Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

COMPARATIVE STUDY ON ARTICULATION OF THE RIGHTS OF ACCESS TO INFORMATION AND OF PERSONAL DATA PROTECTION

Bertil Cottier
Honorary professeur
Law school of the Lausanne University (Switzerland)

November 2021

This study was carried out with the support of the programme co-funded by the European Union and the Council of Europe under the PAII-T programme. The European Union and the Council of Europe are not responsible for the content of this study or for the use of the data contained therein.

COMPARATIVE STUDY ON ARTICULATION

OF THE RIGHTS OF ACCESS TO INFORMATION AND

OF PERSONAL DATA PROTECTION

Table des matières

1. Introduction

1.1. Terms of reference

This study was commissioned by the Council of Europe under the co-operation programme "Support to independent bodies in Tunisia".

Intended mainly for Tunisia authority for access to information (INAI) and data protection authority (INPDP), it provides a summary comparison of different legislative mechanisms for reconciling the right of access to information with the right to data protection.

1.2. Scope

There would have been no point in considering the reconciliation mechanisms established by the three hundred or so bodies of legislation on data protection and public access to official documents that exist across the globe.[1] This study will focus on the practice of foreign legislatures that already have some experience of these issues or have made use of original mechanisms. Where appropriate, it will also consider the two Council of Europe conventions in this field: Convention No. 205 on access to official documents[2] and Convention No. 108 on data protection,[3] since their provisions give effect to each other.

These mechanisms establish not only "rules of conflict", to determine how far data protection should restrict right of access, but also rules of procedural law. Consequently, this study will not confine itself to the various models of such rules (Section 3) but will also address practical issues such as a data subject's right to be heard (Section 4) and the interaction between the data protection authority and the freedom of information authority (Section 5).

It should be noted that the issue of the interrelationship between data protection and right of access hinges on whether or not it is possible to inspect documents containing personal data in order to scrutinise the work of public authorities. The use that an applicant subsequently makes

[1] This figure may seem high, but it takes into account the fact that in federal states it is up to the federal entities themselves (such as Canada's provinces, Australia's states and territories, Germany's *Länder* and Switzerland's cantons) to determine what happens to the information that they hold, with the result that each has adopted its own rules on data protection and access to official documents.

[2] Council of Europe Convention on Access to Official Documents of 18 June 2009 (CETS No. 205, also known as the Tromsø Convention).

[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108); this convention was extensively modernised by the protocol of 10 October 2018 (CETS No. 223).

of the personal data thus obtained is a question that falls outside the scope of legislation on right of access; however, it certainly comes within the ambit of data protection legislation.[4]

1.3. Technical remarks

Terminology: For the sake of clarity, the term *request*, if unqualified, will always mean a request for access based on legislation regarding public access to official documents, the term *applicant* the person making a request for access, and the term *requested authority* the public authority responsible for taking a decision on the request. Further, the term *data subject* refers to the person whose data come under data protection legislation, that is, a person who can be directly or indirectly identified.[5]

Quotations: The relevant provisions will be cited in English here. If the original is in another language, an English translation will be provided.

Hyperlinks: To avoid burdening this study with appendices containing the various pieces of legislation and official reports to which it refers, the reader will be able to consult them directly on screen by means of hyperlinks.

2. The problem

2.1. Two opposing institutions

The relationship between protection of personal data and the right of access to information held by public authorities has always been a source of conflict.

On the one hand, there is free flow of information and discussion of ideas, together with public oversight of government and its organs; needless to say, in these times of disinformation and manipulation of public opinion, it is more important than ever that people should have exact and complete knowledge of the authorities' work.[6]

On the other hand, we have the right to informational self-determination, meaning data subjects' right to determine themselves whether and for which purposes information about them can be

[4] And, where appropriate, of regulations governing proactive release by the government (open data, for example); these regulations include rules on reuse of public data.

[5] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), paragraph 17.

[6] "Media freedom, public trust and the people's right to know", Report by the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe, Doc. 15308, 7 June 2021, paragraph 3.

processed. Over and above this recently established value,[7] it is individual privacy more generally that is at stake. However, protection of privacy must not be used as official cover in order to conceal "compromising information, potential conflicts of interest, any secret understandings, unwelcome truths or even outright cases of corruption".[8]

2.2 A relative opposition

Nevertheless, the conflict between data protection and right of access should not disguise the fact that they have a common purpose: both seek to make government accountable for the information that it holds; it can no longer do whatever it wants with it, being subject to obligations regarding its collection, retention, use and disclosure. Consequently, the rules on data protection and those on access to information each contribute, in their own way, to defining the rules governing public information.

A number of jurisdictions, seeking to give substance to the rules governing public information, have combined the rules on right of access to information with those on data protection in a single statute, as in the Canadian province of Quebec, whose 1982 Act respecting access to documents held by public bodies and the protection of personal information blazed a trail. Taking this unitary approach to its logical conclusion, the Swiss canton of Valais has included rules on the archiving of official records in a topical law (cf. Public Information, Data Protection and Archiving Act 2008).

The fact remains that combining the two aspects in a single piece of legislation does not mean that they are amalgamated: in each case, data protection and freedom of information are covered by their own bodies of rules within separate subdivisions of the single law.[9] These subdivisions are separate because, except for their ambits and some shared concepts (such as personal data), the two fields are only partially congruent: "Right of access and public information relate not so much to personal data as to documents whose basic informational content is often

[7] Upheld for the first time by the German Constitutional Court as "*Recht auf informationelle Selbstbestimmung*" ("Census ruling", BVerfGE, Vol. 65 [1983], pp. 1 *ff.*), this principle has now been recognised by the European Court of Human Rights (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], Application No. 931/13, 27 June 2017, paragraph 137), by the case law of various European countries and by the Council of Europe's modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+) in its preamble.

[8] Flückiger A. (2020), "*La transparence des données personnelles au service de l'intégrité de l'administration*" ["Personal-data transparency to promote government integrity"], *Annuaire de l'Association suisse du droit public de l'organisation 2019-2020*, Bern, p. 79. In the same vein, Council of Europe (2018), *Guidelines on Safeguarding Privacy in the Media*, Strasbourg, p. 13: "Freedom of expression […] would receive a fatal blow if public figures could censor the press and public debate in the name of personality rights."

[9] With one notable exception: the Swiss canton of Zurich. Its 2007 Data Protection and Information Act combines in a single chapter the rules on a general right of access based on freedom of information and a data subject's specific right of access to his or her own data (see sections 20 *ff.*).

immaterial as far as data protection is concerned. Conversely, data protection does not consist solely in setting limits to the communication of such data to the public; it also covers various issues such as collection, internal use, disclosure to individuals or other authorities, destruction and data subjects' option of being able to check and rectify data if necessary."[10]

Consequently, whether data protection and freedom of information are governed by separate laws or by separate chapters in the same law makes little difference in the end: in both cases the legislature cannot dispense with rules for co-ordination.

2.3. Resolving the problem

While combining rules on data protection and rules on access to official documents in a single law cannot in itself prevent conflict, the same is not true of two other "answers": on the one hand, the data subject's consent, and on the other, anonymisation of the document requested.

2.3.1. Consent

All the pieces of legislation considered saw consent as the key to enabling the requested authority to accept a request for access (provided, of course, that there were no other reasons for confidentiality, such as national security or protection of business secrets). The validity of consent is usually determined by the general rules laid down in this field by data protection law. However, some states have established specific rules for access to official documents accepting implied consent when the latter can be inferred from the circumstances, for instance if the data subject has disseminated personal information on social media.

- Example: Section 19, subparagraphs 1(*b)* and (*c)* of Switzerland's Federal Act on Data Protection provide that: "Federal bodies may disclose personal data only if there is legal basis for doing so […] or if: […] b. the data subject has consented in the individual case; c. the data subject has made the data generally accessible and has not expressly prohibited disclosure."

2.3.2. Anonymisation

This operation consists in removing data that could identify the data subject either directly (name, taxpayer number, insurance number, etc.) or indirectly (physical characteristics or correlation of background information). This removal of identifiers is usually done by redaction or just by deletion. Once void of personal data, a document no longer comes under data protection legislation, and therefore there is no impediment to delivering it to the applicant.

---

[10] Vollery L. (2009), "*La loi fribourgeoise sur l'information et l'accès aux documents*" [Fribourg Information and Access to Records Act], *Revue fribourgeoise de jurisprudence*, p. 370, note 68. See also Human Dynamics, *Legal balance of interests between transparency of public life and data protection* (EU-funded project), p. 6: "An act that covers both areas comprehensively will need to be almost as detailed as two single acts because there is little overlap (except for the definitions and the oversight body)."

However, anonymisation raises two problems. Firstly, it is important for it to be identifiable, since applicants must be able to see that they do not have the whole of the document requested; if necessary, they may appeal against what must be regarded as partially denied access.

Secondly, anonymisation may prove unreasonable or disproportionate. This is the case if so much information is removed that the requested document becomes unintelligible or if the work needed to remove all the identifiers (especially indirect ones) is substantial. Moreover, as stated in the explanatory report to Convention 108+, the combination of different types of data could make it possible to identify an individual again, thus invalidating anonymisation.[11] This is also true in the far commoner case of an applicant wishing specifically to inspect documents relating to one or more named individuals. In all three cases, anonymisation can no longer be used; the requested authority then has no other choice but to consider the request in the light of the rules for reconciling data protection and right of access.

3. Rules of conflict for reconciling data protection with right of access

3.1. Compromise as the paradigm

The first countries that had to contend with the conflict between data protection and access to official documents resolved it categorically by giving precedence to one over the other. As a pioneer in transparency, Sweden immediately gave priority to the latter on the grounds that it was impossible to override an institution that had become established as a pillar of national democracy over two centuries.[12] Conversely, France, which has always sought to protect the personality of its citizens,[13] established the pre-eminence of data protection: section 1 of France's 1978 law on access to official documents excludes disclosure of personal data from its ambit.

Such unconditional solutions are no longer appropriate today. More or less satisfactory compromises have everywhere been found in order to square transparency with data protection.[14] A conciliatory approach is expressly advocated by the 2016 EU General Data

[11] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), paragraph 19.

[12] Sweden is well known for being the first country in the world to have enshrined transparency of government, in 1766 (see Chapter 2 of the Freedom of the Press Act); it is not so well known for also being the first country to have passed a data protection bill, in 1973.

[13] It should be noted that France was the first country to make publication of information infringing privacy an offence (1868 Freedom of the Press Act, section 11).

[14] Except in Sweden, where the legislature, against the advice of the national data protection authority, still gives precedence to transparency. Chapter 1, section 7 of Law 2018:218 implementing the GDPR provides that "[t]he EU General Data Protection Regulation and this Act shall not apply to the extent that they come into conflict with the Freedom of the Press Act or the Fundamental Law on Freedom of Expression".

Protection Regulation;[15] Article 86 states, "Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed […] in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation." However, although EU law enjoins member states to adopt rules of conflict, it allows them complete discretion as to the extent and form of the compromise advocated.

The same is true of the Council of Europe; the explanatory report to the Convention on Access to Official Documents (CETS No. 205) enjoins member states to find a compromise whilst being silent on its content: "Documents containing personal data are covered by the scope of this Convention. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108) does not in principle prohibit access of third parties to official documents containing personal data."[16] The convention on data protection, updated in 2018, "permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents".[17]

As for the only global international treaty dealing with right of access to official documents, the 1998 UNECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (also known as the Aarhus Convention) considers conflict but expressly refers to member states' national law to determine to what extent the personal data requested must remain confidential (Article 4.4(*f*)).

Because of the uncertainty that international law – both global and regional – allows to linger over how to settle the conflict between data protection and right of access, it will be readily understood that the paradigm of compromise takes different forms in different countries.

3.2. Compromise mechanisms

3.2.1. General approach and specific approach

Although there are many differences, they often stem from questions of detail. In fact, there are fewer compromise mechanisms than states attempting to resolve the conflict between right of access and data protection. All current mechanisms more or less come under one of two basic approaches:

- *The general approach* (also known as the set-rules method): the legislature specifies the types of personal data and/or types of document containing personal data to which

[15] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR").
[16] Council of Europe (2019), Access to Official Documents: The Council of Europe Convention and its explanatory report, Strasbourg, p. 25.
[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), preamble.

access is either automatically restricted (positive list) or else public (negative list); it should be noted that it is perfectly possible to have a combined positive and negative list.

- Example of a negative list: Section 26 of Norway Freedom of Information Act prohibits, amongst other things, access to entries submitted in connection with official competitions and to photographs of persons entered in official registers.

- Example of a positive list: Section 57 of Quebec's Freedom of Information Act provides as follows:

  "The following personal information is public information:

  (1) the name, title, duties, classification, salary, address and telephone number at work of a member, the board of directors or the management personnel of a public body and those of the deputy minister, the assistant deputy ministers and the management personnel of a government department;

  (2) the name, title, duties, address and telephone number at work and classification, including the salary scale attached to the classification, of a member of the personnel of a public body;

  (3) information concerning a person as a party to a service contract entered into with a public body, as well as the terms and conditions of the contract;

  (4) the name and address of a person granted an economic benefit by a public body by virtue of a discretionary power, and any information on the nature of that benefit;

  (5) the name and address of the establishment of the holder of a permit issued by a public body and which is required by law for the carrying on of an activity, the practice of a profession or the operation of a business."

- *The specific approach*: the legislature does not settle the conflict itself but requires the requested authority to take a decision on access to personal data by weighing the interests of transparency against the interests of personal-data protection[18] with regard to the circumstances of the specific case.

  - Example: Section 5 ("Protection of personal data") of Germany 2005 Freedom of Information Act provides that "[a]ccess to personal data may only be granted

[18] It should be noted that usually the rule of conflict does not apply specifically to data protection but refers to protection of privacy more generally; in this case, legal opinion and/or case law includes protection of personal data in the generic concept of privacy.

where the applicant's interest in obtaining the information outweighs the third party's interests warranting exclusion of access to the information […]".[19]

The courts have frequently provided clarification on how to balance interests by giving greater weight to certain personal circumstances.

- Thus, Swiss courts attach great importance to data subjects' role in society: the more elevated their duties or position, the readier they should be to have their personal data disclosed. The same applies to recipients of state support (or other advantages such as an agency contract). Conversely, a data subject's vulnerability, the extent of the invasion of privacy, or the sensitivity of the information requested will swing the balance in favour of non-disclosure.[20]

- The Slovenian information commissioner for his part considers public interest to weigh heavily if the information requested relates to an issue that has generated public debate, where an issue affects a wide range of individuals or companies, where the information is essential to understanding the whys and wherefores of a decision taken, or where the issue affects public health, public safety or public finances.[21]

Lastly, attention is drawn to the noteworthy initiative by the UK Ministry of Justice, which has produced guidance for domestic public authorities on the questions that a requested authority should necessarily consider when it undertakes a balance of interests. In short, it should be noted that, amongst other things, the authority must look carefully at how the personal information has been obtained (particularly the source and methods of collection), the likely expectations of the data subject and any adverse effects of disclosure on the data subject.[22]

3.2.2 Summary assessment of both approaches

The general approach has the merit of clarity and predictability: for each type of personal information, the legislature itself settles the outcome of the conflict between transparency and data protection. The requested authority will take a decision on access to a requested document in the light of the resulting classification. It has a limited margin of discretion; however, if the information requested does not fall into any of the determined categories – either because the

[19] Freedom of Information Act 2005.

[20] Typical of this nuanced approach was the fate of a request for access to a list of federal officials' external activities: the information for senior officials was disclosed to the applicant but that relating to junior officials was refused (Federal Administrative Court, A-6738/2014, judgment of 23 September 2015).

[21] Banisar D. (2011), *The Right to Information and Privacy: Balancing Rights and Managing Conflicts, Washington*, pp. 20/21.

[22] UK Ministry of Justice (2008), "Freedom of Information Guidance: Exemptions Guidance, Section 40 – Personal Information".

legislature has omitted it or because it is a type hitherto unknown – the requested authority will, in this particular instance, have considerable latitude for interpretation in order to fill the gap.

The specific approach has the advantage of flexibility: rooted in general provisions protecting broadly defined personal interests, it can accommodate the unforeseen; in addition, it is more subtle, since the weighing of interests entails consideration of all the individual features of a specific case. On the other hand, the method has the drawback of leaving a huge margin of discretion to the requested authority – a margin that it can exploit, in the guise of privacy protection, to conceal information that might embarrass it or call it into question; this is the sheltering effect inherent in data protection, a risk already mentioned above.[23]

3.2.3 Hybrid approaches

Wishing to optimise the benefits of each approach, most legislatures have refrained from coming down definitively on one side or the other and have preferred to combine both.

The usual model consists in a balance of interests, coupled with set rules in certain cases.

- Example: Section 5 of Germany Freedom of Information Act introduces the general principle of a balance of interests (see Section 3.2.1 above) but then unconditionally prohibits access to sensitive data (within the meaning of GDPR Article 9.1) without the data subject's consent.

Some legislatures have supplemented balance of interests not with set rules but with the presumption of openness (or, less often, confidentiality); in each case the presumption is rebuttable.

- Example: Article 6 of Switzerland Freedom of Information Ordinance assumes that there is an overriding interest in access in two cases: where the requested document relates to an event of importance to the general public (a political scandal or a corruption case in government, for example), and where the data subject "has a legal or factual relationship with an authority subject to the Freedom of Information Act which affords him significant benefits". The latter case applies specifically to individuals holding an official licence or concession as well as those recipients of financial assistance from public authorities.

Lastly, it should be noted that, when a request is considered, the weighing of interests is the final stage. If a request can be refused straight away for another reason (a set rule, an overriding public interest in confidentiality, or the incomplete or internal nature of the document requested), it is not necessary to carry out a balancing of interests, which is always a complicated and lengthy operation (especially if the data subject has to be consulted, see Section 4 below).

[23] See Section 2.1.

3.2.4 How the requested information is communicated

Some legislatures compel applicants to accept delivery of the requested data as a hard copy, thus prohibiting any direct access to electronic databases held by the authorities. The reason is to prevent any use of records that could jeopardise a data subject's privacy.

3.3. Legal sources of compromise

Rules for co-ordination are usually included in the body of law governing transparency and, less often, in the one governing data protection.

It is clear that the first option is better, since it helps to make law on right-of-access restrictions clearer and more consistent. However, to clarify the relationship between data protection and public access to official documents beyond doubt, legislatures have sometimes included a reference to a freedom of information act in a data protection act.

- Example: Section 12.2 of the Data Protection Act of the Swiss canton of Fribourg provides that "[d]isclosure of personal data to the public shall be […] governed by the legislation on freedom of information".

In rare cases, compromise is governed by rules derived from the provisions on both transparency and data protection. This is the case in Switzerland, where the co-ordination mechanism results from a combination of a general exception for privacy and an anonymisation rule in the Federal Freedom of Information Act (sections 7 and 9) with a rule in the Federal Data Protection Act governing disclosure of personal data by federal bodies (Section 19.1bis). Needless to say, such a convoluted system does not facilitate the task of the authorities enforcing it.

Whether it comes under the body of rules governing transparency or under that governing data protection, the co-ordinating mechanism can result from a combination of provisions from various levels of legislation. Whereas the rule of conflict establishing a balance of interests is often introduced in law, the procedures for implementing it (details of additional set rules, and presumptions of openness or confidentiality, for example) are contained in regulations: government decrees and ministerial circulars, or even non-legal provisions such as recommendations or instructions from bodies responsible for data protection or access to official documents.

- Example: France Freedom of Information Authority (*Commission française d'accès aux documents administratifs*, CADA) and Data Protection Authority (*Commission nationale informatique et libertés*, CNIL) published joint guidance in 2019 on data anonymisation.

Lastly, it should be noted that balance of interests has occasionally been introduced not by the legislature but by the courts seeking to attenuate the rigidity of an exception for infringement of privacy in the event of disclosure that has been worded unconditionally by the legislature.

- Example: Article 6.3 of the freedom of information decree of the Council of the French Community (Belgium) makes provision for an authority to refuse a request if disclosure of the document would constitute an invasion of privacy. This provision without nuance has been relativised by the courts: "Furthermore, an examination of decisions by the various freedom of information authorities and the Conseil d'État highlights the need to balance the applicant's interest in disclosure against the interest in protecting privacy" (ruling of 30 June 2020 by the Freedom of Information Authority of the Wallonia-Brussels Federation).

4. A data subject's right to be heard

4.1. The options

The question of which rights a data subject can or cannot exercise during consideration of an inspection request is one that legislatures have answered very differently from one country to the next. In one, data subjects are totally ignored. In another, they are entitled to give an opinion on whether or not their personal data should be disclosed, but they are not allowed to express their views concerning any overriding public or private (third-party) interests.

While some countries deny the data subject any right to express an opinion, this is to avoid lengthening the procedure. It is obvious that freedom of information requests must be processed promptly (to accommodate media requirements, amongst other things), and consulting the data subject takes time, even though most pieces of legislation granting data subjects the right to be consulted give them little time (two or three weeks at most) to express an opinion.

4.2. *Legal force of data subject's opinion*

The right to be consulted is one thing; the legal effect of such consultation is quite another. In most cases the data subject's opinion amounts to little more than an objection that is not legally binding and which the requested authority is free to accept or dismiss. Only few jurisdictions give the data subject a real right of veto (and even then, it is usually limited to disclosure of sensitive data).[24]

However, although not binding, a data subject's opinion is not without any effect. On the one hand, opposition to acceptance of the request will provide information (such as details of the circumstances behind the objection) that the authority ought to take into consideration when balancing interests; on the other, approval will, in legal terms, be treated as consent to disclosure of the requested data to the applicant.

[24] See Article 6 of Convention 108+, which gives a list of sensitive data.

4.3 Exceptions to the right to be heard

Last but not least, it should be emphasised that the right to be heard is not unconditional, being subject to some statutory and/or judicial exceptions. The main circumstances releasing the requested authority from any obligation to consult the data subject are as follows:

- a strong presumption that the data subject will consent to disclosure of the personal data requested;
- data concerning civil servants;
- a substantial number of people to be consulted;
- a clearly overriding public interest in transparency.

5. Interaction between the data protection authority and the freedom of information authority

Reconciling data protection with freedom of information also means defining the relations between the authorities responsible for each of these fields so that the expertise of one can benefit the other. More specifically, it is a matter of determining how far the data protection authority should be involved in the processing of a request by the freedom of information authority – given that the latter is usually the body responsible for taking decisions on requests relating to inspection of personal data. There are various models:

- *An institutional relationship*: A member of each authority also sits on the other (with or without the right to vote).
  - Examples: In Morocco, the National Supervisory Commission for the Protection of Personal Data (CNDP) and the Freedom of Information Commission (CDAI) are chaired by the same person (section 23 of Law 31-13 on freedom of information); in France, since the passing of the Digital Republic Bill (Law No. 2016-1321), the chair of the freedom of information authority (CADA) is automatically a full member of the data protection authority (CNIL) and vice versa.

- *A procedural relationship*: The requested authority must consult the data protection authority if the request relates to personal data.
  - Example: A mandatory consultation mechanism has been generally introduced in Italy. Without going into detail about its implementation, it should be noted that the data protection authority has ten days in which to give an opinion and that its opinion is not binding.

- *Sharing of regulatory powers*: Both authorities lay down joint recommendations and instructions for requested authorities on how to implement compromise mechanisms.

- Example: In addition to the joint guidance on data anonymisation mentioned above (3.3), the French freedom of information authority (CADA) and data protection authority (CNIL) published a practical guide to uploading and re-using open data in 2016 and a fact sheet on online publishing of local-government documents relating to the exercise of decision-making authority in 2021.

- *Sharing of facilities*: Whilst remaining independent of each other, the two authorities pool facilities and/or material resources.
  - Since 2018, France freedom of information authority (CADA) and data protection authority (CNIL) have been housed in the same building in Paris. This proximity encourages informal discussion.

Lastly, it should be pointed out that a number of countries (including Canada, Germany, Serbia, Slovenia, Switzerland and the United Kingdom) have merged their freedom of information authority with their data protection authority, a move explained by the fact that both fields come under the rules governing public information (see Section 2.2 above). A few years ago, the French government was intending to undertake a similar merger, but it eventually dropped the plan given the different powers of each body (CADA can only issue recommendations, whereas CNIL can order binding measures) and their divergent official cultures.[25]

Nevertheless, it can be pointed out that in countries that have not merged the two bodies, they co-operate closely: "It is therefore necessary that personal data protection supervisory bodies and FOI bodies, in states which have both types of supervisory bodies, work together and are co-ordinated."[26]

6. Tunisian law by comparison

Since the right to information and the right to data protection are given equal weight in Tunisia – both being established by institutional acts[27] – the legislature was unable to dispense with a mechanism to reconcile them. Without it, personal data would have escaped freedom of information on principle; section 47 of Law 2004/63 on protection of personal data specifically prohibits disclosure of personal data to third parties without the data subject's written consent.

Established by sections 24 to 27 of Law 2016/22 on the right to information, this much-needed reconciliation mechanism hinges on balancing the interests concerned. Thus, the first paragraph of section 24 expressly establishes data protection as an exception to freedom of information (in

[25] As for the pros and cons of a combined data-protection and freedom of information authority, see Musar N. and Cottier B. (2017), *Comparative study of different appeal and control mechanisms regarding access to public information in six Council of Europe member states*, Council of Europe, Strasbourg.

[26] Human Dynamics, *Legal balance of interests between transparency of public life and data protection* (EU-funded project), p. 8.

[27] The former by Law 2016/22 on the right to information and the latter by Law 2004/63 on protection of personal data. It should be noted that in Tunisia, as in the majority of countries that today enjoy both transparency and data protection, the latter predates the right to information.

addition to the general exception of privacy protection). However, this specific exception is relative; it can be overturned in the event of an overriding public interest in access (section 24, second paragraph). If however, the data subject's interest in confidentiality prevails, the personal information requested will not be disclosed. Nevertheless, the document containing it will still be accessible: it will be sent to the applicant but without the personal information that must remain confidential, which will first have been obliterated by redaction or removal (section 27).

This reconciliation mechanism, which is specific in nature, is supplemented by just a few additional set rules; section 26 lays down two for freedom of information (crimes against humanity, serious threats to health or the environment), and section 25 establishes one for confidentiality (identity of informers or whistle-blowers).

Lastly, it will be noted that the legislature has made efforts to encourage communication between the national freedom of information authority and the national data protection authority: the former must accept as a full member a senior representative of the latter (Law 2016/22, section 41). This interaction might be taken further: both bodies have signalled their intention of producing together an illustrative list of factors that could be expected to heavily weigh in the balance of interests.

7. Conclusion

At the end of this brief overview, it should be stressed that comparative law highlights three constants:

- while data protection is in no way per se a sufficient reason to reject an access request, it is nevertheless an element that will play a certain role, according to the circumstances;

- anonymisation is a measure that is widely advocated as a practical way of reconciling the interest in transparency with the interest in the protection of privacy; however, this measure reaches its limit when the applicant is specifically seeking information about a particular person;

- the legislator, the case law or even the access to information and data protection authorities (jointly or independently) have sought to define certain types of personal data which, in any case, must be considered as accessible (or at least presumed to be) or, but more rarely, strictly confidential. The first category often includes information on public figures (starting with managers and senior officials) and information on benefits granted by the administration to citizens (in particular grants, concessions, administrative contracts). The second category includes so-called sensitive data.