Partnership for Good Governance


Enhance the right to Personal data Protection in Eastern Partnership countries

# Comparative study of different appeal and control national mechanisms regarding access to public information in six Council of Europe member states

What is better – to have an appeal body only in charge of access to public information or a combined office where personal data protection is under the same umbrella?

**Analysis prepared by Nataša Pirc Musar, PhD and prof. Bertil Cottier, PhD**

**July 2017**

**This document has been produced as part of a project co-funded by the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party.**

# Table of Contents

# 1 Introduction

One could argue that freedom of information (FOI) laws are only as good as the response mechanisms built into the laws themselves, and as good as the efficiency of the appeal procedures. If individuals cannot take an action to enforce their right of access being "shy" of filing a suit, or do not have enough financial resources to do that, FOI laws cannot serve as an active "push" system for more a transparent government. Whether a combined appeal body where FOI and personal data protection (PDP) are under one umbrella is a better or a worse solution for transparency is not an easy question since the complexity of both human rights and their different implementation in the legal systems of the respective countries must be considered. In this study, we will try to present, what needs to be considered when deciding upon the competences of a FOI appeal body and whether to merge FOI and PDP under one body. Financial reasons should by no means be a decisive criterion.

## 1.1 Appeal mechanisms as a guarantee to enforce access to public information

Ombudsmen[1] and information commissioners all admit that, due to strict international and national regulations, PDP is a very complex and difficult area of law. When FOI laws and PDP laws are to be articulated, privacy can very often be used to deny access to public information. It is also the only FOI exemption, which holds the status of a human right. Therefore, the manner in which PDP laws are interpreted is essential. If this exception was an absolute one, the whole transparency regime could be endangered and become inefficient. Blanton for example points out what happened in Japan regarding this question. Namely, reformers in Japan point to the overbroad privacy exemptions as a huge obstacle, since they allow bureaucrats to withhold any personal information whatsoever, whether releasing it would invade the privacy of the person. Consequently, released documents look like Swiss cheese, with every official's name deleted, even the Prime Minister's.[2]

Therefore, to ensure a culture of openness and to give individuals a right to access to information, adequate and effective appeal mechanisms must be in place.

There are five systems of second-instance (appeal) decision-making when dealing with access to public information:

- Appeal before the body which denied access to a document;
- Higher Administrative bodies;
- Court as an appeal body (directly) after the first level decision;
- Ombudsman (as a mediator with no or with binding powers[3]);
- Information Commissioner or Commission.

[1] English plural: conventionally ombudsmen, Wikipedia, http://en.wikipedia.org/wiki/Ombudsman, viewed on 15 June 2017.
[2] Blanton, Thomas, *The World's Right to Know, Foreign Policy*, July/August, 2002, also available at http://www.freedominfo.org/documents/rtk-english.pdf, viewed on 15 June 2017, p. 56.
[3] Most of ombudsmen do not have the power to issue binding decisions but only non-binding recommendations.

The model of the Information Commissioner (IC) was taken from the French practice (CADA – Commission d'accès aux documents administratifs, established in 1978) and Commonwealth countries (Canada has had an IC since 1982, Australia since 1983). These countries have longer tradition in freedom of information than the majority of countries which adopted FOI laws after 1990's. The decision of such a state body is final and no appeal can be made against its decision except a complaint. In most of the countries which have such a body, an administrative dispute may be launched on a point of law since it is clear, that judiciary must be the last instance dealing with the legality of the protection of the right to access to information.

In transition countries (new democracies) it is perhaps more sensible to have an authorised body, an independent state body (*sui generis*), watching over law enforcement and reviewing the conflict between the person obliged to follow the rules of the access to information and the applicant. Article 19, one of the largest non-governmental organisations in the world dealing with the protection of freedom of expression and access to public information, being aware of different legal systems and transparency cultures, recommends that wherever practical, a provision should be made for an internal appeal to a designated higher authority within the public authority who can review the original decision. Furthermore, it recommends that in all cases, the law should provide for an individual right of appeal to an independent administrative body. This may be either an existing body, such as an Ombudsman or Human Rights Commission, or one specially established for this purpose. In either case, the body must meet certain standards and have certain powers. Its independence should be guaranteed, both formally and through the process by which the head and/or board is/are appointed.[4] But in its model law on access to public information, Article 19 recommends having an Information Commissioner[5], meaning that from the Article 19's point of view the system with the Information Commissioner as an appeal body has the least disadvantages and that the applicants can obtain information in the fastest possible way. The Information Commissioner as an appeal body is also recommended by the Atlanta Declaration and plan of action for the advancement of the right of access to information where the signatories stressed that the requester should be guaranteed a right to appeal any decision, any failure to provide information, or any other infringement of the right of access to information to an independent authority with the power to make binding and enforceable decisions, preferably an intermediary body such as an Information Commission(er) or Specialist Ombudsman in the first instance with a further right of appeal to a court of law.[6] The non-governmental organisations have been repeatedly emphasising that it is also important that independent appeal bodies can make binding decisions which "classical" Ombudsmen cannot do. Therefore, the Atlanta Declaration emphasised enforcement and a Specialist Ombudsman

[4] Article 19, *The Public's Right to Know Principles on Freedom of Information Legislation*, London 1999, available at http://www.article19.org/pdfs/standards/righttoknow.pdf, viewed on 15 June, 2017.
[5] *A Model Freedom of Information Law*, available at http://www.article19.org/pdfs/standards/modelFOIlaw.pdf, viewed on 15 June, 2017.
[6] Available at https://www.cartercenter.org/documents/atlanta%20declaration%20and%20plan%20of%20action.pdf, viewed on 15 June, 2017.

with competencies of an appeal body and not the Ombudsman with recommendation competencies only.

## 1.2 Methodology

To show the advantages and disadvantages of a combined FOI and PDP office or countries where FOI and PDP are separated, six countries were chosen for a comparative study. Three of them have a combined office (Serbia, Slovenia and UK), and three do not (France, Italy and Sweden). To show the complexity of the systems, we compared the systems from four points of departure, important for the efficient implementation of the transparency regime into a daily life of public sector bodies – namely if FOI is a constitutional right, which body is competent for appeal (and if the body is in charge for both - FOI and PDP), whether a so called overriding public interest test is implemented into a FOI law and which legal system is a pillar for a legal system (only to show the historical legal roots).

Table 1 – Selected countries[7]

| Aspects to research/ Country | Constitutional provision on FOI | Appeal body | Public interest test included in the FOIA | Legal system |
|---|---|---|---|---|
| Italy | NO | CADA/Ombudsman/ Recommendations | NO | Germanic law |
| France | NO | CADA, only FOI | YES | Germanic law |
| Serbia | | Information Commissioner/ FOI binding decisions – FOI and PDP competences | NO | Germanic law |
| Slovenia | YES | Information Commissioner/ binding decisions – FOI and PDP competences | YES | Germanic law |
| Sweden | YES | Ombudsman/ Recommendations | NO (Harm test) | Scandinavian law |
| UK | NO* | Information Commissioner/ binding decisions. - FOI and PDP | YES (but not for PDP) | Common law |

* The UK does not have a Constitution but the Bill of Human Rights (1998) incorporates the right to freedom of expression and information, in line with the European Convention on Human Right and corresponding case-law.

[7] Country data taken from: Pirc Musar, Nataša.: *How to strike the right balance between access to public information and personal data protection – using a public interest test*, PhD thesis, Vienna University, November 2015.

When deciding what kind of an FOI appeal body to establish beside the general aspects defined in Table 1 the following key aspects should also be considered:

1. **Timeliness** is one of the crucial elements of FOI, because the value of specific information loses its importance if needed for a certain action (for example, for an investigative article by a journalist, for starting a public debate on a current issue, a document which can help the applicant prove something and on grounds of the document decide to start a court or some other legal procedure, or to prove that a public official is corrupt or not taking all the necessary measures needed to fulfil his or her public duty).

2. To ensure timeliness it is essential how **efficient** the appeal procedure is in cases where the public authority declines the access, does not respond or is silent (the so called "administrative silence"). It is therefore important whether the appeal body reacts rapidly or whether the slowness of the appeal mechanism in fact only "helps" the first level body gain more time before giving the information to the public, helps to reduce the importance of potential public debate or even makes the information obsolete, not relevant any more.

3. For efficiency evaluation, **power and significance of the decisions** issued by the appeal bodies are crucial. It is essential to evaluate which type of appeal body is likely to be most effective in ensuring the disclosure of information: the one which can issue binding decisions or the one which can issue only recommendations? Such a decision shall take into consideration also the general legal culture.

4. For the effective protection of FOI, the **costs** that the applicant must pay for gaining the information may also be an important element: the more expensive the appeal procedure, the less likely it is that the applicant will decide to pursue it.

5. In taking decisions on access to information requests, there is always a chance that the public authority will try to hide its mistakes, arising from the requested documents. Precisely in such cases it can make a significant difference whether the appeal body has strong **investigative competences** and is genuinely **independent** of the body it supervises (which would potentially include also the Parliament itself).

Having all these relevant factors in focus, the following questions regarding advantages and disadvantages of the legislation in effect and the planed Draft FOI law should be answered:

- How independent is the appeal authority?
- Does the appeal authority have strong investigative competences (is the appeal inefficient because of the passivity of the public authority – the holder of a document)?
- Can the appeal authority issue binding decisions?
- How high is the possibility of a reversed decision?

- What is the risk of backlogs occurring?
- Can the appeal body itself be sued before the court?
- Is it necessary to hire a lawyer to file an appeal?
- Are there high costs for the applicant to file an appeal?

# 2 Specific country focus

## 2.1 Countries with separate public bodies

### 2.1.1 France

**A. Legal sources and dedicated agencies**

France was one of the first countries in Europe to adopt a so-called Freedom of Information legislation; the relevant statute was passed in July 1978 (*loi 78/753 portant diverses mesures d'amélioration des relations entre l'administration*); this text is now part of the Code governing relations between the public and the administration). This statute was significantly modified in October 2016; the related amendments, which entered into force in July 2017, are part of a comprehensive piece of legislation on various issues pertaining to digital communication (*loi 2016/1321 pour une République numérique*). Six months before the adoption of the statute on access to information, the French Parliament passed the Data Protection Act (*loi 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*). As of today, these two texts are unconnected and there are no plans to merge them in one single act, as it is the case in some jurisdictions (like for instance, Quebec or some Swiss cantons).

Specific administrative agencies were assigned the task of implementing these two legal texts, respectively the Access to administrative documents commission (*Commission d'accès aux documents administratifs*, hereinafter CADA) and the Commission on Informatics and Liberties (*Commission nationale de l'informatique et des libertés*, hereinafter CNIL). Mission, organisation, tasks and powers of the CADA are precised in the third title of chapter III of the Code governing relations between the public and the administration (art. L340-1 to L342-4 as well as the decree 2005/1755). Chapter III of the Data Protection Act (art. 11 to 20), supplemented by a governmental decree 2005/1309, does the same for the CNIL. Both agencies have adopted internal regulations dealing with procedural matters (the latest version of CADA's internal regulation dates back to December 2016; CNIL revised its own regulation in July 2013).

Both CADA and CNIL enjoy the status of independent agencies. As such, they are governed by an overarching legal text, the law on independent authorities, passed by the French Parliament in January 2017 (*loi 2017/55 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes*). This innovative text aims at reinforcing autonomy of independent agencies; hence, it lays down common deontological standards regarding controversial issues like termination of the mandates of members of

independent agencies, incompatibilities with other assignments, finances as well as parliamentary oversight. Noteworthy a commissioner of an independent agency may only be impeached by a decision supported by ¾ of his fellow commissioners. Sole causes for impeachment are grave violations of legal standards or incapacity due to health or injury.

**B. Organisation of the Access to information authority and of the Data protection authority**

*1. CADA*

CADA is composed of 11 (part-time) commissioners appointed by the French Government. The president of CADA must be a judge of the supreme administrative court (*Conseil d'État);* he is designated by the President of the Republic. The composition of CADA is diverse to consider most stakeholders interests: two more high ranking judges, two parliamentarians, one representative of local authorities, four experts originating from different backgrounds (archives, antitrust and competition matters, media, university), as well as one member of the CNIL (see below E). However, no commissioner originates from civil society organisations.

Except for the deputies and the representative of CNIL, a commissioner has a three year mandate , renewable only once.

A staff of 14 civil servants headed by a secretary general assists the commissioners in their tasks. In addition, three highly qualified "rapporteurs" prepare the draft decisions of the CADA and a representative of the Government is allowed to attend the meetings of CADA, but is deprived of any voting rights.

*2. CNIL*

CNIL is composed of 18 (part-time) commissioners. Most them belong to the most important institutions of the state: the legislative branch (four parliamentarians), the judiciary (six superior judges) and the Economic and Social Council (two); each of these institutions appoints its own representatives. Only five commissioners are highly qualified public figures originating from civil society; one is chosen by the president of the Assembly, another one by the president of the Senate; the three last ones are elected by the Government. The 18$^{th}$ commissioner is, as of July 2017, a representative of CADA.

Except for the four commissioners who are parliamentarians (their mandates are synchronised with their legislative mandates), the other commissioners have a five year mandate, renewable once.

CNIL is a huge public body which employs around 200 civil servants (32 % lawyers; 15 % engineers), headed by a secretary general. It has a budget of 16 million Euros. The most important decisions of CNIL are taken at its weekly plenary sessions.

## C. Tasks of the Access to information authority and of the Data protection authority

*1. CADA*

CADA has three major tasks:

- to advice and educate public authorities on access to information issues (in particular by organising training seminars or by issuing specific guidelines) and as of 2017 on online publication by administrative agencies;
- to handle complaints by individuals whose requests to access to information have been totally or partially denied (and as of 2017 on complaints by administrative agencies having been denied access by other administrative bodies);
- to sanction any violation of the national rules implementing Directive 2003/98/EC on the re-use of public sector information (monetary penalties up to two million Euros in case of repeated illegal reuse).

In 2015, CADA processed 5,800 complaints and requests for advice. This record high number of cases dealt with is a matter of serious concern for the president of CADA who denounced the complexity of the rules on access to information regulations as well as the poor knowledge of these rules showed by French civil servants (see the 2015 Annual report of CADA, p. 3ff).

*2. CNIL*

CNIL has five major tasks:

- to inform and educate on data protection issues (to advice individuals and business companies, to issue guidelines and information sheets, to organise training seminars etc.);
- to authorise specific data processing (e.g. sensitive data, trans border data flows);
- to adjudicate complaints by individuals for violation of data protection regulations (around 5,000 complaints are filed each year);
- to monitor compliance with data protection regulations (more than 400 controls are conducted each year according to priorities laid down in a specific annual monitoring program);
- to anticipate new challenges of data protection by conducting studies or by launching ethical debates. The topic of interest for 2017 is algorithms and artificial intelligence.

## D. Powers of the Access to information authority and of the Data protection authority

*1. CADA*

The decisions taken by CADA on complaints by individuals are non-binding (and as such cannot be challenged in court); they are issued as recommendations that the public administration is free to follow or not. However, statistics shows that around 80 % of these recommendations are complied with.

*2. CNIL*

To perform efficiently its important tasks, CNIL has been vested with investigative, adjudicatory and, to a certain extent, regulatory powers. Hence, the injunctions of CNIL are binding; non-compliance can be sanctioned by monetary penalties up to 300,000 Euros.

## E. Relations between CADA and CNIL

*1. From informal mutual information to reciprocated participatory rights*

Until July 2017, CADA and CNIL lived distinct lives with no formal interaction, except that a representative of CNIL attended all meetings of CADA, as one of the 11 commissioners of CADA, to advise fellow commissioners on issues where privacy of individuals is at stake (e.g. interpretation of art. L311-6, which protects private life and trade secrets). Some informal contacts between individual commissioners of both agencies took sporadically place to exchange views on matters of mutual interest.

The adoption in October 2016 of the law 2016/1321 on the digitalisation of the French Republic, which aimed to improve governance over public information, enhanced cooperation between the two independent agencies. According to this new piece of legislation, the president of CADA is now *per se* a commissioner of CNIL and, *vice versa*, the president of CNIL becomes a commissioner of CADA. In addition, in case of an important issue of common interest, the two agencies may convey a joint meeting to discuss the problem. The conflict between privacy and open data might be one of the first issues to be debated in common, as the two agencies have so far expressed somewhat diverging views on this contentious topic.

*2. Fusion of the two agencies?*

According to reliable internal sources, the French government had envisaged in 2015 to merge CADA and CNIL. This intention has not materialised so far, to the contrary. An official study conducted by a former member of both CADA and CNIL (Jean Massot, *Les incidences sur la CNIL et la CADA du projet de loi pour une République numérique*, March 2016) concluded that such fusion was at best premature as the organisational structures, the powers and the working cultures of the two agencies were fundamentally different. The fact that CNIL is vested with decision-making powers whereas CADA only has the right to issue recommendations was one of the concerns. The rapporteur nevertheless conceded that the opportunity of a merger should be re-examined in a few years (i.e. as soon as fruitful experience has been gained on the implementation of the EU General Data Protection Regulation). Should at that point a fusion appear motivated, it would be wise to create two separate sections, one dedicated to data protection issues and the other one to access to information issues. The conclusions of the rapporteur received full support of the then Minister in charge of digitalisation of public life, Ms. Axelle Lemaire.

Nonetheless, one – albeit symbolic – step towards a fusion has been taken: CADA and CNIL will be in the same administrative building.

### 2.1.2 Italy

**A. Legal sources and dedicated agencies**

Until the end of 2016, the legal framework governing access to information in Italy was rather clear. The relevant source was the fifth chapter of the Act on administrative proceedings (*legge 241/1990 sul procedimento amministrativo*, art. 22 to 30). Far from being one of the most liberal FOI laws of the world, the Italian legislation was fairly reinforced by several amendments laid down in 2005 (*legge 15/2005*). Still this legal framework does not provide for the substitution of the paradigm of secrecy of the public administration by the paradigm of transparency; in particular, the requester must demonstrate a direct legal interest in order to access to the requested document. By way of the legislative decree 33/2013 (as amended by the legislative decree 97/2016), the Italian government finally introduced a full-fledged right of access to administrative documents, called general civic access (*accesso civico generalizzato*), with the aim of truly enabling individuals to control the activities of the public administration. Hence, the requester is no more obliged to motivate his or her request.

Nevertheless, the legislative decree 33/2013 is not supposed to supersede the provisions on access to information laid down by the law 241/1990: both sets of norms fully and deliberately coexist in parallel. A regrettable lack of coordination, which undoubtedly creates lots of uncertainty and confusion (inter alia the national data protection authority called for a clarifying intervention of the legislator, see the 2016 annual report of the *Garante alla protezione dei dati*, p. 32). In an attempt to mark the limits of the respective application scopes of the two legal texts dealing with access to information, the National Anti-Corruption Authority issued appropriate guidelines end of December 2016 (*Determinazione 1309/2016*).

Art. 27 of the law 241/1990 establishes a specific administrative body, the Access to administrative documents commission (*Commissione per l'accesso ai documenti amministrativi*, hereinafter CADA); this body, which is subordinated to the Italian Prime Minister, has been vested with the task of handling the complaints of individuals whose requests of access to information were rejected. However, one should underscore that complaints referring to violations of legislative decree 33/2013 are not at all processed by CADA. In fact, they are handled by the ombudsman (*defensore civico*) in case of denial by a local or regional authority, or, at the state level, by the delegate to anti-corruption and transparency matters (*responsabile della prevenzione della corruzione e della trasparenza*) within the national administrative agency which denied access.

The most important text regarding data protection is the Data Protection Code (*Codice in materia di protezione dei dati personali*) which was adopted in 2003 (*legge 196/2003*) and has more than 180 articles. Despite being one of the most comprehensive data protection legislations of the world, the DP Code is supplemented by countless sectorial regulations and code of conducts dealing with specific data protection issues (e.g. processing of personal data for journalistic purposes, for medical research or for creditworthiness evaluations).

Art. 153ff of the DP Code establishes a national data protection authority, called the *Garante per la protezione dei dati personali* (hereinafter the Garante). This independent body is vested with extensive regulatory and adjudicatory powers. Detailed instructions regarding the organisation and the way of functioning of the Garante are to be found in a specific decree (*Regolamento* 1/2000). To secure independence and impartiality, the Garante and attributed staff must respect specific deontological standards on incompatibilities and conflicts of interests laid down in the Code of ethics of the Garante (*Codice etico 1998*).

## B. Organisation of the Access to information authority and of the Data protection authority

*1. CADA*

Like its French counterpart, the Italian CADA is composed of 11 commissioners (reduced from 17 commissioners at its inception in 1990): two senators and two deputies (designated by the presidents of their respective chambers of the Parliament), four judges and prosecutors (designated by the presidents of their respective judicial institutions), a professor of administrative law (designated by the Minister in charge of universities) and the director of the Office of the Prime minister. CADA is chaired by the Undersecretary of state in charge of the general secretariat of the Government.

Except for the parliamentarians, the commissioners have a three year mandate, renewable without limits.

For administrative and secretarial support, CADA must rely on the assistance of the Office of the Prime Minister. As of today, one head of department and six civil servants are specifically assigned to CADA.

*2. The Garante*

The Garante is a collegial authority composed of four members: a president, a vice-president and two commissioners. Two members are appointed by the Senate; the other two by the Chamber of deputies. The four members of the Garante designate their president and vice-president themselves. In case of parity of votes, resolutions will be passed by the president's casting vote.

Members of the Garante should be experts either in law or in informatics. They are elected for a 7 years term; their mandate is not renewable. They are expected to devote all their working time to their mandate and are not allowed to perform any side activities.

The Garante is assisted by a staff of more than a hundred civil servants (*Ufficio del Garante*), headed by a secretary general.

## C. Tasks of the Access to information authority and of the Data protection authority

*1. CADA*

CADA must handle complaints by individuals whose requests to access to official documents has been totally or partially denied by national or supra-regional public authorities (complaints involving local and regional authorities are handled by the *defensore civico*). The numbers of cases dealt with by CADA is steadily on rise, reaching a record high of 1270 in 2015 (15 plenary sessions were needed to handle all the cases). Referral to CADA in case of denial of access is an alternative administrative proceeding: individuals denied access can always appeal directly to the competent administrative tribunal.

CADA has also to deliver opinions (*pareri*) on legal issues pertaining to transparency upon requests of advice from ministries, public entities, regional authorities or municipalities; these opinions, which amounted to 99 in 2015, aim to secure uniform interpretation of the provisions of the legal framework on access to information.

Finally, the CADA has also to produce an annual report on the transparency of the public administration; this survey, which last edition (2015) encompassed around 300 pages, evolved from traditional activities report to a comprehensive and updated analysis of the main issues regarding access to information.

*2. The Garante*

Originally thought as the driving force for data protection matters, the Garante has numerous tasks pertaining to the protection of the right to private life of individuals. In particular, it must:

- supervise compliance by public authorities and private companies with the Code on data protection (as well as with supplementary regulations). For that aim, the Garante carries out on the spot control interventions (in 2016, more than 200 inspections), and may prohibit or block illegal processing operations or order needed adjustments;
- handle formal complaints lodged by individuals (in 2016, around 250 resolutions;,
- grant authorisations to process certain data categories (e.g. data bases containing sensitive data);
- promote the adoption of sectorial codes of conducts;
- advise public authorities, business companies or individuals on specific data protection issues (in 2016, more than 20,000 informal advices);
- raise general awareness on data protection legislation (information campaigns, training seminars etc.);
- and annually report to the Parliament and the Government on the current state of affairs concerning data protection.

## D. Powers of the Access to information authority and of the Data protection authority

*1. CADA*

The nature of the resolutions of CADA is difficult to assess, as it is somewhat in-between binding and non-binding. Technically speaking, the defendant public authority is not compelled to comply with an adverse resolution of CADA. Should it opt for non-compliance, the defendant authority must expressly confirm denial of access within 30 days (the motives of the confirmation should not just reproduce the motives of the initial denial, but consider the motives of the adverse decision of CADA and explain why they are to be refuted). If the defendant authority remains silent passed the deadline, the decision of CADA enters into force. It must be said that CADA is not at all satisfied with this abstruse mechanism and requested many times (lastly in its 2015 annual report, p. 32) a prompt intervention of the legislator to be vested with a binding decision powers as well as with powers to sanction contravening public authorities.

The opinions of CADA on legal issues pertaining to transparency are non-binding.

Thus said, CADA is vested with investigatory powers; in particular, public authorities should upon request provide CADA with all necessary documents or information.

*2. The Garante*

Depending on the kind of tasks performed, the resolutions of the Garante are merely consultative (e.g. opinions or advices) or binding (e.g. authorisations, decisions on appeals lodged by individuals). In the latter event, the Garante can sanction any disregard of the measures that have been ordered (fines up to 100,000 Euros)

In any case, the Garante has full investigatory powers. Noteworthy, it can access databases, request documents, or search premises where data are processed (for private premises a search warrant from the local administrative tribunal is needed).

## E. Relations between the Garante and CADA

Contrary to its French counterpart, the Italian legislator did not opt for any form of mutual exchange of commissioners. Needed coordination between access to information and data protection would have to be provided on a case by case basis. If CADA (or the *defensore civico*) must decide on a case involving access to personal data, the opinion of the Garante should be asked (in order not to lose precious time, the Garante must deliver its opinion within ten days). *Vice versa*, if the Garante must decide in a case involving general access to information, CADA should be given the possibility to express its views. In both cases, the opinions delivered are non-binding. Regarding cases dealing with the new *accesso civico generalizzato* (see above A), the legislator has provided for a similar mechanism of preliminary opinions of the Garante. It is worth mentioning that, in both cases the preliminary opinions of the Garante are published.

Finally, it should be noted that the Guidelines regarding modalities of implementation of the new *accesso civico generalizzato* (see above A) were adopted by the National Anti-Corruption Authority in close cooperation with the Garante (as expressly prescribed by the Government in the legislative decree 97/2016).

### 2.1.3 Sweden

**A. Legal sources and dedicated agencies**

It would be unwise to assess the situation in Sweden without going back to history and underlining the pioneer role of this Nordic kingdom in the fields of both access to information and data protection. Not only was it the first country in the world to adopt a FOI legislation (1766), but it was also the first one to adopt a law on data protection (1973). Sweden proved again to be ground breaking in creating, in 1809, the institution of the parliamentary *ombudsman*, a mediator or public advocate, in charge of addressing complaints of individuals for maladministration or violation of individuals' rights.

Today, openness and transparency are key ingredients of the Swedish political system. Hence, access to information is enshrined at the highest level of the domestic legal order by way of an organic law, the law on the press (*Tryckfrihetsförordningen*, 1949:105). Its second chapter lays down the scope of the right to information and the legitimate grounds for denial of access; it provides also for a speedy and uncostly procedure. The law on transparency and secrecy (*Offentlighets- och sekretesslag*, 2009:400) supplements this fundamental text by precising the modalities of access. This comprehensive piece of legislation (more than hundred articles) lists, one by one, all the exceptions to the right of access. Thus, contrary to most FOI legislations, the Swedish legislation relies not on broad and vague clauses of secrecy (like the "private life"), but on extremely detailed secrecy norms (e.g. more than twenty lengthy articles deal with secrecy of personal data pertaining to social security). This unique legal technique narrows the margin of appreciation of the requested public authority, leaving less room to restrictive interpretations and abusive denials of access. Another distinctiveness of the Swedish legal framework on access to information is the absence of any public body specifically dedicated to the task of dealing with access to information matters. Grievances for denial of access are to be submitted either as appeals to the competent administrative court (*Kammarrätten*) and/or as complaints to the parliamentary ombudsman (*Justitieombudsmannen*, hereinafter JO). Tasks and powers of JO are governed by an organic law (*Riksdagsordningen*, 2014:801; see chapter 13) and by the Act with Instructions for the Parliamentary Ombudsmen (*Lag med instruktion för Riksdagens ombudsmän*, 1986:765; hereinafter the Instructions).

The relevant piece of legislation regarding data protection is the law on personal data (*Personuppgiftslagen* 1998:204); in addition, specific statutes govern certain highly debatable issues, like video surveillance, patient files or credit rating. The law on personal data envisages only the existence of a supervising authority. By way of a decree (initially

1988:912, now 2007:975), the Government created the Data Inspection Board (*Datainpektionen*) and delineated its tasks.

The legislation on access to information and the legislation on data protection are mutually coordinated in so far as the former legislation is given precedence over the latter one. Art. 8 of the law on data protection prescribes that : "*The provisions of this Act are not applied to the extent that they would limit an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide personal data.*"

Both JO and the Data Inspection Board are autonomous public bodies. Their independence from any governmental interference is acknowledged by the Swedish constitution (see art. 2, chapter 12 *Regeringsformen*).

**B Organisation of the Access to information authority and of the Data protection authority**

*1. JO*

JO consists of four ombudsmen; all of them are appointed by the Parliament for a (renewable) four year term. One of the ombudsmen holds the title of Chief Ombudsman; this title is not a sign of any superiority nor seniority; it only shows that this person is responsible for the internal organisation of JO. In particular, he or she defines the different areas of competences of each ombudsman (see *Arbetsordning för Riksdagens ombudsman* 2012).

As a matter of fact, JO is not a collegial body. Each ombudsman supervises a specific entity of the public administration (e.g. armed forces or the judiciary) and/or a specific domain (e.g. health and medical care). In other words, each ombudsman has its own well-delineated sphere of competences which colleagues cannot interfere with (art. 2 of the Instruction precises that "*An Ombudsman is not subject to the supervision of any other Ombudsman.").* Access to information issues are overarching issues, not belonging to a specific domain of public activities; thus, all four ombudsmen might deal with these issues.

A staff of more than 100 persons (many of them lawyers) assists JO.

*2. The Data Inspection Board*

The *Data Inspection Board* is a public body employing around 45 persons (mostly lawyers), headed by a (full time) Director General who is solely responsible for the performance of the Data Inspection Board.

The Government appoints the Director General. Being a civil servant, he or she is hired for an unlimited period. The Director General appoints employees of the Data Inspection Board.

An Advisory Council (*Insynsråd*) monitors the work the Data Inspection Board. Without any adjudicatory powers, this body can only give advices to the Director General. Its seven

members are appointed by the government and hold their position as an accessory assignment (the Council meets four/five times a year).

**C. Tasks of the Access to information authority and of the Data protection authority**

*1. JO*

JO has the overall task of supervising public authorities and denouncing any case of maladministration. Interventions of JO are prompted by a formal complaint of an individual or, more seldom (around 1 % of the cases) by media reports. In 2016, JO deemed less than 10% of the complaints justified and directed criticism towards the contravening or neglectful agency.

As the law commands JO to pay attention to infringements of individuals' fundamental rights, access to information issues are obviously among its major concerns. Therefore, the annual report of JO always dedicates a specific section to this topic, describing in detail six to ten relevant cases (most often cases of delayed handling of the request of access or incorrect interpretation of secrecy provisions).

2. *The Data Inspection Board*

The tasks of the Data Inspection Board are numerous, ranging from raising awareness on privacy issues and giving advice to interested parties, to handling complaints from individuals for violation of data protection standards and undertaking inspections of public and private data bases and data networks. Noteworthy the legislator emphasises the role of the Board in anticipating new challenges and in preventing infringements. Every year, the Government defines general goals for the Data Inspection Board; in its last edition (*Regleringsbrev för budgetåret 2017 avseende Datainspektionen*), the Board was invited to investigate in depth the impact on privacy of the current process of digitalisation of public services.

**D. Powers of the Access to information authority and of the Data protection authority**

*1. JO*

Although the ombudsmen's statements are legally non-binding and public authorities are not obliged to comply. in practice however, they usually do. As JO has acquired, over decades, a solid reputation of integrity and competency, its resolutions are much respected by the authorities. Needless to say, JO enjoys a high level of confidence from the media and the population.

In case of grave maladministration, JO has the right to prosecute the wrongdoer in front of the competent criminal court as well as to call for his or her dismissal.

*2. The Data Inspection Board*

Originally thought as a highly skilled consultative and advisory body, the Data Inspection Board is supposed to favour negotiation over enforcement. The legislator thus vested the

Board with limited adjudicatory and regulatory powers. In some cases, the Board can issue binding decisions (e.g. urgent blocking of an illegal process) or authorisations (e.g. video surveillance or creditworthiness activities), in other cases not (e.g. destruction of illegal data can only be ordered by an administrative court).
In any case, the Board enjoys extensive investigative powers; the supervising authority can request documents, access to databases and search premises where data are processed.

**E. Relations between the JO and the Data Inspection Board**

Contrary to France or Italy, one must note a total absence of formal interaction between JO and the Data Inspection Board. The law does not call for joint sessions or mutual requests for advice. This lack of direct contacts does not mean that the two agencies ignore oneanother, to the contrary. Whenever relevant, JO and the Board pay due consideration to oneanother's resolutions (see for instance JO resolution 1376-2013, a case of secret sensitive personal data sent by e-mail, where extensive reference is made to the jurisprudence of the Board). The more so as Swedish state agencies are generally compelled to cooperate with each other for the sake of individuals (see art. 6. of the decree on administrative authorities, 2007:515).

## 2.2 Combined authorities

### 2.2.1 Slovenia

**1. Status and Responsibilities**

The first FOI legislation was enacted in Slovenia in March 2003 and the first independent Commissioner for Access to Public Information started to work in September 2003. Slovenia decided to merge FOI in PDP after entering the European Union in 2004, since its Inspectorate for Personal Data Protection did not hold a status of an independent state *sui generis* body as demanded by Directive 95/46/EC on the protection of individuals regarding the processing of personal data and on the free movement of such data. The Inspectorate was namely part of the Ministry of Justice and therefore without proper independent powers. In 2005, the Information Commissioner Act was adopted by the parliament and the Inspectorate for Personal Data and Commissioner for Access to Public Information merged to a completely independent public sector body – the Information Commissioner (IC). Before that, in case of no agreement on whether certain personal data could be public or not, the two separate bodies could even sue each other before the Administrative court. It should be stressed that such a law suit was never filed but the disagreements were often debated internally on joint meetings and publicly.

The Commissioner is proposed by the President of the Republic and elected by the relative majority in the Parliament for a 5-year term and can be re-elected for a second term; the candidate must have a university degree and at least 5 years of working experience. IC has its own budget and can employ all the public servants independently. There are approximately 35 staff members employed by the Commissioner, working on both fields.

The Commissioner has three deputies, all are nominated directly by him or her with no political influence. One of them oversees PDP, an other one FOI; the third is the head of PDP inspection unit. IC can issue binding decisions in both legal fields and has inspection rights to search premises when needed also for FOI matters. IC's FOI and PDP decisions can be appealed on a point of law before the administrative Court (administrative dispute).

**2. Detailed competencies**

**A. In the field of access to public information**

In the area of access to public information, the Information Commissioner acts as appeal body, competent for deciding on appeals against the decisions by which another body has refused or dismissed the applicant's request for access, or violated the right to access or re-use public information. In the context of appeal proceeding, the Information Commissioner is also responsible for supervising the implementation of the Act governing access to public information and regulations adopted within the framework of the proceedings. In the field of access to public information, the Information Commissioner also has the competences determined by the Media Act (Article 45). A liable authority's refusal of a request by a representative of the media shall be deemed a decision refusing the request. Failure to respond to the request is considered both a misdemeanour and areason for appeal. The competent authority, that decides on appeals is the Information Commissioner who considers them in accordance with the provision of the Access to Public Information Act (hereinafter the APIA).

When handling a complaint challenging a decision to deny access to public information, the Commissioner is authorised to have access to every data storage medium covered by the law including all classified data.

**B. In the field of personal data protection:**

In the field of personal data protection, the list of duties is of course much longer. The Information Commissioner acts according to the competencies as defined by the Personal Data Protection Act and Article 2 of the ICA, namely:

1. performing supervision over the implementation of the provisions of Personal data protection Act (PDPA) and other laws that regulate the processing of personal data (handle cases of complaints, appeals, notifications and other applications, explaining possible breach of law and perform planned-preventive inspections with personal data controllers in public and private sectors);
2. deciding as appellate body on individuals' complaints when the data controller refuses to give access to the personal data of the data subject after an access request or a request for extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the act governing personal data protection;

3. performing procedures regarding violations in the field of personal data protection (expedient procedure);
4. managing and maintaining a register of filing systems, ensuring its updating and public internet access (Art. 28 of PDPA);
5. ensuring viewing and transcription of data from the register of filing systems (as a rule on the same day or in eight days at the latest – Art. 29 of PDPA);
6. deciding on an individual's complaint regarding processing of personal data based on Art. 9(4) and Art. 10(3) of PDPA;
7. issuing decisions on ensuring an adequate level of personal data protection in third countries (Art. 63 of PDPA);
8. performing procedures for assessing an adequate level of personal data protection in third countries based on findings of supervisions and other information (Art. 64 of PDPA);
9. managing a list of third countries ascertained to have partially or entirely adequate or inadequate personal data protection levels; in case only a partial adequacy of personal data protection is ascertained, the list will also state the scope of adequate protection (Art. 66 of PDPA).
10. managing administrative procedures to issue permissions to transfer personal data to a third country (Art. 70 of PDPA);
11. managing administrative procedures to issue permissions to link public records and registers when one of the filing systems to be linked contains sensitive personal data or if implementation of the linking requires the use of the same connecting code (such as the standardised personal registration number or tax number) (Art. 84 of PDPA);
12. managing administrative procedures to issue declaring decisions on whether a planned implementation of biometric measures in private sector is accordant with the provisions of PDPA (Art. 80 of PDPA);
13. cooperating with government bodies, competent EU bodies for protection of individuals regarding processing personal data, international organisations, foreign personal data protection bodies, institutions, associations, and other bodies and organisations regarding questions of personal data protection;
14. issuing and publishing preliminary opinions to state bodies and public powers holders on harmonising the provisions of proposals of legislation with Acts and other legislation governing personal data;
15. issuing and publishing non-obligatory opinions on conformity of professional ethics codes, general conditions of business or the proposals thereof, with regulations in the field of personal data protection;
16. preparing, issuing and publishing non-obligatory recommendations and instructions regarding personal data protection;
17. the publication on internet page or in any other appropriate manner of preliminary opinions on compliance with positive Acts and other legislation of proposals of Acts and other regulations in the field of personal data protection, as well as publication of requests for constitutional review of statutes (Art. 48 of PDPA); issue internal bulletin and expert publications; publish decisions and court resolutions dealing with personal

data protection, as well as non-obligatory opinions, explanations, positions and recommendations with regard to personal data protection (Art. 49 of PDPA);

18. issuing press releases on performed supervisions and preparing annual reports on its work in the current year and report to the Parliament;

The Information Commissioner is an appellate body, which is competent for supervision over implementation of the Information Commissioner Act, the Access to Public Information Act within the framework of its appellate proceedings, the Media Act and the Personal Data Protection Act.

The Information Commissioner is also entitled to request the Constitutional Court to initiate procedure for the review of the constitutionality or legality of regulations or general acts issued for the exercise of public authority, provided that a question of constitutionality or legality arises about a procedure the Commissioner is conducting.[8]

### 2.2.2 Serbia

**1. Status and Responsibilities**

The Commissioner for Information of Public Importance is an independent and autonomous public authority, established under the Law on Free Access to Information of Public Importance in 2004. Under the Law on Personal Data Protection of October 2008, it was renamed Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: Commissioner) and received new powers as of 1 January 2009.

The Commissioner is appointed by the National Assembly of the Republic of Serbia for a seven year term of office, with a possibility of maximum two re-elections. The incumbent must be an eminent expert in the field of human rights, with a graduate degree in law and at least 10 years of relevant work experience. IC has its own budget and can employ all the public servants independently; there are approximately 80 staff members employed by the Commissioner, working on both fields.

The Commissioner exercises his or her duties independently. He or she shall neither request nor accept orders or instructions of other public authorities or other individuals and may not be held responsible for opinions or suggestions given while performing his or her duties. Pursuant to the law, the Commissioner has two deputies, appointed by the National Assembly on Commissioner's proposal for a seven-year term of office as well, with a possibility of one re-election.

[8] Annual Report for 2014: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual_Report_2014.pdf

**2. Detailed competencies**

The Commissioner has the following powers:

**A. In the field of freedom of information:**

- To handle complaints against decisions passed by public authorities relating to violations of the rights provided for under the Law on Free Access to Information of Public Importance (hereinafter referred to as LFAIPI);
- To monitor public authorities' compliance with the obligations set out in this law and report to the public and National Assembly thereof;
- To initiate the drafting or amendment of regulations implementing and promoting the right to access information of public importance;
- To propose measures public authorities should take to improve their compliance with the law;
- To undertake necessary measures to train the staff of public authority bodies and to familiarise them with their responsibilities about the right to access information of public importance for ensuring effective implementation of the law;
- To inform the public of the content of the law and the rights it regulated and perform other duties under this law,
- To file a motion for review of constitutionality and legality of laws and other general enactments;

**B. In the field of personal data protection:**

- To supervise the implementation and enforcement of the Law on Personal Data Protection (hereinafter referred to as LPDP), i.e. to supervise the enforcement of data protection;
- To decide on appeals in cases set out in this law;
- To maintain a central register of data files;
- To supervise and allow trans-border transfer of data out of the Republic of Serbia;
- To point out the identified cases of abuse in data collection;
- To produce a list of countries and international organisations with adequate provisions on data protection;
- To give his or her opinion on the formation of new data files or introduction of new information technologies in data processing;
- To give his or her opinion in case of doubt whether a data set constitutes a data file within the meaning of the law;
- To give his or her opinion to the Government in the procedure of enactment of instruments governing the methods of data filing and safeguards for particularly sensitive data;
- To monitor the implementation of data safeguards and to propose improvement of those measures;

- To give proposals and recommendations for improving data protection;
- To give prior opinion on whether a certain processing method constitutes specific risk for a individuals' rights and freedoms;
- To keep up to date with the data protection arrangements in other countries;
- To cooperate with authorities responsible for data protection supervision in other countries;
- To determine the way in which data are to be handled if a data controller ceased to exist, unless provided otherwise;
- Regarding maintenance of the Central Register, to publish an inventory of data files in the "Official Gazette of the Republic of Serbia" annually and to post the mandatory Central Register, as a public document, on the Internet.

The Commissioner has also the following duties set under the law:

- Within three months of the end of every fiscal year, to present the National Assembly with an annual report on the activities undertaken by public authorities to implement these two laws and his or her own activities and expenses. The Commissioner shall also present other reports to the National Assembly if he or she deems it necessary. The Commissioner forwards the report submitted to the National Assembly also to the President of the Republic, the Government and the Ombudsman and makes it available to the public by appropriate means;
- To publish and update a manual with practical instructions for the effective exercise of rights regulated by LFAIPI in Serbian and in languages identified as official under the law;
- To inform the public of the content of the manual for implementation of LFAIPI via the press, electronic media, internet, public panel discussions and in other ways;
- To issue instructions for the publication of directories of public authorities.

When handling a complaint challenging a decision to deny access to information of public importance, the Commissioner is authorised to have access to every data storage medium covered by the law, including classified data. Commissioner's FOI and PDP decisions can be appealed on a point of law before the Administrative Court (administrative dispute). In both fields, the Commissioner can issue binding decisions.

### 2.2.3 United Kingdom

**1. Status and Responsibilities**

In the UK as opposed to Slovenia and Serbia, independent Data Protection Authority (the Registrar) was established first and FOI competences were added later. The Data Protection Act came fully into force on 11 November 1987. At that time, the Registrar's Investigations department was formed. In January 2001, the office was given the added responsibility of the Freedom of Information Act and changed its name to the Information Commissioner's Office

(ICO) . On 1 January 2005, the Freedom of Information Act 2000 was fully implemented. Today, more than 400 staff members are employed by the ICO in offices in Wilmslow (England), Northern Ireland, Scotland and Wales, handling more than 16,000 data protection complaints, 5,000 freedom of information complaints and over 200,000 calls to the helpline. The ICO also administrates over 400,000 entries on the Register of Data Controllers.

**2. Detailed competencies**

The Commissioner has the following powers:

**A. In the field of freedom of information**

The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information. If the complaint is not resolved informally (what is the common ICO's practice), the ICO can issue a decision notice (it has a status of a binding decision). If it finds that the public-sector body have breached the Act, the decision notice will say what it need to do to put things right. The ICO also has powers to enforce compliance if public sector bodies have failed to adopt the publication scheme or have not published information as they should, whether or not the ICO has received a complaint about this.

Specifically, where authorities or public sector bodies repeatedly or seriously fail to meet the requirements of the legislation, or conform to the associated codes of practice, the ICO can take the following action:

- to conduct assessments to check organisations are complying with the Act;
- to issue information notices requiring organisations to provide the ICO with specified information within a certain time-period;
- to issue undertakings committing an authority to a particular course of action to improve its compliance;
- to issue enforcement notices where there has been a breach of the Freedom of Information Act or Re-use of Public Sector Information Regulations, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law;
- to issue recommendations specifying steps the organisation should take to comply;
- to issue decision notices detailing the outcome of the ICO's investigation to publicly highlight particular issues with an organisation's handling of a specific request;
- to prosecute those who commit criminal offences under the Act; and
- to report to Parliament on freedom of information issues of concern.

**B. In the field of personal data protection:**

Several tools are available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to impose a monetary penalty notice on a data controller.

The other main powers are:

- to issue information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time-period;
- to issue undertakings committing an organisation to a particular course of action to improve its compliance;
- to issue enforcement notices and 'stop now' orders in case of a breach, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law;
- to conduct consensual assessments (audits) to check organisations are complying;
- to issue assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- to issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010;
- to prosecute those who commit criminal offences under the Act; and
- to report to Parliament on issues of concern.

Part of the ICO's role is to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public.

In some cases, the ICO collates further information on similar issues, looking at the concern alongside others raised about the organisation. In cases where a clear and serious breach of the legislation has taken place, the ICO will take direct action on the specific concern raised. If it decides that there has been a serious failure to comply with the law, it will provide advice and instruction to help ensuring that the organisation behaves well in the future. If an organisation does not take its responsibilities seriously, the ICO may also take enforcement action. In the most serious cases, the ICO can impose monetary penalties of up to £500,000.

The Information Commissioner is an independent official appointed by the Crown (HM the Queen), reporting directly to Parliament, for a five-year term and can be re-elected.

The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal. Appeals from notices are heard by the First–tier Tribunal (Information Rights), part of the General Regulatory Chamber (GRC). The First–tier Tribunal (Information Rights) specifically hears appeals of enforcement notices, decision notices and information notices

issued by the Information Commissioner. The GRC brings together a range of previously separate tribunals that hear appeals on regulatory issues.[9]

The ICO has two deputies, who are appointed by the Commissioner.

# 3. Pros and cons for a combined authority and separate authorities

## 3.1 Advantages for a combined authority (and disadvantages for separate authorities)

1. PDP and FOI are two rights which often have to be balanced and reconciled. Such a balancing exercise is treated differently in different countries. This is the case worldwide, including Europe. While the EU adopted a directive on PDP, which is binding on all EU member states, there is no such single piece of legislation for access to public information. This is also the case in the Council of Europe, namely Convention 108 for the Protection of Individuals regarding Automatic Processing of Personal Data, which was opened for signatures in 1981 and entered into force in 1985 after five countries ratified it.[10] Until now, 50 countries have ratified it.[11] On the contrary, Convention 205 on Access to Official Documents which was adopted in 2009 has not still been not ratified by 10 countries, the minimum number for a Convention to enter into force. Until now, eight years after its finalisation, only nine countries did it. It can be argued that PDP seems less problematic for CoE and EU countries than FOI, but on the other hand this also means that PDP is regulated in a more unified way than FOI. And in situations where FOI is not safeguarded by the country Constitution whereas PDP is, it seems to place one right above the other, which should not be the case according to the European Convention on Human Rights,which does not rank rights. A combined office is therefore better since both rights are to be treated equally and carefully enough to strike the right balance when the collision in FOI cases occurs, thus avoiding having to consult other bodies, to have external "legal fights" but only internal ones which are by no doubt more productive since at the end decision must be reached no matter what. This is also valid for decisions regarding open data or re use of public sector information.

On must honnestly reckon that governments are using, and sometimes abusing, the strictness of the EU Directive 95/46/EC and national PDP legislation to deny access to documents containing personal data. The basic principle of PDP legislation is that personal data processing can only be allowed by law and/or by personal consent. But the fact is that not all real-life situations can be predicted in the legislation. This rule must consequently be interpreted narrowly but not strictly, and profound knowledge of both rights is needed.

[9] Source: https://ico.org.uk.
[10] Information available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, viewed on 16 June, 2017.
[11] Information available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DPgaeJlZ, viewed on 16 June 2017.

2. Except maybe for Finland and Sweden, where secrecy norms are detailed in an unique way, neither national laws nor supra-national FOI and PDP legislation offer specific and concrete solutions when different rights are to be balanced. A case-by-case doctrine should be implemented in a concrete decision-making process. To identify the relevant deciding factors, the overriding public interest test needs to be considered. If a FOI system does not have an overriding public interest test implemented in the law, how can the conflict be solved? Is it appropriate that the moment a decision-maker "hits" an exemption prescribed by the FOIA, access is denied? Are courts the only bodies able to use the proportionality principle to find the right balance? The answer is of course not easy and such complicated legal questions are easily solved if experts from both legal fields, FOI and PDP, work under one roof. If the problem about how to reconcile the rights is solved within one body, there cannot be disputes afterwards between Data Protection Authority and Access to public information appeal body, since the decision is debated internally and both heads of a combined body need to agree on final decisions.

3. Public access to information is essential for maintaining a democratic relationship between governments and the individuals.. Privacy is daily at stake due to a drastic shift in governments' behaviour after the events of 9/11. In the fight against terrorism, government intrusion into privacy is becoming ever more acceptable, because the public opinion has shifted from a grudging acceptance of necessary security to an active demand for guaranteed security. In this context, there is also a trend for governments to withhold more and more documents from public disclosure, and PDP is becoming an increasingly convenient excuse for not revealing the data.[12] Therefore it is important that, when analysing new laws and giving advice to government or oppose governmental proposals of laws, a combined body tries to promote a proportionate legislation and balanced intrusion into one or another human right, as debated in this analysis.

## 3.2 Advantages for separate authorities (and disadvantages for a combined authority)

1. Although both legal texts govern information in the hands of public authorities, the political aim of access to information laws and personal data protection laws diverge fundamentally. The main goal of PDP legislation is to secure the right to privacy of individuals in the information society whereas the main goal of FOI legislation (apart from being an instrument to exercise the fundamental human right of freedom of expression) is to ensure accountability of public administration. These different, sometimes even conflicting goals (see above 3.1.1), are difficult to achieve for a combined control authority. How to promote, at the same time, on the one hand openness and on the other hand confidentiality, without creating confusion and incoherence? The recent French report about a possible merger of its two national control authorities acknowledged this dilemma and recommended not to merge two bodies with such different tasks and cultures (see above 2.1.1).

[12] Pirc Musar, Nataša.: *How to strike the right balance between access to public information and personal data protection – using a public interest test*, PhD thesis, Vienna University, November 2015.

2. In addition, it is worth noting that the Council of Europe never recommended establishing combined authorities. Neither the explanatory report to Convention 205 (access to information) nor the explanatory reports to Convention 108 (data protection) and its additional Protocol 185 (supervisory authorities) address this issue. In addition, it is worth mentioning that the Council of Europe did not set up a European combined body to monitor effective implementation of the two instruments by member states. Convention 205 sets up a "Group of Specialists" and Convention 108 a "Consultative Committee". These two organs are supposed to act independently: no mechanisms of cooperation or consultation are provided for (informal interaction is not even envisaged by the two conventions' respective explanatory reports).

3. To entrust a dedicated control authority with the task of safeguarding and promoting openness and accountability would send a clear signal to both the public administration and the population that a new era of open government has started. A separate body would really incarnate the shift the fundamental shift from a paradigm of secrecy to a paradigm of transparency.

4. There is a clear and direct link between access to information and protection of privacy: the right to privacy is a right that either complements or should be balanced against the right of access to information on a day-to-day basis when FOI appeals and exemptions are in question. It is appropriate to combine the roles of promoting access to information and protecting personal data, but if this task is given to a pre-existing body, sufficient resources must be allocated to the information commission function. There is a danger that this could not be the case if two fields are only merged with no proper human resources evaluation and needs.

# 4 What to consider when building the FOI appeal mechanism

As already mentioned, the question whether to have a combined FOI and PDP or a single competent body should not be a primary question. It can be argued that at least two relevant legal questions should be considered as well. Those are:

1. **What are the appeal possibilities within the national FOI regime?**

This question is relevant due to many factors, among which the possibility that an appeal body can issue binding decisions, the costs of appeal, the backlogs that may occur before appeal bodies, timeliness, the independence of the appeal body, and its investigative powers. The states focused on in the present study provide for the major appeal systems: states where the IC can issue a binding decision, countries with an Ombudsman as an appeal body, and direct access to the courts.

### 2. Is a public interest test laid down in the national FOI Act (FOIA)?

The existence of a public interest test is particularly important for balancing FOI and PDP and is highly relevant for countries where FOI is not a constitutional right, and where the proportionality test based on the national constitution can therefore not be used. If there is no public interest test and no constitutional provision on FOI, the system in effect leaves it to the legislature to decide which documents can be public and which not, meaning that virtually no balancing is possible but only the strict letter of the FOIA is to be obeyed. The relevance of the public's right to know is thus left to administrative rules and an overriding public interest in a document can never trump one of the exceptions.

There is no doubt that laws of Council of Europe member states can be reviewed under the ECHR and that ECHR is directly applicable when judging in a concrete case. But the whole problem lies in the fact that the European Court of Human Rights (ECtHR) still did not clearly and explicitly define that Article 10 contains FOI as a right which can be used by everybody. Hence, the ECtHR jurisprudence is (still) not helpful regarding access to public documents as a right accessible to all the people and not only to the media and civil society groups. This is the basic problem for balancing fundamental rights in countries where FOI is not a constitutional right and ECtHR case-law is of no help; therefore it can be argued that the public interest test is the best possible way to strike the right balance between FOI and PDP within public administration itself. It is also important to stress that public administration, which is always a first level body regarding the FOI request (in many cases also a second instance) is not confident and accustomed to using the constitution or supra national law as a legal ground and argument.[13]

## 4.1 Models of balancing FOI and PDP

### 1. The "trump" (explicit) model

With this model, there is no doubt that balancing rights is possible and even necessary, since the overriding public interest is explicitly mentioned in the national FOIA. Balancing can therefore be considered as an obligation by a public authority. Some FOIAs in EU member states include an overriding public interest test for some exceptions, but not for personal data, hence personal data is an absolute exemption (for example, the UK and the EU). There are, however, some EU member states where personal data is a relative exemption and this model is applicable to those countries (Bulgaria and Slovenia). Outside the EU, Norway has also had this model since 2008, when the FOIA was amended and an overriding public interest test was introduced. This Norwegian FOIA has the most advanced solution for balancing FOI exemptions as there are no absolute exemptions at all. The added value of this model is that balancing must be conducted by all decision-making bodies (the administration, the IC, ombudsmen, judges), in conformity with the explicit legal grounds provided for by the law. This model should be regarded as a "success story" because PDP can always be subject to the

[13] Pirc Musar, Nataša.: *How to strike the right balance between access to public information and personal data protection – using a public interest test*, PhD thesis, Vienna University, November 2015.

overriding public interest test, even if it results in the disclosure of a document that contains personal data and might cause harm to the protected interest (in this case a human right).

It can be argued that this model is the most effective for achieving appropriate levels of transparency.

### 2. The "chance" model

This model can be found in countries where the FOI law establishes a harm test (EU, Sweden[14], and the UK). With this model, there is always a chance that transparency (the overriding public interest) will "lose out" to PDP (unless there is an explicit provision in the law that certain personal data is public), since the disclosure of personal data can often and easily cause harm. For example, to disclose the farm subsidy of a specific farmer or to disclose the salary of a public official would invade the person's privacy, and hence, it could be argued, would cause harm. It should be noted that when public officials are provided with the possibility of applying a harm test to exceptions but not the possibility of using a public interest test, this seems to imply that considerations of privacy and the integrity of the individual enjoy primacy over the general right of access to documents. The bias towards PDP in these FOIAs is obvious because they only require an assessment of whether harm is done to PDP in disclosing certain information, without "balancing" it against the possible harm to FOI in *not* disclosing such information.

This bias is not, however, the same as an absolute protection of PDP, as shown by the Court of Justice jurisprudence regarding the EU FOIA. For example, the Court has established that personal income is undoubtedly protected by the right to privacy and that to disclose salaries is a serious interference with this right as "*it is not impossible that they may suffer harm as a result of the negative effects of the publicity attached to their income from employment*."[15] This model can be advocated from a transparency-perspective as it removes the absolute-exemption approach by requiring refusals to substantiate the likelihood of damage to specific interests that would arise from disclosure of the information in question.

With this model, there are fewer possibilities available to achieve a balanced transparency and fulfil the public's right to know. Nevertheless, in countries with this model, case-by-case balancing is possible and some personal data can be disclosed to improve government accountability.

[14] Even though Sweden use the harm test, it needs to be added that there are extremely detailed secrecy norms changing the whole approach and leaves less room to interpretation (see above Sweden A).
[15] *Österreichisher Rundfunk and Others,* Joined Cases C-465/00, C-138/01 and C-139/01 [2003] ECR I-4989, Para. 89.

### 3. The synergy model

This model offers a fair solution about speediness and prevents possible unwarranted avoidance of the disclosure of information by public officials, since the FOIA (and/or other laws) explicitly requires that certain personal data be publicly available. With this model, the synergy, the balancing, is carried out by the law makers, which decides to define an absolute requirement and consequently to lower the protection of personal data in certain cases (e.g. "the salaries of public officials are public", "high public officials must reveal their personal assets to the public", "all farm subsidies are public") and not by a decision-maker, the holder of a document. The balancing performed by the law makers during the legislative process must always take a proportionality principle into account and hence decide how much disclosure of specific personal data is necessary in a democratic society. Through this kind of synergy between opposing rights, a proper balance is struck in before any potential FOI requests is filed with the public authority. This model enables that all the "non-protected" personal data can be proactively disclosed without any additional balancing needed by the public authority.

This model is usually found in national legal systems accompanying other models, and may considerably contribute to making FOI systems work efficiently, although having this as the only model can question efficiency. The disadvantage of this model is that it is impossible for the law makers to predict all possible conflicts since the day-to-day operations of public sector bodies always brings new conflicts between personal data and FOI. Nevertheless, the more personal data can be defined in advance as being publicly available, the better for FOI, because not all public servants (especially those working in smaller public entities, such as small municipalities, schools, kindergartens and health institutions) in charge of the FOIA are (due to the lack of legal knowledge) capable of carrying out a sophisticated balancing of conflicting rights.

This model can be found, for example, in Hungary, the Czech Republic, Slovenia, and many other countries. The best possible way to implement it in a national FOIA is to define the public accessibility of information in broadest terms, e.g. "all information connected to public funds is to be public". Such provisions can be found in the Slovene and Czech FOIAs.

### 4. The implicit model

This model entails that no public interest or harm test is envisaged in the FOIA, although the proportionality test might still be applied as general principle of law derived from a constitutional law, and hence balancing is always possible and necessary to reach a well-reasoned decision. Due to the functioning of general principles of the law, it is quite probable that, even without the existence of any specific provisions within the FOIA, the decision-making body should apply general principles of law. In the case of conflicting rights, the proportionality principle is the most appropriate one.

The fact that general principles of law cannot be disregarded was shown in the the ECtHR case *HCLU v. Hungary*, in which the Court ruled that refusing access to information that is crucial for public debate and which is held by the authorities, constitutes a violation of the right to freedom of expression established by Article 10 of the ECHR as well as FOI. Although the Hungarian courts, including the Constitutional Court, had denied access to a document because of PDP, the ECtHR found that those decisions were not in accordance with the ECHR.

This model proved to be the least efficient and offers the most possibilities for denying access to personal data since an implicit balancing is rarely applied by public authorities which hold a specific document.

To conclude, it can be argued that the best possible solution for both sides, public authorities and applicants, is to combine the Synergy and "trump" models. Such a combination enables timeliness and a proper balance between the two rights. It also enables public authorities to know in most cases how to react and which personal data to disclose without any specific legal knowledge of constitutional law and balancing human rights. Only in the cases where the law makers did not provide a clear legal provision in the law should the overriding public interest test be used. But it is good to have such a possibility because cases when balancing is needed are a part of the daily course of work of public authorities.[16]

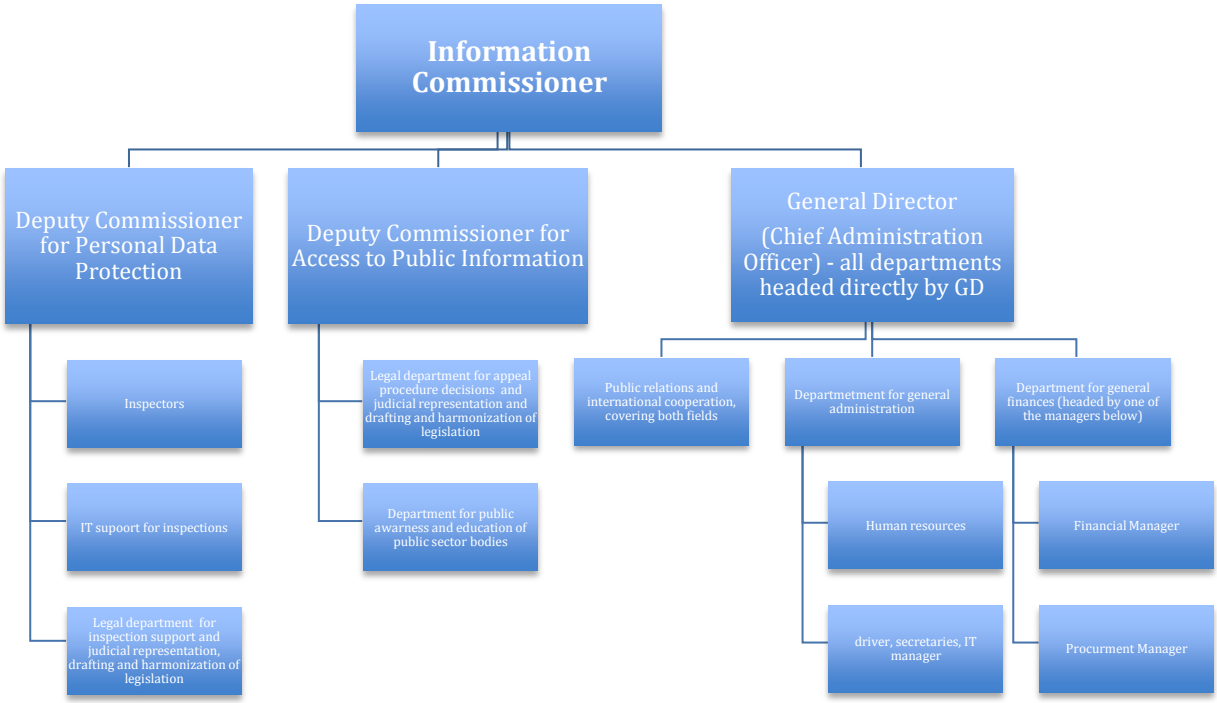
## 5 Conclusion

Regarding efficiency and timely decisions, the better solution for the countries which decide to have an information commissioner or commission as control authority is to merge FOI and PDP under the competence of one single body[17]. This provides for a comprehensive legal knowledge of both human rights and a limitation of possible dispute between two public authorities.18. A combined control authority does not imply that internally employees of FOI and PDP deal indistinctly with both issues; to the contrary, we acknowledge that FOI and PDP have different goals and recommend establishing two separate sub-entities, one in charge of FOI, the other one of PDP; only the commissioner or the board will be responsible for both domains, according to the following model.

16 Models developed by Pirc Musar, Nataša.: *How to strike the right balance between access to public information and personal data protection – using a public interest test*, PhD thesis, Vienna University, November 2015.

[17] Such systems can be found in Mexico, Switzerland, Serbia, Germany, Malta, the UK, Slovenia, Canada on a regional level, etc.

[18] Pirc Musar, Nataša.: *How to strike the right balance between access to public information and personal data protection – using a public interest test*, PhD thesis, Vienna University, November 2015.




Thus said, it should be mentioned that where good governance is a serious matter of concern - in particular, where the new paradigm of transparency of the state is to be resolutely enforced – it could be wise to create two separate control agencies. A "single task" agency is a more effective driving force than an agency simultaneously dealing with two different, sometimes opposite, domains. Should the model of two distinct control agencies be adopted, cooperation mechanisms should be established, following either the French model (exchange of representatives) or the Italian model (mandatory requests of advice). Thus, consistency in matters of common interests will be ensured. In the long run, when both access to information and privacy protection are institutional principles firmly settled and generally respected, a merger can be envisaged.

Finally, it should be underscored that, regardless of the organisation of the control authority (a combined authority or two separate authorities), three requisites are key for its success: independence, investigative powers and financial resources. As already mentioned above - having an overriding public interest test as a balancing legal tool defined in a local FOI law is significantly important to strike the right balance between FOI and PDP. The possibility for a public body to issue binding decisions is also an added value, since recommendation powers are less enforceable, and thus more time is needed to give transparency the value it deserves in modern democracies.

# 6 Authors' biographies

## 6.1 Nataša Pirc Musar

Nataša Pirc Musar was born in 1968 in Ljubljana. After graduating from the Faculty of Law of the University of Ljubljana in 1992, she passed the national bar examination in 1997. After completing her studies, she was employed for six years at the Slovenian national television station as a journalist and news presenter for the main news programme TV Dnevnik. Subsequently, she worked for five years as a news presenter on "24 ur", the primary information programme of the largest commercial television broadcaster in Slovenia, POP TV. Striving for new knowledge, in 2001 she moved to the financial sector, where she joined the largest Slovenian private financial corporation, Aktiva Group, as Head of Corporate Communications. In April 2003, she became the Director of the Training and Communications Centre of the Supreme Court of the Republic of Slovenia. On July 15, 2004, the National Assembly elected her the second Slovenian Commissioner for Access to Public Information. She was nominated for this position by the President of the Republic of Slovenia. Since 31 December 2005, when the Office of the Commissioner for Access to Public Information merged with the Inspectorate for Personal Data Protection, Nataša Pirc Musar has held the office of Information Commissioner until July 2014.

In October 2009, Nataša Pirc Musar was elected Vice President of the Europol Joint Supervisory Body, and in March 2013 President of the JSB Europol.

In 2013, she was a member of the Ad hoc EU USA group of experts with the mandate to discuss the "Snowden" affair with USA (chosen by Council of EU).
Nataša has her own law firm since January 1, 2015, she was also a president of Slovenian Red Cross and president of the Anti-Hate Speech Council for two years.

## 6.2 Bertil Cottier

Full professor (communication law) and former Dean of the Faculty of Communication Sciences at the University of Lugano. From 2006 also Associate Professor at the Law Faculty of the University of Lausanne (Internet Governance) and visiting Professor at the Academy of Journalism (University of Neuchâtel).

Studied law at the University of Lausanne and at the School of Law of Columbia University (New York).

Worked as court reporter for the newspaper "24 Heures" (Lausanne, 1977-1983), then as staff legal advisor for the media law and data protection units of the Federal Office of Justice (Bern, 1984-1987). From 1987 to 2005, deputy director of the Swiss Institute of Comparative Law. From 2004 to 2006, director of the advanced studies program on law, criminality and security of new technologies (Universities of Lausanne and Geneva).

Member of the board the Swiss National Science Foundation, co-editor of Medialex (Swiss journal of communications law), former president of the access to information commission of canton de Vaud and former member of the Data protection commission of the canton of Ticino. Member of the committee in charge of revising the Federal Act on Data Protection.

Expert on Media Law issues for the Council of Europe, the Organisation for Security and Cooperation in Europe (OSCE) and the Geneva Centre for Democratic Control of Armed Forces (DCAF).