:

8. General description of the technical and organisational measures taken by the controller of personal data for their protection:

9. Location (actual address) of personal data processing:

Place
for Seal _____

signature, /full name, position/

Page ☐ Total pages ☐

Appendix 2: Procedure for inspections developed by the Ukrainian Parliament Commissioner for Human Rights

Approved by
Decree of the Ukrainian
Parliament Commissioner for
Human Rights
08 January 2014 №1/02-14

Procedure
for control exercised by the Ukrainian Parliament Commissioner for Human Rights over the observance of legislation on personal data protection

1. General provisions

1.1. This Procedure provides for the control mechanism of the Ukrainian Parliament Commissioner for Human Rights (hereinafter - Commissioner) over the observance of personal data protection legislation requirements through carrying out inspections of individuals, individuals – entrepreneurs, enterprises, institutions and organisations of all forms of ownership, state and local authorities that hold and/or administrate personal data (hereinafter – subject of inspection) as well as drafting and review of inspections results.
1.2. In this Procedure the terms shall be used as follows:
A remote inspection – scheduled or unscheduled inspection of the activity of the subject of inspection by the Commissioner and/or his/her designated officials carried out in the premises of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights based on the documents received from the subject of inspection and explanations without going out to the place of location of the subject of inspection and/or to the place where personal data is processed;
Field inspection – scheduled or unscheduled inspection of the activity of the subject of inspection by the Commissioner and/or his/her designated officials carried out at the place of location of the subject of inspection and/or directly at place where personal data is processed;
Scheduled inspection – inspection of the activity of the subject of inspection carried out according to the plan of inspections drawn up for a certain quarter and a year;
Unscheduled inspection – inspection of the activity of the subject of inspection that is not foreseen by the plan of inspections.
Act of inspection – internal document certifying the fact of conducting the inspection of the activity of the subject of inspection and the state of observance of the requirements of the personal data protection legislation by this subject of inspection;
Improvement Order (requirement) – is an obligatory for compliance within the set term requirement of the Commissioner for Human Rights to stop violations of the requirements set by the legislation on personal data protection submitted (sent) to the subject of inspection.
Other terms provided in this Procedure shall be used as foreseen by the Law of Ukraine "On Personal Data Protection".

2. Organization and carrying out of inspections

2.1. Control over the observance of the legislation on personal data protection by the subjects of inspections shall be carried out by the Commissioner and/or his/her designated officials through carrying out inspections: scheduled, unscheduled, field and remote ones. Scheduled and unscheduled inspections can be field or remote.
Subject-matter of the inspection is the observance of the requirements of the Constitution of Ukraine, the Law of Ukraine "On Personal Data Protection", a Model Procedure for Personal Data Processing as well as acting international treaties of Ukraine in the sphere of personal data protection which the Parliament of Ukraine agreed upon, by the subject of inspection when processing personal data.

2.2 The field check is carried out by the Ukrainian Parliament Commissioner for Human Rights and/or by the following authorised officials (hereinafter - authorised officials):

– Head of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights and his deputy;

– representatives of the Ukrainian Parliament Commissioner for Human Rights;
– heads of departments and their deputies;
– other employees of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights.

The authorised officials exercise their authorities due to the official identification and its supplement, which is an indispensable part of the stuff pass and confirms the volume of the authorities of the employee of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights according to the Regulation on the official identification of employees of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights, approved by Decree of the Ukrainian Parliament Commissioner for Human Rights of 14 December 2012 No. 19/8-12.

2.3. Officials of state authorities including public administration bodies, executive bodies and law enforcement bodies can be involved in the inspection pursuant to the order set by the legislation. If specified persons are involved they shall provide a written obligation on nondisclosure of personal data they get to know as a result of the inspection.
2.4. Field inspections shall be carried out within business hours of the subject of inspection set by the internal labor regulations.
2.5. When conducting the inspection, the Commissioner, designated official and subject of inspection have rights and obligations foreseen by Section 6 of this Procedure.
2.6. Subject of inspection is obliged to provide access to premises, materials and documents necessary to conduct an inspection, provide information and explanations concerning the factual and legal basis for their actions and decisions as well as to ensure relevant conditions to carry out a review of this information.
2.7. Remote inspection shall be carried out by the Commissioner and/or designated officials in the order set by items 3.1 – 3.6 of the Section 3 of the Procedure for carrying out proceedings by the Ukrainian Parliament Commissioner for Human Rights taking into account the provisions of this Procedure.

3. Carrying out a scheduled inspection

3.1. Scheduled inspections shall be carried out according to the annual or quarterly plans approved by the Commissioner before 1 December of the year preceding the target year or before the 25th of the last month preceding the target quarter.
3.2. The plan shall include the categories of subjects of inspections. Having been approved the inspections plan shall be published on the official web-site of the Commissioner.
3.3. Scheduled inspections of a subject of inspection on the observance of requirements of the legislation in the sphere of personal data protection shall be carried out periodically but no more than once a year.
3.4. The date which defines the term until the start of the new inspection shall be the closing date of the previous scheduled inspection.

4. Carrying out an unscheduled inspection

4.1. Unscheduled inspections of subjects of inspection can be conducted based on the existence of one or several grounds/reasons, particularly:
On the initiative of the Commissioner for Human Rights;
When violations of the requirements of the legislation on personal data protection were directly detected by the Commissioner for Human Rights, including as the result of conducting a research of systemic problems concerning the observance of the rights to privacy, respect to private and family life;
Based on the information concerning the violations of requirements of legislation on personal data protection in releases published in mass media or Internet;
Based on the well-grounded petitions of individuals and legal entities with information on violation of the requirements of the legislation on personal data protection committed by an individual, individual-entrepreneur, enterprise, institution and organisation of all forms of ownership, a state or local authorities body holding and/or managing personal data;
When the information provided by the subject of the inspection in response to the request of the Commissioner for Human Rights on remote inspection was misrepresented, and/or if such an information (data) does not give a possibility to evaluate how the subject of inspection executes the requirements of the legislation on personal data protection;
Control over the execution by the subject of inspection improvement orders on elimination of violations of requirements of legislation on personal data protection issued as the result of conducted inspections.

5. Drawing up the results of inspections

5.1. On the results of the conducted scheduled or unscheduled inspection the Commissioner and/or the designated official draw up the act of inspection of the observance of requirements of legislation on personal data protection (hereinafter - Act) in two copies based on the form set by the Supplement 1 to this Procedure.
5.2. Act shall include the following information:
Date, time and place of a draw up;
Positions, last names and initials of persons who have conducted the inspection;
Position, last name and initials of the head of the subject of inspection (his/her designated official) or a last name and initials of an individual – subject of inspection;
Type of inspection (scheduled, unscheduled, field, remote);
For the subject of inspection – state or local authority body: name, location;
For the subject of inspection – legal entity: name, location;
For the subject of inspection – individual and/or individual – entrepreneur: last name, first name and patronymic, place of registration;
Information on date, starting and completion time of the inspection, its general duration;
Facts (conditions) established on the results of the inspection;
Conclusions on the results of the inspection.
When drawing up the Act objectivity and exhaustive description of the findings and data have to be observed.
5.3. Act has to include one of such conclusions:
On absence of violations of the requirements of legislation on personal data protection in the activity of the subject of inspection;
On violations of the legislation on personal data protection by the subject of inspection, their detailed description with reference to the violated norms of acting legislation.
It is forbidden to include in the Act the information on violations that are not proven by documents.
5.4. Act includes all established during the inspection facts on non-execution (improper execution) of the requirements of legislation on personal data by the subject of inspection.
5.5. In case if the subject of inspection fails to provide documents needed to conduct the inspection, the Act shall include this fact stating the reasons.

5.6. Field inspection
5.6.1. On the results of the conducted field inspection the Act shall be drawn up in two copies and signed by the Commissioner or his/her designated official/s who conducted an inspection as well as by the head of the subject of inspection or his/her designated person.
5.6.2. If the subject of the inspection does not agree with this Act, he signs it with his observations. Observations of the subject of inspection concerning the process of exercising control over the observance of requirements of the legislation on personal data protection by the designated officials are the integral part of the Act. With this in place, the last page of all copies of the Act shall include the notice: "With observations".
If the head of the subject of inspection does not agree to sign the Act, the designated official includes relevant notice on this into the Act.
5.6.3. The first copy of the Act shall be submitted to the head of the subject of inspection or to his/her designated person upon signature on the second copy of the Act that shall be kept at the Secretariat of the Commissioner.
If the head of the subject of inspection or his/her designated person denies to receive the second copy of the Act it shall be sent to the subject of inspection within 5 working days by a registered mail with return receipt.
Copy of the Act kept at the Secretariat of the Commissioner shall be supplemented by the materials of the inspection – copies of the documents, excerpts from the documents duly certified by the subject of inspection, explanations, protocols and other documents.

5.7. Remote inspection
5.7.1. On the results of the remote inspection an Act shall be drawn up in two copies signed by the Commissioner and/or his/her designated official/s who conducted the inspection. The first copy shall be sent to the subject of inspection for review and the second shall be kept in the Secretariat of the Commissioner.
5.7.2. The copy of the Act kept at the Secretariat of the Commissioner shall be supplemented by the materials of the inspection – copies of the documents, excerpts from the documents duly certified by the subject of inspection, explanations, protocols and other documents.
5.8. Any corrections and additions to the Act of inspection after its being signed are not permitted. The subject of inspection shall be informed in writing of the detection of slips after the Act has been signed.

5.9. Any information that the Commissioner and/or his/her designated official/s got to know during the inspection is subject to non-disclosure.
5.10. Based on the Act of inspection during which violations of the requirements of the legislation on personal data protection were found, an improvement order on the elimination of violations of the requirements of legislation in the sphere of personal data protection that were found during the inspection shall be issued according to the form set by Supplement 2 to this Procedure (hereinafter - Order).
5.11. The Order shall include:
Number, date and place where the Order was issued;
For the subject of inspection – state or local authority body: name, location;
For the subject of inspection – legal entity: name, location, last name, first name and patronymic of the head of the legal entity;
For the subject of inspection – individual and/or individual – entrepreneur: last name, first name and patronymic, place of residence;
Grounds for the issue of the Order;
Measures necessary to eliminate violations found in the course of the inspection;
Term for Order execution;
Term for informing the Commissioner on the elimination of the found violation by the subject of inspection;
The signature of the designated official/s who conducted the inspection.
5.12. The Order shall be issued in two copies: the first copy shall be sent to the subject of the inspection or to his/her designated person by a registered mail with return receipt within 5 working days from the time when the Act of inspection was drawn up, and the second copy stays at the Secretariat of the Commissioner.
The copy of the Order that stays at the Secretariat of the Commissioner shall have the relevant reference number and mailing date.
5.13. The subject of the inspection has to take measures to eliminate violations defined by the Order within the term defined by the Order (minimum 30 calendar days) and to inform the Commissioner in writing on the elimination of violations together with copies of documents proving that.
5.14. Control over the timeliness and completeness of fulfillment of the requirements stated in the Order is exercised through the examination of the copies of the documents mentioned above and, in case of necessity, through an unscheduled inspection.
5.15. In case of failure to comply with the Order within the term set in it, the Commissioner or his/her designated official draws up a protocol on administrative offence foreseen by the article 188^{40} of the Code of Ukraine on Administrative Offences (hereinafter - CUoAO) according to the form and in the order set by the legislation and the Procedure for drawing up materials on administrative offences.
5.16. If the administrative offence foreseen by article 188^{39} or article 188^{40} of the CUoAO is proven to have been perpetrated by the subject of inspection in the course of inspection, the Commissioner or the designated official pursuant to item 1 of Part 1 of Article 255 of the CUoAO draws up a protocol on administrative offence according to the form and in the order foreseen by the legislation and the Order of drawing up materials on administrative offence.
5.17. If the criminal offence is detected in the course of inspection of the subject of inspection, the Commissioner sends relevant materials to the law enforcement authorities.

6. Rights and obligations of the designated official and officials of the subject of inspection

6.1. A designated official in the course of inspection has the right to:
6.1.1. Free access to the object of inspection upon presentation of service ID card and free access to places of storage of information including computers, magnetic data holders etc.
6.1.2. Get upon his or her requirement and have access to any information (documents) of holders and administrators of personal data necessary to exercise control over the observance of personal data protection including access to personal data, relevant databases or file cabinets, information with limited access.
If the document exists only in the electronic form under the condition that this document is created by the subject of inspection, the subject of the inspection is obliged to provide its paper copy, that ensures its visual reading, certified by the subject of inspection in the order set by the legislation. In case of failure to provide the paper copy that ensures its visual reading the electronic document shall be reviewed upon which the Act of review of the electronic document shall be drawn up according to Supplement 3 to this Procedure.
6.1.3. Receive copies of documents duly certified in order set by the legislation.
6.1.4. Require, within his or her mandate, written explanations of the head and/or officials of the subject of inspection.
6.1.5. To address the prosecution bodies and other law enforcement authorities with the view to fulfill the mandate.

6.1.6. To issue and sign Improvement Orders on prevention and elimination of violations of legislation on personal data protection.
6.1.7. Issue and sign protocols on administrative offences for violations of legislation on personal data protection;
6.1.8. Engage other persons present when the offence was detected to draw up protocol.
6.2. When conducting an inspection, a designated official is obliged to:
6.2.1. Conduct the inspection within the set mandate, fully, objectively and without bias;
6.2.2. Inform the head of the subject of the inspection or his/her designated person on duties and mandate of the designated official, the reason and aim of the inspection, rights, obligations of the head and officials of the subject of inspection;
6.2.3. Inform the head of the subject of inspection or his/her designated person with the results of the conducted inspection and/or protocol on administrative offence;
6.2.4. Define the list of the necessary documents to be examined and the terms for their submission;
6.2.5. Form the results of inspections in due order;
6.2.6. Strictly observe the requirements for drawing up protocols on administrative offences set by the Procedure for forming materials on administrative offences.
6.3. Officials of the subject of inspection including the head of the subject of inspection or his/her designated person, when conducting the inspection, have the right:
6.3.1. To check whether the designated official/s have a service ID card and the grounds for inspection;
6.3.2. To be present during the inspection;
6.3.3. Receive and know the results of the conducted inspection together with the Act and/or the protocol on administrative offence;
6.3.4. To provide explanations and observations to the Act and/or protocol on administrative offences in the written form;
6.3.5. To appeal against the unlawful actions of the designated official in the order set by the legislation.
6.4. Officials of the subject of inspection, including the head of the subject of inspection or his/her designated person, when inspection is conducted, are obliged to:
6.4.1. To provide free access for the designated official to the premises of the subject of inspection and provide access to the documents and other materials necessary for conducting the inspection;
6.4.2. Provide necessary documents and other information, written explanations certified by the signature as well as other copies of documents, necessary to conduct the inspection, certified in the order set by the legislation.
6.4.3. Comply with the requirements of the designated official/s concerning issues of observance of requirements of legislation on personal data protection.

Act of the inspection of the observance of the legislation on personal data protection adopted by the Ukrainian Parliament Commissioner for Human Rights

«___» _____ 20__ _____
(time and place of the inspection)

I/We,,

_____
_,
(position and names of the persons who conduct the inspection)

involving

_____
_,
(position and names)

in the presence of

_____
__
(position, name of the head of a legal person (his/her designated official) or name of a natural person – the subject of the inspection)

Carried out

_____
__
(scheduled, unscheduled, field, uninterrupted)

Inspection of the observance of the legislation on personal data protection

_____
__
(name, address of the legal person or name, place of residence of the natural person - the subject of the inspection)

Starting date of the inspection: «___» _____ 20___ year ____ hr. ____ min.;

Ending date of the inspection: «___» _____ 20___ year ___ hr. ____ min.;

Total duration of the inspection: ____ d (___ hr. ___ min.)

As a result of the inspection, it has been revealed:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Conclusions:

(information on the results of the inspection including detected violations of the legislation on personal data protection)

Comments of legal or natural persons - the subject of inspection

Inspection carried out by:

(position)	(signature)	(name)
(position)	(signature)	(name)
(position)	(signature)	(name)

Act of the inspection is drawn up in two copies:

The first copy of the Act is in _____

The second copy of the Act is in _____

Acknowledged with the Act:

(position)	(signature)	(name)

The copy of the Act received:

(position, name of the head of the legal person (his/her designated official) or name of the natural person – the subject of the inspection)	(signature)	«___» _____ 20__

Appendix 3: Case-handling exercise used completed by the National Centre for Personal Data Protection of the Republic of Moldova

A Right To Be Forgotten Case
for Case-handling Workshop

Completed by the National Centre for Personal Data Protection of the Republic of Moldova

Circumstances

Complaint against a blogger to delete information related to applicant from web page.

The blog post reflected following personal data:
1) details about a court judgement where he was found guilty on paedophilia,
2) information about his job life: that he offers construction works through his company (being only shareholder and only board member) and that his workmanship is poor (he does insufficient job – he fixes and builds things poorly).

The applicant explained that he had served his prison sentence (2 years ago) and it was difficult for him to find new clients and housing due to the fact that people make background check via internet.

He also explained that the remarks of his poor workmanship were slander and made negative impact on him.

1. Receive of complaint, designation of case-handler:

1.1) by which channels can a complaint be submitted and what are more common channels? [by paper-mail, by e-mail, through web-application, orally]

MD
Paper-mail or e-mail with digital signature.

1.2) how the (final) case-handler is designated?

MD
By the Centre's director and head of subdivision

1.3) are all (formal and substantial) checks done only by one case-handler or are they divided (if yes, then how)?

MD
No

1.4) who will sign documents on behalf of Data Protection Authority in this case?

MD
Head of the subdivision where the case-handler activates. For final decisions, it is the centre's director who is responsible.

2. Deadline

2.1) what is the mandatory final deadline for a complaint-based case, (how) can it be extended?

MD
30 days according to art.27 (3) of the Personal data protection Law nr.133. Can be extended on notice each 30 days.

2.2) if there are deficiencies which must be eliminated by the complainant, how it affects the final deadline?

MD
Similar procedure.

3. Preliminary (initial) checks

3.1) what we do if the complaint is not in official language?

MD
We accept, review and respond according to the Law nr.3465 on languages spoken on the territory (in the official state language and Russian).

3.2) which simple formal requirements are preliminarily checked? We assume that:

- the name, signature, date, contact information must be submitted,
- existence of legal competence could be preliminarily checked (is the case under the scope of data protection legislation and under jurisdiction of the Data Protection Authority)
- the exact web-address required in the right-to-be-forgotten-cases,

- is it all correct? anything else?

MD
The right to be forgotten is not expressly transposed into national law but we treat extensively the right to object. They are basically the same requirements as mentioned above and an additional check that the complaint was made within 30 days since the violations.

3.3) how the explanations by related parties (in our case – holder of the blog and other persons made posts in the blog) are asked? Will it done in the initial phase? How their identity is checked?

MD
In written form. The identity is checked based on the information submitted by the applicant. If necessary, we also check the information from state sources or from other means available. This step is not included in the initial phase.

3.4) how quickly should the preliminary checks done by in-house rules?

MD
Within 5-10 days.

4. Substantial check – discretion and reasoning

Substantial aspects to be analysed:

4.1) do we have private law threshold here?
Should two aspects of the complaint distinguished (disclosure of criminal record, criticism of workmanship) in the context of private law threshold?

MD
In Moldova, the publication of judicial decisions is regulated by Law no. 514 of 06.07.1995 which states expressly in art. 47. (3) (e) that prior to their publication, judicial decisions shall be depersonalized. In this case, however, this is not respected and if the sentence is published in its full form without considering the exceptions of Law no.133 (such as public interest), it would be considered a breach.

4.2) if we think that the case is partly or completely above the private law threshold, how we determine the violation of rights? Especially in the context of conflict between right-to-privacy/right-to-be-forgotten and right-to-remember/freedom-of-expression/freedom-of-information? Which discretion we have – excessive damage, ethics? Are we referring here to international and constitutional law?

MD
Article 5, Article 10 and Article 16 of Law no.133 are relevant for the legislation related to access to information, freedom of expression and other laws which expressly mention publication of personal data. In particular, Article 5 (5) of Law 133 is relevant which stipulates that personal data subject's consent is not required if - executing a contract to which the data subject is a party - the data processor fulfilling an obligation according to the law - protecting the data subject - there is a public interest - the data is used for scientific purposes, if the anonymity of the data subject is protected Yes. We refer to international and constitutional law.

4.3) if we think that the disclosure of criminal records is above the private law threshold, which importance have national rules of expiration of criminal records?

MD
Processing data on criminal convictions, procedural measures of coercion and misdemeanours can be performed only by or under the control of public authorities, within the powers granted and the conditions established by law (Article 8 (1) of the Law no.133).

4.4) what is the conclusion – to intervene and initiate proceeding or not?

MD
On the construction company slander accusations, the Data Protection Authority is not the competent body. The police will be the responsible institution for these charges. Regarding the publication of the court decision on the case of pedophilia, the court had to anonymise the publication on the site. In this case, to not affect the independence of the judiciary, the request is sent to the Judiciary inspectorate. However, an assessment of the fairness of the processing of personal data will be given by the court.

4.5) if yes, which measures we could take in this case?

MD
Submitting the case materials to the Judicial inspectorate.

Appendix 4: Example of a concrete case dealt by the UK Information Commissioner's Office

:

This case is about:
- unwanted marketing mail;
- the right to prevent processing for direct marketing purposes; and
- the Mailing Preference Service.

Mrs W wanted a charity to stop sending her marketing mail asking for donations.

She wrote to the charity, enclosing copies of the unwanted mail, and asked them to stop sending it to her. However the charity sent more marketing mail, so Mrs W contacted us.

We advised Mrs W to write to the charity to ask why they were still sending marketing material to her and explain to them that under the Data Protection Act people have the right to ask organisations not to use their name and address for marketing purposes.

We also advised Mrs W to register her details with the Mailing Preference Service, which keeps a list of people who do not want to receive directly addressed marketing mail. Although organisations are not legally obliged to check with the Mailing Preference Service before sending marketing material, most do.

The charity contacted Mrs W and explained that they were very sorry for upsetting and inconveniencing her. They explained that after she had first contacted them, they had suppressed her details from their mailing list, which should have solved the problem. However, they had then bought a new mailing list and hadn't noticed that her name was on it until she wrote to them again.

The charity confirmed that they would suppress the names of customers who had asked not to be contacted from future lists.