Strasbourg, 25 September 2012

CDL(2012)065*
Engl. only

Opinion 672/2012

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

DRAFT OPINION

ON ACT CXII OF 2011 ON INFORMATIONAL SELF-DETERMINATION AND FREEDOM OF INFORMATION

OF HUNGARY

On the basis of comments by

Ms Anne PETERS (Substitute member, Germany)
Mr Bertil COTTIER (Expert, Switzerland)

**This document has been classified restricted on the date of issue. Unless the Venice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe documents.*

TABLE OF CONTENTS

I. INTRODUCTION

1. On 1 February 2012, the Chair of the Monitoring Committee of the Parliamentary Assembly of the Council of Europe requested the Venice Commission to provide opinions on several recent Cardinal Acts adopted by the Hungarian Parliament, including the new Hungarian Act CXII of 2011 on Informational Self-determination and Freedom of Information, adopted in July 2011 (hereinafter referred to as the "Act").

2. The Venice Commission appointed Ms Anne Peters as rapporteur. This Opinion is based on the comments provided by Ms Peters as well as those provided by Mr Bertil Cottier, expert.

3. The present Opinion is based on an official English translation of the Act based on the text which, as indicated by the Hungarian authorities, has legal force as of 1 June 2012 and contains the amendments adopted between the date of adoption of the Act (26 July 2011) and the 1st of June 2012. The translation may not always accurately reflect the original version on all points and, consequently, certain comments can be due to problems of translation.

4. *The present Opinion was discussed at the Sub-Commission on Fundamental Rights (Venice, 13-14 October 2012) and adopted by the Commission at its … plenary session (Venice,).*

II. PRELIMINARY AND GENERAL REMARKS

5. This Opinion should be seen in the context of the Opinion on the new Constitution of Hungary, adopted by the Venice Commission at its 87th Plenary Session (Venice, 17-18 June 2011)[1].

6. On 18 April 2011 the Hungarian Parliament adopted a new Constitution of Hungary, which sets forth that

> *"Every person shall have the right to the protection of his or her personal data, and to access and disseminate data of public interest" (article VI(2)).*
>
> and that
>
> *"The exercise of the right to the protection of personal data and the access to data of public interest shall be supervised by an independent authority" (article VI(2)).*

7. Following its adoption in July 2011, the Act under consideration has attracted strong criticism, linked in particular to the abolition of the institution of the Commissioner on Data Protection and Freedom of Information ((hereinafter the "Commissioner") and its impact on the institutional independence of the supervisory mechanism of the enforcement of informational rights and freedoms.

8. The removal from office, before the expiry of his term, of the former Commissioner, has raised particular concern in the light of the independence principle that should govern, according to the applicable standards, the operation of the information and data protection regulatory bodies. The present Opinion will not address this specific issue, since the case is the subject of an EU infringement procedure under article 28.1 of the Directive 95/46[2].

---

[1] CDL-AD(2011)016, see also document CDL(2011)058, *Position of the Government of Hungary on the opinion on the new Constitution of Hungary*, adopted by the Venice Commission at its 87th Plenary Session (Venice, 17-18 June 2011) transmitted by the Minister for Foreign Affairs of the Republic of Hungary on 6 July 2011.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

III. EUROPEAN AND INTERNATIONAL STANDARDS

9. The opinion will analyse the Act with regard to the fundamental rights protected by the Hungarian Fundamental Law (hereinafter the "Constitution"), as well as by the European Convention on Human Rights (hereinafter, the "ECHR") in its articles 8 (which protects private life) and 10 (on freedom of expression)[3] and article 19 of the International Covenant on Civil and Political Rights (hereinafter, the "ICCPR"), to which Hungary is a party. The General Comment No. 34 of 21 July 2011 is also of relevance for the assessment of the Act.

10. More specific standards are enshrined in the following instruments:

- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[4] (hereinafter "the Convention 108")
- The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows[5] (hereinafter "the Additional Protocol")

11. Even though not yet in force - for lack of a sufficient number of States Parties - the Council of Europe Convention on Access to Official Documents[6], hereinafter "the Convention 205", will also be taken into account, especially since Hungary has already ratified it[7].

12. That said, both Convention 108 and Convention 205 only contain minimum standards. It is up to States Parties to provide more extensive rights and obligations[8].

IV. ISSUES UNDER REVIEW

A. The scope of the Act

13. The Hungarian Act CXII of 2011 regulates both the protection of personal data and the right of access to information. By integrating the two informational freedoms in one single legal act, the Hungarian legislator has chosen to maintain, as an underlying approach, the philosophy of the previous act, the Act LXIII of 1992 on the Protection of Personal Data and the Access of Data of Public Interest.

14. It should be stressed that, if the countries, such as Hungary, having entrusted to a single body the supervision of both data protection and transparency of public administration are few, those which address these two issues in one single legislative text are even fewer. While certain issues - such as the regimes of exceptions to the right to access to information and of those relating to the protection of data, in many respects identical - are undoubtedly common, the task remains a challenging one.

15. First, two different and even opposite aims are covered by the provisions of the same act: while data protection aims to ensure individual self-determination in relation to personal data, the right to information promotes public debate and citizens' control on public activities. Moreover, addressing informational rights in one single Act is difficult due to these rights'

---

[3] Freedom of expression includes, to some extent, the right of access to information (see the ECtHR, , Társaság a Szabadságjogokért v / Hungary, Judgment of 14 April 2010, § 35).

[4] Entered into force for Hungary on 1 February 1998. Hungary made no reservation to the text; on the contrary, it has expanded its scope to the data processed without the aid of electronic or automatic processing (note verbale dated 10 July 1997).

[5] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=1&CL=ENG
Entered into force for Hungary (without any reservation) on 1 September 2005.

[6] Adopted 18 June 2009 (CETS No. 205), not yet in force (needs 10 ratifications, currently 6 ratifications). Besides Hungary also Bosnia and Herzegovina, Lithuania, Montenegro, Norway, Sweden have ratified the Convention. Eight states have signed but not yet ratified: Belgium, Estonia, Finland, Georgia, Moldova, Serbia. Slovenia, Macedonia.

[7] Hungary ratified the Convention 205 on 5 January 2010 (without any reservation.)

[8] See in particular article 11 of the Convention 108.

different scope of application (data protection extends to the private sector, which is generally not the case for transparency) and basic concepts (data protection only applies to personal data, while transparency covers any information; moreover, the concept of sensitive data is totally foreign to transparency). This may in some cases give rise to interpretation and application problems and lead to a reduced level of protection of the rights at issue.

B. The National Authority for Data Protection and Freedom of Information

1. Standards

16. Pursuant to article 1 of the Additional Protocol, the Parties shall establish one or more authorities to ensure compliance with the principles laid down in Convention 108. As stated by paragraph 3 of Article 1, these authorities must exercise their functions "in complete independence". In doing so, the Protocol fills a gap in the Convention 108, which does not require Parties to explicitly create such a supervisory body.

17. The Additional Protocol does not define specific criteria for independence. Its Explanatory report underlines that "*[a] number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These could include the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority or the adoption of decisions without being subject to external orders or injunctions*". The present assessment of the independence of the Hungarian supervisory authority is based on these elements

18. Convention 205, on the other hand, does not oblige Parties to establish a supervisory body. It merely guarantees the existence of a remedy in the event of denied access to data. This may be regular (courts) or special (*ad hoc)* body established by the law and must be, in both cases, "independent and impartial" (art. 8). The Explanatory report to the Convention 205 provides no details about the content of these two notions.

19. The establishment of an independent regulatory body is also an obligation under the EU Data Protection Directive[9] (art. 28 .1).

20. The Court of Justice of the European Union has interpreted the notion of independence broadly. Supervisors "must enjoy the independence allowing them to perform their tasks without outside influence. This independence precludes not only *any influence exercised by the supervised bodies, but also any injunction or any other external influence, be it direct or indirect*[10], which could jeopardize the fulfilment, by those authorities, of their task of establish a proper balance between protecting the right to privacy and free movement of personal data"[11]

21. It should also be noted that the draft General Regulation on the protection of data submitted earlier this year by the European Commission[12] contains a special provision (article 47) devoted to the requirement of independence of national supervisory authorities. While refraining from defining organizational criteria (composition, appointment and dismissal of members), this provision establishes the functional aspects of independence: budgetary autonomy, availability of appropriate human, technical and financial resources[13]

[9] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[10] Italics added.

[11] Case C-518/07 Commission v Germany ECR I-1885, Judgment of 9 March 2010 (ad 30). See also conclusions of the Advocate General of 3 July 2012 (Case Commission v/ Austria C-614/10), in which he denounced the lack of independence of the Austrian data protection Commission as a result of the quality of federal civil servant of the administrator member of the commission, of its secretariat inclusion within the Federal Chancellery and of the Chancellor's right to be informed of the cases handled by the Commission.

[12] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.1.2012, COM(2012) 11 final.

[13] It is understood that no legal provision, no matter how well it is formulated, can guarantee, in practice, sufficient funding or sufficiently qualified personnel.

and the prohibition, on such authorities' members, to carry out ancillary paid or unpaid activities.

22. Since no model of supervision authorities has emerged in Europe, there is a great diversity in Europe in this area in terms of competences, composition and designation modalities' of such bodies.

23. As far as the competencies are concerned, while in countries such as Germany, United Kingdom, Slovenia, Switzerland and Hungary, supervision of the legislation on both data protection and access to information lies with the same authority, the majority of countries have set up specialized bodies. It may be indeed seen as surprising to entrust the same authority with the task of overseeing two laws whose spirit and objectives are diametrically opposed.

24. As regards the composition, there are either supervision committees (a collegial model), or "single person" supervisory authorities (directive model). It is commonly understood that the collegial model provides increased independence guarantees, since possible links with the State or with supervised stakeholders are diluted within the college.

25. The designation mechanism of supervisory bodies is an important and even decisive marker of independence. It is obvious that the designation made by the executive exclusively, which still prevails in some countries (including Estonia, Ireland, Latvia, Luxembourg, Netherlands and Sweden), offers fewer guarantees of independence than the designation by Parliament. Some countries have addressed this problem by subjecting the appointment by the Government to ratification by Parliament (eg Switzerland), which also adds to the concerned bodies' legitimacy.

2. The Hungarian Act

26. Under Act LXIII of 1992 previously in force, oversight was exercised by the independent Data Protection and Freedom of Information Commissioner, elected by Parliament for five years. In Hungarian administrative law, the Commissioner had the position of an ombudsman.

27. New Act CXII of 2011 replaced the Commissioner by the National Authority for Data Protection and Freedom of Information (hereinafter the Authority). It is a directive oversight body, headed by a President (assisted by a vice-President) appointed by the President of the Republic for a term of nine years, at the proposal of the Prime Minister (art. 40 (1) of the Act). The Authority's legal status as "autonomous state administration body" is enshrined in article 38.1 and detailed by articles 38-71 of the Act.

28. The transformation from an ombudsman into an administration authority has attracted criticism, as the oversight body becomes in principle more dependent on those it controls. The Government argued that the transformation was necessary as new information technology required more efficient action, and that an administrative body could work more efficiently than an ombudsman.

29. The Commission does not find that argument fully convincing. The efficiency of an authority depends on its competencies and above all on its human and financial resources. Whether an authority is equipped with sufficient resources in the end depends on the will of the deciding political actors. Nothing prevents them from endowing an ombudsman with the resources which are required to accomplish its tasks.

30. Following infringement proceedings launched by the European Commission in January 2012, Hungary amended the Act and the amendments have restored the independence of the Authority to a considerable extent. The current version of the Act includes particularly detailed provisions aiming at guaranteeing - directly and, in most cases, indirectly – the Authority's independence. It is worth saying that some of these guarantees may not always be found in corresponding legislation of other European countries.

31. A formal guarantee of independence is provided in article 38.5 of the Act:

> *"(5) The Authority shall be independent, subordinated only to law; it may not be given instructions as to the performance of its tasks, and shall perform its tasks separately from other bodies, free of any influence. Tasks for the Authority may only be established by law."*

32. In more concrete terms, the Venice Commission notes that, under art. 52 of the Act, the Authority is entrusted with extensive supervision and intervention powers: on the one hand it is provided with the investigative powers necessary to carry out its tasks (the right of access to contentious data, the right to conduct interrogations), and on the other hand it is entitled to initiate legal proceedings (pursuant to art. 1 al. 1 and 2 of the Additional Protocol).

33. Additional independence guarantees are linked to the function of president of the Authority. These include: its stability (art. 40. 3 which provides for a term of nine years, and art. 45, which defines clearly and exhaustively the grounds for dismissal by the appointing authority and allows the President to defend himself in court); its importance amongst other high level public functions (art. 40, setting up a salary equal to that of a minister); the President's impartiality (articles 40.2 and 40.1 setting out strict conditions and incompatibilities associated to the function)[14].

34. Article 39 guarantees the budgetary autonomy of the Authority (through a specific financial appropriation distinct from that of the public administration and specifically allocated by the Parliament without Government intervention), which is very rare at international level. By the same provision, the Authority is exempted from of annual budgeting principle, thereby enjoying a remarkable financial flexibility.

35. This being so, the Venice Commission wishes to point out also a number of remaining shortcomings and issues of concern.

36. First, due to the designation mechanism set out by the Act, which is the exclusive prerogative of the executive, the new Authority seems more dependent on those it is supposed to control than the old Ombudsman. More precisely, there is criticism that the Parliament is now entirely excluded from the procedure. That said, it should be recalled that Hungary is by far not the only country to favour the appointment by the executive alone. More generally, a comparison with other European countries shows a variety of ways to elect or appoint the head of a freedom of information oversight authority. In Switzerland, the commissioner is proposed by the Government and appointed by the Parliament; in Germany it is the Parliament at the proposal of the Government, while in the UK the commissioner is appointed by Her Majesty.

37. The legal options available to the President of the Republic to terminate the mandate of the President of the Authority before it expires also attracted criticism[15]. In its original version of 2011, the Act provided that the President of the Republic could "discharge" or "disqualify"[16] the President of the Authority in case the latter "fails to perform his duties arising from his assignment for over 90 days" (art. 45 (4) and (5) Act CXII, as of 11 July 2011, entered into force 1 January 2012).

---

[14] It is regrettable, however, that the prohibition only applies to ancillary activities remunerated; it would have been preferable to extend this prohibition to unpaid activities, which are equally likely to create unwanted links (cf. art. 47 of the proposed EU regulation on data protection mentioned above).

[15] See also *Opinion on Hungary's New Constitutional Order: Amicus Brief for the Venice Commission on the Transitional Provisions of the Fundamental Law and the Key Cardinal Laws* (Miklós Bánkuti,Tamás Dombos, Zoltán Fleck, Gábor Halmai, Krisztina Rozgonyi, Balázs Majtényi, László Majtényi, Eszter Polgári, Kim Lane Scheppele, Bernadette Somody, Renáta Uitz), p. 50.

[16] The difference between "discharge" and "disqualification" seems to lie in whether the failure to perform his duties is the fault of the President of the Authority or not.

38. Nevertheless, according to the current version of the Act, which was amended, as mentioned, in the context the European Commission infringement proceedings, the President of the Republic can only remove the President of the Authority under art. 45.1 (d) and (e) of the Act, if: the conditions necessary for appointment[17] are absent; if the President has violated the provisions on the declaration of assets (as laid down in art. 42), or if he is in a conflict of interest in the meaning of art. 41 of the Act. As a safeguard against arbitrary removal, the President of the Authority can now challenge a motion to remove him from office at the Budapest Labour Court (art. 45.6 (b) of the Act).

39. One will also note that art. 38.4 gives the Authority the right to submit proposals for amendments to the legislation on data protection and the right to information. It is not clear however whether the Authority may send its proposals to Parliament directly, which would be an additional guarantee of independence, or must go through the Government channel.

40. Further concern might be raised when it comes to the Authority's staff and their recruitment (regulated by Art. 50 and 51). The Venice Commission finds regrettable that the Act does not explicitly indicate - although this may be inferred from its status of autonomous authority within the meaning of art. 38 - whether the Authority's President, who exercises the "employer's rights over the civil servants and employees of the Authority" may freely recruit the Authority's staff.. It recommends that the Act be amended in order to make it clear that staff recruitment - without any outside interference - is part of the President's prerogatives.

C. The protection of personal data

41. Substantive rules for data protection are set out in articles 4 to 25 of the Act. Overall, the provisions of the Act dealing with data protection are in line with the Council of Europe standards, and in particular with the Convention 108:

- Although improvements can be made (see comments under Section D below), key concepts of personal data, sensitive data, processing and master file have been formulated in comparable terms (art. 2 and 6 of the Convention 108/ art. 3 of the Act);
- The principles of fairness, lawfulness, finality, proportionality and accuracy, which are supposed to govern all data processing have been correctly implemented (art. 5 Convention 108 / art. 4 of the Act);
- The obligation to secure the data has been fully implemented (art. 7 Convention 108/ art. 7 of the Act);
- The Act provides increased protection for sensitive data[18] (art. 6 Convention 108/ art. 5 al. 2 of the Act);
- The data subject enjoys legal remedies to stop unlawful processing of personal data (art. 10 Convention 108/ art. 22 of the Act). The Venice Commission however regrets (though the Convention 108 leaves full discretion to parties in this respect) that the Hungarian legislature has not assigned the supervisory body the power to directly resolve disputes; classical judicial means proved, in countries where these are available, an obstacle to a rapid and efficient implementation of the rights arising from legislation on data protection, as individuals are reluctant to engage in lengthy and inconclusive legal proceedings;
- Finally, the regime of transborder flows (i.e. the principle of "no data export" to countries without adequate protection and its exceptions) as enshrined in art. 7 of the Act is consistent with art. 12 of the Convention 108 and art. 2 of the Additional Protocol.

42. At first glance, the individuals' right of access to personal data concerning them, as provided in article 8 of the Convention 108, seems to be fully guaranteed. Under articles 14 to 17 of the Act, the data subject enjoys the right to freely obtain from the master file an extract from their personal data (as well as the right of rectification and erasure of inaccurate or

[17] See art. 40(1) and (2) of the Act

[18] It should be noted that the Convention 108 merely requires that appropriate safeguards be established, without specifying their nature.

irrelevant data). Furthermore, the regime of exceptions to these rights seems to be in line with the applicable standards (art. 9 Convention 108/ article 19 of the Act).

43. In the Commission's view, several aspects should nonetheless be reconsidered and improved.

44. First, knowing that the Convention 108, in its art. 8.b, guarantees access by data subjects to personal data "without excessive delay", the 30 days' deadline set out in art. 15.4 for meeting an access request is excessive. This is even more regrettable as, in terms of general right of access to data of public interest, the processing time of a request is only 15 days (art. 29 al. 1[19]);

45. Also, according to article 15.5 of the Act, access fees will be charged for a second request in the same year. Since the Convention 108 guarantees a right of access to "reasonable intervals"[20], the Commission considers that only those who unnecessarily multiply access requests should be penalized in this way.

46. The right to correct inaccurate data is granted by the Act in its article 17 to the extent that "the data controller has access to the authentic personal data". The purpose of this restriction, which is not provided for by the Convention 108, is not clear.

47. The Venice Commission further notes that, unlike most legislations governing data protection, the Act does not provide any exception for journalists and the sources they use in their investigation activities. In the absence of a general exception for the press (which is rare in international comparison), it would be wise, at least, to limit data subjects' access so that they will not be allowed to know the source of the information made public by the journalists[21]. The ECtHR has indeed stressed that "[*p]rotection of journalistic sources is one of the basic conditions for press freedom […]. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected*"[22]. The Commission finds it important that the Hungarian authorities consider amending the Act in the light of the above comments.

D. The access to data of public interest

1. Scope of the right

a. Standards

48. The Council of Europe Convention on Access to Official Documents (Convention 205)[23] obliges state parties to guarantee a right to access to official documents, as defined by its Art. 1 (2) (b):

> *"„official documents" means all information recorded in any form, drawn up or received and held by public authorities, recorded in any form" and relates to the official duties of the authority[24].*

[19] It is nonetheless true that, based on article 29.2, the 15 days deadline may be exceptionally extended once.
[20] "Any person shall be enabled […]: b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form" (article 8.b).
[21] The Convention 108 is silent on the issue; its explanatory report (§ 58) emphasizes, however, that the exception to right of access, in favor of "the protection of the rights and freedoms of others", laid down in art. 9, concerns in particular the requirements stemming from the freedom of the press. Directive 95/46 explicitly states the need for exceptions intended for journalistic (and artistic) activities, although it leaves Member States a wide margin of appreciation on the matter.
[22] See Goodwin v./ The United Kingdom, (Application no. 17488/90), Judgment of 26 mars 1996, § 39.
[23] Council of Europe Convention on Access to Official Documents, CETS 205, 18.VI.2009
[24] Council of Europe Convention on Access to Official Documents, Explanatory Report, § 13.

49. It is important to note that, as indicated by its Explanatory report, the Convention's scope includes documents containing personal data[25].

b. The Hungarian Act

50. In general, the Act CXII addresses the main issues pertaining to classical legislation on the right to access to information in a satisfactory manner. The matter is regulated by articles 26 to 37 of the Act (Chapter III, entitled "Access to Data of Public Interest", subtitle 21: "General Rules concerning Access to Data of Public Interest"), while the various categories of data are defined by its art. 3. The three relevant ones are: "personal data"; "data of public interest"; and "data public on grounds of public interest".

51. The Venice Commission particularly welcomes the inclusion, in its scope, of private stakeholders carrying out public duties, as well as the obligation to provide circumstantiated access to a document containing only some secret information and the establishment of a procedure for rapid access to data associated with effective remedies (see comments below).

52. Questionable aspects include, as a major shortcoming, the exclusion of personal data from the scope of the right to information,. According to the Act, transparency only covers "data of public interest" and "public data on ground of public interest". Neither of these two categories covers personal data (see art. 3. points (5) and (6), as well as art. 26. 3).

53. Consultation of personal data by third parties is, in fact, governed by the "data protection" section of the Act. Transparency is therefore very limited since, pursuant to art. 5 of the Act, such consultation is subject either to the consent of the person concerned or to a statutory obligation to provide information.

54. It is important to underline that exclusion of personal data from transparency constitutes a serious obstacle to the fight against corruption and patronage; in this way, documents relating to the benefits granted by the public administration to a third party (grants, authorizations, licenses, granting of public contracts) or staff (promotions) will escape public knowledge

55. In the view of the Venice Commission, this approach is contrary to Convention 205, which does not allow States Parties to protect the private sphere in an absolute manner, and consequently does not allow for a general exclusion of personal data from the right to access to information. Data protection and access to official documents are *a priori* equally legitimate interests, which implies that specific conflicts shall be dealt with by weighing these interests on a case by case basis. The scope of protection should therefore depend on the specific circumstances surrounding the request for access. The Explanatory Report emphasizes that "[the] protection of these interests may[26] prevail over the interest to disclose the information contained in the document"[27].

56. The Venice Commission recommends extending the scope of the right to include access to personal data, while at the same time including, in art. 27 (2) of the Act, the right to privacy and/or private interests as exceptions to the right to access to data of public interest.

57. Improvements and clarifications could also be made to the definitions given by Act to the key categories of data. "Personal data" is defined in a somewhat circular way as data relating to a data subject (art. 3 point (2) of the Act), while a "data subject" is a natural person identified or identifiable on the basis of personal data (art. 3 point (1) of the Act). Under the Act, data that falls under the definition of "personal data" is never data of public interest, since art. 3 point (5) defines "data of public interest" as "other than personal data".

[25] Explanatory Report, § 16.
[26] *May* and not *shall*, cf. Explanatory Report, § 28.
[27] It should however be underlined that there is a range of personal data that are subject to transparency, the data relating to the identity of public servants (cf. art. 26 al. 2).

58. The category of "data public on grounds of public interest" should also be reconsidered, as its scope and purpose are unclear. Article 3 of the Act defines "Data public on grounds of public interest" as a separate category. Nevertheless, according to the system established by Art. 26, "data public on grounds of public interests" may be seen as a sub-category of or equated to "data of public interest", "which is defined in art. 3 point (5) as : information or data, registered in any form, controlled by a body performing government responsibilities; concerning public activities or generated in the course of performing public tasks. It is difficult to understand the reason to create a special regime for these data, especially since the procedure is identical access (art. 28.1 in fine). The Venice Commission considers it important that the exact relationship between the two categories be made clear in art. 3 of the Act.

59. More generally, the Venice Commission notes that Act CXII regretfully uses different and less clear criteria to define the scope of the right to access to data of public interest than those established under the Convention 205. Even though the Act can be read and interpreted in the light of the Convention, it would be preferable to use the definitions '("public authorities" and especially "official documents") provided by the Convention, which reflect the scope of most European freedom of information laws.

2. Exceptions to the right to access to data

a. Standards

60. In the more recent case-law, Art. 10 ECHR has been interpreted more broadly, not only as a right to receive information which is already in the public realm, but also in the direction of a right of access to administrative data and documents.[28]

61. Art. 3 of the Convention 205 enumerates the admissible exceptions - subject to the usual requirements for limitations to fundamental rights under the ECHR[29] - in an exhaustive manner, and sets out concrete mechanisms for the proportionality test, which are typical for freedom of information laws: the harm test and the public interest override. The Explanatory report makes it clear that states have a large margin of appreciation as to how to implement these tests: for each individual case or, by the legislature, through the way in which the limitations are formulated. Legislation may for example set down varying requirements for carrying out harm tests, such as a presumption for or against the release of the requested document or an unconditional exemption for extremely sensitive information. When such requirements are set down in legislation, the public authority should verify, when they receive a request for access to such an official document, whether the requirements in the statutory exceptions are fulfilled. Absolute statutory exceptions should be kept to a minimum[30].

Art. 10 (2) ECHR does not impose stricter standards than the Convention 205.

b. The Hungarian Act

Legal basis

62. Act CXII allows for exemptions to access to information, which are regulated in art. 27, and whose regime varies according to the interest they protect.

63. Information classified under the law on the protection of classified information is excluded from the scope of the Act CXII (Art. 27.1). Similarly, as stated in Article 27.3, business secrets are protected by relevant provisions the Civil Code.

---

[28] See notably ECtHR, no. 37374/05, *Tarsasag v Hungary*, Judgment of 14 April 2009, § 35, 'towards the recognition of a right of access to information'.

[29] Exceptions must be "set down precisely in the law", be 'necessary in a democratic society, have the aim of protecting specific objectives enumerated in Art. 3 (1) of the Convention, and they must be "'proportionate to the aim of protecting" those objectives (Art. 3 (1) Convention 205).

[30] Explanatory Report to Convention 205, § 38.

64. Moreover, art. 27 (2) of the Act provides a list of public interests for the protection of which access to documents can "be restricted by law". It is unclear whether the list of grounds is exhaustive, since art. 27 does not use the word "only", e.g. "right to access may *only* be restricted ...." It is not clear either whether "*by law*" means that Act CXII is in itself the law which allows for restriction, or such restrictions require an additional law or may be introduced by other laws. Assuming that the list is exhaustive, it may be concluded that art. 27 satisfies the requirement of a legal basis. It is nevertheless recommended that the word "only" be added to the text.

Protected values

65. In the Commission's view, all grounds for restriction of access to information in Act CXII are covered by the grounds enumerated in art. 3.1 of the Convention 205. The Commission nonetheless finds that improvements could be made to some of the exemptions listed in article 27 and their specific regime.

66. First, the submission of highly sensitive documents to a general derogatory system defined by a special law is problematic. The Act should regulate the publicity of all official documents and all the more so that the secrecy clause protecting the interests of national defence and domestic security (art. 27. 2) is sufficient to ensure confidentiality. That said, one can imagine, following the example of other countries' laws, a special procedure for accessing highly sensitive information, which would, in particular, require the approval of the authority that created the document and not only that of the authority that holds it

67. Furthermore, it would be important to make sure that the exception concerning legal or administrative proceedings should be limited to the ongoing proceedings (art. 27.2.g).

68. Similarly, the intellectual property exception (art. 27.2.h) should be clarified in the sense that copyright impedes exploitation of the document requested, but shall in no case oppose his simple consultation.

69. More generally, the Commission notes that free access to information is allocated implicitly (cf. art. 29.3, which provides for the payment of a fee in case of costs) and would consider it wise to explicitly state, in the Act, the principle of free access to official documents (as in art. 7.1 of the Convention 205).

Proportionality and balancing of interests

70. Act CXII does not explicitly provide for a harm-test nor for a balancing of interests. Art. 27.2 uses the term "may" which indicates that the data-controlling body has discretion. As a general mater, discretion must be exercised under due consideration of the conflicting interests.

71. Additionally, Art. 30.5 prescribes how discretion of the controlling body must be exercised and allows for denial of access only when then public interests in non-disclosure "prevails."

72. A different, somewhat confusing, regime is established for the protection of internal deliberations (concerning data generated or registered in the course of decision-making). The internal deliberation exception provides both for a balancing of interests (art. 27;5 and for a harm test in Art. 27.6.). The Commission considers that, in order to fully meet the requirements of Convention 205, the Act should clarify the relation between art. 27.5 and art. 27.6, either by explicitly mentioning in art. 27 the need for a balancing of interests *or* for a harm-test, or by making a clear reference to art. 30.

Precision of the law

73. Convention 205 requires that "limitations shall be set down precisely in law". The Act lists the exceptions precisely. Nevertheless, the regime of protection of internal deliberations is confusing (see above). In addition, since the Act itself does not regulate the exemptions

comprehensively, applicants will have to consult other laws in order to find out whether specific information is exempted from disclosure.

74. To ensure conformity with the European and international legal standards set out above, the balancing of interest mentioned in art. 30.5 should be inserted in art. 27. Moreover, for clarity reasons, it is recommended that the regime of exceptions as a whole be regulated in the Act, including access to highly sensitive documents and to business secrets.

3. Complaint Procedure and Procedure on Declassification

a. Standards

75. Convention 205 sets two standards. First, applicants shall have access to a *review procedure* before a court or another independent or impartial authority established by the law (art. 8.1). The Explanatory Report states: "This review body must be able, either itself to overturn decisions (…) or to request the public authority in question to reconsider its position"[31]. Second, applicants shall have access to an *expeditious and inexpensive review or reconsideration procedure*, be it before court or another independent body, or within the administrative system (Convention 205, Art. 8.2).

76. Further standards are enshrined in Art. 13 ECHR and Art. 2 (3) ICCPR.

b. The Hungarian Act

Investigation by the Authority

77. Besides turning to court, an applicant may request the Authority to conduct an investigation. According to Article 52 (1), "*Anyone is entitled to request an investigation from the Authority, on the grounds of violation of rights relating to the control of personal data, access to data of public interest or data public on grounds of public interest, or in the event of immediate threat of the above*". It is important to note that the Act does not state that a person may only claim a violation of his own rights. According to art. 52.2, the investigation by the Authority is a *sui generis* proceeding, and not an administrative proceeding falling under the general rules. Moreover, turning to the Authority is neither a precondition nor an impediment for judicial review. Art. 31 (1) states that, "should" the applicant request an investigation by the Authority, litigation can be initiated within 30 days of the Authority's refusal to assess his request in substance. The proceedings before the Authority are free of charge (art. 52.4) and the deadline for dealing with a notice is (according to the English version of the law) two days.

78. Should the Authority find these rights violated or immediately threatened, it "shall call on" the data controller to remedy the violation or eliminate the immediate threat and/or make specific recommendations that would help effectively address the situation. In case the data controlling authority fails to comply with the Authority's request or recommendations, "further measures", can be taken by the latter, including initiating judicial review, in accordance with Article 64 of the Act. Specific recommendations may also be made to the legislator when the Authority establishes that "*the violation of rights or its immediate threat ensues from an unnecessary, ambiguous or inappropriate provision of legislation or regulatory instrument of public law, or the lack or deficient nature of the legal regulation of data control issues*" (see Articles 56 to 58) .

Judicial proceedings

79. Based on art. 31.1 of the Act, applicants may turn to the court in case the deadline to answer an access request has expired without result or in order to challenge the determination of fees for making a copy. The possibility to challenge a refusal to grant access to information is not mentioned, which seems to be a textual omission, since it follows from paragraphs (2) and

[31] Explanatory Report to Convention 205, § 64.

(3) of the same article. Taking into account that “refusal” is probably the most important ground for judicial complaints, the Commission recommends that the refusal to grant access be explicitly mentioned in paragraph 1.

80. In the Venice Commission’s view, the remedial mechanism provided by the Act is in line with both requirements stated by Convention 205 in its art. 8.1 and art. 8.2. For reasons of clarity, it might however be preferable to list all the options of an applicant to challenge a refusal to grant him or her access to information in one single provision of the Act. Also, increased clarity should be provided concerning the relationship between the two types of proceedings.

81. Further consideration is also required as to the procedure for the supervision of classified data, which clearly excludes the possibility for an applicant to request declassification. Art. 62 (3) of the Act expressly states that administrative procedures on declassification of classified information can only be initiated by the Authority, which seems not to be in conformity with the standard set by Article 8 of the Convention 205, which requires a review procedure for any type of access’ denial.

V. CONCLUSIONS

82. The Hungarian law on self-determination and freedom of information (Act CXII/2011, as of 1 June 2012) may be considered, as a whole, as complying with the applicable European and international standards.

83. Despite this overall positive assessment, several points would need consideration and improvements:

- The mode of designation of the President of the National Authority for Data Protection and Freedom of Information does not offer sufficient guarantees of independence, as the executive, which is the main stakeholder controlled, has the leading and exclusive role in the nomination process;

- Personal data are excluded from the scope of the general right to information;

- The right of data subjects to access their personal data does not allow for an exception to protect media sources;

- The scope and purpose of key concepts for the right to access to data of public interest and their inter-relations are insufficiently clear and may be source of difficulties in the interpretation and application of the Act.

- The provisions on the remedial mechanism should be clarified: the two options might be mentioned in one provision and the relationship between the two options should be made clear; also, in article 31.1 of the Act, “refusal” of access should be mentioned as a ground for review.

84. The Venice Commission invites the Hungarian authorities to revise the Act in the light of the recommendations contained in this Opinion. It remains at the disposal of the Hungarian authorities for any further assistance.