IN THE EUROPEAN COURT OF HUMAN RIGHTS **APP NO. 60646/14**
BETWEEN:-

PRIVACY INTERNATIONAL **Applicant**

- v -

THE UNITED KINGDOM **Respondent Government**

THIRD-PARTY INTERVENTION SUBMISSION BY ARTICLE 19, THE CAMPAIGN FOR FREEDOM OF INFORMATION AND THE ACCESS TO INFORMATION PROGRAMME

INTRODUCTION

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19), the Campaign for Freedom of Information (CFOI), and the Access to Information Programme (AIP) by the leave of the President of the Court granted on 28 April 2017 pursuant to Rule 44 §3 of the Rules of Court.

2. ARTICLE 19 is an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. The Campaign for Freedom of Information is a non-profit organisation working to improve public access to official information in the UK. The Access to Information Programme (AIP) is a Bulgarian NGO established in 1996 with the mission to promote and enhance the exercise of the constitutional right of access to information.

3. As recognised by the Grand Chamber in *Magyar Helsinki Bizottság v. Hungary*[1], domestic laws and international instruments have "evolved to the point that there exists a broad consensus, in Europe (and beyond) on the need to recognise an individual right of access to State-held information in order to assist the public in forming an opinion on matters of general interest". As set out below, this right of access to information applies to all public bodies, regardless of their function. Further, absolute exemptions for certain types of information are disproportionate.

I. ACCESS TO PUBLIC INFORMATION IS WITHIN THE SCOPE OF ARTICLE 10 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

4. The Court has consistently recognised that the public has a right to receive information of general interest. According to its established case-law, access to information held by public authorities falls under the ambit of Article 10 of the Convention. Information gathering as an essential preparatory step in journalism is considered an inherent, protected part of press freedom.[2] Consequently any denial is subject to the justification required under Article 10(2) of the Convention. This approach derives from the concept that: "In view of the interest protected by Article 10, the law cannot allow arbitrary restrictions which may become a form of indirect censorship should the authorities create obstacles to the gathering of information".[3] In such circumstances, "the censorial power of an information monopoly" represents an interference with "the exercise of the functions of a social watchdog, like the press." The case-law under Article 10 now recognises the right of access to government held information extends the latter to a larger group of players in public life. Alongside NGOs[4] the Court has recognised the right of a historian[5] and an

[1] *Magyar Helsinki Bizottság v. Hungary*, App no. 18030/11, § 31-63, 148
[2] *Dammann v. Switzerland, § 52.*
[3] *Társaság a Szabadságjogokért v. Hungary*, § 27.
[4] See *Társaság*, *Youth Initiative for Human Rights v. Serbia*, *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria* and *Magyar Helsinki Bizottság*.
[5] *Kenedi v. Hungary*.

activist[6] to access documents as guaranteed by that provision.

5. In numerous cases, the Court has found that access to a wide range of information, including an MP's petition to the Constitutional Court, documents of the former security services, permissions for transaction of land plots, statistics about phone communication intercepts, municipal funds to deal with stray dogs and names of pro-bono public lawyers and the number of their cases, constituted a matter of public interest.[7] The volume of documents sought is not a matter that is subject to scrutiny under Article 10 of the Convention. Either a single document or a whole set of documents may equally be considered to be information of importance to public discussion.[8] Thus, withholding all the respective public body's decisions issued within a certain period of time following a request for disclosure is in breach of Article 10 of the Convention if the information sought is "ready and available".

6. In the *Magyar Helsinki* case the Court clarified some of the above considerations. Whether given information is to be considered of public importance is subject to assessment of the circumstances of each case. In the Court's view, a need for disclosure may exist "where, inter alia, disclosure provides transparency on the manner of conduct of public affairs and on matters of interest for society as a whole and thereby allows participation in public governance by the public at large." Therefore information on any aspect of public affairs may be accessible information. What is relevant for the information to qualify as being of public interest is rather the extent to which the public is affected, especially but not limited to in cases that affect the well-being of citizens or the life of the community. Consequently, whether certain information is subject to the general right of access is not dependent on the sector of functioning or the specifics of the public body at stake.

1. Value of information related to secret surveillance

7. Under the case-law, information related to national security and intelligence is not excluded from the scope of information that may be of public interest. On the contrary, the *Youth Initiative for Human Rights* case involved information about the Serbian intelligence agency's operations in 2005 and namely – how many people had been subjected to electronic surveillance in that period.[9] In another case, involving matters under Article 8 of the Convention, *Association of European Integration and Ekimdzhiev v. Bulgaria*, the Court noted that the lack of regularly reporting to the general public on the matters of secret surveillance conducted (including surveillance performed by intelligence services) amounted to a deficiency in the system that should guarantee the fundamental right of privacy against misuse of intercepts.[10] The approach was further upheld by the Grand Chamber of the Court.[11]

8. Consequently, Article 10(2) of the Convention does not create an absolute exemption from access for any type of information which might be of legitimate public interest. In addition, information related to national security and intelligence matters has been regularly recognised as data of such public interest. Therefore, access to such data under the conditions and possible restrictions relating to sensitive information has already been considered important for the preparation of public watchdogs to participate in public discussions.

9. That approach of the Strasbourg authorities has been consistent also with the provisions of the Convention on Access to Official Documents. Neither the European Convention on Human Rights, nor the latter one provides for any grounds for exceptions that might exclude entirely certain bodies or categories of bodies. On the contrary, the definition of official documents under the Convention on Access to Official Documents[12] and the Court's considerations as to the nature of information of general interest[13] make clear that any such information should be made accessible by the bodies that hold it except in cases prescribed by law, where the restriction is proportionate to the protected interest and necessary in a democratic society.

---

[6] *Guseva v. Bulgaria.*
[7] *Kenedi v. Hungary*; *Österreichische Vereinigung; Youth Initiative for Human Rights v. Serbia; Guseva v. Bulgaria; Magyar Helsinki Bizottság v. Hungary;* See *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria.*
[8] *Österreichische Vereinigung § 44.*
[9] *Youth Initiative for Human Rights v. Serbia, § 6.*
[10] *Association of European Integration and Ekimdzhiev v. Bulgaria,* § 88.
[11] See *Roman Zakharov v. Russia*, § 283.
[12] Article 1, letter "b". Discussed below in section II.
[13] See *Magyar Helsinki Bizottság v. Hungary,* § 161-163.

2. Could an absolute exception be "necessary in a democratic society" within the meaning of Article 10, § 2 of the Convention?

10. The Court has constantly accepted in its practice that "freedom of expression constitutes one of the essential foundations of a democratic society; subject to Article 10(2), it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb."[14] The exceptions to that right must be narrowly interpreted and the necessity for any restrictions must be convincingly established.

11. These principles are of particular importance as far as public watchdogs are concerned. Whilst the bounds set, inter alia, in the "interests of national security" should be respected, it is nevertheless incumbent on watchdogs to impart information and ideas on matters of public interest. Not only do they have the essential role of imparting such information and ideas: the public also has a right to receive them. This is at the core of their vital role as "public watchdogs".

12. The Court has also established that "the adjective 'necessary', within the meaning of Article 10(2), implies the existence of a "pressing social need". The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with a European supervision, embracing both the law and the decisions applying it, even those given by independent courts. The Court is therefore empowered to give the final ruling on whether a "restriction" is reconcilable with freedom of expression as protected by Article 10.[15]

13. The Court's task to that end is not limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith, but to look at the interference complained of in the light of the case as a whole and determine whether it was "proportionate to the legitimate aim pursued" and whether the reasons adduced by the national authorities to justify it are "relevant and sufficient".

14. These principles are precisely established and found applicable when the question involves the applicability of the restriction for the sake of national security. In the *Spycatcher* case, the Court dealt with these principles establishing nearly 30 years ago whether the interference with the applicant's right with the aim to protect *inter alia* the interest of "national security" was justified.

15. Based on the cases above, it is not reasonable to accept an interpretation which finds that absolute exemptions are permissible in any form under Article 10(2) of the Convention, and allowing the discretion of States to exercise the margin of appreciation to the level of excluding an entire public body or sets of bodies from the obligations under the Convention, thus limiting their transparency and accountability to the public.

16. That approach is also endorsed by the Court's emphasis that "the object and purpose of the Convention, as an instrument for the protection of human rights, requires that its provisions must be interpreted and applied in a manner which renders its rights practical and effective, not theoretical and illusory."[16]

17. Therefore the exclusion of public bodies from the access regime is not consistent with Article 10 of the Convention.

II. INTERNATIONAL LAW APPLIES TO ALL BODIES AND DOES NOT ALLOW FOR ABSOLUTE EXEMPTIONS

1. International Human Rights Law

(a) Public Authorities under international law

18. The right to information, like all other recognised human rights, is universally held to apply to all public authorities. There is no generally recognised exemption for bodies which are conducting certain functions, such as the intelligence and security services.

19. As noted in the *Magyar Helsinki* case, the UN Human Rights Committee in General Comment 34 found that the right to information is a part of Article 19 of the International Covenant on Civil and Political Rights ("ICCPR"). In the General Comment, the Committee reaffirmed its previous opinions that the

[14] See *Handyside v . UK*, § 49, *Lingens v. Austria*, § 41.
[15] See *Observer and Guardian v. UK*, § 59.
[16] See *Magyar Helsinki Bizottság v. Hungary,* § 121.

obligations of the ICCPR apply to all parts of government, stating: "All branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local – are in a position to engage the responsibility of the State party."[17]

20. This broad application is also found in other related UN treaties. Under the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters ("Aarhus Convention"), there is a right of access to information held by any "Public Authority" under Article 2(2). In the UK, this right of access applies to security and intelligence services through the Environmental Information Regulations 2004.

21. The Global Principles on National Security and the Right to Information ("The Tshwane Principles"), which synthesize international law relating to national security and have been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and the COE Parliamentary Assembly define public authorities as including "all bodies within the executive, legislative, and judicial branches at all levels of government, constitutional and statutory authorities, including security sector authorities; and non-state bodies that are owned or controlled by government or that serve as agents of the government."[18]

(b) Application of right to information to information relating to national security

22. The right to information applies to all information held by public authorities, including that relating to national security. Any exemptions for national security or public order which limit the right must be clearly set out in law and must conform to the strict tests of necessity and proportionality.

23. In General Comment No. 34, the Human Rights Committee specifically sets out the legitimate grounds under which information can be withheld under Article 19(3) of the ICCPR including protection of national security or of public order.[19] It lays down specific conditions and it is only subject to these conditions that restrictions may be imposed (the traditional human rights "three part test"). The Committee specifically addressed restrictions on access to information and freedom of expression for national security reasons:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information.

24. In its periodic evaluations of states' compliance with the ICCPR, the Committee has examined national laws on protection of state secrets and reaffirmed that governments cannot withhold everything they deem sensitive.[20] The Committee has also expressed concern about the UK restrictions on access to information relating to national security.[21]

25. Other international agreements follow this model. Under Article 4(4)(b) of the UNECE Aarhus Convention, information can be withheld only if "the disclosure would adversely affect…. International relations, national defence or public security". However, it also states that "grounds for refusal shall be interpreted in a restrictive way, taking into account the public interest served by disclosure and taking into account whether the information requested relates to emissions into the environment." Further, Article 4(6) requires that non-exempt information is released when it "can be separated out without prejudice to the confidentiality of the information exempted."

---

[17] UN Human Rights Committee, General comment No. 34, Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, p.7, repeating its finding in General Comment No. 31 [80] on "The Nature of the General Legal Obligation Imposed on States Parties to the Covenant".

[18] The Global Principles on National Security and the Right to Information (The Tshwane Principles), 2013. https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

[19] See General Comment 34, pp 21-36.

[20] Concluding Observations of the Human Rights Committee: Uzbekistan. 26/04/2001. CCPR/CO/71/UZB

[21] Concluding Observations of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland. CCPR/CO/73/UK,CCPR/CO/73/UKOT, 5 November 2001; Concluding observations of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/6, 30 July 2008.

26. The UN Special Rapporteur on Freedom of Opinion and Expression, in cooperation with the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, issued a special declaration on freedom of information in 2004, stating that secrecy cannot override disclosure of information in the public interest.[22]

27. UN bodies have also regularly found that certain types of information cannot be withheld such as information on human rights violations,[23] the use of the death penalty[24] and environmental hazards.[25]

28. The Tshwane Principles definitions state that: "A national security interest is not legitimate if its real purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party, or ideology; or suppression of lawful protests."

2. Council of Europe Standards on Right to Information

29. As described in the *Magyar Helsinki* case, the Council of Europe has adopted a number of standards on the right to information. These standards set out which public authorities and other bodies are subject to access rules as well as the permissible limits on access to information. All of the standards apply to all public bodies and require narrow and non-absolute exemptions.

(a) Application of the right to all public authorities

30. COE standards take a comprehensive approach to the application of the right to information to all public authorities. This is a long standing approach of the Committee of Ministers and the Parliamentary Assembly, and has been incorporated into the treaty agreements.

31. The Committee of Ministers has long held that access to information should apply to all public authorities. In Recommendation No. R (81) 19 on access to information held by public authorities, the Committee stated that the right of access should apply to all "public authorities other than legislative bodies and judicial authorities". In Recommendation Rec(2002)2 of the Committee of Ministers to the Member States on Access to Official Documents, the Committee of Ministers defined public authorities as "government and administration at national, regional or local level".

32. The Convention on Access to Official Documents (CETS 205- "Tromsø Convention"), which currently has 9 of the 10 ratifications needed to go into force follows the Committee of Ministers in defining public authorities as all "government and administration at national, regional and local level" (Article 1(2)(a)).

33. The Parliamentary Assembly in Resolution 1954 (2013) on National security and access to information stated "As a general rule, all information held by public authorities should be freely accessible; in addition, business enterprises, including private military and security companies, have the responsibility to disclose information in respect of situations, activities or conduct that may reasonably be expected to have an impact on the enjoyment of human rights." (9.1)

(b) Legitimate restrictions on national security information

[22] International Mechanisms for Promoting Freedom of Expression, Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2004.
[23] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/68/362, 4 September 2013, pp 37, 106.
[24] Communication No. 1470/2006, CCPR/C/101/D/1470/200628 March 2011.
[25] Report of the Special Rapporteur of the Sub-Commission on Prevention of Discrimination and Protection of Minorities, E/CN.4/Sub.2/1994/9, 6 July 1994; Also see Report of the Special Rapporteur on the implications for human rights of the environmentally sound management and disposal of hazardous substances and wastes, Başkut Tuncak, A/HRC/30/40, 8 July 2015.

34. In Recommendation Rec(2002)2, the Committee of Ministers stated that access to official documents relating to national security, defence and international relations can be denied only "if the disclosure of the information contained in the official document would or would be likely to harm any of the interests mentioned in paragraph 1, unless there is an overriding public interest in disclosure."

35. In Resolution 1954 (2013), the Parliamentary Assembly stated that "access to information forms a crucial component of national security, by enabling democratic participation, sound policy formulation and public scrutiny of State action" (p. 3). The Resolution "stresses the need to place reasonable limits upon the use of national security to justify restrictions to access to information" (p. 5).

36. Article 3(1)(a) of the Tromsø Convention provides that states may limit the right of access to official documents for reasons of "national security, defence and international relations", while 3(1)(b) allows for limits relating to public safety. However, these limits are not absolute and require both harm and public interest tests. Article 3(1) requires that all limitations "shall be set down precisely in law, be necessary in a democratic society and be proportionate". Further, Article 3(2) allows states not to disclose information if it "would or would be likely to harm any of the interests" but they must also consider any "overriding public interest in disclosure" before withholding the information.

3. Other Regional Human Rights Bodies

37. Other major regional and international bodies have also recognised the right to information as a key aspect of freedom of expression. Under these approaches, the right clearly applies to all public authorities. Further, the exemptions relating to national security are not absolute, and are subject to harm and public interest tests.

38. The Organization of American States' Model Inter-American Law on Access to Public Information defines public authorities as "including the executive, legislative and judicial branches at all levels of government, constitutional and statutory authorities, non-state bodies which are owned or controlled by government, and private organizations which operate with substantial public funds or benefits (directly or indirectly) or which perform public functions and services insofar as it applies to those funds or to the public services or functions they undertake."[26]

39. The Inter-American Court of Human Rights in the case of *Gomes Lund* ruled that limits on access to information "must be necessary in a democratic society and oriented to satisfy an imperative public interest." Further, the court stated that public authorities cannot use exemptions relating to state secrets or confidentiality to withhold information relating to human rights violations.[27] Under the Model Law, information can only be withheld for national security or other purposes when "it is legitimate and strictly necessary in a democratic society" and it would "create a clear, probable and specific risk of substantial harm' (Article 41(b)). The exemption does not apply if the information relates to serious violations of human rights or crimes against humanity (Article 45) or when the information is over 12 years old unless it is approved by an independent information commission. The exemption can also be overridden when there is a public interest stronger than the harm (Article 44).

40. A similar system has also been adopted by the African Union. The Declaration of Principles on Freedom of Expression in Africa states that "everyone has the right to access information held by public bodies" without any exemptions. The African Commission on Human and Peoples' Rights' Model Law on Access to Information for Africa further defines public bodies as "any body (a) established by or under the Constitution; (b) established by statute; or (c) which forms part of any level or branch of government." Under the Model Law, information, including intelligence-related information can only be withheld for national security or defence purposes, if its release would "cause substantial prejudice to the security or defence of the state" (Article 30). Information cannot be withheld simply because it has been classified (Article 26) and is subject to a public interest test which requires disclosure unless "the harm to the interest protected under the relevant exemption that would result from the release of the information demonstrably outweighs the public interest in the release of the information (Article 25).

[26] Commentary and Guide for Implementation for the Model Inter-American Law on Access to Information [AG/RES. 2514 (XXXIX-O/09]

[27] Case of Gomes Lund et al. ("Guerrilha Do Araguaia") v. Brazil, Judgment of November 24, 2010.

III. NATIONAL PRACTICES ON THE RIGHT TO INFORMATION DO NOT ALLOW FOR ABSOLUTE EXEMPTIONS

41. The right of information is now widely recognised globally as a fundamental human right. As of the writing of this brief, 117 countries have adopted comprehensive national laws or regulations which set out a right of access to information held by public bodies.[28] The recognition of the right is even more widespread in Europe. Almost all Council of Europe member states recognise the right of individuals to access state held information. Forty-four of the forty-seven member states have enacted freedom of information ('FOI') legislation. Draft laws are currently being considered by the parliaments of two of the remaining three, Cyprus and Luxembourg. Over thirty member states also have provisions in their constitutions guaranteeing a right to information.

42. A total of forty-one of the forty-seven member states have ratified the Aarhus Convention. EU member states are required to also implement the Directive on public access to environmental information.[29] The right of access under both the Convention and Directive applies to environmental information held by security and intelligence agencies.

43. The scope of many countries' laws is not limited to public authorities but extends to private bodies that have public functions, provide public services or receive public funds. For example, the Slovenian law applies to information held by "state bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors"[30] as well as private entities subject to the "dominant influence" of the public sector.[31]

1. Exclusion of security bodies from laws

44. In most national FOI laws, the definition of public authority encompasses security and intelligence agencies whose information may have to be disclosed, subject to appropriate exemptions.

45. The United Kingdom[32] and Malta[33] appear to be the only two member states that completely exclude intelligence and security agencies from the scope of their FOI laws, though even in these countries the Aarhus Convention and EU Directive require compliance with the right to environmental information.

46. Some countries exclude certain functions of the security and intelligence agencies but do not exclude them from the legislation altogether. Ireland's Garda Síochána is subject to its FOI law although only in relation to "administrative records relating to human resources, or finance or procurement matters".[34] The Czech law excludes information about the "the performance of duty of the intelligence service".[35] The Croatian FOI law does not apply to "information subject to confidentiality obligations, pursuant to the act governing the security and intelligence system".[36] The Turkish law provides that "information and documents regarding the duties and activities of the civil and military intelligence units, are out of the scope of this law", although "information and documents, that affect the professional honour and working life of the persons, are within the scope of right to information."[37]

47. The German law excludes the intelligence services and other Federal Government bodies,[38] but only in relation to their duties of carrying out extended security checks and investigations into persons who are to

[28] See Banisar, David, National Right to Information Laws, Regulations and Initiatives. Available at SSRN: https://ssrn.com/abstract=1857498
[29] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC.
[30] Access to Public Information Act 2003, Article 1(1).
[31] APIA, Article 1.a
[32] According to section 84 of the Freedom of Information Act 2000 "government department" does not include the Security Service, the Secret Intelligence Service, the Government Communications Headquarters or National Crime Agency.
[33] Freedom of Information Act 2009, Article 5(4)(f).
[34] Freedom of Information Act 2014, Part 1(n) of Schedule 1. Under Section 42(b) of the Act records held or created by the Garda Síochána that relate to a number of areas including the Emergency Response Unit, the Special Detective Unit, the Security and Intelligence Section and the Criminal Assets Bureau are exempt.
[35] Law on Free Access to Information 1999, Section 11(3)(c).
[36] Law on the Right of Access to Information 2013, Article 1(4).
[37] Law on the Right to Information 2003, Article 18.
[38] Federal Act Governing Access to Information held by the Federal Government 2005, Section 3(8).

be employed by the intelligence service.[39] Other information about the work of these services can be withheld where it is classified or where disclosure may be harmful.

48. The Netherlands FOI law excludes information processed by or on behalf of the intelligence services, but a public right of access is provided in the Act dealing with the intelligence and security services itself.[40] The Annual Report of the General Intelligence and Security Service provides statistics on how many requests to inspect information were dealt with and granted, as well as the results of appeals against refusals to allow inspection.[41]

49. These are the exceptions. In the majority of member states, security bodies are covered by the FOI law, subject to specific exemptions for classified information or for disclosures likely to harm national security.

2. Exemptions for Classified information

50. Around half of member states' FOI laws exempt classified information. In some cases this is the sole exemption used to protect national security. In other cases a further exemption may apply where disclosure of unclassified information is likely to cause harm. The definition of classified information in these countries generally operates by reference to the likely harm from disclosure. For example, the Polish FOI law states that the right to information is subject to "the protection of other secrets being statutorily protected."[42] According to the Polish Protection of Classified Information Act of 2010 "Information is classified at a level based on the harm that unlawful disclosure would cause: "top secret" involves an "exceptionally grave harm" to the state's legal interests, "secret" involves "grave harm", "confidential" involves "harm" and "restricted" a deleterious effect on the body's ability to perform its duties."[43]

51. In some countries the FOI regulator or courts have the power to order declassification. In Romania, classification "shall apply as long as unauthorized disclosure or dissemination of that information may damage the national security and defense, public order or the interests of public or private legal persons" and over-assessment of the level or period of classification may be contested in the courts.[44] Under the Hungarian law, if the National Authority for Data Protection and Freedom of Information finds the law on the protection of classified information has been infringed, it can instruct the classifier to modify the level or term of classification or have it declassified.[45] In Slovenia, "If the applicant holds, that information is denoted classified in violation of the Act governing classified data, he can request the withdrawal of the classification".[46] If the body refuses the request, the applicant can appeal to the Information Commissioner, who can determine whether the information has been properly classified and whether the public interest in disclosure prevails. In Bulgaria, the administrative courts can rule over the lawfulness of the classification under the Access to Public Information Act.[47]

52. In some countries information about matters such as human rights violations, violations of the law and corruption may not be classified at all. For example, in the Slovak Republic information cannot be classified if it concerns "(a) an unlawful or incorrect procedure or unlawful decision of public agents and public authorities, (b) criminal activity of public agents, (c) uneconomic, inefficient and ineffective handling of public funds, (d) serious jeopardy or damage to the environment, life and health, (e) salary particulars, material provision and material advantages of public agents."[48] Similar provisions are found in the state

[39] The duties under section 10(3) of the Security Clearance Check Act relate to the carrying out of extended security checks and investigations for persons who are to work for a federal intelligence service or other authority belonging to the Federal Government which carries out duties of comparable security-related sensitivity.
[40] Information and Security Services Act 2002, Chapter 4.
[41] General Intelligence and Security Service Ministry of Interior and Kingdom Relations, Annual Report 2016 (Table 5 and 6) https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2017/04/04/annual-report-2016/AIVD+Annual+Report+2016.pdf
[42] Law on Access to Public Information 2001, Article 5(1).
[43] 'Polish Law on Right to Information and Classification' (2011), Adam Bodnar and Irmina Pacho.
[44] Government Decision no. 585/2002 – The National Standards on the Protection of Classified Information in Romania, Article 17.
[45] Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, Section 63.
[46] APIA, Article 6(4). The public interest test for classified information does not apply to information is denoted with one of the two highest levels of secrecy or is based on classified information of another country or international organisation.
[47] Access to Public Information Act (2000), Article 41, para 4
[48] Act of 11 March 2004 on the Protection of classified information and on the amendment and supplementing of certain acts, Article 4(1).

secrets laws of Azerbaijan, Croatia[49], Georgia[50], Latvia[51], Moldova[52], Romania[53], Russia[54] and Ukraine[55].

3. Exemptions referring to harm to national security interests

53. Some countries' FOI laws do not exempt classified information as such but only permit information to be withheld where disclosure would be harmful. For example, administrative documents can be withheld under the French law if disclosure would undermine the confidential nature of national defence, foreign policy, security of the state, public security or the safety of persons.[56] The Netherlands law states that disclosure shall not take place "insofar as it…might damage the security of the State."[57] The Norwegian Act provides an exemption for documents "when this is required by national security interests or the defence of the country."[58] Under the Portuguese Act "Documents which contain information, knowledge of which is deemed capable of endangering or damaging the internal and external security of the State, shall be subject to prohibited access or access with authorisation, for such time as is strictly necessary, by means of their classification as such in accordance with specific legislation."[59] And in Sweden "The right of access to official documents may be restricted only if restriction is necessary with regard to…the security of the Realm or its relations with another state or an international organisation".[60]

54. In Ireland, records can be withheld if disclosure "could reasonably be expected to affect adversely" the security of the state.[61] However, this test does not apply to information "obtained or prepared for the purpose of intelligence" or which "relates to the detection, prevention or suppression of activities calculated or tending to undermine the public order or the authority of the State".[62]

55. In several countries, a more demanding test of harm applies. Under the Albanian law the right to information may only be restricted "if giving the information causes a clear and serious harm to…national security, as defined in the legislation for classified information"[63] but "The right to information is not automatically refused when the information sought is found in documents classified as 'state secret'. In this case, the public authority, receiving the information request, starts immediately the classification review procedure".[64] In Bosnia, the test is whether "disclosure would reasonably be expected to cause substantial harm"[65], in Montenegro "would significantly endanger"[66], and in Serbia "seriously threaten".[67]

4. Disclosure in the public interest

56. In a number of countries even where disclosure may be harmful to national security, information may nevertheless be disclosed on public interest grounds. Under the Ukrainian law information can be withheld in the interests of national security if disclosure could "cause significant harm" and "the harm from publication of the information outweighs the public interest in obtaining the information".[68] However, the public interest test does not apply to the exemption for state secrets.[69] The Estonian law excludes

[49] Data Secrecy Act 2007, Article 3.
[50] Law on State Secrets 1996, Article 8.
[51] Law on Official Secrets 1996, Section 5.
[52] Law No. 245 of 2008 on State Secrets, Article 8.
[53] Law on Free Access to Information of Public Interest 2001, Article 13.
[54] Law of the Russian Federation No 5485-1 of July 21, 1993 on State Secrets, Article 7.
[55] Law on State Secrets 1994, Article 8(4).
[56] Law on Access to Administrative Documents, Article 6(2). The reply from France to an EU Council questionnaire on public access to documents and/or information in Member States (14194/12) explained: "The requirement to protect State security, public security and personal safety may in some cases impede the release of information bodies involved in maintaining public order. In assessing the degree of risk, CADA decides on a case-by-case basis, taking account of the specific circumstances and local context." 15196/12 ADD 1, 19-10-2012.
[57] Open Government Act 1991, Section 10(1)(b).
[58] Freedom of Information Act 2006, Section 21.
[59] Law on Access and Reuse of Administrative Documents 2007, Article 6(1).
[60] Freedom of the Press Act, Chapter 2, Article 2(1).
[61] FOIA, Section 33(1).
[62] FOIA, Section 33(3).
[63] Law on the Right to Information 2014, Article 17(2)(a).
[64] LORTI, Article 17(5).
[65] Freedom of Access to Information Act, Article 6(a).
[66] Law on Free Access to Information 2005, Article 9(1).
[67] Law on Free Access to Information of Public Importance 2009, Article 9(3).
[68] Law on Access to Public Information, Article 6(2).
[69] LAPI, Article 8.

information classified as a state secret. Other information may be withheld if is "intended for internal use" but the there is a limited public interest test for information relating to an offence or accident.[70]

57. In the UK information that is held by a body *other than* the intelligence and security agencies themselves and has not been supplied by or relates to those bodies can be withheld where necessary to safeguard national security.[71] This exemption is subject to a public interest test, though minsters are able to protect their decisions on both the exemption and the public interest from challenges.[72]

58. In some countries, such as Albania, Bosnia, Macedonia, Moldova, Montenegro and Serbia, the public interest test also applies to classified information. The Bosnian law requires information covered by any exemption to be disclosed "where to do so is justified in the public interest having regard to both any benefit and harm that may accrue from doing so."[73] The public interest test in the Slovenian law applies to classified information, except that which is denoted with one of the two highest levels of secrecy or is based on classified information supplied by another country or international organisation.[74] In Croatia, the public interest test applies to classified information with the prior consent of the Office of the National Security Council.[75]

IV. CONCLUSION

59. The right of access to information held by public bodies is a fundamental human right under decisions of the Court, and is also recognised by the United Nations, other prominent international human rights bodies and all but three COE member states.

60. It is broadly accepted that the right applies to all public authorities, regardless of their function. Any absolute exclusion of any state body from the access regime is inconsistent with the Convention as interpreted in the light of the Court's established case-law.

61. Further, any limitation on the right must meet the standard tests of being prescribed by law, and being proportionate and necessary.

62. Domestic practice throughout the Council of Member states shows that the UK and Malta are the only two states that allow for all information from their security and intelligence services or relating to them to be absolutely exempt from access to information laws.

David Banisar
Senior Legal Counsel
ARTICLE 19

Maurice Frankel
Director
Campaign for Freedom of Information

Alexander Kashumov, attorney-at-law
Head of Legal Team
Access to Information Programme

19 May 2017

[70] Public Information Act 2000, Section 38(1).
[71] FOIA, Section 24.
[72] FOIA, Section 24(3) and Section 53(2).
[73] FAIA, Article 9(1). Article 9(2) adds that "In determining whether disclosure is justified in the public interest, a competent authority shall have regard to considerations such as but not limited to, any failure to comply with a legal obligation, the existence of any offence, miscarriage of justice, abuse of authority or neglect in the performance of an official duty, unauthorized use of public funds, or danger to the health or safety of an individual, the public or the environment."
[74] APIA, Article 6(2).
[75] LRAI, Article 16(1). Classified information "originating or exchanged within the framework of cooperation with international organisations or other countries" is excluded from the Act.