ANA KNEŽEVIĆ BOJOVIĆ
MARIO RELJANOVIĆ

FREE ACCESS TO INFORMATION

MONOGRAPH 181

An analysis of the regulatory frameworks in selected Western Balkan countries

INSTITUTE OF COMPARATIVE LAW

Belgrade 2022

INSTITUTE OF COMPARATIVE LAW
MONOGRAPH 181

FREE ACCESS TO INFORMATION

An analysis of the regulatory frameworks in selected Western Balkan countries

Ana Knežević Bojović, PhD

Mario Reljanović, PhD

Belgrade, 2022

INSTITUTE OF COMPARATIVE LAW

FREE ACCESS TO INFORMATION

An analysis of the regulatory frameworks in selected Western Balkan countries

Publisher
Institute of Comparative Law in Belgrade, Serbia

For the Publisher
Prof. Dr. Vladimir Čolović

Series: Public Sector Integrity in the Western Balkans
Series editor: dr Ana Knežević Bojović

Reviewers
Prof. Dr. Ágoston Mohay, Associate Professor,
University of Pécs Faculty of Law, Hungary
Prof. Dr. Lucia Mokrá, Faculty of Social and Economic Sciences,
Comenius University in Bratislava, Slovakia
Prof. Dr. Jelena Ćeranić Perišić, Institute of Comparative Law in Belgrade, Serbia

Proofreading
Svetlana Imperl

Prepress
Dogma, Belgrade

Print
Tri O d.o.o., Aranđelovac

Printed in 150 copies

ISBN-978-86-80186-81-8

doi:10.46793/80186818.FAI

TABLE OF CONTENTS

LIST OF ABBREVIATIONS	
BiH	Bosnia and Herzegovina
CIDS	Centre for Integrity in the Defence Sector of Norway
CC	Criminal Code of Serbia
CLB	Criminal Law of the BiH
CLFBiH	Criminal Law of the FBiH
CLRS	Criminal Law of the Republic of Srpska
CoE	Council of Europe
CPC	Criminal Procedure Code of Serbia
CPLB	Criminal Procedure Law of BiH
ECtHR	European Court of Human Rights
EU	European Union
FBiH	Federation of Bosnia and Herzegovina
FOI	Freedom of Information
LCSB	Law on Civil Service in the Institutions of Bosnia and Herzegovina
LFAIB	Law on Freedom of Access to Information of Bosnia and Herzegovina
LHROB	Law on the Human Rights Ombudsmen of Bosnia and Herzegovina
LPB	Law on Police Officers of Bosnia and Herzegovina
LPCIB	Law on Protection of Classified Information of Bosnia and Herzegovina
LSAFB	Law on Service in the Armed Forces of Bosnia and Herzegovina
RFAIRS	Law on freedom of access to information of the Republic of Srpska
RFAISFBH	Law on freedom of access to information of Federation of Bosnia and Herzegovina
RTI	Right to information
UN	United Nations

1. RIGHT TO INFORMATION – INTRODUCTORY REMARKS

Integrity is a notion contrary to the notion of corruption. Integrity is the approach to the key values – behaving in accordance with certain key values and being consistent in their use. One of such key values that helps prevent corruption is transparency.[1] Without transparency, there is no true democracy – a form of government that should serve and be used by all citizens. Transparency is now a central tenet of democratic societies and, it is hoped, a vehicle for increased citizen oversight of government.[2] This is why freedom of Information has been described as "oxygen to democracy."[3]

Freedom of Information (FOI), or the right to information (RTI)[4], can be defined as the **right to access information held by public bodies**.[5] It reflects the fundamental premise that all information held by governments and governmental institutions is in principle public, and may only be withheld, if there are legitimate reasons for not disclosing it, such as, typically, privacy and security.

The principle of democracy is repeatedly invoked in scholarly writings and case-law as the "pillar" of freedom of information.[6] It is also pointed out that transparency and openness partake a double nature: they are both a norm and an instrument;[7] as a norm, transparency and openness are part of the value systems of liberal democracy and of human rights, envisaging the right of citizens to know what is going on in the public sector and for a duty of government to be transparent and open. As an instrument, it strives toward higher efficiency and effectiveness, by forcing governments to be more attentive so as to stand public scrutiny.[8]

[1] A. Knežević Bojović, R. Radević, "Free Access to Public Information, Integrity and Good Governance in the Western Balkans", in: *Integrity and Good Governance in the Western Balkans* (eds. A. Rabrenović, A. Knežević Bojović), Regional School of Public Administration, Danilovgrad 2018, 195.

[2] B. Worthy, P. John, M. Vannoni, "Transparency at the Parish Pump: A Field Experiment to Measure the Effectiveness of Freedom of Information Requests in England", *Journal of Public Administration Research And Theory*, 2016.

[3] *The Public's Right to Know: Principles on Freedom of Information Legislation*, London, June 1999.

[4] The terms will be used interchangeably throughout the study.

[5] *About Freedom of Information (FOI),* http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/about/, 24.2.2022.

[6] H-J. Blanke, R. Perlingeiro, *Essentials of the Right of Access to Public Information: An Introduction*, Springer International Publishing 2018, 17.

[7] C. D. Dacian, P. Kovac, A.T. Marseille, *From the Editors: The Story of a Data-Driven Comparative Legal Research Project on FOIA Implementation in Europe*, Springer International Publishing, 2019, 3.

[8] However, some authors warn that the positive impact of transparency on accountability is often more theoretical than empirical – a useful overview is provided in N. Zúñiga, M. Jenkins, D. Jackson, *Does More Transparency Improve Accountability?*, Transparency International, 2018. http://www.jstor.org/stable/resrep20498 (24.2.2022.), who also posit that the potential of transparency to lead to more accountability depends in great manner on contextual considerations, including political will. Similarly, Žuffová shows that FOI laws and open government data alone are insufficient to curb corruption: instead, they need to be coupled with democratic traditions, independent judicial institutions and media

Blanton[9] posits that most FOI laws in the world came about because of competition for political power between parliaments and administrations, ruling and opposition parties, and present and prior regimes. While this observation may be particularly true for the first freedom of information law ever passed – the Swedish 1766 Freedom of the Press and the Right of Access to Public Records Act and the US Freedom of Information Act, adopted in 1966 in the United States of America,[10] the expansion of FOI legislation worldwide was not caused solely by this type of political competition. Scholarly literature[11] attributes the development of FOI legislation and practice to three complementary causes:

- the end of the vast majority of military dictatorships and the breakdown of the former Eastern Bloc, resulting in a process of democratisation and increased citizens' interest in a critical confrontation with their recent history, coupled with the wish to supervise the political actors who used to withhold information from the public;
- a broad interpretation of the classical right to information and the codification of a special right to access to information at international level;
- socio-economic change together with restructuring of the economy in favour of the tertiary sector and the digital revolution.

Freedom of information is also recognised as a basic human right within the wider political rights framework.[12] As Mendel notes,[13] numerous international bodies with responsibility for promoting and protecting human rights have authoritatively recognised the fundamental human right to access information held by public bodies, as well as the need for effective legislation to secure respect for that right in practice. Further, as more countries engaged in freedom of information regulatory initiatives, incorporating it in their national constitutions and/or national legislation,[14] the conceptualization of freedom of information legal framework has expanded beyond human rights and citizen participation into the concept of accountability.[15] Recently, Calland

freedom. M. Žuffová, "Do FOI laws and open government data deliver as anti-corruption policies? Evidence from a cross-country study", *Government Information Quarterly*, Volume 37, Issue 3, 2020, 101480, https://doi.org/10.1016/j.giq.2020.10148.

[9] L. Blanton, "The World's Right to Know", *Foreign Policy*, No. 131 (Jul. - Aug 2002), 50-58.

[10] As pointed out by Banisar (D. Banisar, *Freedom of Information Around the World 2006: A Global Survey of Access to Government Records Laws*, Privacy International, London 2006, available at: https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/intl/global_foi_survey_2006.pdf, 24.2.2022.), President of the United States Lyndon Johnson stated on that occasion: "I signed this measure with a deep sense of pride that the United States is an open society in which the people's right to know is cherished and guarded."

[11] H-J. Blanke, 8.

[12] T. Mendel, "Freedom of information: An internationally protected human right", *Comparative Media Law Journal*, 1/2003, available at http://allianceforlife.org/wp-content/uploads/2013/09/Freedom-of-Information.pdf, (24.2.2022.); D. Banisar (2006).

[13] T. Mendel, *Freedom of Information: A comparative legal survey*, UNESOC, Paris, http://portal.unesco.org/ci/en/files26159/12054862803freedom_information_en.pdf/freedom_information_en.pdf., 24.2.2022.

[14] See: M. Gomez, "The Right to Information and Transformative Development Outcomes", *Law and Development Review 2019*; 12(3): 837–864, 838. According to Global RTI rating, as of 2021, a total of 132 countries have enacted freedom of information laws. https://www.rti-rating.org/, 24.2.2022.

[15] L. Camaj, "From 'window dressing' to 'door openers'? Freedom of Information legislation, public demand, and state compliance in South East Europe", *Government Information Quarterly*, Volume 33, Issue 2, 2016, 346-357, https://doi.org/10.1016/j.giq.2016.03.001.

and Bentley[16] have shown that freedom of information legislation improves democratic practice by facilitating social and institutional change, leading to better informed and more participatory citizenry and resulting in increased governmental transparency, accountability, and improved quality of decision-making. However, recent research shows that many countries face substantial challenges in ensuring compliance with FOI legislation, particularly within the early years of its implementation; implementation on local level is also a challenge.[17]

While current mainstream democratic political culture can be safely said to proclaim openness and transparency as values, states continue to reserve their prerogatives to classify information as secrets.[18] Even though state secrets are meant to protect the national security, or the defence, these are very vague notions, and there is a clear need to strike a sound balance between the right to information, on the one hand, and the preservation of confidentiality of information related to national security and defence.[19] This aspect of the FOI legislation is complemented by the principle that FOI legislation and practice should systematically tackle the culture of official secrecy.[20] But how do states respond to this challenge, in legislative terms? How do they implement the said principles established on international level?

This study examines the compliance of regulatory frameworks governing FOI with relevant international standards in four former SFRY countries. The study covers Bosnia and Herzegovina and its two entities – the Federation of Bosnia and Herzegovina and the Republic of Srpska (the legislative frameworks of the entities are examined in order to get a fuller grasp of the state of play in the complex regulatory context of Bosnia and Herzegovina), Montenegro, North Macedonia and Serbia. It builds on the previous research on cross-cutting integrity issues in the selected Western Balkan and CEE countries conducted by the Institute of Comparative Law in 2013[21] and a subsequent study aimed at guiding and facilitating the training of civil servants in ReSPA (Regional School of Public Administration) member states, also conducted by the Institute of Comparative Law in 2018.[22] Further, the present study was informed by the analysis carried out by the Institute of Comparative Law at the request of the Centre for Integrity in the Defence Sector from Norway.[23]

The countries were selected due to their shared legal and societal history, as all of them were former SFRY republics, and due to their common European integration

[16] R. Calland, K. Bentley, "The Impact and Effectiveness of Transparency and Accountability Initiatives: Freedom of Information Development", *Policy Review* 31/2013, s69–s87. doi:10.1111/dpr.12020.
[17] G. Michener, S. Nichter, "Local compliance with national transparency legislation", *Government Information Quarterly*, Volume 39, Issue 1/2022, 101659, https://doi.org/10.1016/j.giq.2021.101659.
[18] F. Cardona, *Freedom of speech, right to know and reporting unlawfulness: the lifeblood of preventing abuse of power and corruption in the defence sector*, CIDS, 2020.
[19] *Ibid.*
[20] Article 19, *The Public's Right to Know: Principles on Right to Information Legislation*, 2016.
[21] *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector* (ed. Aleksandra Rabrenović), Institute of Comparative Law, Belgrade, 2013.
[22] *Integrity and Good Governance in the Western Balkans* (eds. A. Rabrenović, A. Knežević Bojović), Regional School of Public Administration, Danilovgrad, 2018.
[23] https://portal.cids.no/.

context.[24] All of their regulatory frameworks are affected by external conditionality,[25] where some cross-fertilization also occurs among them in the transposition of EU acquis and implementation of international standards. This is because former SFRY countries, precisely due to their common legal history, tend to examine the regulatory solutions of their neighbours when implementing reforms in order to identify best practices, but also potential pitfalls in regulation and implementation.[26]

The countries included in the study are at different stages of EU accession process, with Montenegro and Serbia as frontrunners, North Macedonia having recently acquired the status of a candidate and Bosnia and Herzegovina only having applied for candidacy.[27] This difference, in theory, could set them apart in terms of level of compliance of their respective legislations with international standards also in the domain of FOI, as it is an important element of both democracy and the rule of law. The study will, to an extent, test this hypothesis. While the main focus of the research is on the legal frameworks, some references to implementation practices and interpretative approaches of relevant public administration bodies and courts are cited sparingly and contextually. This is done in order to shed additional light on a particularly relevant issue or to illustrate the disparity between the compliance with international standards

[24] Camaj bases the selection of countries included in her analysis on similar grounds. CIDS opts for the countries where it actively pursuits its activities, thus including Albania but excluding Serbia (the study on Albanian legislative framework was carried out by an Albanian expert Zhani Shapo).

[25] External conditionality in this context is viewed through the EU bargaining model known as External Incentive Model (EIM). In the said model, the European Union sets the adoption of its norms and rules as conditions that the target states (prospective candidates for the membership) have to fulfil in order to receive a reward. EU conditions comprise both political conditions (such as democracy and the rule of law) and regulatory conditions (pertaining to the EU's public policies). The model accordingly distinguishes between democratic conditionality and acquis conditionality. There is an ample body of scholarly research on EU conditionality, where the following are relevant reference materials: F. Schimmelfennig, U. Sedelmeier, "The Europeanization of Eastern Europe: the external incentives model revisited", *Journal of European Public Policy*, 27(6)/2020, 814-833; H. Grabbe, *The EU's Transformative Power Europeanization Through Conditionality in Central and Eastern Europe*, Palgrave Macmillan UK, Basingstoke 2006; J. G. Kelley, *Ethnic Politics in Europe: The Power of Norms and Incentives*, Princeton University Press, Princeton 2004; G. Pridham, *Designing democracy: EU enlargement and regime change in post-communist Europe*, Palgrave Macmillan UK, Basingstoke 2005; F. Schimmelfennig, S. Engert, H. Knobel, *International socialization in Europe: European organizations, political conditionality and democratic change*, Palgrave Macmillan UK, Basingstoke 2006; F. Schimmelfennig, U. Sedelmeier, "Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe", *Journal of European public policy*, 11(4)/2004, 661-679; F. Schimmelfennig, U. Sedelmeier (eds.), *The Europeanization of Central and Eastern Europe*, Cornell University Press, Ithaca 2005; M. A. Vachudova, *Europe undivided: democracy, leverage, and integration after communism*, Oxford University Press, Oxford 2005; A. Zhelyazkova, I. Damjanovski, Z. Nechev, F. Schimmelfennig, "European Union conditionality in the Western Balkans: external incentives and Europeanisation", in J. Džankić, S. Keil, M. Kmezić (eds), *The Europeanisation of the Western Balkans*, Palgrave Macmillan, 2019, 15-37. Some reflections on the regulatory responses of Serbia with regards to EU conditionality can be found in: A. Knežević Bojović, V. Ćorić, A. Višekruna, "Spoljašnje uslovljavanje Evropske unije i regulatorni odgovori Srbije", *Srpska politička misao* 3/2019, 233-253, https://doi.org/10.22182/spm.6532019.10. An insightfull take on the instruments utilised in the new EU accession methodology can be found in: J. Ćeranić Perišić, "Bliža integracija zemalja Zapadnog Balkana sa Evropskom Unijom na osnovu nove metodologije proširenja EU", *Srpska politička misao* 3/2020, https://doi.org/10.22182/spm.6932020.7, 153-157; J. Ćeranić Perišić, "Izazovi evropskih integracija zemalja Zapadnog Balkana dve decenije nakon početka procesa", *Primena prava i pravna sigurnost : zbornik radova 34. susreta Kopaoničke škole prirodnog prava - Slobodan Perović*, 2021, Tom 3, 399-412.

[26] These practices do not seem to be thoroughly investigated in legal literature in the region; the claim rather relies on first-hand author's experience of engagement on various preparatory and analytical tasks for the purpose of policy or legislative reforms in several countries included in the analysis. The authors have participated in the said efforts either as a part of a wider group of Institute of Comparative Law researchers so tasked by a government body, or as individuals engaged in working groups or technical support project activities.

[27] 2021 Communication on EU Enlargement Policy, Strasbourg, 19.10.2021 COM (2021) 644 final.

in law *de lege lata* and its practical implementation, which does seem to be a feature in the Western Balkan countries.[28] The study further seeks to explore specific rules from the FOI domain that apply to police officers and military personnel, who operate in the sectors where the balancing of conflicting interests of transparency and secrecy are most readily visible. The research, however, does not address the rules governing secrecy through a standalone analysis – instead, it addresses them in the context of possible limitations to free access to information, and only to the extent necessary to highlight their complex relations. Similarly, the study does not address the legislation governing personal data protection.

The examination of the freedom of information, or right to information legislation, is particularly relevant for the countries included in the study, given their shared legal background of limited theoretic and practical recognition of the FOI principles, coupled with the culture of secrecy. It has been pointed out in scholarly literature[29] that in former SFRY, the right to information was perceived for the most part as the right to be informed[30] and that it was granted primarily to journalists and media outlets, which were at the time organised as publicly- or socially-owned bodies. While the principle of administrative transparency was recognised in the SFRY constitution and upheld in the laws governing associated labour,[31] there existed a parallel complex system of regulations defining the term "secret", [32] which were mutually inconsistent and where grounds for classification were used lightly.[33] Some authors further indicate that SFRY, in fact, nurtured the culture of secrecy, in which some issues were not to be discussed, and that the majority simply kept quiet and accepted the division of the allowed and prohibited issues tacitly.[34] Intensive legislative activity with regard to FOI in the countries created in the territory of the former SFRY ensued only in the first decade of the 21st century, mainly as part of wider legislative activities related to the accession to the European Union i.e. the alignment of their legislation with Union acquis. The European trend of the detailed legal regulation of free access to information of public importance emerged at that very time. The four countries covered by the study incorporated the emerging international standard in their legislation relatively quickly. The first one to do so was Bosnia and Herzegovina – in 2000.[35] Serbia adopted its first FOI

[28] DiFi, for instance, measures a considerable 56% of cases where there is some compliance between normative standards and national administrative practices, and an additional 20% with demonstrated inadequate compliance. DiFI, *Defence against corruption - The risk of corruption in the defence sector in 9 countries in Southeast Europe*, 2015, https://cids.no/wp-content/uploads/pdf/difi/difi_memo_2015-1_defence_against_corruption._the_risk_of_corruption_in_the_defence_sector_in_9_countries_in_southeast_europe.pdf, 24.2.2022.

[29] A. Knežević Bojović, "Free Access to Information of Public Importance", in: A. Rabrenović (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade, 2013, 131-152.

[30] V. Čok, *Javno informisanje, javnost rada i dostupnost informacija - pravna teorija i zakonodavstvo*, Savremena administracija, Belgrade 1982, 80.

[31] A. Knežević Bojović, 2013.

[32] J. Popović, "Legislative Regulation of Data Confidentiality in the Countries on the Territory of the Former Socialist Federal Republic of Yugoslavia", *Atlanti*, Vol. 20, Trieste 2010, 229-238.

[33] R. Šabić, "Otvorena pitanja primene zakona o slobodnom pristupu informacijama od javnog značaja u periodu nakon usvajanja zakona o tajnosti podataka", in: "Pristup informacijama od javnog značaja i zaštita tajnih podataka", OEBS and Center for Advanced Legal Studies, Belgrade 2012, 26.

[34] J. Kregar, V. Gotovac, Đ. Gardašević, *Regulacija prava na pristup informacijama*, Transparency International Hrvatska, 2004, 4.

[35] Law on free access to information of Bosnia and Herzegovina – LFAIB (Zakon o slobodi pristupa informacijama u Bosni i Hercegovini, *Službeni glasnik BiH*, no. 28/00).

statute in 2004,[36] Montenegro in 2005,[37] while North Macedonia was the last to do so, in 2006.[38] In addition to the statute, all the countries adopted the relevant bylaws – the regulations that stipulate the fees for access to information, and rules of procedure/ statutes of the oversight bodies for free access to information of public importance. The statutes of all four analysed countries were amended several times, for several reasons: sometimes interventions were introduced in order to respond to the advancement of supranational standards in this field, sometimes to address the legislative ambiguities that have created problems in the implementation of the FOI law, and sometimes to manage the balance between the rules governing the freedom of information and secrecy rules, but unfortunately, not necessarily in order to further transparency and facilitate access to what the governments perceived as potentially sensitive information. It is therefore particularly interesting to examine the current state of play in this field, while the conclusion will also provide an opportunity to reflect on the changes compared to the situation in 2013.

[36] Law on free access to information of public importance – LFAIS (Zakon o slobodnom pristupu informacijama od javnog značaja, *Službeni glasnik RS*, nos. 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021).
[37] Law on free access to information (Zakon o slobodnom pristupu informacijama, *Službeni list RCG*, no. 68/05).
[38] Law on free access to information of public importance (Закон за слободен пристап до информации од јавен карактер, Службен Весник на РМ no. 13/2006, 86/2008 and 6/2010).

2. RIGHT TO INFORMATION – MAIN SOURCES OF INTERNATIONAL STANDARDS

Right to information is regulated by a comprehensive and complex body of international hard and soft law, both at universal and regional levels. In the context of the present research, the most important legal instruments are those developed by the United Nations, Council of Europe and the European Union.

2.1. UN LEGAL INSTRUMENTS

In its very first session in 1946, the UN General Assembly adopted Resolution 59(I), stating, "Freedom of information is a fundamental human right and the touchstone of all the freedoms to which the United Nations is consecrated". Article 19 of the UN Universal Declaration of Human Rights[39] stipulates freedom of opinion and expression as follows, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Similar formulation is provided also in Article 19 of the UN International Covenant on Civil and Political Rights,[40] stating, "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression recognised the principles relating to freedom of information and stated that everyone has the right to seek, receive and impart information and that this imposes a positive obligation on States to ensure access to information, particularly with regard to information held by Government in all types of storage and retrieval systems.[41]

In a more extensive commentary in 1998 (E/CN.4/1998/40), the Special Rapporteur moved beyond understanding the right to information as an element of freedom of expression, generally aiming at securing democracy, towards the understanding that: "the right to seek and receive information is not simply a converse of the right to freedom of opinion and expression but a freedom on its own" (Paragraph 11); the right "imposes a positive obligation on States to ensure access to information", in particular,

[39] Universal Declaration of Human Rights. General Assembly resolution 217 A (III) of 10 December 1948.
[40] International Covenant on Civil and Political Rights, General Assembly Resolution 2200A (XXI) of 16 December 1966.
[41] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, E/CN.4/1999/64,29 January 1999, accessed on March 15, 2021.

by "freedom of information legislation, which establishes a legally enforceable right to official documents for inspection and copying" (Paragraph 14); the right to "access to information held by the Government must be the rule rather than the exception" (Paragraph 12).

Further, the Special Rapporteur's commentary on the right to information (E/CN.4/2000/63) – establishing it as "a right in and of itself" - endorsed the set of principles drawn up by the non-governmental organization Article XIX, The Public's Right to Know: Principles on Freedom of Information Legislation, based on "international and regional law and standards, evolving State practice, and the general principles of law recognized by the community of nations".

In 2005, the UN organisation adopted the UN Convention Against Corruption.[42] Article 10 of this Convention, under the title "Public reporting", encourages the state parties to take such measures as may be necessary to enhance access to information as one of the means used in the action against corruption.

Access to information was given special importance in the Aarhus Convention, adopted in 1998.[43] Article 4 of this Convention requires the state parties to adopt and implement legislation that would ensure that public authorities, in response to a request for environmental information, make environmental information available to the public[44]). The Convention stipulates also the obligation of state parties to ensure within the framework of the national legislation that environmental information is made available to the public without a legitimate interest having to be stated. To this date, the Aarhus Convention has been ratified or acceded to by 46 countries, including Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia.[45] The European Union also acceded to the Convention.[46]

Access to information is also embedded in the UN Sustainable Development Goals (SDGs). More precisely, target 16.10 of SDGs is to "Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements".[47]

---

[42] United Nations Convention against Corruption, resolution 58/431 of October 2003.

[43] Convention on access to information, public participation in decision-making and access to justice in environmental matters, done at Aarhus, Denmark, on 25 June 1998.

[44] Article 2 of the Convention defines environmental information as any information on the state of elements of the environment, affecting or likely to affect the elements of the environment, the state of human health and safety, conditions of human life, cultural sites and built structures, inasmuch as they are or may be affected by the state of the elements of the environment.

[45] North Macedonia was the first of the four analysed countries to ratify the Aarhus Convention, as early as 1999. Bosnia and Herzegovina ratified in the Aarhus Convention in 2008, while Montenegro and Serbia ratified it in 2009. https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVII-13&chapter=27&clang=_en., 24.2.2022.

[46] European Union signed the Aarhus Convention in 1998 and ratified it in 2005. https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVII-13&chapter=27&clang=_en, 24.2.2022.

[47] *Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels*, https://sdgs.un.org/goals/goal16, 24.2.2022.

2.2. Council of Europe legal instruments

The Council of Europe also recognises freedom of information as a fundamental human right under Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[48] Article 10, Paragraph 1 of the Convention states: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

As with other rights and freedoms guaranteed by this Convention, the scope of the right to information is specified through the caselaw of the European Court of Human Rights (ECtHR). Over the years, the ECtHR has changed its approach to interpreting freedom of information as a fully-fledged unconditional right stemming from Article 10 of the Convention. Contrary to a somewhat broadened interpretation, as seen in the cases of *Sdružení Jihočeské Matky v. Czech Republic*[49] and *Társaság a Szabadságjogokért v. Hungary*[50], the recent caselaw of the ECtHR shows a more reticent approach. [51] Namely, the Court has held that Article 10 does not confer on the individual a right of access to information held by a public authority, nor oblige the Government to impart such information to the individual.[52] However, the court recognises that such a right or obligation may arise, firstly, where disclosure of the information has been imposed by a judicial order which has gained legal force and, secondly, in circumstances where access to the information is instrumental for the individual's exercise of his or her right to freedom of expression, in particular "the freedom to receive and impart information" and where its denial constitutes an interference with that right.[53]

This does not mean that the ECtHR denies the linkages between freedom of expression and freedom of information, but that it has started to build a specific set

[48] *European Convention for the Protection of Human Rights and Fundamental Freedoms*, https://www.echr.coe.int/documents/convention_eng.pdf, 24.2.2022.

[49] European Court of Human Rights, Application no. 19101/03, judgment 10 July 2006.

[50] European Court of Human Rights, Application no. 37374/05, judgment 14 April 2009. In the case of *Kenedi v. Hungary*, the Court explicitly recognised the obligation of the state, in circumstances when the requested information is available and does not require the government to gather any data, to refrain from interfering with the flow of information requested by the applicant. This right was recognised to a certain extent back in 2006, when the Court in the case of *Sdružení Jihočeské Matky v. Czech Republic* found that Article 10 of the Convention could imply the right to information held by a public authority. In the judgement in the case of *Társaság a Szabadságjogokért v. Hungary*, in Paragraph 35, the Court recognised that the Court had recently advanced towards a broader interpretation of the notion of freedom to information, which also implied free access to information.

[51] For additional insight into caselaw see: European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights Freedom of Expression (updated 31 August 2020)*, https://www.echr.coe.int/documents/guide_art_10_eng.pdf, 24.2.2022. In interpreting the ECHR, the European Court of Human Rights applies the evolutive approach i.e. resorts to the principle of the ECHR as a living instrument. See: V. Ćorić, A. Knežević Bojović, "Indirect Approach to Accountability of Corporate Entities through the Lens of the Case-Law of the European Court of Human Rights", *Strani pravni život* 4/2018, p. 30, doi: 10.5937/spz0-20339 and V. Ćorić Erić, *Odnos Evropskog suda pravde i Evropskog suda za ljudska prava*, doctoral thesis, Belgrade University Law Faculty, 2013, pp. 345-346, available at: https://nardus.mpn.gov.rs/handle/123456789/2642, 6.4.2022.

[52] *Ibid*.

[53] European Court of Human Rights, *Magyar Helsinki Bizottság v. Hungary*, Application no. 18030/11, *Cangi v. Turkey*, Application no. 24973/15.

of standards with regard to this right. Namely, ECtHR considers that whether and to what extent the denial of access to information constitutes an interference with an applicant's freedom-of-expression rights must be assessed in each individual case and in the light of its particular circumstances, having regard to the following criteria:

1. The purpose of the information request;
2. The nature of the information sought;
3. The role of the applicant;
4. The availability of the information.

It should be noted that within the Council of Europe, the right to information is not regulated only by the European Convention for the Protection of Human Rights and Fundamental Freedoms. Quite the contrary, the Council of Europe has been engaged in developing the standards for access to information for decades.[54] Two documents from that regulatory framework need to be singled out: Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents[55] and the Council of Europe Convention on Access to Official Documents from 18 June 2009.[56] The Recommendation was, in fact, used as basis for the aforementioned Convention, which entered into force on 1st December 2020. It is in force in respect of Bosnia and Herzegovina, Estonia, Finland, Hungary, Iceland, Lithuania, Montenegro, Norway, the Republic of Moldova, Sweden and Ukraine.[57] In its Article 2, the Convention requires that the signatory states "guarantee the right of everyone, without discrimination on any ground, to have access, on request, to official documents held by public authorities" and to "take the necessary measures in its domestic law to give effect to the provisions for access to official documents". The Convention allows certain limitations to this right, which must be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting a *numerus clausus* set of interests. It envisages that the applicant for an official document shall not be obliged to give reasons for having access to the official document, which is an important feature of RTI, and is a much broader right than that recognised by the ECtHR (supra). Further, the Convention envisages in Article 10 that an applicant whose request to access an official document has been denied, expressly or implicitly, must have access to a review procedure before a court or another independent and impartial body established by law.

2.3. European Union legal instruments

European Union has also recognised the issue of access to information from its establishment. Namely, free access to information was guaranteed in Article 255 of the Treaty Establishing the European Community to all natural or legal persons

[54] D. Banisar, 11.
Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents, https://wcd.coe.int/ViewDoc.jsp?id=262135, 24.2.2022.
[55] *Ibid.*
[56] *Convention on Access to Official Documents*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205, 24.2.2022.
[57] *Chart of signatures and ratifications of Treaty 205*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=205, 24.2.2022.

residing or having their registered office in a Member State. Further, the Declaration on the Right of Access to Information[58] was annexed to the Maastricht Treaty. That was done when the Council and the European Parliament adopted the Regulation No. 1049/2001 regarding public access to European Parliament, Council and Commission documents.[59] The approach adopted in the Regulation corresponds to the Nordic concept of access to information.[60] The Treaty of Lisbon confirmed the commitment of the European Union to the implementation of the right to information – Article 15 reiterates that any citizen of the Union, any natural or legal person residing or having its registered office in a Member State shall have the right to access documentation of the EU authorities, bodies, and agencies.[61] Furthermore, the Charter of Fundamental Rights,[62] in Articles 41 and 42, explicitly guarantees the right of every person to have access to his/her file and documents of the EU institutions. As emphasised,[63] in less than two decades, access to information in the EU law has evolved from a situation of a mere favour being granted to an individual by the institutions into one of a true subjective fundamental right.

In addition to having adopted the regulation guaranteeing the right to information held by public authorities, the European Union introduced, through its secondary legislation, the obligation of Member States to incorporate into their national legislation regulations ensuring access to information in particular sectors – for example, in the environmental sector.[64]

2.4. Soft-law instruments

Apart from the mentioned hard-law instruments, it is important to consider the principles and methodological positions in a number of soft-law instruments. The Right to information principles – The Public's Right To Know: Principles on Freedom of Information Legislation developed by Article 19 (hereinafter: the Article 19 Principles), a global civic organisation[65] constitute a soft-law source of high credibility.

The global RTI Rating tool measures the strength of the legal framework for the right to access information held by public authorities based on 61 indicators. The importance of the RTI rating does not lie only in the systematic approach, but it also stems from the growing external conditionality effected through global performance

[58] *Declaration No. 17 on the right of access to information*, https://www.cvce.eu/en/obj/treaty_on_european_union_declaration_no_17_on_the_right_of_access_to_information_maastricht_7_february_1992-en-c93fe321-0e77-43a0-b316-d0d45635ff98.html, 24.2.2022.

[59] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *OJ L 145,* 31 May 2001*,* 43–48.

[60] M. Augustyn, C. Monda, *Transparency and Access to Documents in the EU: Ten Years on from the Adoption of Regulation 1049/2001*,
http://www.eipa.eu/files/repository/eipascope/20110912103927_EipascopeSpecialIssue_Art2.pdf.

[61] Consolidated version of the Treaty on European Union, *Official Journal of the European Union C 83/13*.

[62] Charter of Fundamental Rights of the European Union, *Official Journal of the European Union 2010/C 83/02*.

[63] OECD, "The Right to Open Public Administrations in Europe: Emerging Legal Standards", *SIGMA Papers*, No. 46 (2010), OECD Publishing, Paris, https://doi.org/10.1787/5km4g0zfqt27-en., 8.

[64] *Directive 2003/4/EC of 28 January 2003 on public access to environmental information, repealing Council Directive 90/313/EEC*.

[65] Article 19, *What we do*, https://www.article19.org/what-we-do/.

indicators.[66] The limitation of the RTI in terms of its potential conditionality lies in the fact that it measures the legal framework alone, and does not take into account the practices; therefore, consequently, high ratings are comparatively easy to achieve. Further, it does not seem that the governments of developing economies, such as the ones included in the study, see immediate effects from conditionality in the sphere of FOI legislation.

SIGMA Principles of Public Administration,[67] which define what good governance entails in practice and outline the main requirements that countries should follow during the European Integration process, including a monitoring framework, recognise RTI as one of key principles related to accountability of public administration. Indicator 4.2.1: Accessibility of public information measures the extent to which the legal and institutional framework regarding access to public information is established, but also covers the practical application of these legal requirements.

2.4.1 Tshwane principles as a lex specialis soft-law instrument in the defence sector

One of the most important international documents aimed at developing and providing clear guidelines for the public authorities involved in drafting and implementing the legislation on free access to information in the sphere of national security, is: *Global Principles of National Security and the Right to Information,* or *Tshwane Principles*.[68] It is to be noted that the said principles have been proposed by the civil society in a large sense and are hence only a soft-law instrument.

The Tshwane Principles underline that national security should be used as grounds for denying access to information only in exceptional cases, and that it should be interpreted narrowly.[69]

In this regard, it is stated that only the authorities that have exclusive jurisdiction over this area (national security protection) can use these grounds for refusing access to information. Furthermore, the Principles indicate that the very fact that a presumption of *national security protection* exists, cannot in itself constitute sufficient grounds for denying access to information.

[66] Doshi, Kelley and Simmons strongly and rightfully argue that global performance indicators are powerful conditionality mechanism which has resulted in changes in regulatory behaviour of many countries (R. Doshi, J. G. Kelley, B. A. Simmons, *The Power of Ranking: The Ease of Doing Business Indicator and Global Regulatory Behavior*, Internet, https://ssrn.com/abstract=3318360, 06/05/2019.). Nevertheless, the desired effects of such conditionality may not be effected. While one of the expected outcomes of the Ease of Doing Business conditionality is altering investor sentiment in terms of attracting more foreign direct investments, research has shown that with regards to Western Balkan countries the correlation between the Ease of Doing Business ranking and foreign direct investment is in fact limited. (B. Jovanovic, B. Jovanovic, "Ease of doing business and FDI in the ex-socialist countries", *International Economics and Economic Policy*, vol. 15(3)/2018, 587-627).

[67] *The Principles of Public Administration 2017 edition*, https://www.sigmaweb.org/publications/Principles-of-Public-Administration-2017-edition-ENG.pdf, 24.2.2022.

[68] Open Society Justice Initiative, *The Global Principles on National Security and the Right to Information (The Tshwane Principles)*, https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles, 24.2.2002.

[69] A. Rabrenović, R. Radević, "Granice prava na slobodan pristup informacijama u sektoru bezbednosti - primer Crne Gore", *Strani pravni život*, 3/2016, 23-38.

Tshwane Principles further seek to define the types of information that the public administration authorities have the right to withhold on national security grounds.[70] In a nutshell, the goal is to streamline the practices of limitations on national security grounds only to the types of information the disclosure of which may have serious implications on national security, thus preventing the permeation of the culture of secrecy of everything even remotely connected to national security (e.g. quantities for meals in the Army one can use to deduce information on the distribution of troops from).[71] At the same time, the Principles suggest that it is a good practice for the national legislation to set forth an exclusive list of information categories that are specified narrowly. In order to facilitate the implementation of what is referred to as the "public interest test", the Principles also list the information categories, which imply a strong presumption of overriding public interest in favour of disclosure.[72]

[70] Principle 9, Item a) of Tshwane Principles: Information that Legitimately May Be Withheld.

[71] Another example of the futility of classifying certain documents were military maps of the Yugoslav Army and the first decade of the 21st century. Although they have not been changed since the 1970s, and, what's more, even though at that time more up-to-date and detailed data could be accessed through the Google Maps services, the military leadership insisted on keeping them classified. M. Reljanović, "Vojna tajna u nacionalnom zakonodavstvu i praksi", in: S. Gajin *et al.*, *Zaštita podataka o ličnosti i poverljivi podaci*, Open Society Fund, Belgrade 2005, 142-144.

[72] Principle 10 of Tshwane Principles: Categories of Information with a High Presumption or Overriding Interest in Favour of Disclosure.

3. KEY INTERNATIONAL STANDARDS IN THE AREA OF RIGHT TO INFORMATION

The first important standard relating to free access to information implies that the person requesting information is not obliged to state reasons for the request.[73] This standard reflects the very essence of this right – access to information must be free and it cannot be conditional. The request is also not conditional on the requester potentially being wronged by the requested public act.[74] At the same time, the formal requirements for the submission of requests should be minimal.[75] If the request is not precise enough, the public authority cannot ignore it, and has to assist the applicant in specifying his/her request more precisely,[76] and in identifying the document containing the requested information.[77][78] However, if that is not possible, the authority is not obligated to fulfil the request.[79]

Any public authority that receives requests for information, i.e. documents, should consider the requests without any discrimination, on an equal basis.[80] The requests should be considered promptly, or within a reasonable timeline that is known in advance,[81] and if that cannot be done within the specified timeline, the applicant should be informed thereof.

The request for access to information of public importance can be denied, if it is obvious that it is manifestly unreasonable,[82] that is, if the request is clearly frivolous or vexatious and is only intended to disrupt the activities of the public body.[83] This

[73] Article 4, paragraph 1 of the Council of Europe *Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents* (hereinafter: Recommendation); Principle 1, the ARTICLE 19 Principles; Article 6 of the *Regulation No. 1049/2011 regarding public access to European Parliament, Council and Commission documents* (hereinafter: Regulation)

[74] V. V. Vodinelić, S. Gajin, *Slobodan pristup informacijama: ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Belgrade, 2004.

[75] *Convention on Access to Official Documents*, Article 3, Paragraph 4 (hereinafter: COE Convention).

[76] Article 6, Paragraph 2, of the Regulation.

[77] Article 5, Paragraph 1 of the CoE Convention.

[78] In Anglophone legislations, this standard is also sometimes referred to as the "duty to assist", e.g. in the Freedom of Information Act of the United Kingdom (Section 16). However, the said duty may transgress the mere obligation of assistance in clarification of the request. In Canadian legislation, the duty to assist implies that the competent person within the public body will "make every reasonable effort to assist the person in connection with the request, respond to the request accurately and completely and, subject to the regulations, provide timely access to the record in the format requested", clearly further extending the obligation of the public body to conduct a reasonable search for the requested records (see: B. Roziere, K. Walby, "The duty to assist in Canadian Freedom of Information law", Canadian Public Administration, Volume 63, Issue 4/2020, 582-601, https://doi.org/10.1111/capa.12392).

[79] CoE Convention, Article 5, Paragraph 5.

[80] Article 2 of the CoE Convention.

[81] Article 4, Paragraph 4 of the CoE Convention. The Regulation also envisages in Article 7 that the requests are to be dealt with promptly, but also sets out a 15-day time limit as a maximum.

[82] Article 5, Paragraph 5 of the CoE Convention.

[83] Principle 5, Article 19 RTI Principles.

could also include the cases when the applicant resubmits the same request several times. [84]

An important standard states that even in the case of partial denial of the request, the justification of the reasons for the denial must be given and provided in writing.[85]

For access to information to be truly free, it must not imply high costs for the applicant. That means that no fees can be charged for insight into original documents.[86] However, a public authority may charge the applicant for the issuance of copies of documentation, but such fees must be reasonable, and cannot exceed the real costs of reproduction and delivery of the document.[87]

An applicant whose request for an official document has been denied, expressly or impliedly, whether in part or in full, shall have access to a review procedure before a court or another independent and impartial body established by law.[88] Optimally, this supervisory body monitors the implementation of free access to information legislation, and has the power to set standards, make prescriptions and impose sanctions.[89]

All restrictions on free access to information of public importance must be clearly and explicitly specified by law, and at the same time such restrictions must be necessary in a democratic society and proportional in relation to the objective they seek to protect.[90]

Various legal instruments include converging, yet not identical lists of protected interests that can justify restrictions to access to information. The list of exceptions envisaged in the Council of Europe is rather wide[91], and includes the following:

a. national security, defence and international relations;
b. public safety;
c. the prevention, investigation and prosecution of criminal activities;
d. disciplinary investigations;
e. inspection, control and supervision by public authorities;
f. privacy and other legitimate private interests;
g. commercial and other economic interests;
h. the economic, monetary and exchange rate policies of the State;
i. the equality of parties in court proceedings and the effective administration of justice;
j. environment; or
k. the deliberations within or between public authorities concerning the examination of a matter.

[84] Section VI 6.
[85] Article 5, Paragraph 6 of the CoE Convention, Section VI 7 of the Recommendation.
[86] Article 7, Paragraph 1 of the CoE Convention, Section VIII 1 of the Recommendation
[87] Article 7, Paragraph 2 of the CoE Convention, Section VIII 2 of the Recommendation. Article 10 of the Regulation envisages that in addition to direct access in electronic form, copies of less than 20 A4 pages are free of charge.
[88] Article 8 of the CoE Convention, Section IX 1 and 2 of the Recommendation.
[89] SIGMA Principles of Public Administration, Accountability, Principle 2, Point 8.
[90] Article 3 of the CoE Convention, Section IV1 of the Recommendation.
[91] Article 3 of the CoE Convention.

The EU Regulation envisages a narrower set of exceptions in its Article 4. Firstly, it states that the institutions shall refuse access to a document, where disclosure would undermine the protection of

(a) the public interest as regards public security, defence and military matters, international relations, the financial, monetary or economic policy of the Community or a Member State; (b) privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

It further states that access to a document will be refused, if the public interest test shows that there is no overriding public interest in disclosure, where disclosure would undermine the protection of:

- commercial interests of a natural or legal person, including intellectual property,
- court proceedings and legal advice,
- the purpose of inspections, investigations and audits.

Finally, the EU Regulation envisages that access to a document, drawn up by an institution for internal use, which relates to a matter where the decision has not been taken by the institution, shall be refused, if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure.

Article 19 RTI principle 4 underlines that exceptions should not only be provided in law in an exhaustive list, but that the list should be limited to matters recognized under international law, such as law enforcement, privacy, national security, commercial and other confidentiality, public or individual safety, and the effectiveness and integrity of government decision-making processes.

The right to information may be denied, if the release of information contained in the document would or could affect any of the aforementioned interests, unless there is an overriding public interest to make such information available to the public.[92] RTI Principles developed by Article 19 underline that, in order for access to information to be restricted, a three-part test must be conducted and the following conditions met:

- the information must relate to a legitimate aim, as provided for in international law;
- disclosure must threaten to cause substantial harm to that aim; and
- the harm to the aim must be greater than the public interest in having the information.

The test reflects the principle of seeking a balance between the right of the public to know and the need to protect the aforementioned interests, not differentiating between the protection of the national security interests and the protection of intellectual property rights. As seen above, the European Union, on the other hand, adopted a somewhat different approach in its regulations, granting a higher degree of protection

[92] CoE Convention, Article 3, Paragraph 2, Section IV 2 of the Recommendation, EU Regulation Article 4.

of the legitimate public interest (national security, military issues, but also protection of privacy[93]) compared to the issues that essentially constitute private interest, such as, for example, commercial and economic interests (e.g. intellectual property rights). Therefore, with respect to the allowed restrictions of the right to information of public importance, the view that should be accepted is that no category of information is exempt from the free access regime *per se*, while at the same time adopting the standard that the bodies deciding on exemptions must interpret these restrictions strictly.[94]

[93] The reasons for this should be found in the detailed and comprehensive EU regulations relating to personal information protection.

[94] OECD, "The Right to Open Public Administrations in Europe: Emerging Legal Standards", *SIGMA Papers*, No. 46, OECD Publishing, Paris 2010, p. 40, https://doi.org/10.1787/5km4g0zfqt27-en.

4. METHODOLOGICAL APPROACH TO STANDARDS AND INDICATORS

The approach taken in the study is to analyse the current regulatory frameworks in force in the four countries in selected aspects related to FOI. A conscious choice was made to focus on issues that regulate the procedure for access to information, and the way in which the competent public authorities are meant to respond to requests for access to information. As Michener and Nichter duly point out, how governments respond to citizen demands is fundamental to FOI's democratic raison d'être.[95] Consequently, promotional measures and open data measures are not examined. Particular attention was given to the limitations of the right to access information.

In order to provide a benchmark for the assessment, the study identifies key international standards and indicators in the given area. Indicators were developed for each standard in order to facilitate and guide the assessment. The standards and indicators drew considerable inspiration from the indicators used in the RTI rating methodology, and were also informed by the hard- and soft-law documents that outline the relevant standards. The intention, however, was not to duplicate this complex and comprehensive effort. Rather, the approach taken was to identify major issues and synthetize the relevant underlying rules related to them. Consequently, the standards and indicators do not fully coincide with that of the RTI. Further, the qualitative assessments of compliance with relevant standards and their subsequent quantification are not informed by the RTI rating and may differ from it.[96]

Wherever possible, the definitions and lists were developed with a reference to the Council of Europe Convention. One important deviation from this approach is the exclusion of one of the allowed limitations of the right to information: environmental protection. The underlying interest that would be preserved under this restriction of the RTI is the protection of an endangered species (for instance, its location), based on the rules of the Aarhus convention. However, due to very laconic coverage of this issue in the legislations of the analysed countries, and potential misunderstandings as to the purpose of these restrictions, it was left out of the standard.

The standards examined in the study are the following:

1. Adequate legal framework guaranteeing free access to information is in place
2. Free access to information applies to a wide scope of information holders

[95] G. Michener, S. Nichter, S. (2022).

[96] The current RTI ratings for the countries included in the study differ considerably. Serbia is ranked at the third place with a score of 135 (out of 150). North Macedonia is ranked at the 24th place with a score of 112. Bosnia and Herzegovina is ranked at the 37th place with a score of 102. Montenegro is ranked in the lowest place of the four countries – 60th, with a score of 89. However, an important caveat needs to be taken into account: RTI rating related to some of these countries has not been updated for years, and did not take into account some of the legislative amendments effected since the rating was performed. It, therefore, bears the risk of being somewhat outdated.

3. Requesting procedures are not complicated, are not strictly conditions and are free, while access fees are proportionate to actual costs
4. The procedure for dealing with requests is conducted within a reasonable timeline
5. Exceptions to free access to information are clearly formulated in law and not extensive, while a public interest override and harm test are envisaged and applied
6. There is a designated supervisory authority overseeing the implementation of the legislation on public information with the power to set standards, make prescriptions and impose sanctions.

The core of the study consists of a detailed qualitative assessment of the level of alignment of the national regulatory frameworks of the four countries with the relevant international standards, based on the defined indicators. The assessment takes into account the provisions of national constitutions, primary and secondary legislation. The study goes one step further, as the qualitative assessment is also quantified for each indicator and standard.

The quantification of the assessment is based on the approach used by SIGMA. Consequently, the methodology consists of two layers of quantified assessment.

The first layer includes assessment per indicator within each standard. Each standard includes one or more indicators. Within this assessment, points are awarded to each indicator on a 0-3 scale, as per the Table 1. The 0-3 scale was chosen given that the indicators are, for the most part, defined in rather straightforward terms, often not allowing for a nuanced approach to the assessment of compliance with the relevant standard. A four-point scale was, therefore, deemed optimal.

Table 1: Points awarded per indicator

Point	Point description
0	Not in line with standards
1	Mostly not in line with standards
2	Mostly in line with standards
3	Fully in line with standards

The second layer of assessment is done, once all the indicators within one standard are awarded their respective points. Then, the average point is calculated **per standard.** The average point per standard is calculated by dividing the sum of all points awarded with the number of indicators for the given standard. The average point for the standard is then translated to a quantified standard value on a 0-5 scale, as per Table 2. Since standards, as a rule, comprise two or more indicators (with some exceptions), and were purposefully defined to be more complex, the selected six-tier scale allows for nuances to be assessed and identified when it comes to compliance with or departures from the standard.

Table 2: Standard values

Average point	Standard value	Description of standard value
0 – 0.50	0	Not in line with standard
0.51 – 1.00	1	Mostly not in line with standard
1.01 – 1.50	2	Significant departures from standard
1.51 – 2.00	3	Some departures from standard
2.01 – 2.50	4	Mostly in line with standard
2.51 – 3	5	In line with standard

The quantification is presented in tables at the level of each standard. The intention of the quantification is not to "name and shame", but rather to provide a simplified, yet informative outlook on the state of play with regard to each of the relevant regulatory frameworks, and to pinpoint the respective strengths and weaknesses. The study does not offer a definitive quantitative assessment, but rather offers a qualitative interpretation of the data collected in the conclusion.

When it comes to the police and defence sector, the specific rules applicable to the defence and police sector only were singled out and described, but were not quantified.

5. COMPLIANCE OF THE LEGISLATION OF ANALYSED COUNTRIES WITH KEY INTERNATIONAL STANDARDS

5.1. General Civil Service

Standard 1. Adequate legal framework guaranteeing free access to information is in place

Indicator 1

The legal framework recognises a fundamental right of access to information.

The majority of analysed countries recognises the right to information as a fundamental right in their constitutions. The Constitution of Montenegro[97] also recognises the right to information in the part of the constitution regulating political rights and freedoms. The Constitution of North Macedonia[98] recognises the right to information under the heading of regulating fundamental rights. Right of access to information is recognised in the Constitution of the Republic of Serbia[99], as one of the human rights, in Article 51 Paragraph 2, which guarantees everyone the right of access to data held by state bodies and organisations entrusted with public authority, while also prescribing that the right is regulated in more detail by the law. A notable exception is Bosnia and Herzegovina, which recognizes this right in the constitution only implicitly. Namely, Bosnia and Herzegovina (hereinafter: BiH) has a specific constitutional order, bearing in mind the constitutional text[100] is a part of the General Framework Agreement for Peace in Bosnia and Herzegovina. Although there is no explicit mention of the right to access information in the text of the BiH Constitution, it can be implicitly derived from the wording that "Bosnia and Herzegovina and both entities will ensure the highest level of internationally recognized human rights and fundamental freedoms". Constitutions of the **Federation of Bosnia and Herzegovina**[101] (hereinafter: FBiH) and of the **Republic of Srpska**[102] do not contain provisions on RTI.

[97] Constitution of Montenegro (Ustav Crne Gore, *Službeni list CG*, nos. 1/2007 and 38/2013-1).

[98] Constitution of North Macedonia (Уставот на Република Северна Македонија, *Службен Весник на РМ*, no. 52/91, 1/92, 31/98, 91/01, 84/03, 107/05, 3/09, 49/11, 6/19, *Службен Весник на РСМ* no 36/19.).

[99] Constitution of the Republic of Serbia (Ustav Republike Srbije, *Službeni glasnik RS*, no. 98/2006).

[100] Annex IV of the General Framework Agreement for Peace in Bosnia and Herzegovina and *Official Gazette* no. 25/2009 – Amendment I.

[101] Constitution of the Federation of Bosnia and Hercegovina (Ustav Federacije Bosne i Hercegovine, *Službeni list FBiH*, no. 1/1994).

[102] Constitution of the Republika Srpska (Ustav Republike Srpske, *Službeni glasnik Rep. Srpske*, nos. 21/92 –tekst, 28/94, 8/96, 13/96, 15/96, 16/96, 21/96, 21/02, 26/02, 30/02, 31/02, 69/02, 31/03, 98/03, 115/05, and 117/05).

All the analysed countries have adopted laws governing the right to access information.

The Law on Freedom of Access to Information in **BiH** (LFAIB) was adopted in 2000 and has been amended several times since then. The entities have enacted their own laws on the same matter. In the **Republic of Srpska**, the Law on freedom of access to information[103] (hereinafter: RFAIRS) and in **FBiH** the Law on freedom of access to information in FBiH[104] (hereinafter: RFAISFBH) were enacted in 2001 (RFAISFBH was later amended in 2011).

Montenegro regulates access to information in more detail in the Law on Access to Information. The Law does not expressly recognise the right of access to information as a fundamental right, but it states in Article 5 that access to information is aimed at democratic control of government powers and at the exercise of human rights and freedoms. It also states that access to information is exercised on the level of standards included in ratified international human rights' treaties and generally accepted rules of international law.

In **North Macedonia**, RTI is regulated in detail by the Law on Access to Information.[105] The Law[106] stipulates that all legal or natural persons have the right of access to information, including foreign legal or natural persons, in accordance with this Law, and other laws, which includes the Law on General Administrative Procedure.[107]

In **Serbia**, the Law on free access to information of public importance (hereinafter: LFAIS),[108] regulates in detail the rights of access to information of public importance held by public authorities, with a view of exercising and protecting the public interest to know and attaining free democratic order and an open society." The law, therefore, reaffirms the importance of the right to information for the rule of law.

The laws of Serbia, Montenegro, and North Macedonia are therefore fully in line with standards. The regulatory solution in BiH is somewhat different. While the country and its entities all have statutes that regulate RTI, there is no clear indication in those statutes that RTI is recognised as a human right, which renders their regulatory framework either mostly or not at all in line with the relevant standard.

---

[103] Law on freedom of access to information (Zakon o slobodi pristupa informacijama, *Službeni list FBiH*, no. 20/2001).
[104] Law on freedom of access to information (Zakon o slobodi pristupa informacijama, *Službeni list Rep. Srpske*, no. 32/2001, 48/2011).
[105] Law on free access to information of public character (Закон за слободен пристап до информации од јавен карактер *Службен весник на РСМ* no.101/2019)
[106] Article 3 of the Law.
[107] Law on general administrative procedure (Законот за општата управна постапка, *Службен весник на РМ* no.145/2015). As Article 1, Paragraph 2 of the Law on Access to Information of Macedonia stipulates that the right of access to information is effected through that law, the Law on General Administrative Procedure and other laws.
[108] Law on free access to information of public importance (Zakon o slobodnom pristupu informacijama od javnog značaja, Sl. glasnik RS", br. 120/2004, 54/2007, 104/2009, 36/2010 i 105/2021

Indicator 2

The legal framework creates a specific presumption in favour of access to all information held by public authorities, subject only to limited exceptions.

The legal frameworks of the four analysed countries are not uniform, when it comes to creating a specific presumption in favour of access to all information. The normative frameworks of BiH envisage such a presumption. In Montenegro and North Macedonia, the situation is somewhat different and subject to a number of caveats.

In **BiH**, general presumption in favour of access to all public information is set out in Articles 1, 2 and 4 of the LFAIB, stipulating that the aim of the law is to establish that information under the control of a public body is a public good of value and that public access to this information promotes greater openness and accountability of those public bodies. Further, the law recognises that such information is necessary for the democratic process, and that therefore any natural or legal person has the right of access to such information, while public authorities have an appropriate obligation to publish the information. The law also expressly envisages that it has to be interpreted so as to facilitate and promote, to the greatest extent and without delay, the publication of information under the control of a public body at the lowest acceptable price. Furthermore, Article 4 of the LFAIB stipulates that the right of access is subject only to formal actions and restrictions as set forth in LFAIB. Identical norms are stipulated in Articles 1, 2 and 4 of the RFAISFBH and Articles 1, 2 and 4 of the RFAIRS.

The **Montenegrin** Constitution also prescribes limitations to the right of access to information. It states in Article 51, Paragraph d, that access to information may be restricted, if that is in the interests of protecting life, public health, morality and privacy, the conduct of criminal proceedings, security and defence of Montenegro, or foreign, monetary and economic policy. This normative approach is in line with the manner in which the Constitution of Montenegro regulates other rights and their possible limitations, but it is not common in comparative practices of the Western Balkan countries. Furthermore, the legal framework of Montenegro does not create a specific presumption in favour of access to all information held by public authorities. Firstly, it expressly exempts a rather broad set of information held by public authorities from the scope of the law. The provisions of the Montenegro Law on Access to Information do not apply to:

1) parties to court, administrative and other proceedings based on law, where access to information from such proceedings is prescribed by a legal act
2) information that must be kept secret pursuant to the law governing data classification,
3) classified information held by international organisations or other countries, and classified information that originate from or are exchanged as a part of cooperation with international organisations or other countries.

This means that the legal framework of Montenegro *a priori* does not favour access to all information held by public authorities**.**

The legislation of **North Macedonia** does not create an explicit presumption in favour of access to all information held by public authorities. However, the presumption is present implicitly in the provisions of the Law. Firstly, the Law defines the notion of "information of public character" as any information created or held by the information holder, pursuant to its competences.[109] Secondly, the Law envisages that a harm test needs to be conducted in order to refuse access to information subject to the *numerus clausus* set of exceptions to right to access.[110] Nevertheless, the North Macedonian Law defines the notion of public interest in an unusual, and rather limiting terms. More specifically, this law states that public interest implies, but is not limited to, situations where access to information would:

1) detect abuse of official position and corrupt behaviour
2) detect unlawful gain or spending of budgetary funds
3) reveal a potential conflict of interest
4) prevent and reveal serious threat to human life and health
5) prevent and detect threats to the environment
6) help understand the issues with regard to which a public policy is being developed or that are subject of public debate
7) enable equal treatment of every citizen before the law.

Commonly, in comparative law, these are the situations when there is an absolute presumption that a public interest exists and that a harm test need not be conducted at all.

In **Serbia**, presumption in favour of access to all public information is set forth in Article 2 of the LFAIS. Firstly, the law defines information of public importance as information held by a public authority body, created during or relating to the operation of a public authority body, which is contained in a document and concerns anything the public has a justified interest to know, regardless of the fact whether the source of information is a public authority or another person, the medium on which the information is held, the date the information was created, the way in which information was obtained, or any other similar properties. This definition is in accordance with the principle that all information held by public authorities are presumed as public, unless some type of exception set forth in LFAIS or another law could be applied to them. Furthermore, Article 4 stipulates that justified public interest to know is deemed to exist whenever information held by a public authority concerns a threat to, or protection of, public health and the environment, while with regard to other information held by a public authority, it shall be deemed that justified public interest to know exists, unless the public authority concerned proves otherwise. Finally, Article 8 stipulates that right to information may, in exceptional circumstances, be subject to limitations set forth in LFAIS, but only to the extent necessary in a democratic society to prevent a serious violation of an overriding interest based on the Constitution or law. An additional layer of protection of RTI is provided in Paragraph 2 of the same Article, envisaging that nothing in the law shall be construed as justifying the revocation of a right conferred by this Law or its limitation to an extent exceeding that provided for in Paragraph 1 of

[109] Article 3 of the Law.

[110] Article 3 of the law envisages the harm test, while the exceptions are set forth in Article 6, Paragraph 1.

this Article. The legislator's commitment towards ensuring access to information that originates from the work of the civil service is further supported by the provisions of the Law on Civil Servants[111] (hereinafter: LCS), which stipulates that the information on the work of civil servants is available to the public, according to the law governing free access to information of public importance. However, a problematic Article 7 of the Law on Tax Procedure and Tax Administration[112] considerably deviates from the standard by creating a presumption that the interest of preserving the confidentiality of certain categories of tax data always overrides the interest concerning the access to information of public importance. Namely, this Article first defines the notion of tax secret, which covers every document, information, data or fact concerning the taxpayer obtained by officials and other persons involved in the tax, misdemeanour, preliminary investigation or court procedure, singling out data on technical inventions, patents or technological procedures applied by the taxpayer as additionally protected. This, rather unclearly worded norm, goes on to state that breach of data confidentiality jeopardizes the interest of taxpayers and public interest of the Republic of Serbia, which override the interest concerning the access to information of public importance. This means that, contrary to the provisions of the LFAIS, which envisages that limitations to RTI can only be imposed by the LFAIS, the Law on Tax Procedure and Tax Administration introduces a limitation of the RTI. Further, the provisions of the Law on Tax Procedure and Tax Administration do not call for a harm test to be conducted – thus again disregarding the general RTI framework.

The regulatory frameworks of Serbia and North Macedonia are mostly in line with standards. Due to the extensive constitutional and legislative norms on limitations to RTI, the regulatory framework of Montenegro is ranked the lowest, and is assessed as mostly not being in line with the standard. On the other hand, the legislative frameworks of BiH, FBiH and the Republic of Srpska are fully in line with the international standard.

[111] Law on Civil Servants (Zakon o državnim službenicima, *Službeni glasnik RS*, nos. 79/2005, 81/2005 – correction, 83/2005 – correction, 64/2007, 67/2007 – correction, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018 and 157/2020).
[112] Law on Tax Procedure and Tax Administration (Zakon o poreskom postupku i poreskoj administraciji, *Službeni glasnik RS*, nos. 80/2002, 84/2002, 23/2003, 70/2003, 55/2004, 61/2005, 85/2005 (other law), 62/2006 (other law), 61/2007, 20/2009, 72/2009 (other law), 53/2010, 101/2011, 2/2012, 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 (authentic interpretation), 112/2015, 15/2016, 108/2016, 30/2018, 95/2018, 86/2019, 144/2020).

1. Adequate legal framework guaranteeing free access to information is in place

Indicators	Value	BIH			MKD	MNE	SER
1. The legal framework recognizes a fundamental right of access to information	0-3	BIH	FBIH	RS	3	3	3
		1	0	0			
2. Indicator 2 The legal framework creates a specific presumption in favour of access to all information held by public authorities, subject only to limited exceptions.	0-3	3	3	3	2	1	2
Total points		4	3	3	5	4	5
Average points		2	1.5	1.5	2.5	2	2.5
Standard	0-5	4	2	2	4	3	4

Standard 2. Free access to information applies to a wide scope of information holders

Indicator 1

The right of access applies to the executive branch, to the legislature, to the judicial branch, including both administrative and other information, with no bodies excluded.

All the analysed countries envisage a broad scope of application of the RTI, as it applies to a wide set of public bodies. This implies that, in principle, their governments are committed to transparency. The regulatory frameworks of all four countries are in line with the relevant standards.

Namely, the four analysed countries prescribe that access to public information applies to the following categories of bodies:

- Executive bodies
- Legislative bodies
- Judicial bodies
- Administrative bodies, including independent agencies
- Local government and local self-government bodies.[113]

In **BiH, FBiH and the Republic of Srpska** the right to access public information also applies to bodies that perform a public function, and are appointed or established in accordance with the law (Article 3, Paragraph 1, Point b).

The **Montenegrin** Law further envisages[114] that the Agency for Access to Personal Data Protection and Access to Information keeps a special information system related to access to information, providing a database on public authorities. Similarly, the **North Macedonian** law envisages that the Agency for protection of the right to free access to public information publishes, on its webpage, the list of holders of information and their appointed officers who are in charge of access to information.[115] The published list is comprehensive, but not exhaustive, as the Agency is obliged to update it regularly.[116]

The scope of information holders in the legislative framework of **North Macedonia** is regulated in a rather circumventing manner. In Article 1 the Law envisages that it applies to state authority bodies and other bodies and organisations determined by law, bodies

[113] Article 3, Paragraph 1, Subparagraph b of the LFAIB, and also laws of the Repulic of Srpska and Federation BiH; Article 9 of the Montenegrin Law on Access to Information, Article 1 of the North Macedonia Law on Access to Information and North Macedonia Constitution.

[114] Article 41 of the Law.

[115] Article 5 of the Law.

[116] The list is available at http://komspi.mk/%d0%bb%d0%b8%d1%81%d1%82%d0%b0-%d0%bd%d0%b0-%d0%b8%d0%bc%d0%b0%d1%82%d0%b5%d0%bb%d0%b8-%d0%bd%d0%b0-%d0%b8%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d0%b8%d0%b8/, 24.2.2022.

of the municipalities, the city of Skopje and the municipalities within that city. This is reiterated in Article 3 of the Law, which defines the holders of information. The notion of "state authority bodies" and "other bodies and organisations determined by law" is not elaborated further in the Law. The scope of their meaning must therefore be deduced primarily from the text of the Constitution.[117] North Macedonian Law on access to information also explicitly states that political parties are also holders of information with regard to activities of public interest in the part pertaining to income and expenditure.

After the changes made in 2021, the **Serbian** Law contains probably the most exhaustive list of bodies to which the right to access applies. Nominally, the law stipulates that it applies to all public authority bodies.[118] LFAIS (Article 3) defines a public authority body as a: central government body; a territorial autonomy body; a local self-government body; an organization vested with public powers; public company, institution, organization and other legal entity, which is established by a regulation or decision of the central government body, a territorial autonomy body, or a local self-government body; These norms were firmly supported in practice, which was of particular importance in affirming that judicial bodies are also obliged to apply the rules on right to access.[119]

Indicator 2

The right of access applies to State-owned enterprises (commercial entities that are owned or controlled by the State), other public authorities, including constitutional, statutory and oversight bodies (such as an election commission or information commission/er) and to private bodies that are vested with public authority

With the exception of BiH, the regulatory frameworks of the analysed countries are in line with this standard. This is particularly important given the considerable number of state-owned or state controlled enterprises in the countries included in the study.

In **BiH**, pursuant to Article 3 of the LFAIB, any entity that is owned or controlled by a public authority shall be considered a public body to which LFAIB applies. This means that the BIH law does not apply to private bodies that perform a public function. Normative solution in the entity laws of the **Republic of Srpska** and the **Federation of Bosnia and Herzegovina** is identical.

[117] The Constitution of North Macedonia singles out the following bodies of state authority: National Assembly, President, Government, courts, and public prosecutors' offices. The Constitution also recognises the Constitutional Court. "Other bodies and organisations" should be understood as those regulated by a wide set of other laws. Veljanovska and Dukovski (S. Veljanovska, S. Dukovski, "The Law on Free Access to Information of Public Character and its Respect from the Judicial Council of RN Macedonia", *Horizonti 2021*, 1 (28), 1-8) confirm that all FOI legislation in North Macedonia is equally binding on every segment of the judicial system, therefore to the courts, Judicial Council, Judicial Academy etc.

[118] This means that the right to access applies to both elected and non-elected public bodies. On the difference between the elected and non-elected public bodies, see: M. Matijević, "Adequate Representation of Persons Belonging to National Minorities in Public Sector: The Nature, Content and Scope of Obligations in the Comments of the Advisory Committee for the Framework Convention", *Strani pravni život*, 4/2020, 56-57. doi: 10.5937/spz64-29799.

[119] See, for instance, Decision No. 07-00-01752/2011-03 of the Commissioner for information of public importance and personal data protection ascertaining that a court is a public authority in terms of Article 3 of the Law.

In **Montenegro**, Article 9 of Law on Access to information envisages that the term "public authority" includes all administrative bodies, institutions, companies or other legal persons founded, co-founded by the state or local self-government, or in majority ownership of the state or local self-government. The term also covers legal persons which are mostly financed from public revenues, and natural persons, entrepreneurs and legal persons who are vested with public powers or manage a public fund.

North Macedonian Law on Access to Information envisages that state bodies and organisations, municipal and town bodies, institutions and public services and legal and natural persons vested with public authorities are subject to this law. There is no limitation to the scope of the bodies subject to the law, so it must be understood to meet the relevant international standard.

In **Serbia**, the bodies to which RTI legislation applies include a wide array of companies owned or controlled by the state. More specifically, it is applied to a company whose founder or member is a central government body, a territorial autonomy body, or a local self-government body, or one or more of these authorities, with 50% or more of shares or stakes in sum or with more than half of the members of the governing body; a company whose founder or member is one or more bodies of public authorities with 50% or more shares or stakes in the sum; a legal entity whose founder is an abovementioned company. Further, in accordance with the Article 3 of LFAIS, any entity financed exclusively or mainly from the public funds, regardless of whether it is private or state-owned, shall be considered a public authority to which LFAIS applies. This covers both natural persons, and legal persons performing activities of general interest, as well as natural and legal persons vested with public powers e.g. notaries public, public enforcement agents; schools, hospitals etc. also need to apply the provisions of this law. Finally, any legal entity that has generated more than more than 50% of the income from one or more public authorities is covered by RTI legislation, to the extent to which the information relates to the activities financed by such revenues. Churches and religious communities, however, are explicitly exempted from this obligation. The said legal framework seems to be offset by inadequate practices on the part of the state-owned or state-controlled companies, which have been identified by the Serbian Commissioner for Information of Public Importance and Personal Data Protection such as refusing to be served with the legal documents and acts sent to them by the given Commissioner.[120]

This means that while the legislations of Serbia, Montenegro and North Macedonia are fully in line with international standards, the laws of BIH and the two analysed entities are mostly not in line with relevant international standards.

[120] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Nov način Izigravanja prava na pristup informacijama od javnog značaja*, 15/04/2019, https://www.poverenik.rs/sr/%D1%81%D0%B0%D0%BE%D0%BF%D1%88%D1%82%D0%B5%D1%9A%D0%B0/3095-%D0%BD%D0%BE%D0%B2%D0%B8-%D0%BD%D0%B0%D1%87%D0%B8%D0%BD-%D0%B8%D0%B7%D0%B8%D0%B3%D-1%80%D0%B0%D0%B2%D0%B0%D1%9A%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%BF-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B0%D0%BC%D0%B0-%D0%BE%D0%B4-%D1%98%D0%B0%D0%B2%D0%BD%D0%BE%D0%B3-%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%98%D0%B0.html , 24.2.2022. This information is also relevant in the context of the balance of powers, as underlined by: L. Glušac, T. Tepavac, "Narušavanje podele i ravnoteže vlasti: dominacija egzekutive u Srbiji", in *Otete institucije u Srbiji: teorija i praksa*, Belgrade 2019, 80-102.

2. Free access to information applies to a wide scope of information holders

Indicators	Value	BIH			MKD	MNE	SER
1. The right of access applies to the executive branch, the legislature, to the judicial branch, including both administrative and other information, with no bodies excluded.	0-3	BIH	FBIH	RS	3	3	3
		3	3	3			
2. The right of access applies to State-owned enterprises (commercial entities that are owned or controlled by the State), other public authorities, including constitutional, statutory and oversight bodies (such as an election commission or information commission/er) and to private bodies that are vested with public authority	0-3	1	1	1	3	3	3
Total points		4	4	4	6	6	6
Average points		2	2	2	3	3	3
Standard	0-5	3	3	3	5	5	5

Standard 3. Requesting procedures are not complicated, are not strictly conditioned and are free, while access fees are proportionate to actual costs

Indicator 1

Requesters are not required to provide reasons for their requests and are only required to provide the details necessary for identifying and delivering the information

All four analysed countries have almost identical legal solutions when it comes to this indicator and, except for the legislation of North Macedonia, are fully in line with the relevant international standard. The legislation of North Macedonia is mostly in line with this standard.

According to Article 11, Paras. 2-4 of the **BIH** LFAIB, request for access to information must include sufficient data on the nature and content of the information requested, as well as the address of the applicant. The public authority does not have the power to examine or request reasons for the justification of the request. Entity laws contain the same normative solutions.

The Law on Free Access to Information of **Montenegro** stipulates that all national or foreign natural or legal persons have the right of access to information without the obligation to state the reasons and explain the interest behind the request for information. The Law further requires that the request for access to information should include the title of the information or the data based on which the requested information can be identified. The requester may also include information he or she considers relevant in this request; this is an option, not an obligation.

The **North Macedonian** law envisages[121] that the requester does not need to state the reasons for the request, but does have to state explicitly that it is a request for access to information. The requester must indicate the information requested and the desired method of access to the information.[122]

In **Serbia**, LFAIS clearly stipulates (Art. 15 Para. 2 – 4) that the request to a public authority to exercise the right of access to information of public importance contains the name of the public authority, the full name and surname and address of the applicant, as many specifics as possible of the requested information, as well as other details which could facilitate the search for the requested information (if known to the applicant). An applicant, however, is not required to specify the reasons for a request.

[121] Article 11, Paragraph 5.
[122] Article 11, Paragraph 4.

Indicator 2

There are clear and relatively simple procedures for making requests. Requests may be submitted by any means of communication, with no requirement to use official forms or to state that the information is being requested under the access to information law.

With regard to procedures for making requests, the legislations of Montenegro and North Macedonia envisage the possibility for the request to be made orally, in writing, or in electronic format.[123] Conversely, the legislations of BiH, FBiH and the Republic of Srpska explicitly stipulate that the request can be made only in writing. This means that the latter legislations are partially in line with the standard.

In **BiH**, according to Article 11, Paras. 2-4 of the LFAIB, requests for access to information may only be submitted in writing, in one of the official languages of BiH. Apart from this norm, LFAIB does not contain any other restrictions. There is no prescribed form for making the request, as there is no provision on the means of communication that can be used to submit a request. Entity laws contain the same normative solutions.

Montenegrin Law on Access to Information prescribes the procedure for filing the request for access and the contents of the request in Articles 18 and 19. The written request is to be submitted directly, by regular mail or electronically, and the oral request should be submitted directly to the authority, on the record. The Law states that the public authority may prescribe a form for the request for access to information, but that it must act on all requests, regardless of whether they have been filed on the prescribed form or not.

The **North Macedonian** Law does not include detailed provisions on how the oral request is made. If the request is made in writing or in electronic format, it is submitted on a universal form, which is prescribed by the Director of the Agency for the Protection of the right to free access to public information. The Law offsets this provision by stating that the request is to be filed on the form or in other manner envisaged by law. The Instruction for the method of implementation of the Law on Access to Information,[124] states in Article 5 that the request can be submitted either on the prescribed form or through an ordinary, regular submission. However, it would have been better if this provision was included in the law, not in a secondary, guidance act. At the same time, the Instruction clearly states that a request made in writing can be submitted directly, in which case it must be stamped upon receipt, or via registered mail with return receipt. It is unclear why the guidance limits the submission of request by mail to only registered mail with return receipt, since the North Macedonian Law on general administrative procedure does not include such limitations.[125]

[123] Article 18 of the Montenegrin Law, Article 12 of the North Macedonian Law.

[124] *The Instruction for the method of implementation of the Law on Access to Information* (Упатство за спроведување на Законот за слободен пристап до информации од јавен карактер, бр. 01-158/1) issued by the Director of the Agency for the protection of the right of access to information, available at https://aspi.mk/wp-content/uploads/2020/09/Упатство-за-спроведување-на-Законот-за-СПИЈК.pdf, 24.2.2022.

[125] See Article 40 of the North Macedonian Law on general administrative procedure.

In **Serbia**, the procedure provided by the law is simple and clearly defined. According to Articles 15 and 16 of the LFAIS, the applicant files the request for access to information and is subsequently informed about the time, place and manner of insight, or a copy of the information is provided for him/her. Request can be filed in free form; a public authority may prescribe a sample request form, but it shall nevertheless have the duty to take into consideration all requests not filed on such form. The requester does not need to state that access is requested according to LFIAS. The request is filed in writing. However, a public authority shall also have the duty to grant an applicant access to information where a request for information is made verbally and entered on relevant records. LFAIS does not set forth the means of communication for making the request. The norms of LFAIS can be nevertheless interpreted to mean that there are no obstacles for the request to be filed in electronic form (by e-mail or other means of electronic communication), as long as the request contains all the necessary elements.

Indicator 3

Public officials are required to provide assistance to help requesters formulate their requests, or to contact and assist requesters where requests that have been made are vague, unduly broad or otherwise need clarification. Public officials are required to provide assistance to requesters who require it because of special needs, for example because they are illiterate or disabled.

The legislations of all four analysed countries and two entities in BiH envisage some form of assistance to be provided to the requesters in order to help them formulate their requests. Unfortunately, none of the legislations include explicit norms on the obligation of the public officials to provide assistance to requesters with special needs. This renders them mostly in line with the relevant standard.

In **BiH**, according to Article 18 of the LFAIB, public body is obliged to take all necessary measures to assist any natural or legal person seeking to exercise any right within the meaning of that Law. This norm is not further elaborated. Furthermore, Article 20, Paragraph 1, Point 1 of LFAIB stipulates that every public body is obliged to publish and submit a guide including the information needed to address the public body and its information officer, the essential elements of the application process, together with a sample request in writing, categories of information exempted from access, the procedure for access to information, the costs of reproduction, access to a remedy, and all relevant deadlines. Entity laws contain the same normative solutions. The guide operationalizes *ex ante* assistance to requesters to an extent, as it provides useful information and guidance on how to make the request, but cannot replace assistance in formulation of the request.

The **Montenegrin** Law on Access to Information prescribes that, if the request is incomplete or incomprehensible and therefore cannot be processed, the public authority

should give the applicant a time limit of eight days from the date of the request to correct the irregularities, and should inform the applicant on how they can be corrected. If the applicant fails to do so, the public authority will adopt a conclusion rejecting the request.[126] There is no specific provision on the assistance to be provided by public officials to persons who require it because of special needs. The Law on Access to Information, however, prescribes in Article 23 that once access is granted, it shall be provided to disabled persons in the manner and form corresponding to their abilities and needs. This is not elaborated further in the Law or secondary legislation.

North Macedonia regulates the issue of assistance to requesters in formulating their requests in Article 17 of the Law on Access to Information. This Article envisages in its Paragraph 1 that in case the request for information is incomplete and thus cannot be processed by the holder, the holder shall ask the requester to supplement the request and indicate that otherwise the request will be dismissed. Paragraph 2 of the same Article states that the official in charge of access to information shall provide advisory assistance to the requester, so that the request may be supplemented. The Law does not include any additional details on how the assistance is to be provided. There are no rules prescribing how the assistance is to be provided to requesters with special needs. The Instruction on the implementation of the Law on Access to information, the relevant bylaw, does not remedy this situation, as it does not provide any additional guidance. It would have been better, if additional guidance were provided to designated officials on how to provide assistance to the requesters, particularly given that access to information is recognised as one of the fundamental human rights.

In Article 15, the **Serbian** LFAIS envisages that, if the request is incomplete so that it cannot be executed, i.e. it is not clear to which information it refers, the authority will request its supplementation, by instructing the applicant on ways to rectify the deficiencies in the request. If an applicant fails to rectify the deficiencies by the specified deadline, i.e. within eight to 15 days, and if the deficiencies are such that they prevent the processing of the request, the public authority shall pass a decision dismissing the request as deficient. The LFAIS does not contain any additional provisions prescribing assistance to requesters who necessitate it because of special needs. It only prescribes some forms of external assistance in cases when access is already granted. Namely, the LFAIS states that if a person is unable to access a document containing the requested information without an escort, then access shall be allowed with the attendance of an escort (Art. 16 Para. 10). LFAIS does not contain other specific norms regarding providing assistance to people with special needs. It is interesting to note that the Recommendation of the Protector of Citizens (Ombudsperson) of the Republic of Serbia no. 10791 of 17 March 2017 to the institutions for the execution of criminal sanctions indicated that it was necessary to provide convicted persons with access to the text, i.e. a printed copy of a document located at a certain address on the Internet which was indicated by a public authority in response to a request for free access to information of public importance. It further instructed the Directorate for the execution of criminal sanctions to regulate the procedure that will enable convicted persons to inspect the requested documents in such situations.

[126] Article 28 of the Law.

Indicator 4

It is free to file requests. There are clear rules relating to access fees, which are set centrally, rather than being determined by individual public authorities. These include a requirement that fees be limited to the cost of reproducing and sending the information (so that inspection of documents and electronic copies are free) and that a certain initial number of pages (at least 20) are provided for free.

In all analysed countries, the filing of requests is free. Access fees are set centrally in all the countries and are generally limited to the cost of reproducing and sending the information.

In **BiH**, according to Article 16 of the LFAIB, the public body shall not charge fees for the submission of applications or for written notifications. Prices are determined only for reproduction services and are set by a decision of the Council of Ministers. For standard size copies, the first 20 pages are free of charge. Entity laws contain similar provisions, as there are no charge fees for the submission of application. The prices are determined only for reproduction services and are stipulated by the instruction of the Ministry of Justice (of the Republic of Srpska and FBiH). In both entities, first 10 pages of standard copies are free of charge (Article 16 in both laws).

Montenegrin Law on Access to Information prescribes that the applicant does not pay any fee for the request, but he/she carries the actual costs incurred for the authorities for duplicating, scanning, and delivering the requested information. These costs are prescribed by the Decree on the Reimbursement of Expenses in the Process of Accessing Information.[127] There is no provision on a certain number of pages being provided for free. This renders the Montenegrin framework mostly in line with the relevant standard.

North Macedonian Law on Access to Information expressly states that the request for access to information is free of any charge.[128] It envisages that the requester shall only pay the material costs for obtaining a copy or electronic copy of the document. If the requested information is voluminous, the information holder may ask the requester to pay the costs for reproduction of information in advance. The fees are regulated in the Decision on establishing the fees for covering the material costs for the provided information borne by the information holder, which was adopted in 2006[129] and amended in 2017[130].

[127] Decree on the Reimbursement of Expenses in the Process of Accessing Information (Uredba o naknadi troškova u postupku za pristup informacijama, *Službeni glasnik RS*, no. 66/2016).

[128] Article 28 of the Law.

[129] Decision on establishing the fees for covering the material costs for the provided information borne by the information holder (Одлука за утврдување на надоместок за материјалните трошоци за дадената информација од имателите на информаци, https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/)

[130] Decision on amending the decision on Decision on establishing the fees for covering the material costs for the provided information borne by the information holder (Одлука за дополнување на одлуката за утврдување

In **Serbia**, according to LFAIS, it is free to file requests. Moreover, inspection of contents of the document containing the requested information is provided free of charge. However, rules on issuing a copy of the document envisage that the applicant needs to reimburse the necessary costs of reproduction and any costs of related postal services. The government passed a list of reimbursable expenses based on which public authorities calculate such costs.[131] The expenses are set realistically. However, the bylaw has not been updated since 2006, and consequently includes some outdated solutions and related pricing e.g. the price for obtaining a copy of a document on a floppy disc or an audio tape. Neither the LFAIS nor the bylaw envisage a general rule, whereby the applicants would be exempted from reimbursement of costs. The bylaw does provide the public authorities with the option of not charging the issuing of copies of the document, in cases when the costs of reproduction are low (under 50 dinars), particularly in cases when the copies are sent in electronic form. This provision also seems outdated, given the technological advances and the reasonable assumption that a considerable number of requesters will in fact prefer to obtain electronic copies of the requested documents, and moreover, the public authorities generate an increasing number of documents in electronic format only. In addition, the LFIAS does have important exceptions from the duty of reimbursement for certain categories of requesters and for certain categories of information. Namely, journalists who request a copy of a document for professional reasons and nongovernmental organizations focusing on human rights that request a copy of a document, for the purpose of performing their registered activities, are exempted from the duty to reimburse the costs of issuing a copy of the document. The same applies to all persons who request information regarding a threat to, or protection of, public health and environment. However, the LFIAS also prescribes an exception from this rule, in cases where requested information has already been published nationwide or is available online (LFAIS, Art. 17). When it comes to the practical implementation of the said norms, it may be interesting to note that in the decision 07-00-02878/2016-03 of 14 March 2018, the Commissioner for Information of Public Importance and Personal Data Protection stated that the competent authority did not violate the law, if it allowed the applicant access to information at its premises, instead of sending copies of the requested documents. Also, in the decision 07-00-03228/2016-03 of February 28, 2018, the Commissioner pointed out that the competent authority does not have an obligation to translate the requested information, even if it is available only in a language the applicant does not understand.

Due to some additional requirements prescribed by the legislation, as well as the fact that only the legislation of BiH envisages that the first 20 pages are provided free of charge, the legislations of Montenegro and North Macedonia, as well as of the

на надоместок за материјалните трошоци за дадената информација од имателите на информации, https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/)

[131] Regulation on the amount of compensation of necessary costs for issuing a copy of documents on which is information of public importance (Uredba o visini naknade nužnih troškova za izdavanje kopije dokumenata na kojima se nalaze informacije od javnog značaja, *Službeni glasnik RS*, no. 8/2006).

two entities in BiH, are mostly in line with the standard. Serbian regulatory framework is mostly in line with the standard when it comes to providing a certain initial number of pages of the requested documents free of charge. While the exception in favour of journalists, NGO watchdogs and those requesting information related to potential threats to public health and environment are commendable (and unique in the regulatory framework of the neighbouring countries), it still does not render the Serbian regulatory framework fully in line with the standard. Further, there is an evident need to update the relevant bylaw so as to render it more responsive to the technological developments. The regulatory framework of BiH is fully in line with the standard.

3. REQUESTING PROCEDURES ARE NOT COMPLICATED, ARE NOT STRICTLY CONDITIONED AND ARE FREE, WHILE ACCESS FEES ARE PROPORTIONATE TO ACTUAL COSTS

Indicators	Value	BIH			MKD	MNE	SER
		BIH	FBIH	RS			
1. Requesters are not required to provide reasons for their requests and are only required to provide the details necessary for identifying and delivering the information	0-3	3	3	3	2	3	3
2. There are clear and relatively simple procedures for making requests. Requests may be submitted by any means of communication, with no requirement to use official forms or to state that the information is being requested under the access to information law.	0-3	1	1	1	2	3	3
3. Public officials are required to provide assistance to help requesters formulate their requests, or to contact and assist requesters where requests that have been made are vague, unduly broad or otherwise need clarification. Public officials are required to provide assistance to requesters who require it because of special needs, for example because they are illiterate or disabled	0-3	2	2	2	2	3	2
4. It is free to file requests. There are clear rules relating to access fees, which are set centrally, rather than being determined by individual public authorities. These include a requirement that fees be limited to the cost of reproducing and sending the information (so that inspection of documents and electronic copies are free) and that a certain initial number of pages (at least 20) are provided for free.	0-3	3	2	2	2	2	2
Total points		9	8	8	8	11	10
Average points		2.25	2	2	2	2.75	2.5
Standard	0-5	4	3	3	3	5	4

Standard 4. The procedure for dealing with requests is conducted within a reasonable timeline

Indicator 1

Public authorities are required to respond to requests as soon as possible. Clear and appropriate procedures are in place for situations where the authority to which a request is directed does not have the requested information.

There are clear and reasonable maximum timelines with clear limits on timeline extensions

The legislations of the four analysed countries are similar and are mostly in line with relevant international standards. However, the reasons for this assessment differ between countries, due to specificities in national regulations. Namely, the laws of Serbia and Montenegro clearly set out an urgent deadline for response to the request in cases where the life or freedom of a person are contingent on access to the requested information, which is a solution that can be assessed as fully convergent with relevant international standards. On the other hand, the legislation of Montenegro includes some unusual norms related to cases where the public authority does not hold the requested information, which causes the Montenegrin regulatory framework to be assessed as not fully compliant with the standard. Furthermore, the legislations of BiH and North Macedonia, although prescribing precise timelines (in North Macedonia, the timeline is at the top of the acceptable range), do not promote prompt responses to the requests, rendering them not fully in line with international standards.

In **BiH**, Article 14, Paragraph 5 of the LFAIB sets a general time limit for the initial response of the public body to the applicant to 15 days. If the public body is unable to comply with the request due to the lack of formal conditions, it shall, as soon as possible, but no later than eight days from the day of receipt of the request, notify the applicant in writing (Article 12, Paragraph 1 of the LFAIB). If the public body receiving the request is not the competent public body, it shall, within eight days from the day of receipt of the request, forward the request to the competent public body and inform the applicant by letter (Article 13, Paragraph 1 of the LFAIB). Same solutions and identical deadlines are provided by the laws of the entities (Articles 13 and 14 of both laws).

In **Montenegro**, the public authority is obliged to act upon the request for access to information within 15 days from the date of the request. If it is necessary to protect life or freedom of a person, the response to the request must be given promptly, and no later than within 48 hours.[132] The specified time limit of 15 days may be extended by the public authority by additional eight days, if the requested information is particularly extensive, if it contains some information that is classified as a secret, or if its identification requires searching a large volume of information, which significantly

[132] Article 31 of the Law.

impedes the regular activities of the public authority. The public authority must inform the applicant about any such extension within five days from the day of receipt of the request. Montenegrin Law on Access to Information does not actively promote prompt response to the request, except in cases of the need to protect life of freedom of a person. However, the prescribed timelines can be considered reasonable.

Montenegrin Law on Access to Information states that, if the public authority does not hold the requested information, it is under the obligation to forward the request to the public authority that holds the information, if it knows which authority it is, and to inform the requester thereof. This provision presents a relativisation of the obligation to assist the requester and of the proactive role of the public bodies in enabling access to information, and it is not in line with relevant international standards.

When it comes to **North Macedonian** legislation, the general norm, included in Article 21, is that the holder of information shall respond to the request for access to information 20 days after receiving the request at the latest. This time limit is at the top of the range considered as acceptable in the RTI rating methodology. North Macedonia does not explicitly state that the holder of information shall respond to the request promptly, or, in other words, it does not actively encourage promptness in handling request for access to information.

This time limit may be extended, if the information holder needs a longer period of time, if it is necessary – due to reasons specified by law – for a part of the document to be withheld, or due to the volume of the requested document. The timeline can be extended for a maximum of 30 days. The information holder is obliged to inform the applicant about the extension of the time limit, seven days after the receipt of the request at the latest. If the information holder fails to act within the specified time limits, the applicant has the right to file a complaint.

The Law of North Macedonia also includes rules for situations where the entity that has received the request for access does not hold such information. In such a case, the public authority is under the obligation to transfer the request to the authority where the information is held, and informs the requester thereof. This needs to be done within three days.

In **Serbia**, there are clear rules of procedure for the public authorities on how to proceed after receiving the request for information and maximum timelines are set by LFAIS (Art. 16 Paras 1-4). Regular procedure time limits are set on 15 days, with a possibility to be extended up to 40 days in total. Urgent procedures are limited to 48 hours, without possibility for extension. These apply when the request relates to information which can reasonably be assumed to have a bearing on the protection of a person's life or freedom and/or the protection of public health and the environment. In such cases, a public authority must inform the applicant whether it holds the requested information, grant access to the document or issue a copy thereof within 48 hours of receipt of the request. In non-urgent cases, the general timeframe is set at 15 days from the receipt of a request at the latest, within which the public authority must inform the applicant whether it holds the requested information or not, and grant access to the

document or send a copy thereof. The LFAIS also envisages the possibility of extending the general timeline, if the public authority is justifiably prevented from observing the 15-day time limit. The public authority is then obliged, within seven days of receipt of the request at the latest, to inform the applicant thereof and set another deadline, which shall not be longer than 40 days. The Law does not regulate in more detail what justified causes the public authorities may invoke. If the request is denied, LFAIS sets some basic rules and time limits in that regard (Art. 16 Para. 12). Namely, if a public authority refuses to inform an applicant, either entirely or partially, whether it holds the requested information, to grant the applicant access or to issue or send a copy of the document to the applicant, it is under the obligation to pass a written ruling, including a rationale, within 15 days of receipt of the request at the latest. The ruling must also indicate the available relief against such decision. If the request refers to insight, i.e. obtaining a copy of a document containing classified information determined by another authority, the authority shall, within eight days from the day of receipt, submit the request to the authority that determined the confidentiality of the information and inform the applicant accordingly. The deadline for acting upon the request by the authority that determined the secrecy of the data shall begin to run from the day of submission. If the request refers to information whose secrecy has been determined by the authority that decides on the request, if the authority determines that the reasons for which the information was classified as secret have ceased, it shall make a decision to declassify and provide the applicant with access to the requested information. If the request is denied because requested information is secret (including professional secret), public authority has to state those reasons in the rationale of the ruling (Art. 16 Paras. 5, 6 and 13).

4. The procedure for dealing with requests is conducted within a reasonable timeline

Indicators	Value	BIH			MKD	MNE	SER
1. Public authorities are required to respond to requests as soon as possible. Clear and appropriate procedures are in place for situations where the authority to which a request is directed does not have the requested information. There are clear and reasonable maximum timelines with clear limits on timeline extensions	0-3	BIH	FBIH	RS			
		2	2	2	2	2	3
Total points		2	2	2	2	2	3
Average points		2	2	2	2	2	3
Standard		4	4	4	4	4	5

Standard 5. Exceptions to free access to information are clearly formulated in law and not extensive, while a public interest override and harm test are envisaged and applied

Indicator 1

The standards in the RTI Law trump restrictions on information disclosure (secrecy provisions) in other legislation to the extent of any conflict.

The legislations of the four analysed countries do not envisage any cases in which there is an absolute presumption that the public's interest to know trumps secrecy provisions. Their legislations, however, generally prescribe that the right to access information can only be restricted in limited cases and following a harm test. The notable exception is Montenegro, which excludes classified information from the scope of the RTI law.

In **BiH**, general right to access to information, with exceptions, is regulated in Articles 4 and 5 of the LFAIB. According to them, there is always a presumption of the justified interest of the public to know. The law stipulates that in each given case the competent public authority may refuse the request, only if it determines that a justified restriction exists or if it finds, after an examination, that disclosure is not in the public interest. Same solutions and identical deadlines are provided by the laws of the entities (Articles 4 and 5 of both laws).

Montenegrin legislation is not in line with this standard. As explained before, the Law excludes from its scope all information classified pursuant to the Law on Data Secrecy.[133] Literally interpreted, this would mean that, when a piece of information is classified, access to it can and will be denied, without conducing the harm test. However, recent jurisprudence of the Montenegrin Administrative Court[134] shows that there is some ambiguity as to whether the Law on Data Secrecy trumps the provisions of the Law on Access to Information in Montenegro. The said case dealt with a request to information which was undoubtedly classified pursuant to the Law on Data Secrecy. In its reasoning, the court did not invoke the absolute exemption of classified data from the scope of the Law on Access to Information, but instead examined whether there was a prevailing public interest to allow access to requested information.

In **North Macedonia**, the Law on Access to Information prescribes in Article 6, Paragraph 1 that the request for access may be denied, if the information requested is classified in accordance with the law, and has an appropriate degree of classification. However, this restriction is not absolute, as the information holder is under the obligation to assess the potential harm to the interest that is protected against the public interest in favour of disclosure.

[133] Law on Data Secrecy (Zakon o tajnosti podataka, *Službeni list RCG*, no. 14/2008, 76/2009, 41/2010, 40/2011, 38/2012, 44/2012, 14/2013, 18/2014, 48/2015 and 74/2020).

[134] Administrative Court of Montenegro, judgment U. 2757/18 of 21.1.2020.

In **Serbia**, according to Article 4 of LFAIS, justified public interest to know shall be deemed to exist whenever information held by a public authority concerns a threat to, or protection of, public health and the environment. With regard to other information held by a public authority, it shall be deemed that justified public interest to know exists, unless the public authority concerned proves otherwise. As already indicated, the provisions of the Law on Tax Procedure and Tax Administration render the norm of Article 4 of the LFIAS ineffective when it comes to tax secrets.

While the regulatory frameworks of BiH, FBiH and the Republic of Srpska, as well as that of North Macedonia are fully in line with international standards, the regulatory framework of Serbia is mostly in line with the standard, and the regulatory framework in Montenegro is not in line with the standard.

Indicator 2

Limitations to the right to access information should be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting, in particular:

i. **national security, defence and international relations**
ii. **public safety;**
iii. **the prevention, investigation and prosecution of criminal activities (with special focus on police when analysing this sector);**
iv. **privacy;**
v. **commercial and other legitimate economic interests;**
vi. **the equality of parties concerning court proceedings;**
vii. **inspection, control and supervision by public authorities;**
viii. **the economic, monetary and exchange rate policies of the state**
ix. **the deliberations within or between public authorities concerning the examination of a matter**

The legislations of the analysed countries are broadly in line with relevant international standards with regards to limitations to the right of access to information.[135] This assessment, however, needs to be put into context. The limitations of the right

[135] There is evidence, however, that they are used in order to permeate the culture of secrecy or conceal corruption. For instance, in BiH, a request for access to information regarding the public call and subsequent award of a contract for restoration of the castle in Banja Luka made by an informal citizens' group was rejected, since the information was deemed to fall under the exemption concerning deliberations within public authorities. This decision was later upheld by the Supreme Court and the Constitutional Court of BIH. See: BiH Constitutional Court, Decision on admissibility and on merits, Ustavni sud BiH, No. AP 461/16 of 6.6.2018. Similarly, a Montenegrin watchdog organisation, MANS, has issued a publication presenting case studies of practices where access to information was denied by invoking limitations prescribed in RTI legislation in order to minimise the flow of information on corrupt government practices. See: MANS, *Tajnama skrivaju korupciju – studije slučajeva*, https://www.mans.co.me/tajnama-skrivaju-korupciju/. Access: 24.2.2022. The above cases are just paradigmatic examples of the divergence between the legislative frameworks and the practices; nevertheless, let us recall that this study does not aim at fully exploring the issue of deficiencies in implementation, but rather focuses on the legislative frameworks.

to information are mostly set forth in RTI laws, with the exception of Montenegro, which sets out these limitations both in the Constitution and in the statute – what is more, the two texts are not congruent. However, absolute exceptions from the scope of RTI law, or relative limitations, subject to the harm test and/or public interest test, are set forth in the laws governing information secrecy, or rather, in the rules and conditions for classification of information. The interplay between RTI laws and laws on classification of information is a complex one, and there are various regulatory solutions that govern this situation. In order for the scope of RTI law to be understood, the legislation on classification of information must also be examined, at least to the extent necessary to clearly identify the type of information that is unambiguously subject to limitations to access. However, there is more. In all four analysed countries, other laws also prescribe various types of secrecy, or rather, various classes of information that must be kept secret or confidential by those who learn them in their official capacity.[136] These classes of secrecy do not fall under the scope of either RTI or classification laws – but the confidentiality must be observed, nonetheless. Some of these classes of information logically fall under the categories that are deemed as justified limitations to RTI, such as professional secret, others – less so. The situation is additionally complicated by the fact that these types of secret information are not defined; instead, their meaning needs to be deduced from the legislator's intention. This often sets a rather broad margin of appreciation, both in the implementation of those laws, and their subsuming under the rules of the RTI or classification laws. Finally, a particular challenge for those working in the public sector lies in the fact that unauthorised disclosure of various types of secrets – and this relates not only to classified information, but also to the information that can be declared secret in terms of other laws – constitutes a disciplinary offence, and, in some cases, even a criminal offence. Therefore, the problem an RTI officer in the public sector can face is a complex one. He/she must take into account not only RTI legislation and legislation governing classification of information, but also be mindful of numerous sectoral laws, so as to make a balanced and lawful decision on whether to allow access and potentially face disciplinary or criminal charges, or invoke one of the prescribed limitations and restrict access. This is why the analysis provided below includes a foray into a complex set of legal acts, including penal legislation, tax and company laws, and laws governing the status of civil servants. It should be seen primarily as an illustration of the complexity of the relevant regulatory framework and a testament of its internal divergence.

1. Limitations in RTI legislation

In **BiH**, the general provision on exemptions is found in Articles 6-8 of the LFAIB. The Law prescribes that the competent public authority may establish an exception in cases where the disclosure of information can reasonably be expected to cause

[136] This also applies to electronic communication and data in electronic form, i.e. to various forms of information carriers. See: M. Reljanović, "Krivičnopravna zaštita elektronskih tajnih podataka", in: S. Gajin (ed.), *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Belgrade 2012, 38-51.

significant damage to the legitimate objectives of the following categories of protected interest:

a) foreign policy, defence and security interests, as well as the protection of public security;
b) the interests of monetary policy;
c) the prevention of crime and any detection of crime; and
d) protection of the decision-making process of a public body in giving opinions, advice or recommendations by a public body, an employee of a public body, or any person performing activities for or on behalf of a public body, and does not include factual, statistical, scientific or technical information.

In **Montenegrin** legislation, the limitations on the right of access to information are prescribed both in the Constitution and in the Law on Access to Information[137]. However, the scope of these exceptions i.e. protected interests differs in these two acts. The table below shows a cross-comparison of these norms.

As can be seen from the table above, the provisions of the Law on Access to Information are not always a legislative operationalization of the constitutional norm. While in some cases the norms of the Law on Access to Information envisage well-founded grounds for both allowed limitations of the right to access and exceptions from the limitations, for instance, with regards to the limitation on the grounds of moral and privacy, in other cases the Law lists too broad a set of grounds for exception. For instance, in the case of criminal proceedings, effectively only the information on the conviction could not be limited pursuant to the Law. Furthermore, the Montenegrin Law on Access to Information introduces new limitations, not envisaged by the Constitution and not fully grounded in relevant international standards. The Law further includes an unnecessary provision, which relates to the security protection, defence, and foreign, monetary and economic policies in accordance with the laws regulating confidentiality of information classified in accordance with secrecy regulations. This is because classified information is already fully exempt from the law. The prescribed possibility of restricting access to information in case it constitutes a business or tax secret according to the law needs to be viewed in the light of the fact that Montenegro does not have a single piece of legislation that regulates the concept of business secret in a uniform manner; instead, this concept is mentioned in many different laws, such as the Law on Business Organisations and Labour Law. This exemption, although not uncommon in comparative practice,[138] needs to be put into context of the existing practices in Montenegro. Namely, in the practices of both Tax Administration and Administrative Court, tax secret provisions have been interpreted as follows: the fact that a piece of information constitutes a tax secret means that it suffices to indicate this fact when conducting the harm test, and that fact, by itself, constitutes a sufficient harm test. While it seems manifest that such interpretation should not be supported, unfortunately, it has been confirmed in the caselaw of the Montenegrin

[137] Article 14 of the Law.
[138] A. – M. Hambre, *Tax Confidentiality – A Comparative Study and Impact Assessment of Global Interest*, Örebro University 2015, www.oru.se/publikationer-avhandlingar, 24.2.2022.

Constitution	**Law on Access to Information**
Life	
Public health	
Moral and privacy	Privacy, pursuant to the law governing personal data protection, except for data related to: - high-ranking public officials where it relates to the discharge of public office, income, property and conflict of interest of those persons and their relatives as per the law governing conflict of interest, - allocated public funds, except social security, health care, and unemployment benefits.
Conducting of criminal proceedings	Crime prevention, investigation and prosecution in order to ensure protection from disclosure of any information referring to: - prevention of committing a criminal offence, - crime reporting and perpetrators, - contents of all actions undertaken in the course of pre-trial and criminal proceedings, - evidence collected through observation and investigation, - secret surveillance measures, - protected witnesses and collaborators of justice, - - effective conduct of the proceedings.
Security and defence of Montenegro Foreign, monetary and economic policy	- Security protection, defence, foreign, monetary and economic policies in accordance with the laws regulating confidentiality of information that is classified in accordance with secrecy regulations.
	Performance of official duty in order to ensure protection from disclosure of any information referring to: - inspection and supervision plans, - public authorities' internal and inter-agency consultations for defining positions for the elaboration of official documents and proposal of decisions for specific cases, - collegiate bodies' actions and decision-making, - initiation and conduct of disciplinary proceedings.
	- Protection of private and commercial interests from disclosure of any information that relates to the protection of competition, as well as of business secrets related to intellectual property rights.
	- If the information constitutes a business or tax secret, in accordance with the law.

Administrative Court.[139] This cannot be considered as compliant with relevant international standards.

In **North Macedonia**, the limitations of the right to access information are set forth in the Law on Access to information, in its Article 6.
The limitations include the following:

1. Classified information, in accordance with the law
2. Personal data the disclosure of which would imply a violation of personal data protection
3. Information the disclosure of which would imply a violation of confidentiality of tax procedure
4. Information obtained or compiled for the purpose of investigation, criminal or misdemeanour procedure, for conducting administrative and civil proceedings, the disclosure of which would have harmful consequences for the course of the proceedings
5. Information endangering intellectual or industrial property rights (patent, model, trademark…).

The limitation related to classified information in fact implicitly includes limitations on the grounds of national security, defence and international relations.
The exception related to the confidentiality of tax procedure relates to the notion of tax secret, defined in the Law on Tax Procedure.[140] This Law sets out as one of its principles the principle of tax secret, which covers all documents, information, data or other facts about the taxpayer that have been obtained in tax, misdemeanour or court procedure, data on inventions or patents or technological procedures applied by the taxpayer, and all business secrets. This exemption seems rather broad; what is more, it protects information that is already protected by the rules of the Access to Information law – industrial property rights. This exception can be interpreted to fall under the "commercial and other legitimate economic interest".

In **Serbia**, LFAIS (Art. 1 Para. 8) stipulates that access to information may, in exceptional circumstances, be subject to limitations set forth in this Law, to the extent necessary in a democratic society to prevent a serious violation of an overriding interest based on the Constitution or law. Preclusions and limitations of free access to information of public importance are deemed to exist in several cases (Art. 9-10 and 13-14).

[139] Administrative Court of Montenegro, Decision U. 7765/18 of 3.7.2019. presented the following position: "More precisely, in view of the legal provisions above, and starting from the fact that the first-instance authority has carried out the harm test regarding disclosure of the information concerned to establish that such disclosure would constitute violation of the Law on Tax Administration regulating the rights and obligations of the tax authority and taxpayers in the process of determining, collecting and controlling taxes and other charges, as well as that this specific case is concerned with a tax secret, the Court hereby finds that both the first-instance and the second-instance authorities properly concluded that no requirements had been met to grant access to the requested information in accordance with Article 13 of the Law on Free Access to Information."

[140] Law on Tax Procedure (Закон за даночна постапка, *Службен весник* на PM no. 13/06; Одлука на Уставен суд У.228/2006, У. 237/06, У. 213/2007, У. 219/2008; *Службен весник на РМ* nos. 105/2009,133/2009,145/2010,171/2010, 53/2011, Одлука на Уставен суд У.112/11; *Службен весник на РМ* 39/2012, 84/2012, 187/2013, 15/15, 97/15, 129/15, 154/15, 23/2016, 35/18, *Службен весник на РСМ* nos. 275/19 and 290/2020).

Namely, a public authority may deny access to information of public importance, if such access would: 1) pose a threat to the life, health, safety or another vital good of a person; 2) threaten, obstruct or impede crime prevention or detection, indictments for a criminal offence, pre-trial proceedings, trial, execution of a sentence, or enforcement of punishment, conducting proceedings in terms of the law governing the protection of competition, or any other legally regulated procedure, or fair treatment and fair trial, until the end of the procedure;[141] 3) pose a serious threat to national defence, national or public security, or international relations,[142] or violate rules of the international arbitration law; 4) significantly reduce the state's ability to manage economic processes in the country, or significantly hinder the realization of legitimate economic interests of the country, or jeopardize the implementation of monetary, foreign exchange or fiscal policy, financial stability, foreign exchange reserve management, supervision of financial institutions or issuing banknotes and coins; 5) make available information or a document classified pursuant to law or an official act based on law, or which constitutes a business or professional secret, or information obtained in the process of representation, where the represented person did not authorise such disclosure, pursuant to the law governing the work of the Public Attorney's Office, the disclosure of which could have severe legal or other consequences for the interests protected by law that prevail over the public's right to know; 6) violate the right of intellectual or industrial property or endanger the protection of artistic, cultural and natural assets; 7) endanger the environment or rare plant and animal species. These limitations were introduced by the 2021 amendments to the Law and differ from its previous wording, as they extend the scope of possible limitations. It is particularly striking that they include exemptions such as proceedings related to protection of competition , given that this was previously used by public authorities as grounds for denying access to information in some high-profile cases, and such decisions were later overturned by the Commissioner for Information of Public Importance and Personal Data Protection.[143]

A public authority does not have to allow an applicant to exercise his/her right to access information, if such information has already been published and made accessible nationwide or online. In that case, the authority shall, in response to the request, indicate the information carrier (official gazette number, title of the publication, etc.), where and when the requested information was published, unless it is generally known.

[141] Such treatment is incriminated as a criminal offence in the Criminal Code (Krivičnik zakonik, *Službeni glasnik RS*, nos. 85/2005, 88/2005 – correction, 107/2005 – correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). According to the criminal offence "Violation of Confidentiality of Proceedings" (Art. 337) "(1) Whoever without authorisation discloses information he has come by in connection with court, minor offences, administrative or other proceedings established by law, where the law stipulates that such information may not be made public, or has been declared confidential by a decision of the court or other competent body, shall be punished by a fine or imprisonment of up to one year. (2) Whoever without permission of the court makes public the course of proceedings against a juvenile or the disposition reached in such proceedings, or who makes public the name of the juvenile against whom proceedings were conducted, or information that may reveal the identity of the juvenile, shall be punished with imprisonment of up to two years. (3) Whoever without authorisation discloses information on the identity or personal data of a person protected in criminal proceedings, or data regarding a special protection programme, shall be punished by imprisonment of from six months to five years. (4) If the offence referred to in Paragraph 3 of this Article results in serious consequences for the protected person or the criminal proceedings are prevented or hindered to considerable extent, shall be punished by imprisonment from one to eight years."

[142] This exception is elaborated in Data Secrecy Law.

[143] See, for instance decisions of the Commissioner for information of public importance and personal data protection no. 07-00-00381/2013-03 of 26.11.2014. and no. 07-00-02115/2011-03 of 14.6.2012.

Another limitation is provided for in Article 14 of the Law. The authority may restrict the applicant's exercise of access to information of public importance, if this would violate the right to privacy, the right to protection of personal data, the right to reputation, or any other right of the person to whom the requested information relates, except: the person agreed to it; if it is a person, occurrence or event of public interest, and especially if it is a public official in terms of the law governing the prevention of conflicts of interest in performing public functions, and if the information is related to the performance of his/her public function; if it is a person whose behaviour gave rise to the request for information. Information of public importance from a document containing personal data may be made available to the applicant in a way that ensures that the public's right to know and the right to protection of personal data can be exercised together, to the extent prescribed by law governing personal data protection and by LFAIS. It is unclear how the given provision relates to the severability clause, which is also envisaged by the LFAIS, as the LFAIS does not give clear primacy to any of the two regimes. This formulation, therefore, provides a wide margin of appreciation, which is a definite step back from the previous wording of the law.

2. Legislation on classified information

The **BiH** Law on Protection of Classified Information[144] (hereinafter: LPCIB) defines classified information as "a fact or means relating to public security, defence, foreign affairs or intelligence and security activities of Bosnia and Herzegovina, which must, in accordance with the provisions of the Law, be protected from unauthorized persons and which has been classified by an authorized person. Classified information is one whose disclosure to an unauthorized person, the media, organization, institution, body or other state, or body of another state, could cause a threat to the integrity of Bosnia and Herzegovina, especially in the area of: a) public safety, b) defence, c) foreign affairs and interests, d) intelligence and security interests of Bosnia and Herzegovina, e) communication and other systems important for state interests, judiciary, projects and plans important for defence and intelligence-security activity, f) scientific, research, technological, economic and financial affairs of importance for the security of the functioning of the institutions of Bosnia and Herzegovina, i.e. security structures at all levels of the state organization of Bosnia and Herzegovina." (Article 4, Paragraph 1, P. a) and Article 8). However, according to Article 9 of the same Law, the information by which secrecy is determined with the intention of concealing a committed criminal offense, exceeding or abuse of authority, with the aim of concealing any illegality or concealing an administrative error, will not be considered as classified information. LPCIB regulates four levels of data secrecy: "top secret", "secret", "confidential" and "restricted" (Article 19 and 20). It is important to emphasize that Article 86 of the same Law contains provisions on former and actual types/levels of data secrecy: "Classified information ... in the transitional period, shall be processed as follows: a) data marked

[144] Law on protection of classified information (Zakon o zaštiti tajnih podataka, *Službeni glasnik BiH*, nos. 54/05 and 12/09).

STATE SECRET as TOP SECRET, b) information marked OFFICIAL or MILITARY SECRET – STRICTLY CONFIDENTIAL as SECRET, c) information marked OFFICIAL or MILITARY SECRET – CONFIDENTIAL as CONFIDENTIAL, d) data marked OFFICIAL or MILITARY SECRET – INTERNAL as INTERNAL. This was important during the established transitional period (which lasted for three years), in which all other laws had to be harmonized with this Law.

The **Montenegrin** Law on Data Secrecy[145] envisages that classified data is data whose disclosure to an unauthorised person would or could incur damaging consequences to security and defence, foreign, monetary or economic policy of Montenegro. This Law further states that classified information of foreign states and international organisations so marked and forwarded to the competent bodies in Montenegro is also considered classified information. The classification of information, according to the legislation of Montenegro, is not limited to the defence and security sector only, but is broader in scope, as it relates to the issues of foreign, economic and monetary policy of the country.

The Law on Data Secrecy of Montenegro further envisages that information can be classified, if this is necessary in a democratic society, and if the protected interest overrides the interest for free access to information. It envisages four degrees of classification: TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED.

The Law on Data Secrecy includes an important provision, stating that data cannot be classified in order to conceal committing of a criminal offence, endangerment of the environment, limitation of competition, excess or abuse of power, unlawful act or action or administrative error of a public authority. The Law, however, does not expressly state that if information is classified in contravention of this rule, it is not deemed as classified.

The legislative framework of Montenegro is not in line with relevant international standards. Furthermore, it is clearly not internally aligned. Various pieces of legislation contradict each other and the resulting whole makes for an incoherent national system. It is worth noting that the Law on Data Secrecy of Montenegro envisages that disclosure of classified information to an unauthorised person constitutes a misdemeanour.[146]

The most important law in **North Macedonia** according to which information can be classified is the Law on Classified Information.[147] According to this Law, classified information is information from the scope of public authorities, which refers to the public security, defence, foreign affairs or security or intelligence activities of the state, and which, according to law, must be protected from unauthorized access, and is marked with an appropriate degree of classification in accordance with this law.

The North Macedonian Law on Classification of Information further states that classified information may also include documents, technical means, machinery, equipment, i.e. separate components or weapons or tools that have been produced or are in the process of production, as well as confidential inventions related to defence and of

[145] Article 3 of the Law.

[146] Article 82 of the Law.

[147] Law on Classified Information (Закон за класифицирани информации, *Службен Весник на РСМ*, no. 275/2019).

interest to the security of the state. This means that the notion of classified information is set within the defence domain and along the lines of the Tshwane Principles. The Law supports this conclusion by stating in Article 7 that the information subject to classification in particular relates to: a) public safety, b) defence, c) foreign affairs, d) security, intelligence and counterintelligence, e) systems, devices, inventions, projects and plans relevant for public safety, defence and foreign affairs, and f) to scientific research and technological, economic and financial matters of importance for the state.

The Law envisages the following four degrees of classification: STATE SECRET, SECRET, CONFIDENTIAL and RESTRICTED.[148] However, the Law stipulates in Article 12 that the information the disclosure of which would reduce the efficiency of operation of state and local government bodies and the legal entities established by them, shall be marked with „FOR RESTRICTED USE", and even though this is not a degree of classification, free access shall not be allowed to information so labelled. This is a rather problematic provision, since it leaves ample room for discretion. Public bodies have a wide margin of appreciation they can resort to in deciding not to classify information, but to mark it with "for restricted use". This way they can prevent free access to information, which may not be related to the defence, public safety or other protected interests that are otherwise set forth when defining classified information.

In Article 21 the Law also states that, if the classified information conceals exceeding of powers, abuse of office or any other unlawful act, or a punishable offence, such information will not be considered classified.

Data Secrecy Law[149] (hereinafter: DSL) of **Serbia** restricts access to data of importance to the Republic of Serbia, which is marked with a certain degree of secrecy in a legally prescribed procedure and according to legally determined criteria. Data of interest to the Republic of Serbia is any data or document available to a public authority, which refers to territorial integrity and sovereignty, protection of the constitutional order, human and minority rights and freedoms, national and public security, defence, internal affairs and foreign affairs (DSL, Art. 2 Para. 1 P. 1). However, data labelled as classified with purpose of concealing crime, exceeding authority or abusing office, or with a view to conceal some other illegal act or proceedings of a public authority, shall not be considered classified (DSL, Art. 3). DSL regulates four levels of data secrecy: "top secret", "secret", "confidential" and "restricted" (Art. 14). In practice, information classified to a certain degree of secrecy was, as a rule, excluded from the scope of the LFAIS.[150]

However, it should be noted that a clear boundary of the scope of classification of certain data has been established in the practice of the Serbian Commissioner for Access to Information of Public Importance and Personal Data Protection. Namely, in the decision 07-00-00865/ 2014-03 of 30 May 2014, the Commissioner ordered the Security Information Agency (BIA) to submit data on the number of persons against whom specific investigative measures regarding wiretapping means of communication

[148] Article 8 of the Law.

[149] Data Secrecy Law (Zakon o tajnosti podataka, *Službeni glasnik RS*, no. 104/2009).

[150] This also refers to the data that the Serbian authorities receive through international exchange. See: M. Reljanović, „Međunarodna saradnja Republike Srbije u razmeni i zaštiti tajnih podataka", in: S. Gajin, G. Matić (eds.), *Primena Zakona o tajnosti podataka*, Belgrade, 2014, 46-66.

were requested, emphasising that statistical processing of data on wiretapped persons cannot pose a real threat to the security of the state, as BIA asserted when rejecting the request to publish the requested information. Furthermore, the Commissioner stated on the issue of how information from a classified document should be made available as information of public importance: "In addition to the fulfilment of the formal condition, which implies that the classification of the document or the contained data was made in accordance with the provisions of the Law on Data Secrecy ("Official Gazette of RS" No. 104/09), it is necessary to assess the fulfilment of another essential, material condition, whether the disclosure of such information could have serious legal or other consequences for the interests protected by law and which of the two interests is more important." The case in question, however, did not result in access to information being granted to the requester. Quite the opposite, the requester had to file an application to the European Court of Human Rights (ECtHR),[151] due to not having been granted access by the BIA. In assessing whether the restrictions at issue had been in accordance with domestic law, the ECtHR found that they were not.

A similar position to that of the Serbian Commissioner cited above was also taken by the Serbian Constitutional Court. Namely, in its decision UŽ-1823/2010 of May 23, 2013, it stated as follows: "... The Constitutional Court assesses that 'necessity in a democratic society' is a factual issue that must be assessed in each specific case. It follows that the fact that a document is formally and legally classified as a strictly confidential document is not sufficient to deny public access, but it is necessary that behind that classification there exists the interest to be protected, which in concrete circumstances prevails over the right of the public to know."

The Administrative Court, however, takes a different standing, which is evident in a number of its decisions. For instance, in its judgment in the case 25 U.1210/18 of June 22, 2018, the Administrative Court supported the position of the Ministry of Defence and annulled the decision of the Commissioner ordering the publication of information contained in the personal files of employees and former employees of the Army of Serbia (Yugoslavia). The Administrative Court thereby supported the view that, in cases where data or a document is declared confidential, the test of overriding interest is not required and that only stating the regulations according to which the classification of data as confidential was performed is considered a sufficient (adequate) test of the competent authority.[152]

[151] European Court of Human Rights, *Youth Initiative for Human Rights v. Serbia*, Application no. 48135/06.

[152] Similar views of the court were expressed in the judgments in the cases: 17 U.1209/18 of 11.5.2018; 22 U.1203/18 of 19.10.2018.; 21 U.1207/18 of 31.20.2018, as well as a number of other cases initiated based on requests for access to information of public importance submitted by the civil society organization Humanitarian Law Centre, after the Ministry of Defence denied the requested information. Such reasoning is not a consequence of the interpretation of only the regulations on confidential data of significance for the defence of the country, but it is rather general standard of interpretation of the law, and that standing is clearly visible from the position of the Administrative Court in the judgment in case 22 U.8346/18 of 19.10.2018,which contains identical reasoning used in relation to data marked as confidential under the Law on Prevention of Money Laundering and Terrorist Financing. The opposite practice of the Administrative Court, however, existed in relation to the same Law and the reports of the Directorate for the Prevention of Money Laundering of the Ministry of Finance in the judgment in case 9 U.2489/11 of 8.3.2013, when the court found that this Directorate "was obliged to prove that it acted in accordance with the LFAIS", precisely insisting that in addition to the formal fulfilment of the conditions, it is necessary to prove that there will be real damage to the public interest, if the information in question was published. It can therefore be concluded that the caselaw of the Administrative Court has evolved over time into a very narrow interpretation of the obligation of the competent authority, when it comes to this issue.

3. Secrecy provisions in other laws

There are additional rules in **BiH** on exceptions regarding confidential commercial information and privacy protection. Namely, where the competent public authority justifiably determines that the request for access to information involves confidential commercial interests of a third party, the competent public authority shall, by urgent procedure, inform the third party by letter of the details of the request. The notice sent by letter informs the third party about the immediate disclosure of information, if the third party does not respond by letter, within 15 days of receipt of the letter, that he considers such information confidential, and states the reasons for damage arising from disclosure. Upon receipt of such a response, the competent public authority shall establish an exception. With regards to privacy protection, the BiH law states that the public authority establishes such an exception, when it reasonably finds that the information requested includes personal interests relating to the privacy of a third party."

All of these exceptions are further elaborated by special laws.

Same exceptions are determined in entity laws, except that, logically, instead of foreign policy, defence and security interests, as well as the protection of public security and interests of monetary policy, which are under exclusive jurisdiction of BiH, exceptions are restricted to defence and security interests, as well as the protection of public safety.

According to Article 38, Paragraph 1 of the Company Law of the **Republic of Srpska**[153], a business secret is considered to be information on business, determined by the founding act, deed, or by the partnership agreement, or the agreement of the members of the company, i.e. by the founding act, or the statute of a joint stock company, which is obvious to cause significant damage to the company, if it comes into the possession of a third party. However, information whose disclosure is mandatory in accordance with the law, or which is related to the violation of the law, good business practices or principles of business ethics, including information for which there is a reasonable suspicion of existence of corruption, cannot be considered a business secret, and the publication of this information shall be deemed legal, if it aims at protecting the public interest (Article 38, Paragraph 2). Unauthorized disclosure of a trade secret is provided for as a misdemeanour under the same Law, and the person who disclosed a trade secret must compensate for the damage caused by it. Business secret is defined in Article 38 of the Company Law of **FBiH**[154] as business information which can obviously cause significant harm to the company, if it comes into the possession of a third party without the consent of the company. The data that are public under the law and other regulations and data regarding violation of law and other regulations, cannot be classified as a business secret. Trade secret means information specified as such by the law or rules of a business organization or legal entity for which the owner has taken reasonable steps to keep it secret, and the disclosure of which to an unauthorized person could have detrimental effects on the business organization's or a legal entity's economic interests.

[153] Company Law of the Republic of Srpska (Zakon o privrednim društvima Rep. Srpske, *Službeni glasnik Rep. Srpske*, nos. 127/2008, 58/2009, 100/2011, 67/2013, 100/2017 and 82/2019).

[154] Company Law of the FBiH (Zakon o privrednim društvima FBiH, *Službeni list FBiH*, no.81/2015).

In **Montenegro,** tax secret is envisaged in the Law on Tax Administration,[155] which prescribes the obligation of the tax authority to keep the tax secret. Article 16 of this law offers a definition of the tax secret as any information or dataset on the tax debtor held by the tax authority, except for certain categories of information.[156]
Labour Law[157] prescribes in Article 171 that one of just causes for dismissal is disclosure of a business secret so determined by the employer. The Company Law[158] defines a business secret as information or dataset that is not fully generally known or available to persons who otherwise operate with this type of data, which has an economic value due to not being generally known, and which is subject to appropriate measures aimed at protecting its confidentiality. Business secret also covers information so declared by the law.[159] The Company Law envisages that the founders of the company, its members, majority shareholders, CEOs, liquidators, but also employees, have to keep the confidentiality of the company's business secret. It also envisages certain exceptions from this obligation[160] in cases when the obligation to disclose is established by law or a decision of the competent state authority, if disclosure is in the company's interest, or if disclosure was done in order to inform the public of a punishable offence. Business secret is also prescribed in the Law on Tourism and Hospitality, Law on Notaries, Law on Public Enforcement Agents, Law on Competition and numerous other laws.

Legislation of **North Macedonia** also envisages other types of secrets, such as business secret in the Law on Labour Relations[161], the Company Law[162] or a bank secret in the Law on Banks[163], etc. However, the provisions of the mentioned laws do not use the term "classified information" in the sense in which it is used in the Law on Access to Information. The exemption should, therefore, be interpreted strictly and understood only as relating to classified information in accordance with the Law on Classified Information.

In Serbia, business secret is defined in a general manner by the Law on protection of business secrets. Its Article 2 defines business secrets as information that meet one of the following criteria:

[155] Law on Tax Administration (Zakon o poreskoj administraciji, *Službeni list RCG*, nos. 65/01, 80/04, 29/05, 20/2011, 28/2012, 8/2015, 47/2017 and 52/2019).
[156] These categories are: information declared as not being a tax secret by the tax debtor in writing; information that cannot be linked to a specific tax debtor or cannot be otherwise identified; information related to the existence of a tax debt, if the security is registered in public records; information on registration of the tax debtor; information on the value of immovable property and the list of the tax debtor published quarterly by the tax authority.
[157] Labour Law (Zakon o radu, *Službeni list RCG*, no. 74/2019 i 8/2021).
[158] Company Law (Zakon o privrednim društvima, *Službeni list RCG*, no.65/2020).
[159] Article 43 of Montenegrin Company Law.
[160] Article 44 of Montenegrin Company Law.
[161] Law on Labour Relations (Закон за работните односи, *Службен Весник на РМ*, nos. 62/2005, 106/2008, 161/2008, 114/2009, 130/2009, 50/10, 52/10, 124/10, 47/11, 11/12, 39/12,13/13, 25/13, 170/13, 187/13, 113/14, 20/15, 33/15, 72/15, 129/15, 27/16, 120/18 *and Службен весник на РСМ* no. 267/20), Article 35.
[162] Company Law (Закон за трговските друштва, Службен Весник на РМ, nos. 28/2004, 84/2005, 25/2007, 87/2008, 42/10, 48/10, 24/11, 166/12, 70/13, 119/13, 120/13,187/13, 38/14, 41/14, 138/14, 88/15, 192/15, 6/16, 30/16, 61/16, 64/18, 120/18 and *Службен Весник на РСМ* no. 290/20).
[163] Law on Banks (Закон за банките, *Службен весник по*. 67/07, 90/09, 67/10, 26/13, 15/15, 153/15. 190/16 и 7/19 and *Службен весник на РСМ* no.101/19, 122/21).

(1) they are not generally known, or they are not known or easily accessible in terms of the structure and set of their components to persons who in the course of their activities normally come into contact with this type of information;
(2) have commercial value because they represent a secret;
(3) the person lawfully controlling them has, in the given circumstances, taken reasonable steps to maintain their secrecy".

Article 240 Para. 1 of the Criminal Code of **Serbia**[164] (hereinafter: CC) also incriminates disclosure of a business secret, but also the act of obtaining it without authorisation, envisaging the sanction of imprisonment from six months to five years for this offence. The CC also provides its own definition of the notion of business secret, which covers "information and documents defined by law, other regulation or decision of competent authority issued pursuant to the law as a commercial secret whose disclosure would cause or could cause harmful consequences to the enterprise or another commercial entity." Article 17 of the Law on protection of business secrets, however, sets boundaries on what can be considered as one, excluding from its scope of application the following cases: exercise of the right to freedom of expression and information, in accordance with the Constitution of the Republic of Serbia, the European Convention for the Protection of Human Rights and Fundamental Freedoms and judgments of the European Court of Human Rights, the Charter of Fundamental Rights of the European Union, laws on information of public importance, as well as the law governing public information and media, in accordance with the freedom and diversity of the media; disclosure for the purpose of disclosing criminal offenses and other illegal acts, provided that the person who obtained, used or disclosed a business secret acted for the purpose of protecting the public interest; disclosing a business secret by employees to their representatives within the legal performance of the function of a representative, in accordance with special regulations, provided that the disclosure of a business secret was necessary for the legal performance of the function of a representative; in order to protect the rights recognized by a special law; disclosure in connection with the provision of legal assistance to lawyers in accordance with the regulations governing the position of the bar.

While in general it could be argued that the existence of a single piece of legislation governing business secret is a good regulatory solution, which aims at reducing fragmentation, the actual norms of the relevant Serbian law are problematic. In fact, they can be assessed as backsliding, when compared to the previous regulatory solution in Serbia. A useful illustration of such backsliding can be found in the wording of the exception envisaging that the provisions of the Law shall not apply in cases of disclosing criminal offences. This means that such information still has a character of a business secret. Conversely, the previous Serbian law envisaged that such information would no longer have the character of a business secret. Furthermore, the way in which the Law on the protection of business secrets defines a business secret seems to be subject to a wide margin of appreciation e.g. on the part of the employer, who could declare almost any type of information as a business secret in a company bylaw or even a labour contract.[165]

[164] Criminal Code of Serbia (Krivični zakonik Srbije, *Službeni glasnik RS*, nos. 85/2005, 88/2005 - correction, 107/2005 – correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019).

[165] See for examples of abuses under the previous law: M. Reljanović, *Zlostavljanje nije poslovna tajna*, https://pescanik.net/zlostavljanje-nije-poslovna-tajna/, 24.2.2022.

It should be noted that business secret is also regulated by the Company Law, in a similar manner (Articles 72 and 73): "Business secret is information whose disclosure to a third party could harm the company, as well as information that has or may have economic value because it is not generally known, nor is it easily accessible to third parties that could benefit economically by its use or disclosure. Business secret is also information that is determined as a business secret by law, other regulation or act of the company. ... Disclosure of data ... shall not be considered a violation of the duty to maintain business secrets, if such disclosure is: 1) obligation prescribed by law; 2) necessary for the purpose of performing business or protecting the interests of the company; 3) done to the competent authorities or the public solely for the purpose of pointing out the existence of an act punishable by law."

In the practice of the Commissioner for Access to Information of Public Importance and Protection of Personal Data, in several cases, situations have been considered as to whether information that was classified as a business secret could be treated as information of public importance. Of particular importance in this regard was the decision of the Commissioner in the case of "Železara Smederevo d.o.o.", which emphasised that the LFAIS is a *lex specialis* in relation to certain other laws by which information might be declared as secret – in that sense, it was sufficient that some information meets the requirements of LFAIS to be considered that there was a public interest to know it. In similar circumstances in the "Air Serbia" case, the Commissioner emphasised that "the reasons for denying access to information cannot be abstract and hypothetical, but must be concrete, clearly identifiable and in relation to concrete information. Arguments for denying access to information cannot be based only on the assumption of the first instance body about the possible behaviour of the other contracting party, i.e. a foreign partner in the business that is the subject of the contract." In the situation when the public company declared the information on environmental protection to be a business secret, the Commissioner ordered their publication, noting that this is information that is of exceptional importance to the public. Finally, in one of its decisions the Commissioner pointed out: "In order for the first instance body to restrict access to information of public importance with a call for confidentiality of information, it is obliged to prove in the conducted procedure that it is necessary in a democratic society to protect the overriding interests comparing to the interest of the public to know. This implies convincing evidence of possible real harmful consequences in the event that the information is made available to the public, and not highlighting only a formal reason, i.e. the fact that the information is a business secret."

There is no particular law on professional secret. CC incriminates "Unauthorised Disclosure of Secrets" (Art. 141): "(1) Lawyers, physicians or other persons who disclose without permission secrets that had come to their knowledge during the performance of their professional duties, shall be punished with a fine or imprisonment of up to one year. (2) Whoever discloses a secret in public or in other person's interest when such interest prevails over the interest of non-disclosure of the secret shall not be punished for the offence referred to in Paragraph 1 of this Article." It is clear that professional secret is not absolute and cannot be viewed on the same level with classified information that the state has classified as secret. There is, however, no closer determination what may be considered as prevailing interest.

As already mentioned, Criminal Procedure Code[166] (hereinafter: CPC) regulates exclusions from the duty of testifying in cases of professional secret (Art. 93 Para 1. P. 2-3): "The duty to testify does not apply to: ... 2) a person who would by his statements violate the duty of maintaining confidentiality of information acquired in a professional capacity (a religious confessor, lawyer, physician, midwife, etc.), unless released from such obligation by a special regulation or a statement of the person for whose benefit the confidentiality was established; 3) a person who is the defence counsel, in connection with what he was told by the defendant." All these types of professional secret have been recognized in the Law on Civil Procedure as well (Art. 248 Para. 1): "A witness may refuse to testify about: 1) what the party has entrusted to him as its proxy; 2) what the party or other person confided in the witness as a religious confessor; 3) facts learned by the witness as a lawyer, doctor or in the exercise of another occupation, if there is an obligation to maintain professional secrecy."

Law on Advocacy regulates "lawyers' secret": "A lawyer is obliged, in accordance with the statute of the bar association and the code, to keep as a professional secret and to make sure that the persons employed in his/her law office do the same, everything that the client or his/her authorized representative entrusted to him/her, or in the case in which he/she provides legal assistance in another way learned or obtained, in preparation, during and after the termination of representation."

On the other hand, one's medical records are secret both by the law on health documentation and records in the field of healthcare (Art. 7) and the Law on personal data protection (Art. 17 Para. 1). Exceptions to the duty of keeping medical professional secret are linked to restrictions from various laws: a doctor may violate the duty of custody over professional secrets, when required by law, based on the patient's explicit consent, if a patient is physically, mentally or legally incapable of making his/her own decisions, as well as if revealing of the data is in public interest.

As elaborated before, the Law on Tax Procedure and Tax Administration regulates the tax secret.

The norms regulating secrecy or confidentiality of data and business secrets in the laws of the analysed countries do not seem unproportionate. In some cases they seem to reiterate, in specific terms, the confidentiality requirements already set forth in the Law on Personal Data Protection – for instance, the Montenegrin Law on Tourism and Hospitality sets out the obligation of the tourist agency not to disclose personal data of the travellers, which at any rate should not be disclosed as per personal data protection regulations. This approach may be attributed to the remnants of the previous legislative interventions that had preceded the adoption of personal data laws, and also to the sometimes overly formalistic approach in legislation of the countries included in the analysis, whereby sectoral laws need to regulate certain issues in considerable level of detail. In other cases, the definition of business secrets or the categorisation of certain information as classified is indeed in line with the relevant sectoral standards. However, despite the observed proportionality of the norms regulating business secrets or confidentiality in a variety of laws, their relations with the access to information

[166] Criminal Procedure Code of Serbia (Zakonik o krivičnom postupku, *Službeni glasnik RS*, nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019).

laws are not clearly regulated. This provides a broad field for interpretation and a wide margin of appreciation in deciding on whether to allow access to information or not.

4. Criminal offences related to disclosure of secrets

Criminal Law of **BiH**[167] (hereinafter: CLB) contains several norms on information secrecy. Article 1, Paragraph 24 contains another definition of classified data: Closer analysis, however, shows that this definition is the same as the one from the LPCIB, except it has been adapted for the use in CLB (contains appropriate reference to LPCIB).

CLB incriminates "espionage", among other things, as disclosing classified information, handing it over or making it available to a foreign state, foreign organization or a person who serves them, or obtaining information for that purpose (Article 163, Paras. 1 and 4). There is an additional incrimination for disclosing classified information (Article 164). However, it is stipulated in the same Article (Paragraph 9) that there is no criminal offense of disclosing classified information, if someone publishes or mediates in disclosure of classified information whose content is contrary to the constitutional order of BiH, with the aim to reveal to the public irregularities related to the organization, operation or management of the service, or with the aim of disclosing to the public facts that constitute a violation of the constitutional order or an international treaty, if the publication does not have serious detrimental consequences for BiH.

Criminal Procedure Law of **BiH**[168] (hereinafter: CPLB) contains outdated terminology and mentions types of classified information that are no longer used, contrary to the cited provision of Article 86 of the LPCIB. Same discrepancies are repeated in the Law on Civil Service in the Institutions of Bosnia and Herzegovina[169] (hereinafter: LCSB). Namely, Article 54 of that law prescribes disclosure of state, military and official secrets, as well as violation of the regulations on keeping these secrets, as a violation of official duty, for which disciplinary liability is provided. LCSB, however, does not contain a definition of these terms.

Criminal Code of the **Republic of Srpska**[170] (hereinafter: CLRS) and Criminal Law of the **FBiH**[171] (hereinafter: CLFBiH) contain almost identical definitions of several relevant terms (Article 123, Paragraph 1 of the CLRS and Article 2 of the CLFBiH).

[167] Criminal Law of BiH (Krivični zakon BiH, *Službeni glasnik BiH*, nos. 3/2003, 32/2003 – correction, 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015 and 35/2018).

[168] Criminal Procedure Law of BiH (Zakon o krivičnom postupku BiH, *Službeni glasnik BiH*, nos. 3/03, 32/03 – correction, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 29/2007, 53/07, 58/08, 12/09, 16/09, 53/09 – other law, 93/09, 72/13 and 65/18).

[169] Law on Civil Service in the Institutions of Bosnia and Herzegovina (Zakon o državnoj službi u institucijama BiH, *Službeni glasnik BiH*, nos. 12/02, 19/02, 8/03, 35/03, 4/04, 17/04, 26/04, 37/04, 48/05, 2/06, 50/08 – other law, 43/09, 8/10, 40/12 and 93/17).

[170] Criminal Code of the Republic of Srpska (Krivični zakonik Rep. Srpske, *Službeni glasnik Rep. Srpske*, nos. 64/2017, 104/2018 – decision of Constitutional Court and 15/2021).

[171] Criminal Law of the FBiH (Krivični zakon FBiH, *Službeni list FBiH*, nos. 36/2003, 21/2004 – correction, 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 and 75/2017).

Firstly, secret is defined as a piece of information or a document determined by law, other regulation or general act of a competent body adopted pursuant to the law, the disclosure of which would have harmful consequences for the security or interest of the entity. Official secret is defined as information or a document that has been declared an official secret by the law, another regulation or a general act of the competent institution adopted pursuant to the law. Professional secret is specified as information on the personal or family life of the parties that is learned by lawyers, defence attorneys, notaries, doctors or other health workers, religious ministers and other professionals in the performance of their profession or occupation. Business secret is considered to be information and documents that have been declared a business secret by law, other regulation or decision of the competent authority of a company, the disclosure of which could have harmful consequences for a company or other legal entity.

CLFBiH contains a definition of the military secret,[172] as information or a document that has been declared a military secret by law, other regulation or an act of the competent body of the Federation adopted pursuant to the law.

The basic criminal offence of unauthorised disclosing a secret of **Republic of Srpska** is incriminated in Article 292 of the CLRS. Article 291 of the same Law contains incrimination of the criminal offence of espionage. Among other actions, the act of committing this crime includes disclosure, surrendering of or making available secret economic or official data or documents to a foreign state, foreign organization or a person who serves them, as well as obtaining classified information or documents with the intention of disclosing them or handing them over to a foreign state, foreign organization or a person serving them. CLRS also contains an incrimination of unauthorised disclosure of official secret (Article 323). Further on, official secret is defined as secret data, whose disclosure would have or could have detrimental consequences for the service. However, the term "service" is not further elaborated. Finally, Article 337 of the CLRS regulates the criminal offense of violating the secrecy of court proceedings.

Criminal offence of unauthorised disclosing a secret of the **FBiH** and espionage (Articles 158 and 157) is incriminated in the similar manner as in the **Republic of Srpska,** except that it covers military secret as well. Article 388 contains the incrimination of unauthorized disclosure of official secret. There will be no such criminal offence, in case that information that has been declared as official secret is used or published, if its content is contrary to the constitutional order of the FBiH, with the aim of revealing irregularities in the organization, operation and management of the service, provided that such publication has no harmful consequences for the FBiH. Finally, Article 350 of the CLFBiH regulates the criminal offense of violating the secrecy of court proceedings.

Article 154 of the CLRS contains incrimination of the unauthorized disclosure of professional secret by "lawyer, doctor or other person". Unauthorized disclosure of professional secret in FBiH is incriminated by Article 187 of the CLFBiH and it covers information learned in the exercise of their profession by lawyer, defence counsel, notary public, medical doctor, dentist, midwife or other health care professional, psy-

[172] Article 2 of the Law.

chologist, guardianship worker, religious confessor or any other person in the exercise of his/her profession, unless disclosure has been made in the general interest or in the interest of another person that outweighs the interest of secrecy. As previously mentioned, on the basis of the Criminal Code and the Code of Criminal Procedure of the Republic of Srpska and FBiH, it can be concluded that professional secrecy refers to a large number of explicitly mentioned professions and activities.
Disclosure and unauthorized acquisition of a trade secret is stipulated by Article 259 of the CLRS and by Article 254 of the CLFBiH, as well as criminal offence of disclosure and use of stock exchange classified information (Article 255).

The Criminal Code of **Montenegro**[173] envisages a number of criminal offences related to disclosure of certain types of secrets. First of all, the Criminal Code envisages the criminal offence of disclosure of a business secret.[174] Montenegro does not have a systemic law that regulates the notion of a business secret; instead, it is regulated only indirectly in a number of other laws, such as the Law on the Protection of Competition, Company Law, Obligation Relations Law, Law on Public Procurement, Law on Official Statistics, Law on Customs Service, Law on Banks etc.).[175] The Criminal Code also defines a business secret as information and documents that are declared a business secret by a law, other regulation or decision of a competent authority, the disclosure of which would or could cause harmful consequences for a company. This determination is not very helpful; what is more, it leaves ample room for discretion. Further, the Criminal Code of Montenegro envisages two criminal offences that sanction the disclosure of data classified pursuant to the Law on Data Secrecy: the criminal offence of espionage,[176] which entails disclosure of classified data to a foreign state, foreign organisation or a person serving them, and the criminal offence of disclosure of classified data, which entails disclosing, handing over or otherwise making available classified data to an unauthorised person.[177] A qualified offence exists, if the crime was committed during a state of war, armed conflict or a state of emergency. The Criminal Code states that data directed towards endangering the constitutional order and safety of Montenegro, grave violations of fundamental human rights, and the data aimed at concealing a committed criminal offence punishable by imprisonment of up to five years or more are not considered classified in terms of the latter criminal offence. The Criminal Code of Montenegro also envisages the criminal offence of violation of secrecy of proceedings,[178] which entails unauthorised disclosure of information learned in court, misdemeanour, administrative or other proceedings, which cannot be published according to law, or which has been declared secret by a ruling of the court or other competent authority.

[173] Criminal Code of Montenegro (Krivični zakonik Crne Gore, *Službeni list RCG*, nos. 2003, 13/2004, 47/2006, 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, 49/2018, 3/2020 and 26/2021).
[174] Article 280 of the Law.
[175] Institut Alternativa, *Poslovne tajne javnih preduzeća - Paradoksi prakse u Crnoj Gori*, http://media.institut-alternativa.org/2019/10/poslovne-tajne.pdf, 24.2.2022.
[176] Article 368 of the Law.
[177] *Ibid.,* Article 369.
[178] *Ibid.,* Article 391.

The Montenegrin Law on Civil Servants[179] stipulates that disclosure of confidential data constitutes a grave violation of official duty, which results in disciplinary action and sanctions.[180] Disciplinary liability does not prevent criminal liability.[181]

The **North Macedonian** Law on Classified information specifies misdemeanours and criminal offences for the actions of disclosure of classified information, or information marked as „FOR RESTRICTED USE". Firstly, the Law envisages in Article 97 a fine of 500-1000 EUR for a misdemeanour to be imposed on a legal entity that discloses information marked as "FOR RESTRICTED USE". Secondly, in Article 103 the Law stipulates the criminal offences of announcing, handing over or otherwise disclosing of classified information. The existence of the offence is conditional upon certain consequences of disclosure, such as endangerment or violation of interests of North Macedonia, or on the fact that information was obtained illegally. The envisaged sanction is imprisonment. A qualified offence is also envisaged, if the criminal offences are committed during a state of war. Attempt of one of those criminal offences is also punishable. Further on, the North Macedonian Law also provides for the criminal offence of authorised disclosure of classified information, which has been learned in court or other procedure. The prescribed sanction is imprisonment. Moreover, the North Macedonian Criminal Code[182] envisages in Article 281 that disclosure of a business secret to an unauthorised person constitutes a criminal offence.[183] Additionally, the North Macedonian Law on Civil Servants[184] also envisages that disclosure of confidential information and disclosure of classified information constitute a disciplinary offence.[185]

It is evident that the regulatory framework of all four analysed countries that governs right to information and information secrecy is very complex. In most cases, the RTI laws envisage limitations that are broadly in line with the standard, but this perception of alignment is thwarted by a closer look in the rules relating to secrecy in numerous laws that regulate neither RTI nor classification of information. The wide margin of appreciation in assessing whether a certain piece of information falls into some category of secrecy, combined with the threat of disciplinary or criminal liability in case of disclosure, makes the tasks of RTI officers in public bodies particularly challenging, as they must take into account this wide array of legal rules when making their decisions, and cannot always rely on RTI laws to protect them.

[179] Law on Civil Servants (Zakon o državnim službenicima i namještenicima, *Službeni list RCG*, nos. 2/2018, 34/2019 and 8/2021).
[180] Article 95 of the Law.
[181] *Ibid.,* Article 93.
[182] Criminal Code (Кривичен законик, *Службен Весник на РМ*, nos. 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018).
[183] Also see: *Заштита на деловна тајна и законско регулирање во Република Македонија*, https://konstantinovic-milosevski.mk/mk/2021/02/12/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%B4%D0%B5%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0-%D1%82%D0%B0%D1%98%D0%BD%D0%B0-%D0%B8-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D1%81%D0%BA%D0%BE-%D1%80%D0%B5/, 24.2.2022.
[184] Law on Civil Servants (Закон о јавните службеници, *Службен Весник на РМ*, nos. 27/14, 199/14, 48/15, 5/16, 142/16 и 11/18, 275/10 and *Службен Весник на РСМ* 14/20).
[185] Article 73 of the Law.

Criminal Code of **Serbia** incriminates "espionage" as criminal offence that consists in having someone "disclosing, handing over or making available military secrets, economic or official information or documents to a foreign state, foreign organisation or a person in their service" (Art. 315 Para. 1). According to this Article, secrets are "such military, economic or official information or documents that are designated as secret by law, other regulations or decision of competent authority passed pursuant to the law, as well as information and documents whose disclosure would or could cause harm to the security, defence or political, military or economic interests of the country".

There are significant inconsistencies between DSL and other laws. Thus, the CC incriminates the disclosure of a state secret as a type of secret, and not as a degree of secrecy (Art. 316). The definitions of state secrets in CC and DSL are different. CC defines it as "information or documents that are by law, other regulations or decision of competent authority passed pursuant to law designated as a state secret, and whose disclosure would or could cause harm to the security, defence or political, military or economic interests of Serbia". DSL however, defines "top secret" level[186] as the highest level of secrecy "assigned in order to prevent irreparable grave damage to the interests of the Republic of Serbia" (DSL, Art. 14 Para. 1 p. 1). Furthermore, Article 369 of the CC incriminates divulging of the so-called "official secret", which is defined as "information and documents declared as an official secret by law, other regulation or decision of the competent authority issued pursuant to law, whose disclosure would cause or could cause damage to the service". However, DSL does not recognize this sort of secret information. Finally, in Article 415 there is incrimination of "divulging military secrets". Similarly to previous definitions, military secret is defined as "information designated as a military secret by law, other regulations or decisions of competent authorities passed pursuant to law, whose disclosure would or could cause damage to the Army of Serbia or to the defence and security of the country". Again, this type of secret information is unknown to DSL, or the legal system in general.

All three definitions have similar restrictions – what will not be considered classified information: "A state secret within the meaning of Paragraph 5 of this Article shall not be information or documents directed at serious violations of fundamental human rights, or at compromising the constitutional order and security of Serbia, as well as information and documents that are aimed at concealing a committed criminal offence punishable by law with imprisonment of up to five years, or a harsher penalty." (Art. 316 Para. 6);

"Data and documents directed at serious violations of fundamental rights of man, or at endangering the constitutional order and security of Serbia, as well as data and documents that have as objective concealing of a committed criminal offence punishable under law by imprisonment of five or more years, shall not be deemed official secrets within the meaning of Paragraph 4 of this Article." (Art. 369 Para. 5);

[186] Although official translations of these laws use different terms, in Serbian language in both laws the term "državna tajna" is used.

"Information or documents directed at serious violation of fundamental human rights or at compromising the constitutional order and security of Serbia, as well as information and documents aimed at concealing a committed criminal offence punishable under the law by imprisonment of five years or a more severe penalty shall not be deemed a military secret within the meaning of Paragraph 4 of this Article." (Art. 415 Para. 5).

Criminal Procedure Code regulates exclusions from the duty of testifying (Art. 93 Para. 1 p. 1): "The duty to testify does not apply to: 1) a person who would by his/her statement violate the duty to preserve a state, military or official secret, until the competent authority or person from public authorities revokes the secrecy of information or releases him/her from that duty;"... Again, we can conclude that CPC regulates types of secret information that are not consistent with the DSL, repeating solutions from the CC.

Finally, the same discrepancies are repeated in LCS. Article 23 of this Law determines the obligation of a civil servant or an employee to keep state, military, official and business secrets in accordance with special regulations. Again, state, military and official secret are neither defined nor specified in more details – yet, according to Article 109, Paragraph 1, Point 5, disclosure of an official or other secret constitutes a serious breach of duty, for which civil servant or employee may be dismissed from duty and held criminally liable.

These inconsistencies lead to uncertainty as to what types of exceptions exist, when it comes to the availability of information of public importance. Although the DSL was adopted more than 10 years ago, the period in which the LCS, CC and the CPC have been changed several times (CPC was actually adopted after DSL, in 2011), no effort has ever been made to harmonize these laws with DSL.

When it comes to classification, the legislations of the analysed countries converge, when it comes to the rules on degrees of classification; this is unsurprising as the new classification laws were mostly developed so as to adhere to NATO standards. The legislations of the four countries are also convergent, when it comes to providing more detailed regulation of the types of information that can be classified. Where they all seem to fall short, however, is the provision of additional guidance on the issue, particularly in the security sector.

The legislation of all the countries can only be assessed as being mostly not in line with standards; the legislation of Montenegro is particularly problematic due to internal incongruence of its laws and a wide scope of exclusion from the general RTI rules.

Indicator 3

A harm test applies to all exceptions, so that it is only where disclosure poses a risk of actual harm to a protected interest that it may be refused.

Some form of harm test is envisaged in the legislations of all four countries. Except for Montenegro, the laws are fully or mostly in line with the relevant standard.

In **BiH**, according to the Article 9 of the LFAIB, competent public body shall publish the requested information, notwithstanding the established exception, if it is justified by the public interest, and take into account any benefit and any harm that may result from it. In deciding whether the disclosure of information is justified in the public interest, the competent public authority shall consider circumstances such as, but not limited to, any breach of a legal obligation, the existence of any offense, miscarriage of justice, abuse of power or negligence, unauthorized use of public funds, or a danger to the health or safety of an individual, the public or the environment. If it has been determined that the publication of the requested information determined by the competent public body as an exception is in the public interest, the competent public body shall issue a decision informing the third party that the information will be published after the expiry of the period of 15 days from the day of receipt of the letter. Entity laws contain same provisions (Article 9 in both laws). In practice, however, there are significant deviations from this rule. Thus, the Report on the implementation of the FOI of the organization Transparency International for 2021 states that "The main problem in the conduct of public authorities is the non-application or misapplication of the harm test (Article 9 FOIA). In many cases, public authorities refuse access to information only on the grounds that certain information is considered exempt from publication without conducting a public interest test. ...

In cases when the delivery of various contracts (on public procurement of goods, work contracts, etc.) was requested from public authorities, it is noticeable that the refusal was reasoned with a reference to exceptions in confidential commercial information. It should be emphasized that public authorities automatically responded that information could not be provided without considering the public interest and contacting a third party, whose commercial interests were sought to be protected."[187] It is also interesting that in the Ombudsman's survey from 2019, most public bodies stated that they have not had the opportunity to conduct a harm test so far: "Public interest research is the most demanding, but also the most important part of processing requests for access to information. When asked how public authorities conduct the harm test, most public authorities submitted an answer stating that they have not considered so far requests within which they would be obliged to examine the public interest."[188]

[187] Transparency International, *Izvještaj o primjeni Zakona o slobodi pristupa informacijama u 2021. godini*, Banja Luka 2021, 4. This was also emphasized in the judgment of the District Court in Banja Luka in the case 11 0 U 014028 14 U (Judgment of 31.3.2015.), when the request for information was rejected due to the protection of personal data of third parties. However, the rejection decision did not contain a harm test, nor an explanation of how certain data stored in a school (name and surname of the person to whom the diploma of completed education was issued) may be considered personal data, and thus unavailable to public. In similar circumstances, the necessity of conducting the test was pointed out by the same court in case 11 0 U 014493 14 U (Judgment of 31.3.2015.).

[188] Institucija ombudsmena/ombudsmana za ljudska prava Bosne i Hercegovine, *Specijalni izvještaj o iskustvima u primjeni zakona o slobodi pristupa informacijama u Bosni i Hercegovini*, (Institution of the Ombudsmen/ Ombuds-

In **Montenegrin** legislation, the harm test applies to most, but not all exceptions. The Law envisages (Article 16) that access to information shall be limited, if the disclosure of information would jeopardize a protected interest envisaged by the law, that is, if disclosure would incur damaging consequences to the protected interest, which exceed the public's interest to know, unless there is an overriding public interest, which is also envisaged by the Law on Access to Information. However, the harm test does not apply to the exception related to privacy, nor to the exception related to the security, defence, foreign, economic and monetary policy of the country, which are classified. This norm seems to have been carried over from the previous versions of the Law, as the currently valid version in fact excludes all classified information from its scope.
Consequently, the Montenegrin legislation is not fully in line with this standard.

The **North Macedonian** law envisages that the harm test applies to all exceptions. The harm test is defined as a test to establish whether the disclosure of information would result in consequences to the protected interest that would outweigh the public's interest to know. The wording of the North Macedonian law seems somewhat unclear, as it does not refer to any "harm" that may be incurred to the protected interest, but to "consequences", presumably, adverse consequences. The provision of the North Macedonian law implies the existence of a public interest test, as the consequences to protected interest should not outweigh the public interest. However, this provision is set too broadly and is not in line with relevant standards. The Instruction on the application of the Law is more specific in this regard, as it states in Article 9 that access may be refused, only if the harm test establishes that a grave damage would be incurred to the protected interest if the information is disclosed. The recently published Guidebook on conducting the harm test[189] reiterates the interpretation offered in the Instruction, underlining that such potential grave damage to the protected interest needs to be established in each individual case, where the protected interests are those established in Article 6 of the North Macedonian Law. These clarifications are more in line with the relevant international standards, but not fully convergent with the statutory provisions.

In **Serbia**, Article 4 of the LFAIS envisages a statutory presumption in favour of the public's right to know. As elaborated before, the LFAIS creates an irrefutable presumption of such a right in cases when the information concerns jeopardizing or protection of the public health or the environment. In other cases, it is up to the public authority to refute the assumption of the public's right to have access to information. This means that, to be able to withhold information, a public authority must apply the harm test and show that there is an overriding interest based on the Constitution or the law that needs to be protected to withhold the information (Article 8). The Commissioner corroborated this[190] by stating that, "when dealing with requests for access to information

man for Human Rights of Bosnia and Herzegovina, *Special Report on Experiences in the Application of the Law on Freedom of Access to Information in Bosnia and Herzegovina*), Banja Luka 2019, 36.

[189] *Прирачник за спроведување на Тестот на штетност* (*Harm Test Implementation Manual*), https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/, 24.2.2022.

[190] Decision of the Commissioner for Information of Public Importance and Personal Data Protection of Serbia 071-01-2956/2019-03 of 30.5.2019.

regarding events in connection with which the public's interest to know is greatly enhanced, public authorities must provide strong and solid evidence in support of claims that by accessing the requested information, some legally protected interests would be so seriously and severely violated, that even the public interest to know whether the competent state authorities are acting lawfully cannot be considered a predominant and more important interest in that particular situation." The Serbian legislation is therefore in line with the standard. It should be noted, however, that neither the law nor any bylaws regulate the procedure for conducting the harm test in more detail, which renders this task complicated. The published Guidebook for the implementation of the LFAIS does provide some level of additional and useful guidance, but based on the evidence from practice elaborated above, it does seem to suffice. Some authors argue that this provision is not properly implemented in practice, neither by the public bodies nor by the Commissioner.[191]

Indicator 4

There is a mandatory public interest override, so that information must be disclosed where this is in the overall public interest, even if this may harm a protected interest. There are 'hard' overrides (which apply absolutely), for example for information about human rights, corruption or crimes against humanity, environment protection.

Out of the four analysed countries, only Montenegro includes a clear mandatory public interest override.

In **BiH**, according to the Article 9 of the LPCIB, the information by which secrecy is determined with the intention of concealing a committed criminal offense, exceeding or abuse of authority, with the aim of concealing any illegality or concealing an administrative error, will not have the character of secrecy. Furthermore, according to Article 164, Paragraph 9 of the CLB there is no criminal offense of disclosing classified information, if someone publishes or mediates in disclosure of classified information whose content is contrary to the constitutional order of BiH, with the aim to reveal to the public irregularities related to the organization, operation or management of the service, or with the aim of disclosing to the public facts that constitute a violation of the constitutional order or an international treaty, if the publication does not have serious detrimental consequences for BiH.

There are no provisions on this indicator in legislation of the entities.

Montenegrin Law on Access to Information envisages a public interest override.[192] Overriding public interest for disclosing information or part of information exists, if the requested information includes data that duly indicate towards:

[191] S. Gajin, "Odmeravanje suprotstavljenih interesa u primeni Zakona o slobodnom pristupu informacijama od javnog značaja", *Srpska politička misao 4/2018*, 231-248, https://doi.org/10.22182/spm.6242018.11.

[192] Article 17 of the Law.

- corruption, failure to observe regulations, unlawful use of public funds or abuse of powers in exercise of public office
- suspicion that a criminal offence was committed or existence of grounds to challenge a judicial decision
- unlawfully obtaining or spending public funds
- jeopardizing public safety
- jeopardizing life
- jeopardizing the environment.

If the overriding public interest exists, the public authority is under the obligation to provide access to information.

Legislation of **North Macedonia** does not include a mandatory public interest override.

In **Serbia**, the justified public interest to know is deemed to exist whenever information held by a public authority concerns a threat to, or protection of, public health and the environment, while with regard to other information held by a public authority, it shall be deemed that justified public interest to know exists, unless the public authority concerned proves otherwise. This means that RTI sets out hard overrides. Hard overrides are also set in the DSL, which states in Article 3 that data marked as classified with a view to concealing crime, exceeding authority or abusing office, or with a view to concealing some other illegal act or proceedings of a public authority, shall not be considered classified. Further, hard overrides are set forth in the CC (norms cited above in Standard 5, Indicator 2). Moreover, Article 26 of the DSL envisages that the National Assembly, the President of the Republic and the Government may declassify specific documents, regardless of the level of classification, should that be in public interest, or in order to perform international obligations. However, as explained above, the Law on Tax Procedure and Tax Administration envisages a significant exception from the cited norms. Consequently, the Serbian legal framework is mostly in line with the standard.

Indicator 5

There is a severability clause, so that where only part of a record is covered by an exception, the remainder must be disclosed.

The legislations of all analysed countries envisage a severability clause.

In **BiH**, According to Article 10 of the LFAIB, if part of the requested information is identified as an exception, the competent public body shall set aside such part and publish the rest of the information, unless this separation has made the information incomprehensible. Entity laws contain identical provisions (Article 10 of both laws). In practice, it happens that the competent public authority does not apply this clause. Thus, the Appellate Administrative Council of the Court of Bosnia and Herzegovina,

in its judgment on the CSO lawsuit regarding complete denial of all data on concluded contracts in the State Investigation and Protection Agency, concluded, on reasoning that the requested contracts indeed contained personal data that could not be published (such as home addresses and ID numbers of persons), but that this should not be an obstacle to the partial publication of information. The Court emphasized: "Denying access to information to a non-governmental organization that has a prominent role in the fight against corruption, nepotism and illegal spending of budget funds by calling for formal obstacles established by law, is not the task of state bodies. They are not custodians of information, but their transmitters, who are obliged to make them as accessible as possible to the democratic public and its democratic institutions".[193]

The **North Macedonian Law** on Access to Information envisages a similar severability clause in Article 6, Paragraph 4. However, instead of the comprehensibility requirement, it makes the access conditional on not jeopardizing the safety of the document.

Montenegrin Law on Access to Information includes a severability clause in Article 24. Namely, it states that if access is restricted to a part of the information, the public authority is under the obligation to provide access to the information, after deleting the part of information to which access is restricted. When doing so, the exception is marked with the words "deleted" and information is provided on the extent of the deletion (number of lines, paragraphs and pages). The deletion is done in a way that cannot destroy or damage the text, that is, the content of the information.

In **Serbia**, severability clause is clearly stipulated in Article 12 of the LFAIS, which envisages that, if requested information of public importance can be extracted from other information contained in a document which a public authority has a duty to disclose to an applicant, the public authority concerned shall allow the applicant access only to a part of the document which contains the extracted information and advise him/her that the remainder of the document is not available. However, this stipulation is somewhat thwarted by the provisions of Article 14 of the LFAIS relating to the protection of privacy and other personal rights, including the right to reputation. More specifically, this Article envisages that the public authority can limit access to information, if this would violate the right to personal data protection, the right to privacy, the right to reputation or other personal right to which the information personally pertains. Article 14 does envisage certain exceptions from this rule, but also includes in its Paragraph 3 a norm which is relevant in the present context: information of public importance from the document containing personal data can be made available to the requester in a way that enables the public's right to know and the right to personal data protection to be effected jointly. First of all, this provision seems to be excessive, as the same goal is set out to be achieved by the severability clause. Secondly, a purely linguistic interpretation of the said provision could imply that this type of balancing of interests is reserved for personal data alone, and not to the other cases of potential violations of the protected

[193] Court of Bosnia and Herzegovina, Judgment No. S1 3 U 016743 14 Uvp of 11.3.2015. This possibility is also pointed out by the District Court in Banja Luka in previously cited cases 11 0 U 014028 14 U and 11 0 U 014493 14 U of the District Court in Banja Luka.

rights of privacy and reputation. The lack of clear mutual referencing between Articles 12 and 14 of the LFAIS thus seems problematic, having the potential to jeopardize the severability clause on rather vague grounds such as reputation. Article 12 of the DSL (Para. 3) contains solutions for documents with different degrees of secrecy, envisaging that, in cases when a smaller part of a document contains classified data, such part shall be separated from and attached to the document as a separate enclosure marked with the relevant level of classification.

The way in which severability is envisaged in most analysed legislations is mostly in line with the relevant standard.

Indicator 6

When refusing to provide access to information, public authorities must state the exact legal grounds and reason(s) for the refusal

All the analysed legislations envisage that grounds and reasons for refusal must be stated in the ruling whereby access to information is refused. It is the level of detail in this regulation that renders some countries mostly in line with the standard, as the case is with the legislations of Montenegro, Serbia and North Macedonia, or fully in line with the standard, as the case is with the laws in BiH.

The **BiH** legislation stipulates that, if access to information is refused, in whole or in part, the competent public authority shall inform the applicant accordingly. The mentioned ruling contains the legal basis for the status of information exclusion in terms of the Law, including all material issues that are important for making a decision, as well as the taking into account of the public interest factors of (Article 14, Paragraph 3 of the LFAIB). Entity laws contain the same normative solution (Article 14, Paragraph 3 of both laws).

Montenegrin Law on Access to Information envisages that the ruling refusing access must include a detailed explanation of the grounds on which access to information is refused. The law does not specify that the ruling must include the elaboration of the harm and public interest test. Since the Law states that the procedure related to request for access to information is conducted pursuant to the provisions of the Law on Administrative Procedure,[194] it is worth examining the provisions of this law related to rulings. The Law on Administrative Procedure states that the reasoning of a ruling must include a summary of the request, the facts based on which the ruling was passed, the regulations based on which the ruling is passed, the grounds that refer to the decision made in the holding of the ruling and the main reasons for the decision. While this provision is useful, it still would have been better, if the Law on Access to Information had stated that the reasoning of the ruling must include reference to legal grounds, the harm test and a public interest test.

[194] Law on Administrative Procedure (Zakon o upravnom postupku, *Službeni list RCG*, nos. 56/2014, 20/2015, 40/2016 and 37/2017).

In **North Macedonia**, the Law on Access to Information states in Article 20 that the public authority holding the information must pass a ruling on its decision both in cases when the request is granted and when it is fully or partially denied. North Macedonian Law on Access to Information envisages that the ruling passed with regards to the request for access to information, in cases when the request is partially or fully denied, must include the reasons for refusal and the results of the conducted harm test. The Instruction on the application of the Law on Access to Information regulates this issue in somewhat more detail. Firstly, it states that the ruling whereby the request is fully or partially refused must include the reasoning for such refusal. It then reiterates that the official of the authority is under the obligation to conduct a harm test before refusing access, with the aim of establishing whether in that specific case the consequences for the protected interest override the public interest stipulated by the law. Finally, it states that the conducted harm test must be referred to in the holding of the ruling, while the reasoning must include: a reference to the exemption protecting the given interest in terms of Article 6 of the Law on Access to Information and an elaboration of the specific facts that have resulted in the conclusion that the disclosure of information would cause significant harm to the protected interest. The provisions of the Instruction render the regulatory framework of North Macedonia more in line with international standards; however, it would have been better if the cited norms were included in the law in this level of detail.

In **Serbia**, LFAIS expressly stipulates (Art. 16 Paras. 12 – 13) the obligation of the public authority to pass a decision, including the rationale for such a decision, in cases when it refuses to inform an applicant, either entirely or partially, whether it holds the requested information, to grant an applicant access to a document containing the requested information or to issue or send to an applicant a copy of the document. As explained in the text above (standard 4, indicator 1), such decision must be passed within 15 days from the receipt of the request. The decision must also instruct the requester the available relief against such decision. If the request is denied because requested information is secret (including professional secret), public authority has to state those reasons in the decision rationale.

5. **EXCEPTIONS TO FREE ACCESS TO INFORMATION ARE CLEARLY FORMULATED IN LAW AND NOT**

Indicators
1. RTI Law does not exclude *a priori* any category of information from its scope of application except for classified information originating from foreign countries and international organizations
2. Limitations to the right to access information should be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting, in particular: i. national security, defence and international relations ii. public safety; iii. the prevention, investigation and prosecution of criminal activities (with special focus on police when analysing this sector); iv. privacy; v. commercial and other legitimate economic interests; vi. the equality of parties concerning court proceedings; vii. inspection, control and supervision by public authorities; viii. the economic, monetary and exchange rate policies of the state ix. the deliberations within or between public authorities concerning the examination of a matter
3. A harm test applies to all exceptions, so that it is only where disclosure poses a risk of actual harm to a protected interest that it may be refused.
4. There is a mandatory public interest override, so that information must be disclosed where this is in the overall public interest, even if this may harm a protected interest. There are 'hard' overrides (which apply absolutely), for example for information about human rights, corruption or crimes against humanity, environment protection.
5. There is a severability clause, so that where only part of a record is covered by an exception, the remainder must be disclosed.
6. When refusing to provide access to information, public authorities must state the exact legal grounds and elaborate the harm and public test conducted
Total points
Average points
Standard

EXTENSIVE, WHILE A PUBLIC INTEREST OVERRIDE AND HARM TEST ARE ENVISAGED AND APPLIED

	Value	BIH			MKD	MNE	SER
	0-3	BIH	FBIH	RS			
		3	3	3	3	0	2
	0-3	1	1	1	1	1	1
	0-3	3	3	3	2	1	3
	0-3	1	0	0	1	3	2
	0-3	2	2	2	2	3	3
	0-3	3	3	3	2	2	2
		13	12	12	11	10	13
		2.17	2	2	1.83	1.5	2.17
	0-5	4	3	3	3	2	4

Standard 6. There is a designated supervisory authority overseeing the implementation of the legislation on public information with the power to set standards, make prescriptions and impose sanctions.

Indicator 1

If the request has not been dealt with within the specified time limit, or if the request has been refused, requesters have the right to lodge an external appeal with an independent administrative oversight body (e.g. an information commission or ombudsman).

The legislations of all four analysed countries envisage the right to an external appeal with an independent administrative oversight body. This means that they have all adopted the model of administrative-procedural protection of FOI with the participation of an independent controlling body with executive powers.[195] However, the law of the Republic of Srpska envisages the appeal to be addressed to a body (the Ombudsman of the Republic of Srpska) that is no longer operational.

In **BiH**, the initial complaint is internal, addressed to the head of the competent second instance public body (Article 14, Paragraph 4 of the LFAIB). According to the Chapter 6 of the LFAIB, Ombudsmen is a competent external body. Its general competencies apply to individual cases, but there are no special procedures regarding this issue. In practice, this means that an individual dissatisfied with decisions regarding access to information may turn to the Ombudsmen in the regular complaint procedure, as regulated by the Law on the Human Rights Ombudsmen of Bosnia and Herzegovina[196] (hereinafter: LHROB).[197]
There is an unusual normative situation in the **Republic of Srpska**. Pursuant to Article 14, Paragraph 3 of the RFAIRS, a citizen who is dissatisfied with the second-instance decision may contact the Ombudsman of the Republic of Srpska. This solution is elaborated in Articles 21 and 22. However, institution of Ombudsman of the Republic of Srpska ceased to operate at the end of 2009, with the adoption of the Law on the Termination of the Law on the Ombudsman of the Republic of Srpska – Protector of Human Rights[198].

[195] For a comparative perspective on different models of protection of RTI see:
D. Milenković, "Upravno-procesna i drugi slični oblici zaštite prava na pristup informacijama u komparativnom pravu", *Strani pravni život*, 3/2015, 115-131, https://www.stranipravnizivot.rs/index.php/SPZ/article/view/163, 24.2.2022. Milenković also points out that in some countries, this independent administrative body providing administrative-procedural protection of the FOI is at the same time the body vested with similar powers with regard to personal data protection. Stanić delves into a comparative analysis of the manner in which members of such bodies are composed in the context of their independence in Albania, Bosnia and Herzegovina, North Macedonia and Montenegro; in terms of FOI, his insights related to the Montenegrin Agency with such dual competences are useful (see: M. Stanić, "Izbor članova nadzornog tela za zaštitu ličnih podataka kao garantija nezavisnosti – primeri Albanije, Bosne i Hercegovine, Crne Gore i Severne Makedonije", *Strani pravni život*, 3/2020, 125-135. doi: 10.5937/spz64-28379.
[196] Law on the Human Rights Ombudsmen of Bosnia and Herzegovina (Zakon o Ombudsmenu za ljudska prava Bosne i Hercegovine, *Službeni glasnik BiH*, nos. 19/2002, 35/2004, 32/2006, 38/2006 – correction, and 50/2008 – other law).
[197] The institute of Ombudsman in Bosnia and Herzegovina is not universally perceived as a fully independent and operational institution. See: E. Mrkaljevic, *Dvadeset godina djelovanja Institucije ombudsmana u Bosni i Hercegovini*, http://fcjp.ba/templates/ja_avian_ii_d/images/green/Enesa_Mrkaljevic3.pdf, 24.2.2022.
[198] Law on the Termination of the Law on the Ombudsman of the Republic of Srpska – Protector of Human Rights (Zakon o prestanku važenja Zakona o Ombudsmanu Republike Srpske – zaštitniku ljudskih prava, *Službeni glasnik Rep. Srpske*, no. 118/2009).

This situation has occurred due to the inconsistency of this regulation with the institutional changes that have taken place both at the BiH level and entities level (abolition of entity ombudsmen). It is thus unclear whether there is an external independent administrative oversight body. RFAISFBH does not contain any provisions regarding this standard, and it simply refers out to the Ombudsmen of BiH (Article 21).[199]

In **Montenegro**, the applicant, or another person having an interest, may appeal the acts passed by public authorities related to requests on access to information with the Agency for Protection of Personal Data and Access to Information (hereinafter: "the Agency"), through the public authority that has decided upon the request in first instance. The only exception to this is the decision denying access to the information containing pieces of information marked as classified – in this case, the decision cannot be appealed, and it may be contested only by a lawsuit to initiate an administrative dispute. The Agency has been originally established by the provisions of the Law on Personal Data Protection,[200] which states in Article 49 that the Agency is autonomous and independent, and has the status of a legal person. The decisions on appeals against legal acts related to the requests for access to information are passed by the Agency management body – the Agency Council.

North Macedonian legislation envisages both situations. Firstly, it states that if the information holder does not enable access to information within the time limits prescribed by law, and fails to pass and serve the ruling, it shall be deemed that access was refused, and the requester has the right to file an appeal with the Agency within 15 days (Article 20, Paragraph 3). Further, in Article 27, the Law envisages that the requester has the right to appeal against the ruling refusing or dismissing the request within 15 days from the day of receiving the ruling. The appeal is filed with the Agency for Protection of the Right to Free Access to Public Information of North Macedonia. The Agency is also regulated by the Law on Free Access to Information, in Articles 29 – 37 of the Law. The Law defines the Agency as an autonomous and independent state body. The Agency is funded from the state budget, and is accountable before the Parliament of North Macedonia. The Director of the Agency and the director's deputies are appointed by the North Macedonian Parliament for a period of 6 years, following a public advertisement of vacancies.

In **Serbia**, the most important independent administrative oversight body is the Commissioner for Information of Public Importance and Personal Data Protection. The Commissioner is elected by the National Assembly of the Republic of Serbia.[201] Com-

[199] According to Ohranovic (A. Ohranovic, *Pozicija ombudsmena u upravnom postupku i postupcima pred sudovima BiH, obim i vrsta ovlaštenja i mogućnosti koje mogu koristiti*, Fondacija centar za javno pravo, Sarajevo 2017, 7), in practice requests are made to the ombudsman and a number of them result in recommendations being made, but these are not always effected.

[200] Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti, *Službeni list RCG*, nos. 79/2008, 70/2009, 44/2012 and 22/2017).

[201] The term of office of the Commissioner is eight years and the same person cannot be elected to this position twice. The Commissioner is autonomous and independent in the exercise of his/her competence. Commissioner cannot be held liable for the opinion he/she has expressed or for the proposal he has made in the exercise of his jurisdiction, and in the case of the initiation of proceedings for a criminal offense committed in the exercise of his jurisdiction, may not be detained without the approval of the National Assembly (LFAIS, Arts. 30 and 32

petence and duties of the commissioner arise from the LFAIS and the Law on Personal Data Protection.

The LFAIS lists (LFAIS, Art. 22, Para. 1 – 3) the cases in which the applicant may lodge a complaint with the Commissioner. These are the following:

1) A public authority rejects or denies an applicant's request, within 15 days of receiving of the relevant decision or other document;
2) A public authority failed to reply to a submitted request within the statutory time limit;
3) A public authority made the issuance of a copy of a document containing the requested information conditional on the payment of a fee exceeding the necessary reproduction costs;
4) A public authority does not grant access to a document containing the requested information;
5) A public authority does not grant access to a document containing the requested information and/or does not issue a copy of the document; or
6) A public authority otherwise obstructs or prevents an applicant from exercising his/her freedom of access to information of public importance, in contravention to the provisions of LFAIS.

However, complaints shall be inadmissible, if lodged against decisions of the National Assembly, the President of the Republic, the Government of the Republic of Serbia, the Supreme Court of Serbia, the Constitutional Court the Republic Public Prosecutor and the National Bank of Serbia. In such cases, the requester may initiate administrative dispute before the administrative court. While such a solution, on the one hand, ensures that requesters have legal relief against the decisions of the highest state authorities, it is disputable to what extent such remedy can be deemed effective, given the excessive overload and the duration of proceedings before the Administrative court.[202] Further, it is unclear whether the term "Government" covers only the government in the narrow sense of the word (ministers and prime minister), or it also encompasses various other bodies e.g. secretariats, which are established by the Government.[203]

Also, no appeal may be lodged against the decision of the Commissioner deciding on the request submitted to the Commissioner as a public authority.[204]

[202] The Court Rules of Procedure in Serbia do not envisage a special registry for this type of cases, but classifies them as U cases, along with a number of other types of administrative cases. Therefore, accurate statistical data is not available. However, some indication of the caseload of administrative judges can be seen from the annual reports on the work of courts. *The 2020 statistical report on the work of the Administrative Court* (https://www.vk.sud.rs/sites/default/files/attachments/SUDOVI%20POSEBNE%20NADLEŽNOSTI_0.pdf, 24.2.2002.) shows that the total caseload of U cases is 64.051 cases, or 129,40 cases per judge on average. Further, judges on average have 1.040,51 unresolved cases, out of which on average just under 46 cases per judge are old cases.

[203] See: N. Nenadic, *Zakon o slobodnom pristupu informacijama – šta je poboljšano, a koji problemi nisu rešeni*, https://pescanik.net/zakon-o-slobodnom-pristupu-informacijama-sta-je-poboljsano-a-koji-problemi-nisu-reseni/, 24.2.2022.

[204] Milovanović, Davinić and Cucić criticize this solution, attributing it to inherent flaws of the Serbia LFAIS. (D. Milovanović, M. Davinić, V. Cucić, "Free Access to Information in Serbia: A European Perspective" in: *The Laws of Transparency in Action*, Palgrave Macmillan, Cham, 2019, 530). They argue that a solution allowing both appellants and the public authorities to challenge the decisions of the Commissioner before the Administrative Court would have been a better middle ground and also conducive of the development of caselaw of the court. While this observation has validity from the theoretical standpoint, in practice it would almost certainly result in unreasonably long time for a final decision to be taken, given the ever-increasing competence of the Serbian Administrative Court (according to the Report on the work of courts of special competence in Serbia in 2020, the Administrative Court had a total of 71.747

An administrative dispute may be instituted against a decision of the Commissioner before the Administrative Court (LFAIS, Art. 27, Para. 1) and the procedure is considered urgent.

The laws of all the countries are nominally fully in line with the standard, with the caveat that the law of the Republic of Srpska can be deemed as ineffective in practice, as explained above.

Indicator 2

The decisions of the independent oversight body are binding. The independent oversight body has the necessary mandate and power to perform its functions.

The laws of the analysed countries range considerably when it comes to the mandate, powers and the binding nature of the decisions of the independent oversight bodies as envisaged in the law.

When it comes to **BiH**, the mandate and the powers of the Ombudsmen, which is the independent oversight body in RTI context, stem from the LHROB. According to Article 23, Paragraph 2 of the LHROB, Ombudsmen may at any time request any document they deem necessary for an inquiry. Furthermore, government bodies are obliged to provide the Ombudsmen with appropriate assistance in the investigation and control. At the time of the investigation, the Ombudsmen shall have access to any government body in order to verify the requested information, conduct personal interviews and review the necessary documents. The Ombudsman may not be denied access to files or administrative documents or other documents related to the activity or activity under investigation. (Article 25 of the LHROB). Finally, Ombudsmen may request the government bodies to submit to them the documents they deem necessary for the performance of their function, including those which have been registered as confidential or secret in accordance with the law. In such cases, the Ombudsmen will exercise the necessary discretion for them and will not make them available to the public. The inquiry conducted by the Ombudsmen and their staff, including procedural measures, shall be conducted with the utmost discretion, without prejudice to any considerations which the Ombudsmen find should be included in the report. Special protection measures will be taken for documents that are kept confidential or secret. When the Ombudsmen consider that a document, which has been kept confidential or secret and which has not been submitted by government bodies, may be of crucial importance for the proper conduct of the investigation, they shall inform the Presidency of Bosnia and Herzegovina. (Article 28 of the LHROB). According to the LHROB, Ombudsmen do not pass binding decisions.

cases in that year, having resolved only 23736. See*: Statistika o radu sudova posebne nadležnosti u Republici Srbiji za period 1.1. – 31.12.2020. godine*, ttps://www.vk.sud.rs/sites/default/files/attachments/SUDOVI%20POSEBNE%20NADLEŽNOSTI_0.pdf, 24.2.2022. It is questionable whether such delays would have effectively contributed to building not only the practice, but the culture of free access to information.

As previously mentioned, the **FBiH** law refers to the Ombudsmen of BiH, while in the Republic of Srpska there is inconsistency of regulations and thus a legal gap (reference to the institution of the Ombudsman of the **Republic of Srpska**, which has ceased to exist). In FBiH, according to the Article 14, Paragraph 5, an administrative dispute before the administrative court may be initiated against the second-instance decision – this solution is not present in the law of the Republic of Srpska.

The powers of the **Montenegrin** Agency for Personal Data Protection and Access to Information are regulated in both the Law on Access to Information and the Law on Administrative Procedure. The Law on Access to Information stipulates in Article 37 that an appeal can be lodged to the Agency for Personal Data Protection and Free Access to Information. An exception from this rule exists in cases when access to information was denied in lieu of classified information – in that case, the legal remedy is administrative dispute. The appeal is decided on by the Agency's Council. The appeal to the Agency does not suspend the execution of the ruling on access to information. Montenegrin law on access to information only stipulates that the Agency has to pass a ruling on the appeal within 15 days from the day the appeal was filed, while the powers the Agency has when deciding on the appeal are regulated in the Law on Administrative Procedure.

Montenegrin Law on Access to Information also prescribes that, in order to decide on appeals, the Agency's Council has the right to obtain the information or part of the information to which access is requested, as well as other information and data necessary for making the decision, and has the right for an inspection authority which controls office administration to establish whether the public institution holds the requested information. It can, therefore, be concluded that some of the powers of the Agency's Council necessary for the performance of its function are somewhat derivative.

The provisions of the **North Macedonian** Law on Access to Information are not too detailed when it comes to regulating the decisions of the Agency. Article 30 of the Law sets out that the Agency, inter alia, conducts administrative proceedings and decides on appeals against the decision by which the information holder have refused or dismissed the request for access to information. The Law also states in Article 27 that, if the Agency fails to pass a ruling on the appeal within the set timeline, the requester has the right to initiate administrative dispute. This means that the ruling of the Agency is final in terms of the Law on Administrative Dispute[205]. It is further stated in the same Article of the Law that the information holder is under the obligation to implement the ruling of the Agency within 15 days from the day of its receipt and to inform the Agency thereof. Failure to implement the ruling and to report the Agency is envisaged as a misdemeanour in Article 39 of the Law on Free Access to Information. Article 40 of the Law envisages that a Misdemeanour Commission of the Agency, comprised of Agency employees, is in charge of conducting misdemeanour proceedings and prescribing the relevant sanctions. This is an important power vested with the Agency, aimed at providing it with adequate powers to perform its function. The Law, unfortunately, does not

[205] Law on Administrative Dispute of Macedonia (Закон за управни спорови, *Службен Весник на РСМ*, No. 96/2019).

go into details as to what the Agency's ruling on the appeal may be – this is regulated in more detail in the Instruction, which states that the Agency can: dismiss the appeal, sustain the appeal and order the information holder to act in accordance with the Law, to deny the appeal as unfounded, to sustain the appeal and order the information holder to provide access to information, to sustain the appeal and return the case to the first-instance body to be acted on again.

In **Serbia**, the Commissioner's decisions shall be binding, final and enforceable. The Commissioner's decisions shall be administratively enforced by the Commissioner by coercive means (coercive action or fines, as appropriate), in accordance with the law pertaining to general administrative proceedings. The decisions relate both to cases when the appeal is lodged against a request that has been denied, and in cases when the public authority failed to decide on the request. In the procedure of administrative enforcement of the Commissioner's decisions, complaints against enforcement shall not be admissible. If the Commissioner is unable to enforce his/her decisions the Government shall, on request, assist him/her in the administrative enforcement of such decisions by taking actions within its sphere of competence, with recourse to direct enforcement, in order to ensure compliance with the Commissioner's decisions. (LFAIS, Art. 28). The Commissioner can force the executor – the public authority to fulfil the obligations from the decision of the Commissioner by indirect coercion, by imposing fines. The fine is imposed by a decision in the range of 20,000 to 100,000 dinars and can be imposed several times. The imposed fine is executed by the court in accordance with the law which regulates execution and security. (Art. 28a).

The Commissioner is also authorized to submit a request for initiating misdemeanour proceedings for misdemeanour's provided for by this Law, when in the appeal procedure he/she assesses that there is a misdemeanour. (Art. 28b, Para. 1).

It is interesting to note that ever since this mechanism was introduced in the LFAIS in 2010, the Serbian Government has never assisted the Commissioner in executing the requests for free access to information. From 2010 to 2020, the Commissioner requested the Serbian Government to assist him in executing the requests in 340 cases, and none of these requests for assistance was supported[206], regardless of the political establishment in power.

Within the first ten years of implementation of LFAIS, the number of executed requests for information, based on the appeals proceedings held before the Commissioner, has been fairly high, ranging from astonishing 95.8% per cent in 2015 to 88.6% in 2018.[207] The Commissioner's annual reports show that in around 50-70% of the cases, public bodies would provide information to an applicant as soon as they would learn that appeals proceedings were initiated before the Commissioner, which would result in a suspension of proceedings. If this was not the case, the Commissioner would finalise the proceedings and impose a fine to the public body in question.

[206] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Godišnji izveštaj za 2020. godinu* (Commissioner for Free Access to Information and Personal Data Protection of Serbia, *Annual Report 2020*), https://www.poverenik.rs/sr-yu/o-nama/godisnji-izvestaji.html, 24.2.2022., 12-13.

[207] A. Rabrenović, A. Knežević Bojović, "The Right of an Individual to Free Access to Information – The Case of Serbia", in: M. Novaković, J. Kositć (eds.), *The Position of the Individual in Modern Legal Systems*, Institut za uporedno pravo, Belgrade 2019, 145-166, 27.

Due to the inherent limitations described above, the laws of the BiH, FBiH and the Republic of Srpska are assessed as being mostly not in line with the standards. The legislations of Montenegro and Serbia are mostly in line with the standard, whereas the legislation of North Macedonia legislation is fully in line with the standard.

Indicator 3

In deciding on an appeal, the independent oversight body has the power to order appropriate remedies for the requester, including the declassification of information

As the case is with the mandate and the powers of the oversight body, its power to order appropriate remedies for the requester is also regulated in different ways in the legislations of the analysed countries. The lack of power to order remedies stems both from the choice of the independent oversight body i.e. Ombudsmen in BiH, and the legislative inadequacies, in Montenegro.

In **BiH**, according to Articles 29 and 32 of the LHROB, on occasions when investigation shows that the abuse, arbitrary procedure, discrimination, error, negligence or omission, which are the subject of the complaint, was committed by an official in a government body, the Ombudsmen may submit these findings to that official. On the same day, the Ombudsmen will forward these documents to the official's superior and make recommendations which they deem necessary. The Ombudsmen may make recommendations to government bodies with a view to adopting new measures. Government bodies that receive such recommendations are obliged to respond in writing and inform the Ombudsmen about the effect of the recommendations within the deadline set by the Ombudsmen. Such limited powers of the Ombudsmen render the BiH legislative solution incompliant with relevant international standards.

As previously mentioned, the FBiH law refers to the Ombudsmen of BiH, while in the Republic of Srpska there is inconsistency of regulations and thus a legal gap (reference to the institution of the Ombudsman of the Republic of Srpska, which has ceased to exist).

Montenegrin Law on Access to Information prescribes a very short time limit for the Agency Council to take all necessary actions on the appeal – a total of 5 days. The Law does not go into additional detail on what the decisions are to be passed with regards to the first instance ruling. The provisions of the Law on Administrative Procedure[208] state that the second-instance authority examines the lawfulness of the ruling, and, if a margin of appreciation was used in the passing of the ruling, it also assesses the effectiveness of the solution. The second instance authority can deny the appeal, fully or partially annul the ruling, or amend the ruling. Since classified information are exempt from the scope of Montenegrin law, the Agency cannot order declassification.

[208] Article 126 of the Law.

In **North Macedonia**, the Law on Access to Information does not include any reference to the power of the Agency to declassify information. The Instruction similarly remains silent in this regard. The Law on Classification of Information states in Article 18 that the information can be declassified by the creator of the information or the person authorised by the creator of the information. The exact manner of declassification is regulated by a Government Decree. A specific decree governing this issue has not been adopted. The Law on Access to Information and the Law on Classification of Documents include no mutual references, except for one norm of the Law on Access to Information, which envisages that classified information may be exempt from free access, under certain conditions. Given the powers of the Agency in the appeal procedure, which includes the detailed examination of the grounds on which access to information has been refused, it would logically follow that the Agency has the right to access classified information, at least on a need-to-know basis, as envisaged in the Law on Classification of Information, in order to decide on the case. There seems to be no direct power of the Agency to declassify information, unless such power is granted to the Agency by the creator of the classified information. It, therefore, seems that the Agency, when deciding on an appeal, and ordering the information holder to provide access to information, could have the power to order declassification of information. However, this power is not expressly regulated.

In **Serbia**, the LFAIS envisages in Article 24 that the Commissioner can order the public authority to enable access to information to the requester. Neither the LFAIS nor the DSL vest the Commissioner with the power to directly declassify information. LFAIS (Art. 24 Para. 7) gives the Commissioner authority to demand declassification. If in the procedure on appeal against the decision to reject the request related to classified information the Commissioner determines that the reasons for which the information was determined as secret have ceased, i.e. that the information is not classified as secret in accordance with the law regulating the determination and protection of classified information, he/she shall issue a decision approving the appeal, and order the authority to revoke the confidentiality of the requested information and provide the applicant with access to that information. DSL includes another important norm, whereby declassification of information is done pursuant to a ruling of the Commissioner, or of the competent court. Namely, Article 25 of the DSL mandates the authorised person of the public authority to declassify data or documents containing secret data, and enable the petitioner to exercise his/her rights, and, if necessary, anonymise the personal data included therein, basing such decision on the ruling of the Commissioner, or on the basis of a decision of the competent court. If the authorised person fails to do so, he/she is deemed to have committed a misdemeanour (DSL, Art. 99, P. 8).

Consequently, none of the legislations can be assessed as being fully in line with the standard. While the legislation of Serbia and North Macedonia are mostly in line with the standard, and the legislations of BiH, FBiH, Republic of Srpska and Montenegro are mostly not in line with the standard.

Indicator 4

In the appeal process, the government bears the burden of demonstrating that it did not operate in breach of the rules.

None of the analysed countries have explicit provisions on the burden of proof in the appeal process. BiH legislation does include some norms that may be interpreted as implicitly prescribing that the government bears the burden of demonstrating that it did not operate in breach of the rules. However, this is not sufficient to assess that any of the legislations is in line with the standard, even partially.

In **BiH**, this criterion is indirectly set forth in the rules of procedure conducted by the Ombudsmen, whereby the authorities are obliged to co-operate in relation to the allegations in the complaint which the Ombudsmen are investigating), but there is no explicit legal provision regulating burden of proof.

As previously mentioned, the **FBiH** law refers to the Ombudsmen of BiH, while in the **Republic of Srpska** there is an inconsistency of regulations and thus a legal gap (reference to the institution of the Ombudsman of the Republic of Srpska, which has ceased to exist).

Montenegrin Law on Access to Information does not have any special rules on the burden of proof. Consequently, the provisions of the Law on Administrative Procedure apply.

The regulations of **North Macedonia** do not include detailed norms on the burden of proof in the appeal process with regard to access to information. The Law on Access to Information regulates the entire administrative procedure rather laconically, and more detailed provisions can be found only in the Instruction on the implementation of the Law. The Instruction, while being more detailed as to the extent of examination of the rulings passed by the information holders on appeal and the outcomes of this procedure, does not expressly regulate the issue of the burden of proof. The only case where the requester clearly does not bear the burden of proof, according to the instruction, is the case when the information holder has not responded to the request at all, also known as “administrative silence”. In this case, the Agency shall sustain the appeal and order the information holder to act in accordance with the Law. However, this does not mean that access to information will be granted – most likely this means that the information holder shall be ordered to repeat the procedure.

In **Serbia**, the burden of proof to demonstrate compliance with the duties set forth in this Law shall rest with the public authority concerned (LFAIS, Art. 24, Para. 4). This norm clearly envisages that the burden of proof is borne by the Government.

6. **There is a designated supervisory authority overseeing the implementation of the legislation on public information with the power to set standards, make prescriptions and impose sanctions.**

Indicators	Value	BIH			MKD	MNE	SER
1. If the request has not been dealt with within the specified time limit, or if the request has been refused, requesters have the right to lodge an external appeal with an independent administrative oversight body (e.g. an information commission or ombudsman).	0-3	BIH	FBIH	RS	3	3	3
		3	3	0			
2. The decisions of the independent oversight body are binding. The independent oversight body has the necessary mandate and power to perform its functions.	0-3	1	1	0	3	2	2
3. In deciding on an appeal, the independent oversight body has the power to order appropriate remedies for the requester, including the declassification of information.	0-3	1	1	0	2	1	2
4. In the appeal process, the government bears the burden of demonstrating that it did not operate in breach of the rules.	0-3	0	0	0	0	0	3
Total points		5	5	0	8	6	10
Average points		1.25	1.25	0	2	1.5	2.5
Standard	0-5	2	2	0	3	2	4

5.2. Legal regime for police and military

The legal regimes for the security sector do not differ considerably from the legal regime applicable to civil servants, when it comes to access to information and classification of data. This is not surprising, given that the limitations to free access to information that are inherent to the security sector, which are grounded in the specific needs of the police and the military, are already embedded in the general legal regime. The only point of slight convergence can be found in the legal regimes applicable to the disciplinary liability of police officers and military personnel, and to an extent, to the scope of potential beneficiaries of the right to free access to information. However, these convergences are more nuances than differences that would entail this regime to be considered as a separate legal regime. The threat of disciplinary or even, in some cases, criminal liability, however, can be seen as an additional disincentive for police officers and military personnel to fully embrace free access to information as a general interest that overrides secrecy.

When it comes to the defence sector standards, it should be noted that none of the legislations in the analysed countries clearly define the types of information that the public administration authorities have the right to withhold on national security grounds. The definitions found in laws on classification of information are very general, and more detailed regulation in secondary legislation is also lacking. Serbia is an exception in this regard, as it does prescribe in more detail the criteria for classification of information both applicable to the entire public service, with regard to the classification as "top secret" and "secret"[209] or to the two lower degrees of classification in the military[210] and the police.[211] The ordinances are useful in as much as they stratify the various degrees of potential harm that could be caused to protected interests, if the information were to be disclosed. Nevertheless, they remain rather general and still provide a relatively wide margin of appreciation.

5.2.1. Police

Standard 5. Exceptions to free access to information are clearly formulated in law and not extensive, while a public interest override and harm test are envisaged and applied

The Law on Police Officers of **Bosnia and Herzegovina**[212] (hereinafter: LPB) contains several norms regarding confidentiality of information.

[209] Ordinance on more detailed criteria for setting the classification degree of "TOP SECRET" and "SECRET" of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Državna tajna" i „Strogo poverljivo", *Službeni glasnik RS*, no. 46/2013).

[210] Ordinance on more detailed criteria for setting the classification degree of "CONFIDENTIAL" and "RESTRICTED" in the Ministry of Defence of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Poverljivo" i „Interno" u Ministarstvu odbrane, *Službeni glasnik RS*, no. 66/2014).

[211] Ordinance on more detailed criteria for setting the classification degree of "CONFIDENTIAL" and "RESTRICTED" in the Ministry of Interior of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Državna tajna" i „Strogo poverljivo" u Ministarstvu unutrašnjih poslova, *Službeni glasnik RS*, no. 105/2013).

[212] Law on Police Officers of Bosnia and Hercegovina (Zakon o policijskim službenicima Bosne i Hercegovine, *Službeni glasnik BiH*, nos. 27/04, 63/04, 5/06, 58/06, 58/06, 15/08, 50/08 – other law, 63/08, 35/09 and 7/12).

Article 37 of the LPB regulates the duty to maintain secrecy: "A police officer shall keep as secret all materials of confidential nature which he/she comes across, except when the performance of duties or legal provisions require otherwise. The head shall issue regulations on the handling of confidential information and official secrets used within the police body, which are not military or state secrets. This regulation sets forth the criteria for determining what is considered confidential information. The Minister may, for a valid reason or at the request of an authorized body, release the current or former police officer from the obligation to maintain official secrecy. The obligation to keep the official secret referred to in Paragraphs 1 and 3 of this Article shall continue even after the termination of the employment of the police officer." It can be concluded that the clause on data secrecy is classically formulated, but that inconsistency with the LPCIB also appears here (norming official, military and state secret as types of secret information).

Law on Police of **the Republic of Srpska** [213] provides for the obligation of a police officer to keep secret all confidential information and materials obtained until the cessation of their secrecy, except when the performance of duties or tasks or legal provisions require otherwise, during and after the termination of service. The Minister of the Interior may, for a justified reason or at the request of an authorized body, release the current or former police officer from the obligation to keep secret information (Article 57). Classified information is kept in accordance with the applicable regulations, and in order to provide access only to those persons who have been granted access to classified information of the appropriate level and who need this information in the performance of their work tasks (Article 143, Paragraph 2). Disclosure of data obtained by the employee by performing work and tasks, or in connection with performing work and tasks to unauthorized persons, is a serious breach of duty (Article 117, P. 7). A sanction of termination of employment may be imposed for this violation (Article 119, Paragraph 2, p. 2).

Law on the Internal Affairs of the **FBiH**[214] contains two provisions regarding classified information. Classified information are stipulated as an exception to the general rule, stipulating the duty of the police to inform the public on all important data regarding their competence (Article 9, Paragraph 4), and unauthorized disclosure of classified information is envisaged as a disciplinary offense in relation to the director of police. Other police officers are disciplinary liable according to the general rules of disciplinary responsibility of civil servants (Article 80, Paragraph 1 and Article 89, P. 10).

According the **Montenegrin** Law on Internal Affairs, police officers are under the obligation to adhere to the standards of police work, particularly those stemming from international document, including, inter alia, the duty of protecting confidential and personal data. There are no additional special rules that would constitute a separate legal regime when it comes to access to data or confidentiality.

[213] Law on Police of the Republic of Srpska (Zakon o policiji Rep. Srpske, *Službeni glasnik Rep. Srpske*, nos. 57/2016, 110/2016, 58/2019 and 82/2019).

[214] Law on the Internal Affairs of the FBiH (Zakon o unutrašnjim poslovima FBiH, *Službeni list FBiH*, nos. 81/2014).

When it comes to access to information and classification of information, the **North Macedonian** Law on Interior Affairs[215] envisages in Article 5 some small derogations from the general legal regime applicable to access to information and data confidentiality. Firstly, it states that the Ministry provides information to citizens, legal persons and state authorities on issues from its competence for which they are directly interested. Contrary to the provisions of the Law on Access to Information, the Law on Interior Affairs does not recognise foreign citizens as potential addressees of information provided by the Ministry of the Interior. Further, the Law on Interior Affairs makes the disclosure of information conditional on direct interest. Similar provisions can be found in the North Macedonian Law on the Police.[216] This is not in line with the provisions of the Law on Access to Information, which clearly states that the requester does not need to justify or elaborate the grounds for the request. Secondly, the Law on Interior Affairs and the Law on Police state that information, data and reports that are classified cannot be shared, unless they meet the requirements set forth in a separate law. This can be understood as a reference to the Law on Access to Information, which prescribes a harm test to be conducted, even if the information is classified, and to the provisions on the Law on Classified Information, stating that information that is classified in order to conceal exceeding of powers or their abuse, or the committing of a punishable offence, is not considered classified. The Law on Interior Affairs further states that only the Minister of the Interior or an employee authorised by the Minister can disclose and share the relevant information, while the Law on Police vests these powers to the employee so authorised by the Minister. The Law on Interior Affairs envisages disciplinary liability for disclosing classified information (Article 187) and also expressly states that criminal or misdemeanour liability does not consume disciplinary liability (Article 184-b).

5.2.2. Military

It should be noted that in Bosnia, in accordance with the Law on Defence of Bosnia and Herzegovina[217], BiH has the entire jurisdiction over the Army of Bosnia and Herzegovina, so that the entity laws regulating this matter ceased to apply on 1 January 2006.

The Law on Service in the Armed Forces of Bosnia and Herzegovina[218] (hereinafter: LSAFB) contains one norm regarding confidentiality of information.

---

[215] Law on Interior Affairs of North Macedonia (Закон за внатрешни работи, *Службен Весник на РМ*, nos. 42/20 14,116/2014,.33/15,33/15.5/16,120/16, 127/16, 142/16, 190/16, 21/18, *Службен Весник на РСМ*, 108/19, 275/19).

[216] Law on the Police (Закон за полиција, *Службен Весник на РМ*, nos.114/06, 148/08, 6/09,145/12, бр.41/14,33/15, 31/16,106/16, 120/16, 21/18, 64/18), Article 10.

[217] Law on Defence of Bosnia and Herzegovina (Zakon o odbrani BiH, *Službeni glasnik BiH*, no. 88/2005).

[218] Law on Service in the Armed Forces of Bosnia and Herzegovina (Zakon o službi u oružanim snagama Bosne i Hercegovine, *Službeni glasnik BiH*, nos. 88/05, 53/07, 59/09, 74/10 and 42/12).

Standard 1. Adequate legal framework guaranteeing free access to information is in place

In **Serbia**, regarding the general principle of publicity of work, Law on Serbian Armed Forces[219] (hereinafter: LSAF) contains the solution that the defence minister shall determine the method of issuing public information on the Serbian Armed Forces activities (Art. 30).

Law on civilian service[220] does not contain the principle of publicity. On the contrary, all data about the organization or institution, except from the data available to the public, are considered business i.e. an official secret. This norm is not aligned with the general legal framework governing data secrecy, business and official secret, and it is unclear how it is implemented in practice.

A person in civilian service is obliged to keep data he/she learned in the civilian service as a secret even after finishing the civilian service, and failing to do so is considered as misdemeanour (not excluding potential criminal liability instead of it, in case of grave breaches of the law) (Arts. 36 and 63).

Standard 5. Exceptions to free access to information are clearly formulated in law and not extensive, while a public interest override and harm test are envisaged and applied

Article 161, Paragraph 1, Point m) of the LSAFB establishes violation of regulations on classified or confidential data or information as a disciplinary offense. There are no other norms dealing with access to information or data confidentiality, except for general reference to application of the LPCIB.

Montenegrin Army Law[221] includes provisions that regulate data confidentiality. Firstly, it states in Article 68 that an Army serviceperson is under the obligation to protect and keep confidential data and personal data in accordance with the law, and that this obligation remains even after the army service is terminated. Violation of this data confidentiality constitutes a disciplinary offence.[222] Montenegrin criminal legislation does not envisage the criminal offence of disclosing a military secret.

The regime related to classified information in **North Macedonia** is closely linked to the issues of defence and security. In addition to the general legal regime governing classified information, the Law on the Service in the Republic of North Macedonia Army[223] envisages in its Article 19 the obligation of those in Army service to keep clas-

[219] Law on Serbian Armed Forces (Zakon o Vojsci Srbije, *Službeni glasnik RS*, nos. 116/2007, 88/2009, 101/2010 – other law, 10/2015, 88/2015 – decision of the Constitutional Court, 36/2018 and 94/2019).

[220] Law on civilian service of Serbia (Zakon o civilnoj službi, *Službeni glasnik RS*, no. 88/2009).

[221] Montenegro Army Law (Zakon o Vojsci Crne Gore, *Službeni list RCG*, nos. 51/2017 and 34/2019).

[222] Article 157 of the Law.

[223] Law on the Service in the Republic of North Macedonia Army (Закон за служба во Армијата на Република Северна Македонија, *Службен Весник на РМ*, nos. 36/10, 132/10, 23/11, 47/11, 148/11, 55/12, 29/14, 33/15, 193/15, 71/16, 101/19, *Службен Весник на РСМ*, nos 275/19 and 14/20).

sified information. Namely, the law states that both military and civilian personnel are under the obligation to keep secret the classified information they have learned in performance of army service or in connection to it, even after the termination of service. The North Macedonian Law on Defence[224] also states in Article 139 that members of the Army are under the obligation to keep and protect classified information relevant for the Army. Further, the Law on Service in the Army envisages that only the minister of defence can grant consent that would release a person from this obligation.

This obligation is additionally underlined by the provisions of the North Macedonian Criminal Code, which regulates the disclosure of military secret. This criminal offence is envisaged in Article 349 of the Criminal Code, and is prescribed as communicating, handing over or otherwise making available of data that constitute military secret to an unauthorised person. Military secret, according to the Criminal Code, are data or documents that have been declared as a military secret by a regulation or by a decision of the competent body, on the basis of law, the disclosure of which has had or could have grave damaging consequences to the armed forces and their preparedness to defend the Republic of North Macedonia. However, neither the Law on Defence, nor the Law on Service in the Army or the Law on Classified Information envisage the notion of military secret.

It seems that the regime governing the handling of classified information specifically related to the **North Macedonian** Army is stricter than the general legal regime that applies to all other persons, particularly as the consent whereby a serviceperson or a civilian is freed from the obligation to keep classified information can only be granted by the minister of defence, and not by an official in charge of classified information, in accordance with the relevant law. What is not clear from the North Macedonian regulatory framework is whether the criminal offence of disclosing a military secret from the Criminal Code is consumed by the criminal offence of disclosing classified information from the Law on Classified Information. Likewise, it is unclear whether the mark of "FOR RESTRICTED USE" can also be resorted to by the Army and the Ministry of Defence, and would disclosure of such information constitute the disclosure of a military secret in terms of the Criminal Code.

In **Serbia**, when performing his/her service, a Serbian Armed Forces member shall be obliged to the following: ... 8) keep data secrecy during the service, as well as after the termination of the service in the period determined by the law governing the protection of secret data, unless in a certain way the law is released from the obligation to keep secret, i.e., authorized to disclose secret data to a certain body or person; (LSAF, Art. 13, Para. 1, P. 8). Classified documentation may be reviewed by the military police inspector or a person he/she authorises, in the presence of a person in charge of establishing classification degree or persons he/she authorises. (Art. 53b, Para. 4). Disciplinary offences shall include the following: ... 15) violation of data secrecy or negligent keeping of official records or data; (Art. 149, Para. 1, P. 15)

[224] Law on Defence (Закон за одбрана, *Службен Весник на РМ*, nos. 42/01, 73/02, 78/02, 5/03, 58/06, 110/08, 51/11, 151/11, 215/15, *Службен Весник* на РСМ no. 42/20).

Law on defence[225] (hereinafter: LoD) regulates that classified data related to the defence system marked as data of interest for the national security of the Republic of Serbia, as well as classified data created in the work of commands, units and institutions of the Serbian Army, the disclosure of which would cause damage to unauthorized persons, are protected in accordance with the law on the protection of data secrecy and cannot be made available to the public. Classified information relevant to the defence system is considered to be: 1) data and documents of importance for the national security system, the disclosure of which to unauthorized persons could cause damage to the interests and goals in the field of defence; 2) data on plans for the use of the Serbian Army, war organization and formation of commands, units and institutions of the Serbian Army, data on combat and other material means, i.e., types of movables intended for defence needs, the disclosure of which could cause damage to operational and functional capacity of the Serbian Army; 3) data on patents important for the defence of the country and means and devices intended for defence that are in the process of adoption and examination; 4) data on military facilities and other real estate important for the country's defence, except for data which, according to the regulations on environmental protection, are necessary for the assessment of the impact on the environment; 5) data on undertaken measures, actions and procedures contained in decisions, orders, announcements and other acts in the field of defence of the country, the disclosure of which would harm the interests of the defence forces. At the proposal of the Ministry of Defence, the Government shall further regulate data relevant to the defence system that must be stored and protected in accordance with the law governing the protection of data secrecy, matters of special importance for the defence system in state bodies, companies and other legal entities that should be protected through application of special security measures, as well as criteria for filling the vacancies where these tasks and jobs are performed. (Art. 102)

Also, there are two more types of secret data in LoD: 1) Persons performing defence planning activities and managers of defence plans in state bodies, bodies of autonomous provinces, local self-government units, companies, other legal entities and entrepreneurs important for defence, are subject to security clearance, and are issued an appropriate certificate in accordance with the law regulating protection of data secrecy (Art. 81, Para. 7). 2) Measures for the protection of military facilities and regions in addition to military facilities and facilities shall be taken through general and special protection measures provided by regulations governing the data secrecy (Art. 67a, Para. 1).

Law on military obligation, work obligation and material obligation[226] contains only one norm, regulating all wartime duty schedule of the reserve army members as a secret (Art. 59). Similar norm is contained in the Law on civilian service (Art. 48): "Data on the schedule in the reserve forces shall be treated as classified data, in accordance with the Law."

[225] Law on Defence of Serbia (Zakon o odbrani, *Službeni glasnik RS*, nos. 116/2007, 88/2009, 88/2009 – other law, 104/2009 – other law, 10/2015 and 36/2018).

[226] Law on military obligation, work obligation and material obligation of Serbia (Zakon o vojnoj, radnoj i materijalnoj obavezi, *Službeni glasnik RS*, nos. 88/2009, 95/2010 and 36/2018).

A fine of 500,000.00 to 1,000,000.00 dinars shall be imposed on a legal entity for a misdemeanour: ... 12) if it does not take the prescribed measures for the protection of classified information (LoD, Article 102);

There are no discrepancies between the LoD and LSAF with DSL regarding the type of classified information (secret data) – they have been completely harmonised. Law on civilian service contains two provision (cited articles 36 and 63) that mention “official secret”.

6. CONCLUDING REMARKS

As indicated before, in 2013, the Institute of Comparative Law in Serbia, in cooperation with the Centre for Integrity in the Defence Sector of Norway (CIDS) conducted a comparative legal study of corruption prevention mechanisms set in place to reduce mistakes or improper behaviour in selected countries of the South-East Europe. The study, *inter alia*, covered arrangements for freedom of access to information.[227] The study concluded that every country in the region has undertaken significant efforts to establish a legal framework for building integrity that should provide the basis for prevention and fight against corruption. In the meantime, a number of changes in international standards and national legislations have taken place. The key developments will be outlined below.

In the period from 2013-2021 there were some legislative developments when it comes to international standards on RTI. Firstly, the Council of Europe's Convention on Access to Official Documents has entered into force on December 1, 2020, and is binding on, inter alia, Bosnia and Herzegovina and Montenegro. This imposes clear international requirements on the two said countries. The European Court of Human Rights (ECtHR) has over the years changed its approach to interpreting freedom of information as a fully-fledged unconditional right stemming from Article 10 of the Convention. Namely, the ECtHR has started to build a specific set of standards with regard to RTI, considering that whether and to what extent the denial of access to information constitutes an interference with an applicant's freedom-of-expression rights must be assessed in each individual case and in the light of its particular circumstances. While the change in the approach does not affect regulatory requirements, it may have implications on jurisprudence.

In 2013, Global Principles of National Security and the Right to Information, or Tshwane Principles were adopted. The Tshwane Principles underline that national security should be used as the grounds for denying access to information only in exceptional cases, and that it should be interpreted narrowly. While, as indicated before, the Principles are only a soft-law instrument, the principles provide useful guidance developed by the civil society. Finally, SIGMA Principles of Public Administration, which define what good governance entails in practice and outline the main requirements that countries should follow during the European Integration process, were revised in 2017, while the underlying methodological framework was revised in 2019.

[227] A. Rabrenović (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade 2013, http://iup.rs/books/legal-mechanisms-for-prevention-of-corruption-in-southeast-europe/, 24.2.2022.

There were no normative developments in **Bosnia and Herzegovina** nor its entities in this legal area in the period from 2013-2021; there were no amendments to the analysed law on RTI (last amendments to LFAIB were made in 2013), and certain observed shortcomings (such as the reference to the ombudsman of the RS, which was abolished, mandatory written form of the request, or the preservation of various types of secrets that cause a conflict with the law governing the classification of classified information without a rational explanation) precisely stem from the neglect of this issue by the legislators. Furthermore, the fact that the competence for monitoring the implementation of the law is entrusted to the institution of the Ombudsman is an additional problem, because it is obviously not an effective mechanism that can provide effective remedies in every particular case. The lack of sanctions for noncompliance with the LFAIB has been identified by some reports as a major deficiency in relevant BiH legislation. The general evaluation is that the normative situation is the same as it was in 2013 and cannot be assessed as satisfactory.

Compared to 2013, in terms of the standards and indicators examined in this study, the legislation governing access to information in **Montenegro** has undergone a major change: the amendments to the Law on Free Access to information in 2017. These amendments have resulted in significant backsliding of the right of access to information, due to the fact that access to classified information is fully exempted from the scope of the law, without the need to perform a harm test. Further, one additional exemption, subject to the harm test has been added – the tax secret. The amendments did nothing to advance the compliance of the rules of the Law on Access to Information with the provisions of the Constitution related to access to information. It is also important to note that the Law on Classified Information has also been amended three times since 2013. The most important changes instituted through the amendments relate to the fact that the categories of data that can be classified can now be regulated in more detail by the public authorities in whose work the classified data are created; previously, this power was vested with the Government of Montenegro only, and it related to the top three degrees of classification, but the Government never adopted such a detailed document. This decentralization of powers has the potential to be beneficial, as the various public authorities can fine-tune the secondary legislation to suit their specific needs and standards. On the other hand, there is concern that the capacities of various sectoral public authorities are not sufficient to deal with this topic systemically and with a view to relevant international standards, which may result in over-classification, and consequently, exemption from the right to free access. When it comes to other categories of confidential information that may be exempt from the rules on access to information, the legislative framework of Montenegro remains fragmented, with the norms on business secret being regulated in a number of laws without a consistent definition. In order for the Montenegrin legislation to be rendered more compliant with relevant international standards, the rules on absolute exemption of classified information need to be changed, rendering classified information subject to the harm test. There is also a need to systemically address the discrepancies between the constitutional and statutory norms regulating allowed exemptions from free access to information.

The regulatory framework of **North Macedonia** governing free access to information has undergone a number of changes since 2013. Firstly, the Law on Access to information, passed in 2006, with amendments in 2008 and 2010, was additionally amended in 2014, 2015, 2016 and 2018. In 2019, a new Law on Access to Information was passed. The adoption of the new law did bring some improvements, bringing the regulatory framework more in line with international standards. The deadline imposed on the public authorities for answering requests for access to information was shortened from the previously too long 30 to 20 days. While this is still at the top of the range of such time limits as per RTI, it is a definite step in the right direction. The second important change has to do with the exemptions from the right of access to information. In the 2019 Law, the number of such exemptions has been reduced so to exclude previously rather wide exceptions, such as the one concerning information regarding commercial or other economic interests, the disclosure of which would have detrimental consequences. These two interventions render the North Macedonian legal framework more in line with relevant international standards. The second law relevant for access to information, the North Macedonian Law on Classified Information, was also adopted in 2019. Most importantly in the context of free access to information, this law explicitly envisages that the degree of classification of information is determined on the basis of an assessment of the possible damage and the consequences that would result from unauthorized access to such information, thus incorporating clearly the harm test in the classification process. This is an important improvement compared to the previous regulatory regime, and one that may prove to be useful in cases, where access to classified information is requested under the law governing free access to information. Just as in the case of Montenegro, North Macedonia still has a highly fragmented regulatory framework, envisaging various types of confidentiality, including a sanctioning regime for cases when such confidentiality is breached. The most notable issue in that respect that still needs to be resolved, is the fact that the North Macedonian Criminal Code has still not been harmonized with the new legislation of classification of information. Namely, the disclosure of state secret is criminalized in Article 317 of the Criminal Code, but other levels of classification are not covered, while the incriminations for protection of military secret, for example, were still envisaged in the law, even though military secret is not regulated by current positive law. The overall impression is that the legislation of North Macedonia has improved compared to the state of affairs in 2013.

In 2021, amendments to the existing Law on Access to Information of Public Importance were passed in **Serbia**; it had previously not been amended since 2010. The amendments introduced some significant changes; unfortunately, not all of them can be deemed as positive. Firstly, the law extended the definition of public authority bodies that RTI applies to, by clearly including natural persons vested with public powers within its scope, such as notaries and public enforcement agents, privately owned commercial entities that provide communal services, and companies where over 50% of the shares are owned by the state, autonomous province or local self-government unit, but also their daughter-companies. This clear definition is a definite step forward.

On the other hand, the amendments have introduced additional grounds for limiting access to information regarding protection of competition, international arbitration law, implementation of monetary, foreign exchange or fiscal policy, financial stability, foreign exchange reserve management, supervision of financial institutions or issuing banknotes and coins, business or professional secret, intellectual or industrial property, protection of artistic, cultural and natural assets, environment or rare plant and animal species – all of these exceptions have yet to be elaborated in more detail through future practice. Furthermore, the amendments have extended the scope of bodies whose decisions regarding requests for access to information are not subject to appeal to the Commissioner, and instead can be challenged only in administrative dispute, by adding the National Bank of Serbia to the list. An improvement is made in as much as procedural rules are specified in cases where access to confidential information is requested. The time limit for the Commissioner's decision on appeal is extended from 30 to 60 days – while this time limit is in principle thus harmonised with the one set by the General Administrative Procedure Act (Art. 174) for the decisions of second-instance bodies, the motivation for this change in fact seems to lie in the workload of the Commissioner (as elaborated in the relevant Bill[228]). While current objective reasons may imply that such extended time limit is more realistic, the message sent thereby is not one that is in favour of ensuring an efficient remedy in cases when access to information is denied by the decision of the first-instance body.

The amendments also increase the term of office of the Commissioner to eight years, but without the possibility of re-election. The Commissioner was given certain additional powers in the implementation of the acts he passed. Thus, now the Commissioner can force the executor – the public authority to fulfil the obligations from the decision of the Commissioner by indirect coercion, by imposing fines. The fines that can be pronounced range from 20,000 to 100,000 dinars and can be imposed several times. The imposed fine is executed by the court in accordance with the law governing enforcement and security. Also, the Commissioner is authorized to submit a request for initiating misdemeanour proceedings for misdemeanour's provided for by this Law, when in the appeal procedure he/she assesses that there is a misdemeanour.

With regard to free access to information, the regulatory frameworks of the analysed countries show a considerable degree of compliance with international standards. Further, they mostly seem to have improved compared to the regulatory framework in 2013, with the exception of Montenegro, which has shown backsliding due to the legislative interventions implemented in 2017. Some backsliding is also visible in the amendments to the 2021 Serbian RTI law: it remains to be seen whether they will be offset by the simultaneous improvements introduced therein. This generally positive assessment can reasonably be attributed to two key factors. Firstly, as shown in previous studies,[229] the legislation on free access to information is relatively novel

[228] Proposal Law on Amendments to the Law on Free Access to Information of Public Importance (Predlog zakona o izmenama i dopunama Zakona o slobodnom pristupu informacijama od javnog značaja), http://www.parlament.gov.rs/upload/archive/files/cir/pdf/predlozi_zakona/2021/1758-21.pdf, 24.2.2022., 25.

[229] See in particular: A. Knežević Bojović, "Free Access to Information of Public Importance", in: A. Rabrenović (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade 2013, 131-152.

in the legal systems of the analysed countries, and is developed under the strong influence of the European accession process and related external conditionality. Furthermore, out of the mutually closely connected legislative trio (information triangle): data secrecy, personal data protection, free access to information[230], the latter was usually the last to be formally adopted. These two factors combined mean that the legislators, when adopting access to information legislation, tend to approach the exercise while having in mind the requirements of the EU accession process and the entailed scrutiny over the proposed and promulgated solutions that will come from a variety of actors, such as the EU Commission, SIGMA, and the Venice Commission. Consequently, they aim for a high degree of compliance between the norms of national legislation and the norms of existing international documents, standards, or best practice examples from the region. While it has been argued, and to an extent proven, that the practical implementation of this legislation leaves a lot to be desired,[231] the letter of the law remains close or identical to the legislative standard. The hypothesis that the progress in EU integration will affect the level of compliance of the countries' FOI legislations with international standards, was not fully confirmed. While all countries have shown some departures from the standard, there are but a few manifest outliers in terms of conformity or lack of conformity with international standards, and in the case of the latter, some countries that are further on the EU accession path, in fact, have lower compliance scores. While the legislative framework of Serbia remains most aligned with relevant international frameworks – a finding that is consistent with its high RTI scoring – the regulatory systems of the other three countries and two entities score almost the same. In fact, advanced compliance with international standards in one indicator is offset by the departure from them in another, and vice versa. This lack of significant differences in overall compliance with international standards can perhaps be attributed to a continued shared approach to RTI, which will be commented on several paragraphs below.

The extent of lack of compliance varies – these are sometimes manifested in insufficiently clear norms or lack of express regulation of a matter, but which do not fundamentally affect the exercise of the right of free access to information. In some, more serious cases, the departures from the standards are considerable. The underlying reasons for such a legislative approach can only be speculated on, but seem to show a preference towards secrecy. And it is precisely in this, most complex point, where the legislation on free access to information prescribes limitations to this freedom, that the majority of legislations do not show full compliance with international standards.

This is also the point in which the legislations on secrecy and free access to information intersect. And while the general and overarching legal framework governing classification of information is also mostly in line with international standards, the analysis shows the existence of a complex body of legislation regulating various types of secrets and imposing confidentiality requirements. Although the existence of

[230] V. V. Vodinelić, "Normiranje informacionog trougla", in: S. Gajin (ed.), *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Belgrade 2019, 19.
[231] See: A. Knežević Bojović (2013).

other types of secrets other than those found in the main legislation governing data classification is not uncommon in any legal system, their numbers, coupled with a lack of clear regulation and differing definitions of the same notion in various legal acts, constitute a serious disincentive for a proactive approach to free access to information. Furthermore, the related disciplinary, and sometimes even criminal liability, in case of unauthorised disclosure of these types of secrets or confidential information surely render the task of a civil servant, a police officer or a militaryserviceperson, when faced with the request to allow access to information, complex and challenging.

The analysis has also shown that the approach apparently taken by the legislators – to copy/paste the relevant norms, without going into too much detail of the related operational requirements, leaves room for improvement of the texts of both primary and secondary legislation.

This approach implies some even more alarming connotations. Careful and comprehensive scrutiny over the regulatory frameworks of all four countries shows a lack of genuine interest, on the part of the legislator and the executive alike, to regulate RTI systemically and consistently, with a view to ensuring that all the rights nominally guaranteed can be truly exercised in practice. An extreme example can be found in the legislation of the Republic of Srpska, which unperturbedly prescribes a legal remedy before an institution which has not been operational for the last twelve years. It does seem that compliance is promoted at face value, but true commitment to overcoming the secrecy legacy of the past is lacklustre.

What is also notable is the lack of consideration towards the ways in which persons with special needs can exercise the right of free access to information.

This last observation is perhaps a testament of the highly fragmented approach to the legislative process, which can often be seen in the regulatory frameworks of Western Balkan countries – one subject-matter is regulated without taking into full consideration its implications on other sectoral legislation.

This fragmented approach also seems to be one of the key factors to the assessed lack of compliance of FOI legislation of the analysed countries with relevant international standards. Another is the observed lack of concern for the actual effectiveness of the RTI norms. If there are instances of rather blatant disregard not only for international standards (e.g. heavily reduced scope of application of RTI law in Montenegro, introduction of dubious and arbitrary rules on additional possibilities for classification of information in North Macedonia), but for the realities of the legal and institutional systems in the home country (e.g. prescribing a remedy before an institution that no longer exists, as the case is in the Republic of Srpska) or a fully-fledged copy-paste approach with little or no additional operationalization – then one can only wonder whether even the best regulatory framework would, in fact, result in satisfactory practice. The most likely answer – an educated guesstimate if you will – unfortunately, is no.

It seems, therefore, that it will take some additional time for the FOI legislation to become fully and more seamlessly integrated in the national legal frameworks in substantive, procedural and institutional terms.

The conclusions made above can be best illustrated with an overview of the extent of compliance of national legislations with the international standards examined in this study, per standard.

1. Adequate legal framework guaranteeing free access to information is in place

The legislations of Montenegro, North Macedonia and Serbia recognise the right to information as a human right. Conversely, the legislative framework of BiH recognizes this right as a human right only implicitly. The constitutions of the FBiH and the Republic of Srpska do not recognise the right to information at all.

The legal frameworks of the four analysed countries are not uniform when it comes to creating a specific presumption in favour of access to all information. The normative frameworks of Serbia and BiH envisage such a presumption. In Montenegro and North Macedonia the situation is somewhat different and subject to a number of caveats. While these render the regulatory frameworks of North Macedonia mostly in line with standards, the legislative framework of Montenegro is mostly not in line with the standard, as it fully excludes classified information from the scope of the RTI rules.

2. Free access to information applies to a wide scope of information holders

All the analysed countries envisage a broad scope of application of the RTI, covering a wide set of public bodies. The legislations of Serbia, Montenegro and North Macedonia also envisage that the right of access also applies to state-owned enterprises, other public authorities, including constitutional, statutory and oversight bodies and to private bodies that are vested with public authority. Conversely, RTI laws of BiH and of the analysed entities do not apply to private bodies that perform a public function.

3. Requesting procedures are not complicated, are not strictly conditioned and are free, while access fees are proportionate to actual costs

In all of the analysed countries, the requesters are not required to provide reasons for their requests, which is in line with the standard. However, the legislation of North Macedonia envisages that the requester has to explicitly state that it is a request for access to information, which is an overly formalistic requirement.

With regards to procedures for making requests, the legislations of Serbia, Montenegro and North Macedonia envisage the possibility for the request to be made orally,

in writing, or in electronic format, which is in line with the standard. Conversely, the legislations of BiH, FBiH and Republic of Srpska explicitly stipulate that the request can only be made in writing, rendering them partially in line with the standard.

The legislations of all four analysed countries and two entities in BiH envisage some form of assistance to be provided to the requesters in order to help them formulate their requests. Unfortunately, none of the legislations include explicit norms on the obligation of the public officials to provide assistance to requesters with special needs. The latter is a departure from the standard which should be systemically addressed.

The filing of requests is free in all four countries. Access fees are set centrally and are generally limited to the cost of reproducing and sending the information, which is in line with the standard. However, some additional requirements are prescribed by the legislations of Montenegro, North Macedonia, and Serbia, rendering them mostly in line with the standard.

4. The procedure for dealing with requests is conducted within a reasonable timeline

The legislations of the four analysed countries are similar and are mostly in line with relevant international standards. The laws of Serbia and Montenegro clearly set forth an urgent deadline for response to the request in cases where the life or freedom of a person are contingent on access to the requested information, which is a solution that can be assessed as fully convergent with relevant international standards. The legislations of BiH and North Macedonia, although prescribing precise timelines (in North Macedonia the timeline is at the top of the acceptable range), do not promote prompt responses to the requests, rendering them not fully in line with international standards.

5. Exceptions to free access to information are clearly formulated in law and not extensive, while a public interest override and harm test are envisaged and applied

The legislations of the four analysed countries do not envisage any cases in which it absolutely presumes that the public's interest to know trumps secrecy provisions. Their legislations, however, generally prescribe that the right to access information can only be restricted in limited cases and following a harm test. The notable exception is Montenegro, which excludes classified information from the scope of the RTI law.

With regard to limitations to the right of access to information, the analysed legal systems are broadly in line with relevant international standards. This assessment, however, needs to be put into context. The limitations of the right to information are

mostly set forth in RTI laws, with the exception of Montenegro, which sets out these limitations both in the Constitution and in the statute, without mutually aligning them. However, absolute exceptions from the scope of RTI law, or relative limitations, subject to the harm test and/or public interest test, are articulated in the rules and conditions for classification of information.

In all four analysed countries, other laws also prescribe various classes of information that must be kept secret by those who learn them in their official capacity. These classes of secrecy do not fall under the scope of either RTI or classification laws – but must be observed, nonetheless. Some of these classes of information logically fall under the categories that are deemed as justified limitations to RTI, others less so. The situation is additionally complicated by the fact that these types of secret information are not defined; instead, their meaning needs to be deduced from the legislator's intention. This often sets a rather broad margin of appreciation both in the implementation of those laws, and their subsuming under the rules of the RTI or classification laws. Finally, a particular challenge for those working in the public sector lies in the fact that unauthorised disclosure of various types of secrets – and this relates not only to classified information, but also to the information that can be declared secret in terms of other laws – constitutes a disciplinary offence, and, in some cases, even a criminal offence. Therefore, the problem an RTI officer in the public sector can face is a complex one, as care must be taken of not only RTI legislation and legislation governing classification of information, but numerous sectoral laws need to be taken into account as well, in order to make a balanced and lawful decision on whether to allow access to information, and possibly face disciplinary or even criminal charges, or invoke one of the prescribed limitations and restrict access. It should be pointed out once again that the norms regulating secrecy or confidentiality of data and business secrets in the laws of the analysed countries do not seem unproportionate. However, despite the observed proportionality of these norms, their relations with the access to information laws are not clearly regulated, which provides a broad field for interpretation and a wide margin of appreciation in deciding on whether to allow access to information or not.

As for the application of a harm test, which is used so that access can be refused only where disclosure poses a risk of actual harm to a protected interest, it should be noted that some form of harm test is envisaged in the legislations of all four countries. The legislations of all analysed countries envisage a severability clause, thus enabling that, where only part of a record is covered by an exception, the remainder must be disclosed.

All the analysed legislations envisage that grounds and reasons for refusal must be stated in the ruling whereby access to information is refused. It is the level of detail in this regulation that renders some countries mostly in line with the standard, as the case is with the legislations of Montenegro, Serbia and North Macedonia, or fully in line with the standard, as the case is with the laws in BiH.

6. There is a designated supervisory authority overseeing the implementation of the legislation on public information with the power to set standards, make prescriptions and impose sanctions.

The legislations of all four analysed countries envisage the right to an external appeal with an independent administrative oversight body. However, the law of the Republic of Srpska envisages the appeal to be addressed to the Ombudsman of the Republic of Srpska, which is no longer operational. The laws of all the countries are nominally fully in line with the standard, with the caveat that the law of the Republic of Srpska can be deemed as ineffective.

When it comes to the mandate, powers and the binding nature of the decisions of the independent oversight bodies, the laws of the analysed countries range considerably. The power of the independent oversight body to order appropriate remedies for the requester is also regulated in different ways in the legislations of the analysed countries. The lack of powers stems both from the choice of the independent oversight body i.e. Ombudsmen in BiH, and the legislative inadequacies, e.g. in Montenegro.

Legal regime for the security sector (army and police)

The legal regimes for the security sector do not differ considerably from the legal regime applicable to civil servants when it comes to access to information and classification of data. The limitations to the free access to information that are inherent to the security sector, which are grounded in the specific needs of the police and the military, are already embedded in the general legal regime. The only point of slight convergence can be found in the legal regimes applicable to the disciplinary liability of police officers and military personnel, and to an extent, to the scope of potential beneficiaries of the right to free access to information. However, these convergences are more nuances, than differences that would entail this regime to be considered as a separate legal regime. The threat of disciplinary or even, in some cases, criminal liability, however, can be seen as an additional disincentive for police officers and military personnel to fully embrace free access to information as a general interest that overrides secrecy.

When it comes to the defence sector standards, it should be noted that none the legislations in the analysed countries clearly define the types of information that the public administration authorities have the right to withhold on national security grounds. The definitions found in laws on classification of information are very general, and more detailed regulation in secondary legislation is also lacking.

BIBLIOGRAPHY

Articles and monographs

1. Augustyn M., Monda C., *Transparency and Access to Documents in the EU: Ten Years on from the Adoption of Regulation 1049/2001*, http://www.eipa.eu/files/repository/eipascope/20110912103927_EipascopeSpecialIssue_Art 2.pdf.
2. Banisar, *Freedom of Information Around the World 2006: A Global Survey of Access to Government Records Laws*, Privacy International 2006.
3. Blanke H-J., Perlingeiro R., *Essentials of the Right of Access to Public Information: An Introduction*, Springer International Publishing 2018.
4. Blanton L., "The World's Right to Know", *Foreign Policy*, No. 131 (Jul. - Aug 2002), 50-58.
5. Calland R., Bentley K., "The Impact and Effectiveness of Transparency and Accountability Initiatives: Freedom of Information Development", *Policy Review* 31/2013, s69–s87. doi:10.1111/dpr.12020.
6. Camaj L., "From 'window dressing' to 'door openers'? Freedom of Information legislation, public demand, and state compliance in South East Europe", *Government Information Quarterly*, Volume 33, Issue 2, 2016, 346-357, https://doi.org/10.1016/j.giq.2016.03.001.
7. Cardona F., *Freedom of speech, right to know and reporting unlawfulness: the lifeblood of preventing abuse of power and corruption in the defence sector*, CIDS, 2020.
8. Ćeranić Perišić, J., "Bliža integracija zemalja Zapadnog Balkana sa Evropskom Unijom na osnovu nove metodologije proširenja EU", *Srpska politička misao* 3/2020, https://doi.org/10.22182/spm.6932020.7, 153-157.
9. Ćeranić Perišić, J., "Izazovi evropskih integracija zemalja Zapadnog Balkana dve decenije nakon početka procesa", Primena prava i pravna sigurnost : zbornik radova 34. susreta Kopaoničke škole prirodnog prava - Slobodan Perović, 2021, Tom 3, 399-412.
10. Čok V., *Javno informisanje, javnost rada i dostupnost informacija - pravna teorija i zakonodavstvo*, Savremena administracija, Belgrade 1982, 80.
11. Ćorić Erić, V., *Odnos Evropskog suda pravde i Evropskog suda za ljudska prava*, doctoral thesis, Belgrade University Law Faculty, 2013, available at: https://nardus.mpn.gov.rs/handle/123456789/2642, 6.4.2022.
12. Ćorić, V. Knežević Bojović, A., "Indirect Approach to Accountability of Corporate Entities through the Lens of the Case-Law of the European Court of Human Rights", *Strani pravni život* 4/2018, pp. 25-37, doi: 10.5937/spz0-20339.
13. Dacian D., Kovac P., Marseille A. T., *From the Editors: The Story of a Data-Driven Comparative Legal Research Project on FOIA Implementation in Europe*, Springer International Publishing, 2019.
14. Doshi R., Kelley J. G., Simmons B. A., *The Power of Ranking: The Ease of Doing Business Indicator and Global Regulatory Behavior*.
15. Gajin S., "Odmeravanje suprotstavljenih interesa u primeni Zakona o slobodnom pristupu informacijama od javnog značaja", *Srpska politička misao 4/2018*, 231-248, https://doi.org/10.22182/spm.6242018.11.
16. Glušac L., Tepavac T., "Narušavanje podele i ravnoteže vlasti: dominacija egzekutive u Srbiji", in *Otete institucije u Srbiji: teorija i praksa*, Belgrade 2019, 80-102.

17. Gomez M., "The Right to Information and Transformative Development Outcomes", *Law and Development Review 2019*; 12(3): 837–864.
18. Grabbe H., *The EU's Transformative Power Europeanization Through Conditionality in Central and Eastern Europe*, Palgrave Macmillan UK, Basingstoke 2006.
19. Jovanović B., Jovanović B., "Ease of doing business and FDI in the ex-socialist countries", *International Economics and Economic Policy*, vol. 15(3)/2018, 587-627.
20. Kelley J.G., *Ethnic Politics in Europe: The Power of Norms and Incentives*, Princeton University Press, Princeton 2004.
21. Knežević Bojović A., "Free Access to Information of Public Importance", in: Rabrenović A. (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade 2013, 131-152.
22. Knežević Bojović A., Ćorić V., Višekruna A. „Spoljašnje uslovljavanje Evropske unije i regulatorni odgovori Srbije", *Srpska politička misao* 3/2019, 233-253, https://doi.org/10.22182/spm.6532019.10.
23. Knežević Bojović A., Radević R., "Free Access to Public Information, Integrity and Good Governance in the Western Balkans", in: *Integrity and Good Governance in the Western Balkans* (eds. A. Rabrenović, A. Knežević Bojović), Regional School of Public Administration, Danilovgrad 2018.
24. Kregar J., Gotovac V., Gardašević Đ., *Regulacija prava na pristup informacijama*, Transparency International Hrvatska, 2004.
25. M. Matijević, "Adequate Representation of Persons Belonging to National Minorities in Public Sector: The Nature, Content and Scope of Obligations in the Comments of the Advisory Committee for the Framework Convention", *Strani pravni život*, 4/2020, 55-68. doi: 10.5937/spz64-29799.
26. Mendel T., "Freedom of information: An internationally protected human right", *Comparative Media Law Journal*, 1/2003.
27. Mendel T., *Freedom of Information: A comparative legal survey*, UNESOC, Paris, http://portal.unesco.org/ci/en/files26159/12054862803freedom_information_en.pdf/freedom_information_en.pdf.
28. Michener G., Nichter S., "Local compliance with national transparency legislation", *Government Information Quarterly*, Volume 39, Issue 1/2022, 101659, https://doi.org/10.1016/j.giq.2021.101659.
29. Milenković D., "Upravno-procesna i drugi slični oblici zaštite prava na pristup informacijama u komparativnom pravu", *Strani pravni život*, 3/2015, 115-131, https://www.stranipravnizivot.rs/index.php/SPZ/article/ view/163.
30. Milovanović D., Davinić M., Cucić V., "Free Access to Information in Serbia: A European Perspective" in: *The Laws of Transparency in Action*, Palgrave Macmillan, Cham, 2019.
31. OECD, "The Right to Open Public Administrations in Europe: Emerging Legal Standards", *SIGMA Papers No. 46 (2010)*, OECD Publishing, Paris, https://doi.org/10.1787/5km4g-0zfqt27-en.
32. Ohranović A., *Pozicija ombudsmena u upravnom postupku i postupcima pred sudovima BiH, obim i vrsta ovlaštenja i mogućnosti koje mogu koristiti*, Fondacija centar za javno pravo, Sarajevo 2017.
33. Popović J., "Legislative Regulation of Data Confidentiality in the Countries on the Territory of the Former Socialist Federal Republic of Yugoslavia", *Atlanti*, Vol. 20, Trieste 2010, 229-238.

34. Pridham G., *Designing democracy: EU enlargement and regime change in post-communist Europe*, Palgrave Macmillan UK, Basingstoke 2005.
35. Rabrenović A. (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade, 2013.
36. Rabrenović A. (ed.), *Legal Mechanisms for Prevention of Corruption in Southeast Europe with Special Focus on the Defence Sector*, Institute of Comparative Law, Belgrade 2013, http://iup.rs/books/legal-mechanisms-for-prevention-of-corruption-in-southeast-europe/.
37. Rabrenović A., Knežević Bojović A. (eds.), *Integrity and Good Governance in the Western Balkans*, Regional School of Public Administration, Danilovgrad, 2018.
38. Rabrenović A., Knežević Bojović A., "The Right of an Individual to Free Access to Information – The Case of Serbia", in: Novaković M., Kostić J. (eds.), *The Position of the Individual in Modern Legal Systems*, Institut za uporedno pravo, Belgrade 2019.
39. Rabrenović A., Radević R., "Granice prava na slobodan pristup informacijama u sektoru bezbednosti - primer Crne Gore", *Strani pravni život*, 3/2016, 23-38.
40. Reljanović M., "Krivičnopravna zaštita elektronskih tajnih podataka", in: Gajin S. (ed.), *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Belgrade 2012, 38-51.
41. Reljanović M., "Vojna tajna u nacionalnom zakonodavstvu i praksi", in: Gajin S. *et al.*, *Zaštita podataka o ličnosti i poverljivi podaci*, Open Society Fund, Belgrade 2005.
42. Reljanović M., „Međunarodna saradnja Republike Srbije u razmeni i zaštiti tajnih podataka", in: Gajin S., Matić G. (eds.), *Primena Zakona o tajnosti podataka*, Belgrade, 2014, 46-66.
43. Roziere B., Walby K., "The duty to assist in Canadian Freedom of Information law", Can. Public Admin., 63/2020: 582-601. https://doi.org/10.1111/capa.12392.
44. Šabić R., "Otvorena pitanja primene zakona o slobodnom pristupu informacijama od javnog značaja u periodu nakon usvajanja zakona o tajnosti podataka", in: "Pristup informacijama od javnog značaja i zaštita tajnih podataka", Belgrade 2012.
45. Schimmelfennig F., Engert S., Knobel H., *International socialization in Europe: European organizations, political conditionality and democratic change*, Palgrave Macmillan UK, Basingstoke 2006.
46. Schimmelfennig F., Sedelmeier U. (eds.), *The Europeanization of Central and Eastern Europe*, Cornell University Press, Ithaca 2005.
47. Schimmelfennig F., Sedelmeier U., "Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe", *Journal of European public policy*, 11(4)/2004, 661-679.
48. Schimmelfennig F., Sedelmeier U., "The Europeanization of Eastern Europe: the external incentives model revisited", *Journal of European Public Policy*, 27(6)/2020, 814-833.
49. Stanić M., "Izbor članova nadzornog tela za zaštitu ličnih podataka kao garantija nezavisnosti – primeri Albanije, Bosne i Hercegovine, Crne Gore i Severne Makedonije", *Strani pravni život*, 3/2020, 125-135. doi: 10.5937/spz64-28379.
50. Vachudova M. A., *Europe undivided: democracy, leverage, and integration after communism*, Oxford University Press, Oxford 2005.
51. Veljanovska S., Dukovski S., "The Law on Free Access to Information of Public Character and its Respect from the Judicial Council of RN Macedonia", *Horizonti 2021*, 1 (28), 1-8.
52. Vodinelić V. V., Gajin S., *Slobodan pristup informacijama: ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Belgrade 2004.
53. Vodinelić V.V, "Normiranje informacionog trougla", in: S. Gajin (ed.), *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Belgrade 2019.

54. Worthy B., John P., Vannoni M., "Transparency at the Parish Pump: A Field Experiment to Measure the Effectiveness of Freedom of Information Requests in England", *Journal of Public Administration Research And Theory*, 2016.
55. Zhelyazkova A., Damjanovski I., Nechev Z, Schimmelfennig F., "European Union conditionality in the Western Balkans: external incentives and Europeanisation", in Džankić J., Keil S., Kmezić M. (eds), *The Europeanisation of the Western Balkans*, Palgrave Macmillan, 2019, 15-37.
56. Žuffová M., "Do FOI laws and open government data deliver as anti-corruption policies? Evidence from a cross-country study", *Government Information Quarterly*, Volume 37, Issue 3, 2020, 101480, https://doi.org/10.1016/j.giq.2020.10148.
57. Zúñiga N., Jenkins M., Jackson D., *Does More Transparency Improve Accountability?*, Transparency International, 2018.

International legal sources

1. Charter of Fundamental Rights of the European Union, *Official Journal of the European Union 2010/C 83/02*.
2. Consolidated version of the Treaty on European Union, Official Journal of the European Union C 83/13.
3. Convention on access to information, public participation in decision-making and access to justice in environmental matters, done at Aarhus, Denmark, on 25 June 1998.
4. Convention on Access to Official Documents, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205.
5. Directive 2003/4/EC of 28 January 2003 on public access to environmental information, repealing Council Directive 90/313/EEC.
6. European Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.echr.coe.int/documents/convention_eng.pdf, 24.2.2022.
7. European Court of Human Rights, *Cangi v. Turkey*, Application no. 24973/15.
8. European Court of Human Rights, *Magyar Helsinki Bizottság v. Hungary*, Application no. 18030/11.
9. European Court of Human Rights, *Sdružení Jihočeské Matky v. Czech Republic*, Application no. 19101/03, judgment 10 July 2006.
10. European Court of Human Rights, *Társaság a Szabadságjogokért v. Hungary*, Application no. 37374/05, judgment 14 April 2009.
11. European Court of Human Rights, *Youth Initiative for Human Rights v. Serbia*, Application no. 48135/06.
12. *International Covenant on Civil and Political Rights*, General Assembly Resolution 2200A (XXI) of 16 December 1966.
13. Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents, https://wcd.coe.int/ViewDoc.jsp?id=262135.
14. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *OJ L 145,* 31 May 2001*,* 43–48.
15. Regulation No. 1049/2011 regarding public access to European Parliament, Council and Commission documents.

16. *United Nations Convention against Corruption*, resolution 58/431 of October 2003.
17. *Universal Declaration of Human Rights*, General Assembly resolution 217 A (III) of 10 December 1948.

National legal sources

Bosnia and Herzegovina

1. Annex IV of the General Framework Agreement for Peace in Bosnia and Herzegovina and *Službeni glasnik*, no. 25/2009 – Amendment I.
2. BiH Constitutional Court (Ustavni sud BiH) decision no. AP 461/16 of 6.6.2018
3. Court of Bosnia and Herzegovina Judgment No. S1 3 U 016743 14 Uvp of 11.3.2015.
4. Criminal Law of BiH (Krivični zakon BiH, Službeni glasnik BiH, nos. 3/2003, 32/2003 – correction, 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015 and 35/2018).
5. Criminal Procedure Law of BiH (Zakon o krivičnom postupku BiH, Službeni glasnik BiH, nos. 3/03, 32/03 – correction, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 29/2007, 53/07, 58/08, 12/09, 16/09, 53/09 – other law, 93/09, 72/13 and 65/18).
6. Law on Civil Service in the Institutions of Bosnia and Herzegovina (Zakon o državnoj službi u institucijama BiH, Službeni glasnik BiH, nos. 12/02, 19/02, 8/03, 35/03, 4/04, 17/04, 26/04, 37/04, 48/05, 2/06, 50/08 – other law, 43/09, 8/10, 40/12 and 93/17).
7. Law on Defence of Bosnia and Herzegovina (Zakon o odbrani BiH, Službeni glasnik BiH, no. 88/2005).
8. Law on free access to information in Bosnia and Herzegovina (Zakon o slobodi pristupa informacijama u Bosni i Hercegovini, Službeni glasnik BiH, no. 28/00).
9. Law on Police Officers of Bosnia and Herzegovina (Zakon o policijskim službenicima Bosne i Hercegovine, *Službeni glasnik BiH*, nos. 27/04, 63/04, 5/06, 58/06, 58/06, 15/08, 50/08 – other law, 63/08, 35/09 and 7/12).
10. Law on protection of classified information (Zakon o zaštiti tajnih podataka, *Službeni glasnik BiH*, nos. 54/05 and 12/09).
11. Law on Service in the Armed Forces of Bosnia and Herzegovina (Zakon o službi u oružanim snagama Bosne i Hercegovine, Službeni glasnik BiH, nos. 88/05, 53/07, 59/09, 74/10 and 42/12).
12. Law on the Human Rights Ombudsmen of Bosnia and Herzegovina (Zakon o Ombudsmenu za ljudska prava Bosne i Hercegovine, Službeni glasnik BiH, nos. 19/2002, 35/2004, 32/2006, 38/2006 – correction, and 50/2008 – other law
13. Law on protection of classified information (Zakon o zaštiti tajnih podataka, Službeni glasnik BiH, nos. 54/05 and 12/09).

Federation of Bosnia and Herzegovina

1. Company Law (Zakon o privrednim društvima, *Službeni list FBiH*, no.81/2015).
2. Constitution of the Federation of Bosnia and Herzegovina (Ustav Federacije Bosne i Hercegovine, Službeni list FBiH, no. 1/1994).
3. Criminal Law of the FBiH (Krivični zakon FBiH, Službeni list FBiH, nos. 36/2003, 21/2004 – correction, 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 and 75/2017).

4. Law on freedom of access to information (Zakon o slobodi pristupa informacijama, Službeni list FBiH, no. 20/2001).
5. Law on the Internal Affairs of the FBiH (Zakon o unutrašnjim poslovima FBiH, Službeni list FBiH, nos. 81/2014).

Montenegro

1. Administrative Court of Montenegro Decision U. 7765/18 of 3.7.2019.
2. Administrative Court of Montenegro Judgment U. 2757/18 of 21.1.2020.
3. Company Law of Montenegro (Zakon o privrednim društvima, *Službeni list RCG*, no.65/2020)
4. Constitution of Montenegro (Ustav Crne Gore, *Službeni list RCG*, nos. 1/2007 and 38/2013-1).
5. Criminal Code (Krivični zakonik Crne Gore, *Službeni list RCG*, nos. 2003, 13/2004, 47/2006, 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, 49/2018, 3/2020 and 26/2021).
6. Labour Law (Zakon o radu, *Službeni list RCG*, no. 74/2019 i 8/2021).
7. Law on Administrative Procedure of Montenegro (Zakon o upravnom postupku, *Službeni list RCG*, nos. 56/2014, 20/2015, 40/2016 and 37/2017).
8. Law on Civil Servants (Zakon o državnim službenicima i namještenicima, Službeni list RCG, nos. 2/2018, 34/2019 and 8/2021Law on Data Secrecy (Zakon o tajnosti podataka, *Službeni list RCG,* no. 14/2008, 76/2009, 41/2010, 40/2011, 38/2012, 44/2012, 14/2013, 18/2014, 48/2015 and 74/2020).
9. Law on free access to information (Zakon o slobodnom pristupu informacijama, Službeni list RCG, no. 68/05)
10. Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti, Službeni list RCG, nos. 79/2008, 70/2009, 44/2012 and 22/2017).
11. Law on Tax Administration (Zakon o poreskoj administraciji, Službeni list RCG, nos. 65/01, 80/04, 29/05, 20/2011, 28/2012, 8/2015, 47/2017 and 52/2019).
12. Montenegro Army Law (Zakon o Vojsci Crne Gore, Službeni list RCG, nos. 51/2017 and 34/2019).

North Macedonia

1. Company Law (Закон за трговските друштва, Службен Весник на РМ, nos. 28/2004, 84/2005, 25/2007, 87/2008, 42/10, 48/10, 24/11, 166/12, 70/13, 119/13, 120/13,187/13, 38/14, 41/14, 138/14, 88/15, 192/15, 6/16, 30/16, 61/16, 64/18, 120/18 and Службен Весник на РСМ no. 290/20).
2. Constitution of North Macedonia (Уставот на Република Северна Македонија, Службен Весник на РМ, no. 52/91, 1/92, 31/98, 91/01, 84/03, 107/05, 3/09, 49/11, 6/19, Службен Весник на РСМ no 36/19).
3. Criminal Code (Кривичен законик, Службен Весник на РМ, nos. 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018).
4. Decision on establishing the fees for covering the material costs for the provided information borne by the information holder (Одлука за утврдување на надоместок за материјалните трошоци за дадената информација од имателите на информаци, https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/)

5. Decision on amending the decision on Decision on establishing the fees for covering the material costs for the provided information borne by the information holder (Одлука за дополнување на одлуката за утврдување на надоместок за материјалните трошоци за дадената информација од имателите на информации, https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%bd%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/)
6. Instruction for the method of implementation of the Law on Access to Information (Упатство за спроведување на Законот за слободен пристап до информации од јавен карактер, бр. 01-158/1) issued by the Director of the Agency for the protection of the right of access to information, available at https://aspi.mk/wp-content/uploads/2020/09/Упатство-за-спроведување-на-Законот-за-СПИЈК.pdf
7. Law on Administrative Dispute of Macedonia (Закон за управни спорови, Службен Весник на РСМ, No. 96/2019).
8. Law on Banks (Закон за банките, Службен весник no. 67/07, 90/09, 67/10, 26/13, 15/15, 153/15. 190/16 и 7/19 and Службен весник на РСМ no.101/19, 122/21)
9. Law on Civil Servants (Закон о јавните службеници, Службен Весник на РМ, nos. 27/14, 199/14, 48/15, 5/16, 142/16 и 11/18, 275/10 and Службен Весник на РСМ 14/20).
10. Law on Classified Information (Закон за класифицирани информации Службен Весник на РСМ, no. 275/2019
11. Law on Defence (Закон за одбрана, Службен Весник на РМ, nos. 42/01, 73/02, 78/02, 5/03, 58/06, 110/08, 51/11, 151/11, 215/15, Службен Весник на РСМ no. 42/20).
12. Law on free access to information of public character (Закон за слободен пристап до информации од јавен карактер, Службен весник на РСМ no.101/2019
13. Law on free access to information of public importance (Закон за слободен пристап до информации од јавен карактер, *Службен Весник* на РМ, no.13/2006, 86/2008 and 6/2010).
14. Law on general administrative procedure of North Macedonia (Законот за општата управна постапка, Службен весник на РМ no.145/2015)).
15. Law on Interior Affairs of North Macedonia (Закон за внатрешни работи, Службен Весник на РМ, nos. 42/2014,116/2014,.33/15,33/15.5/16,120/16, 127/16, 142/16, 190/16, 21/18, Службен Весник на РСМ, 108/19, 275/19).
16. Law on Labour Relations of North Macedonia (Закон за работните односи, Службен Весник на РМ, nos. 62/2005, 106/2008, 161/2008, 114/2009, 130/2009, 50/10, 52/10, 124/10, 47/11, 11/12, 39/12,13/13, 25/13, 170/13, 187/13, 113/14, 20/15, 33/15, 72/15, 129/15, 27/16, 120/18 and Службен весник на РСМ no. 267/20).
17. Law on the Police of North Macedonia (Закон за полиција, Службен Весник на РМ, nos.114/06, 148/08, 6/09,145/12, бр.41/14,33/15, 31/16,106/16, 120/16, 21/18,64/18).
18. Law on the Service in the Republic of North Macedonia Army (Закон за служба во Армијата на Република Северна Македонија, Службен Весник на РМ, nos. 36/10, 132/10, 23/11, 47/11, 148/11, 55/12, 29/14, 33/15, 193/15, 71/16, 101/19, Службен Весник на РСМ, nos 275/19 and 14/20).
19. Law on Tax Procedure (Закон за даночна постапка, Службен весник на РМ no. 13/06; Одлука на Уставен суд У.228/2006, У. 237/06, У. 213/2007, У. 219/2008; Службен весник на РМ nos. 105/2009,133/2009,145/2010,171/2010, 53/2011, Одлука на Уставен суд У.112/11; Службен весник на РМ 39/2012, 84/2012, 187/2013, 15/15, 97/15, 129/15, 154/15, 23/2016, 35/18, Службен весник на РСМ nos 275/19 and 290/2020)

Republic of Srpska

1. Company Law (Zakon o privrednim društvima Rep. Srpske, *Službeni glasnik Rep. Srpske*, nos. 127/2008, 58/2009, 100/2011, 67/2013, 100/2017 and 82/2019).
2. Constitution of the Republika Srpska (Ustav Republike Srpske, Službeni glasnik Rep. Srpske, nos. 21/92 –tekst, 28/94, 8/96, 13/96, 15/96, 16/96, 21/96, 21/02, 26/02, 30/02, 31/02, 69/02, 31/03, 98/03, 115/05, and 117/05).
3. Criminal Code of the Republic of Srpska (Krivični zakonik Rep. Srpske, Službeni glasnik Rep. Srpske, nos. 64/2017, 104/2018 – decision of Constitutional Court and 15/2021).
4. District Court in Banja Luka Judgment 11 0 U 014028 14 U of 31.3.2015.
5. District Court in Banja Luka Judgment 11 0 U 014493 14 U of 31.3.2015.
6. Law on freedom of access to information (Zakon o slobodi pristupa informacijama, Službeni list Rep. Srpske, no. 32/2001, 48/2011).
7. Law on Police of the Republic of Srpska (Zakon o policiji Rep. Srpske, Službeni glasnik Rep. Srpske, nos. 57/2016, 110/2016, 58/2019 and 82/2019).
8. Law on the Termination of the Law on the Ombudsman of the Republic of Srpska – Protector of Human Rights (Zakon o prestanku važenja Zakona o Ombudsmanu Republike Srpske – zaštitniku ljudskih prava, Službeni glasnik Rep. Srpske, no. 118/2009).

Serbia

1. Administrative Court of Serbia Judgment 17 U.1209/18 of 11.5.2018.
2. Administrative Court of Serbia Judgment 21 U.1207/18 of 31.20.2018
3. Administrative Court of Serbia Judgment 22 U.8346/18 of 19.10.2018.
4. Administrative Court of Serbia Judgment 25 U.1210/18 of 22.6.2018.
5. Administrative Court of Serbia Judgment 9 U.2489/11 of 8.3.2013.
6. Constitution of the Republic of Serbia (Ustav Republike Srbije, *Službeni glasnik RS*, no. 98/2006).
7. Criminal Code (Krivični zakonik, Službeni glasnik RS, nos. 85/2005, 88/2005 – correction, 107/2005 – correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019).
8. Criminal Procedure Code (Zakonik o krivičnom postupku, Službeni glasnik RS, nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019).
9. Data Secrecy Law (Zakon o tajnosti podataka, Službeni glasnik RS, no. 104/2009).
10. Decision of the Commissioner for information of public importance and personal data protection No. 07-00-01752/2011-03.
11. Decision of the Commissioner for Information of Public Importance and Personal Data Protection No. 071-01-2956/2019-03 of 30.5.2019.
12. Decision of the Commissioner for Information of Public Importance and Personal Data Protection No. 07-00-00381/2013-03 of 26.11.2014.
13. On of the Commissioner for Information of Public Importance and Personal Data Protection No. 07-00-02115/2011-03 of 14.6.2012.
14. Decree on the Reimbursement of Expenses in the Process of Accessing Information (Uredba o naknadi troškova u postupku za pristup informacijama, Službeni glasnik RS, no. 66/2016).
15. Law on Civil Servants (Zakon o državnim službenicima, Službeni glasnik RS, Nos. 79/2005, 81/2005 – correction, 83/2005 – correction, 64/2007, 67/2007 – correction, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018 and 157/2020).
16. Law on civilian service of Serbia (Zakon o civilnoj službi, Službeni glasnik RS, no. 88/2009).

17. Law on Defence (Zakon o odbrani, Službeni glasnik RS, nos. 116/2007, 88/2009, 88/2009 – other law, 104/2009 – other law, 10/2015 and 36/2018).
18. Law on free access to information of public importance (Zakon o slobodnom pristupu informacijama od javnog značaja, Službeni glasnik RS, nos. 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021)
19. Law on military obligation, work obligation and material obligation (Zakon o vojnoj, radnoj i materijalnoj obavezi, Službeni glasnik RS, nos. 88/2009, 95/2010 and 36/2018).
20. Law on Serbian Armed Forces (Zakon o Vojsci Srbije, Službeni glasnik RS, nos. 116/2007, 88/2009, 101/2010 – other law, 10/2015, 88/2015 – decision of the Constitutional Court, 36/2018 and 94/2019).
21. Law on Tax Procedure and Tax Administration (Zakon o poreskom postupku i poreskoj administraciji, Službeni glasnik RS, nos. 80/2002, 84/2002, 23/2003, 70/2003, 55/2004, 61/2005, 85/2005 (other law), 62/2006 (other law), 61/2007, 20/2009, 72/2009 (other law), 53/2010, 101/2011, 2/2012, 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 (authentic interpretation), 112/2015, 15/2016, 108/2016, 30/2018, 95/2018, 86/2019, 144/2020).
22. Ordinance on more detailed criteria for setting the classification degree of "TOP SECRET" and "SECRET" of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Državna tajna" i „Strogo poverljivo", Službeni glasnik RS, no. 46/2013).
23. Ordinance on more detailed criteria for setting the classification degree of "CONFIDENTIAL" and "RESTRICTED" in the Ministry of Defence of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Poverljivo" i „Interno" u Ministarstvu odbrane, Službeni glasnik RS, no. 66/2014).
24. Ordinance on more detailed criteria for setting the classification degree of "CONFIDENTIAL" and "RESTRICTED" in the Ministry of Interior of Serbia (Uredba o bližim kriterijumima za određivanje stepena tajnosti „Državna tajna" i „Strogo poverljivo" u Ministarstvu unutrašnjih poslova, Službeni glasnik RS, no. 105/2013).
25. Regulation on the amount of compensation of necessary costs for issuing a copy of documents on which is information of public importance (Uredba o visini naknade nužnih troškova za izdavanje kopije dokumenata na kojima se nalaze informacije od javnog značaja, Službeni glasnik RS, no. 8/2006).

Other documents and internet sources (accessed on 24.2.2022.)

1. *2021 Communication on EU Enlargement Policy*, Strasbourg, 19.10.2021 COM(2021) 644 final.
2. *About Freedom of Information (FOI),* http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/about/, 24.2.2022.
3. Article 19, *The Public's Right to Know: Principles on Right to Information Legislation*, 2016.
4. *Chart of signatures and ratifications of Treaty 205*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=205.
5. *Declaration No. 17 on the right of access to information*, https://www.cvce.eu/en/obj/treaty_on_european_union_declaration_no_17_on_the_right_of_access_to_information_maastricht_7_february_1992-en-c93fe321-0e77-43a0-b316-d0d45635ff98.html.
6. DiFI, Defence against corruption - The risk of corruption in the defence sector in 9 countries in Southeast Europe, 2015, https://cids.no/wp-content/uploads/pdf/difi/difi_memo_2015-

1_defence_against_corruption._the_risk_of_corruption_in_the_defence_sector_in_9_countries_in_southeast_europe.pdf, 24.2.2022.

7. Director of the Agency for the protection of the right of access to information, *The Instruction for the method of implementation of the Law on Access to Information* (*Упатство за спроведување на Законот за слободен пристап до информации од јавен карактер*, бр. 01-158/1), https://aspi.mk/wp-content/uploads/2020/09/Упатство-за-спроведување-на-Законот-за-СПИЈК.pdf.
8. European Court of Human Rights, *Guide on Article 10 of the European Convention on Human Rights Freedom of Expression (updated 31 August 2020),* https://www.echr.coe.int/documents/guide_art_10_eng.pdf.
9. Hambre A. – M., *Tax Confidentiality – A Comparative Study and Impact Assessment of Global Interest*, Örebro University 2015, www.oru.se/publikationer-avhandlingar.
10. Institucija ombudsmena/ombudsmana za ljudska prava Bosne i Hercegovine, *Specijalni izvještaj o iskustvima u primjeni zakona o slobodi pristupa informacijama u Bosni i Hercegovini*, (Institution of the Ombudsmen/ Ombudsman for Human Rights of Bosnia and Herzegovina, *Special Report on Experiences in the Application of the Law on Freedom of Access to Information in Bosnia and Herzegovina*), Banja Luka 2019.
11. Institut Alternativa, *Poslovne tajne javnih preduzeća - Paradoksi prakse u Crnoj Gori*, http://media.institut-alternativa.org/2019/10/poslovne-tajne.pdf.
12. MANS, *Tajnama skrivaju korupciju – studije slučajeva*, https://www.mans.co.me/tajnama-skrivaju-korupciju/.
13. Mrkaljevic E., *Dvadeset godina djelovanja Institucije ombudsmana u Bosni i Hercegovini*, http://fcjp.ba/templates/ja_avian_ii_d/images/green/Enesa_Mrkaljevic3.pdf.
14. Nenadić N., *Zakon o slobodnom pristupu informacijama – šta je poboljšano, a koji problemi nisu rešeni*, https://pescanik.net/zakon-o-slobodnom-pristupu-informacijama-sta-je-poboljsano-a-koji-problemi-nisu-reseni/.
15. Open Society Justice Initiative, *The Global Principles on National Security and the Right to Information (The Tshwane Principles)*, https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.
16. OECD "The Right to Open Public Administrations in Europe: Emerging Legal Standards", SIGMA Papers, No. 46, OECD Publishing, Paris 2010, p. 40, https://doi.org/10.1787/5km4g-0zfqt27-en
17. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Nov način Izigravanja prava na pristup informacijama od javnog značaja*, 15/04/2019, https://www.poverenik.rs/sr/%D1%81%D0%B0%D0%BE%D0%BF%D1%88%D1%82%D0%B5%D1%9A%D0%B0/3095-%D0%BD%D0%BE%D0%B2%D0%B8-%D0%BD%D0%B0%D1%87%D0%B8%D0%BD-%D0%B8%D0%B7%D0%B8%D0%B3%D1%80%D0%B0%D0%B2%D0%B0%D1%9A%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%BF-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B0%D0%BC%D0%B0-%D0%BE%D0%B4-%D1%98%D0%B0%D0%B2%D0%BD%D0%BE%D0%B3-%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%98%D0%B0.html
18. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Godišnji izveštaj za 2020. godinu* (Commissioner for Free Access to Information and Personal Data Protection of Serbia, *Annual Report 2020*), https://www.poverenik.rs/sr-yu/o-nama/godisnji-izvestaji.html.
19. *Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels*, https://sdgs.un.org/goals/goal16, 24.2.2022.
20. Proposal of the Law on Amendments to the Law on Free Access to Information of Public Importance (Predlog zakona o izmenama i dopunama Zakona o slobodnom pristupu infor-

macijama od javnog značaja), http://www.parlament.gov.rs/upload/archive/files/cir/pdf/predlozi_zakona/2021/1758-21.pdf.

21. Reljanović M., *Zlostavljanje nije poslovna tajna*, https://pescanik.net/zlostavljanje-nije-poslovna-tajna/.
22. *Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression,* E/CN.4/1999/64,29 January 1999, accessed on March 15, 2021.
23. *Statistika o radu sudova posebne nadležnosti u Republici Srbiji za period 1.1. – 31.12.2020. godine*, ttps://www.vk.sud.rs/sites/default/files/attachments/SUDOVI%20POSEBNE%20NADLEŽNOSTI_0.pdf.
24. *The 2020 statistical report on the work of the Administrative Court*, https://www.vk.sud.rs/sites/default/files/attachments/SUDOVI%20POSEBNE%20NADLEŽNOSTI_0.pdf.
25. *The Principles of Public Administration 2017 edition*, https://www.sigmaweb.org/publications/Principles-of-Public-Administration-2017-edition-ENG.pdf.
26. *The Public's Right to Know: Principles on Freedom of Information Legislation*, London, June 1999.
27. Transparency International, *Izvještaj o primjeni Zakona o slobodi pristupa informacijama u 2021. godini*, Banja Luka 2021.
28. *Заштита на деловна тајна и законско регулирање во Република Македонија*, https://konstantinovic-milosevski.mk/mk/2021/02/12/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%B4%D0%B5%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0-%D1%82%D0%B0%D1%98%D0%BD%D0%B0-%-D0%B8-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D1%81%D0%BA%D0%BE-%D1%80%D0%B5/.
29. *Прирачник за спроведување на Тест на штетност* (*Harm Test Implementation Manual*), https://aspi.mk/%d0%b4%d0%be%d0%ba%d1%83%d0%bc%d0%b5%d0%b-d%d1%82%d0%b8/%d0%bf%d1%80%d0%be%d0%bf%d0%b8%d1%81%d0%b8/.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.751(497-15)

KNEŽEVIĆ Bojović, Ana, 1977-
Free access to information : an analysis of the regulatory frameworks in selected Western Balkan countries / Ana Knežević Bojović, Mario Reljanović. - Belgrade : Institute of Comparative Law, 2022 (Aranđelovac : Tri O). - 117 str. : tabele ; 24 cm. - (Monograph / Institute of Comparative Law ; 181) (Public sector integrity in the Western Balkans)

Tiraž 150. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 107-117.

ISBN 978-86-80186-81-8

1. Reljanović, Mario, 1977- [аутор]
a) Слободан приступ информацијама -- Западни Балкан

COBISS.SR-ID 65189385

ISBN 978-86-80186-81-8