Ass. Prof. Dr. Edina Sudžuka
University of Sarajevo / Univerzitet u Sarajevu
Faculty of Law / Pravni fakultet
e.sudzuka@pfsa.unsa.ba

UDK 342.72/.73 (497.6)

Izvorni naučni rad

PUBLIC INTEREST, PERSONAL DATA PROTECTION AND BANK SECRECY: A BRIEF LOOK AT THE LEGAL SYSTEM OF BOSNIA AND HERZEGOVINA AND FEDERATION OF BOSNIA AND HERZEGOVINA

JAVNI INTERES, ZAŠTITA LIČNIH PODATAKA I BANKOVNE TAJNE: KRATKI PREGLED PRAVNOG SISTEMA BOSNE I HERCEGOVINE I FEDERACIJE BOSNE I HERCEGOVINE

Summary
The secrecy and confidentiality of information are regulated by different laws. Secrets may be state, official, professional, business, and a law which regulates them determines degree of confidentiality, the scope of the protected rights, and its restrictions.
The exercise of economic freedoms, the liberalization of commerce and globalization stimulate the international movement of people and capital, which in some cases, are aimed to escape from tax laws towards tax havens. Unrecorded financial transactions can result in, not only, double non-taxation but also in money laundering and terrorist financing. It is in the best interest of the every state to detect and prosecute organized crime actors and to prevent such activities from recurring. Keeping that in the mind, the emerging requirements aimed at creating global initiatives to combat financial fraud could be seen. In this regard, cooperation between states and the exchange of information on financial transactions and tax matters occur and develop.
Bank secrecy stays as a more or less transparent screen in the space between public interest and private rights.

Key words: *public interest, secrecy, bank secret, exchange of information.*

Sažetak
Tajnost i povjerljivost informacija su uređene različitim zakonima. Tajne mogu biti državne, službene, profesionalne, poslovne, a zakon koji ih regulira određuje stepen povjerljivosti, opseg zaštićenih prava i njihova ograničenja.
Ostvarivanje ekonomskih sloboda, liberalizacija trgovine i globalizacija potiču međunarodno kretanje ljudi i kapitala koji su u nekim slučajevima usmjereni na

bjekstvo od poreznih zakona ka poreznim oazama. Neevidentirane financijske transakcije mogu dovesti ne samo do dvostrukog neoporezivanja, već i pranja novca i finansiranja terorizma. Svakoj državi je u najboljem interesu otkriti i procesuirati počinitelje organiziranog kriminala i sprečavanje recidiva takvih aktivnosti. Imajući to u vidu, mogu se uočiti novi zahtjevi usmjereni na stvaranje globalnih inicijativa za borbu protiv finansijskih zloupotreba. U tom pogledu, saradnja između država između država i razmjena informacija o financijskim transakcijama i poreznim pitanjima se zbivaju i razvijaju.
Bankovne tajne ostaju manje ili više transparentan zaslon u prostoru između javnog interesa i privatnih prava.

Ključne riječi: *javni interes, tajnost, bankovne tajne, razmjene informacija*

Secrecy, secrets and public interest

In the field of finances and financial law we come across different forms of protection of specific data due to presence of exclusive public interest, interest of individuals, or perhaps due to intertwining of the public interest with the interest of individuals, professional groups, business sectors, and similar. It can mostly be said that it is the case of protection of personal data, and more rarely of protection of data pertaining to military, security or business activities of the public sector, meaning the state itself. From its immanent sovereignty, the state draws the right to declare a state secret specific data to which its organs, bodies, undertakings and institutions come across or which they use in performing their duties and tasks, and the nature of which is such that it demands a high degree of confidentiality, meaning secrecy. On the other hand, in line with modern budget principles, there is a demand for transparency in terms of management of public funds. Transparency is one of the principles and modes of combat against corruption, fraud and money laundering. However, in order to ensure fairness, and due to reasons of security, some processes cannot be fully transparent (Cohen & Eimicke, 2008, 49).

Consequently, the data on military expenditures and expenditures on defence, diplomatic missions and their activities, same as the data of state security and intelligence services, can be classified as: military secret, business secret of state-owned enterprises, and as subtypes of state secret[1]

[1] State secret by its definition represents data or written information whose disclosure would have or could have harmful consequences to political, economic or military interests of the country, and any form of unauthorised disclosure, surrender or other activity by which the data or written information are made available to unauthorised persons, meaning persons

they can be categorised as budget secrets and thus justify the deviations from the application of the principle of publicity in adopting and publicising the budget of the state and its political and territorial units. The examples of budget secrets were researched by Birman, stating that in the budget of the Soviet Union in the 1960s there was a discrepancy in budget revenues, and "the inconceivably low official indicators of expenditures on defence"(1981, p. 12), as well as "secret of the deficit nature" (p. 204-206). Particular significance and public interest in specific areas of business activities or public services require the allocation of separate financial means for them through special funds, the so-called secret or black funds. In the context of good management, it is necessary to understand the following: "some public funds are – and maybe have to be – secret special funds assigned for security purposes, which often have to be spent in an enormous hurry (such as during war)" (Trost C.& Gash L. A., 2008, p. 233). Of course, when managing public goods and resources, as well as exercising public interest, it is necessary to take measures to avoid the misuse of public interest by individuals and groups. Bozeman states: "According to the distribution of benefits criterion, public values failure may occur if public goods and services have been captured by individuals or groups, limiting just distribution of vital resources, especially those resources required to sustain life" (2007, 170). The veil of secrecy does not end at the threshold of active state participation in the public sector and directing of public expenditures. The public interest permeates through activities in the field of public finances, as well as activities in the field of monetary finances by entering the pores of financial activities of both individuals as citizens, non-governmental organisations and associations, and business sector, which take place through banks. Although banks and users of their services should establish and maintain a relationship based on trust and confidentiality, the range of data confidentiality that are exchanged between them is however restricted by the public interest[2].

---

who are not authorised to know state secrets are prescribed as a criminal offence (Pravna enciklopedija, 1985, 314).

[2] Although it seemingly looks simple to determine what public interest is and where to draw the delineation line between the public and private, at least in terms of theoretical approach and its description, there are still cases found in practice where the public interest is not specified but it is left to state bodies that enforce legal regulations to interpret them and determine the (non)existence of the public interest. There are situations in social relations in which the state has its primary interest, then the situations in which the public and private interest are intertwined, and relations of private nature behind which is the state in the sense of guarantor of unhampered exercise of human rights and freedoms. "Private interests are protected only when they are explicitly specified by law and only if they are in line with the public interest or its integral part. Public interest is an integral part of the positive legal order of a specific country, it causes only legal consequences and can also be achieved, in the case

Through its laws and institutions, the state introduces and enforces the protection of public interest in the relation between the banks and clients in order to prevent the insertion of money of unknown origin into the monetary system, as well as to detect illegal activities by which individuals and groups accumulate wealth and to identify potential funders of terrorist groups and activities and similar.

Further, the state has a highly important role in regulating[3] economic and other relations in society. In this sense, it establishes the legal framework for activities of participants on the market, i.e. it regulates economic relations and activities of subjects of private law, association of natural and legal persons as economic stakeholders through specific institutional forms, while guaranteeing private ownership, fair competition, the rule of law, and enabling the exercise of fundamental human rights and operation of economic freedoms. However, the private sector does not function as a whole isolated from the rest of society. Urlich (1995) considered that "most business activities have widespread and far-reaching impacts upon society as a whole" and become more public exposed (pg. 1), while on the other side, business depends on its public legitimation and acceptance because there is no one "free enterprise"[4] that exist without responsibility and accountability to the community (pg. 2). When it comes to confidentiality of data Bozeman says that in corporate research and development, early planning and research are closely held secrets as companies strive to develop competitive advantage and for many privately developed technologies early disclosure is not in anyone's interest. However, in the case of research that has the potential to affect literally billions of people, perhaps the rules should be different (2007, 169).
According to Gregory & Stuart (2014), globalisation has made the world smaller, more connected and more competitive through revolutionary changes in the field of information, telecommunications and transport (p.

---

of resistance or opposition to demands contained therein, with the application of state coercion. … content of public interest is often not pre-determined for all cases" (Pravna enciklopedija, 1985, 563).

[3] Regulatory function of the state encompasses the areas in which the market mechanism fails or in which the state has special interests in relation to creating the conditions for conducting economic activities, e.g. with natural monopolies that are difficult to organise on competitive bases (See: Bajec & Joksimović, 2004, 88 & 118).

[4] Ulrich states that today's company and corporations have to be understood as a *quasi-public institution* for two reasons: 1. expected to create values of different kinds according to a variety of societal needs (as its public function), and 2. obliged to be responsible and accountable not only to its owners but to the general public as well (as the way of its public legitimation) (pg. 2-3).

99). Berland (2000) referred to a "technoevolutionism" and noted that it "relies on the assumption that human culture, democracy, freedom, and intelligence must and will progress along with our technology" (Cohen & Eimicke, 2008, p. 243). It is precisely globalisation and accelerated technological progress, meaning their impact on economic development and economic and legal systems of the countries that emphasises the need to monitor international (electronic) communication through sophisticated instruments in order to protect national interests, combat terrorism, prevent illicit financial machinations, tackle smuggling and black market, corruption, money laundering, protect public order and peace, fight against pornography, paedophilia, tackle illicit migration and similar, so economic intelligence services are developed under the guise of protection of economic interests, and *economic espionage* takes place as well[5]. This is why economic information needs to be classified with a specific degree of confidentiality: e.g. Official secret, business secret, top secret; then by specifying the list of users of information; by specifying the destination or the place of safekeeping the information; and when it is the case of information in electronic form, coding methods, meaning encryption, are used (See: Prvulović, 2010, 176, 188).

The secret represents a set of knowledge and information that must be reserved for a narrow circle of individuals whom the possessor of secret must not reveal. Business secret implies a recipe or one of the formulas/methods of production that must remain secret and are known only to the producer, or according to another definition carried by Prvulović, business secrets are: "the facts related to the operation of an economic organisation that are particularly important from the standpoint of business operation of this organisation or from the standpoint of economy or community as a whole, and which may be known only to a limited circle of persons."(2010, 161).
Steiner (1995), in explaining the importance of business secrets and protecting companies against competitors by pursuing a policy of maintaining silence, particularly with regard to such sensitive sectors as strategy, research, and contract negotiations, claimed that: "an information

[5] Espionage represents a criminal offence, and in accordance with provisions of Article 163 of the Criminal Code of BH and article 157 Criminal Code of Federation BH, punishment for an act of espionage is imprisonment for a term between six months and five years, and according to Article 164, paragraph 3, the prescribed punishment is imprisonment for a term between one and ten years for the disclosure of data classified pursuant to the law as "strictly confidential" or with the degree "secret" or as "state secret" or with the degree "top secret". Espionage as a prohibited activity must be separated from the tasks of investigation, intelligence, and protection which every country organizes in order to ensure internal and external security of the country and protect its goods and citizens.

stop in sensitive areas is justified as long as business secrets are not interpreted in a narrow sense and almost everything kept secret. This need not be at the expense of truthfulness. If the reasons given are plausible and understandable, the public is prepared to accept that to safeguard higher interests no statement can be made." (pg.115). Ulrich explicated Kant's comprehension of "reasoning public", in consideration of the general public as the ultimate "locus of morality" for business: "The unlimited forum of the general public is the locus of morality where free and mature citizens come together to argue about fair rules and just standards of their living together." (pg. 4). The state permits in the public interest to publish data on illiquid and insolvent entrepreneurs[6], non-payers[7] of taxes and contributions and similar, because making the public acquainted with unconscientious business operation, over-indebtedness, and illiquidity of business organisations exposes them to shame and "condemnation" of citizens, who are at the same time warned not to engage in business relations with these organizations.

Secrecy and types of secrets in Bosnian and Herzegovinian Legal system

On the track of the aforementioned secrecy, a brief review of secrecy through the legislation of Bosnia and Herzegovina will be made. According to the provisions of the Law on protection of secret data of Bosnia and Herzegovina, secret data is a fact or instrument which pertains to the public security, defence, foreign affairs or intelligence and security activities of Bosnia and Herzegovina, which require protection against unauthorized persons, and which were marked as secret by the responsible person.

Secret is considered to be a data whose disclosure to an unauthorized person, public information means, organization, institution, body or other state or body of another state, could endanger the integrity of Bosnia and Herzegovina, especially in the area of: public security; defense; foreign affairs and interests; Intelligence and security interests of Bosnia and Herzegovina; communication and other systems of importance for state interests, judicature, projects and plans significant for defense and intelligence-security activity; scientific, research, technological, economic

[6] The Central Bank of Bosnia and Herzegovina keeps a Single Account Registry of Business Entities and publishes the Report on Blocked Accounts of legal entities from the Single Register on the website. www.cbbh.ba/Content/Read/28

[7] The Tax administration of the Federation of BH publishes data on tax debtors whose debt owed on the basis of taxes, contributions, and other fees exceeds amount of KM 50.000. http://www.pufbih.ba/v1/novosti/1335/pregled-poreznih-obveznika-sa-iznosom-duga-preko-5000000-km-na-dan-31122018-godine

and financial matters of importance for the security of the functioning of the institutions of Bosnia and Herzegovina, respectively, of the security structures at all levels of the state organization of Bosnia and Herzegovina.

According to the degree of secrecy the classified data referred to in Article 8, articles 19 and 20 of the Law on the secret data protection of BH distinguishes: "top secret" - for data whose unauthorized disclosure would compromise integrity of Bosnia and Herzegovina and caused irreparable damage to the state, "secret" - for data whose unauthorized disclosure would have extremely harmful consequences for the security, political, economic or other interests of Bosnia and Herzegovina, "confidential" - for data whose unauthorized disclosure would cause damage to the security or interests of Bosnia and Herzegovina, "restricted" - for data whose unauthorized disclosure could harm the operation of state, entity or authority, organization and institution at other levels of state organization of Bosnia and Herzegovina.

Criminal Code of the Federation of Bosnia and Herzegovina in Article 2, points 25 to 28 regulates four secrets. For the purposes of this research, official professional and business secrets will be indicated in the order to point their characteristics.

The official secret is a data or document that is declared official secret by law, other regulation or general act of the competent institution in the Federation, the canton, the city and the municipality. Criminal code of the Federation of Bosnia and Herzegovina in the article 388 defines the following: An official or responsible person in the Federation of BH who, without authorization, communicates, conveys or in any other way makes accessible to another person data which constitute official secret, or who obtains such data with an aim of conveying it to an unauthorized person, shall be punished by imprisonment for a term between six months and five years. If this kind of criminal offence is perpetrated for gain or in respect of a particularly confidential information, or for the purpose of making public or using such data outside the Federation, the perpetrator shall be punished by imprisonment for a term between one and ten years. An official or responsible person in the Federation, who perpetrates this offence out of negligence, shall be punished by a fine or imprisonment for a term not exceeding three years.

A business secret is a data or document that is determined by law, other regulation or by a general act of a company, institution or other legal entity, as a business secret, correspond to a production secret, the results of a research or construction work, and other data whose announce to an unauthorized person could have adverse consequences for its economic interests.

A professional secret is specific because it rests on the ethical rules of the profession, and includes personal data and information on family circumstances that are available to employees in certain professions, for example: attorneys, defense lawyers, notaries, doctors of medicine, doctors of dentistry, midwives or others health care workers, psychologists, religious confessors and other persons.

Considering the confidentiality of taxpayer information, Anđelković (2017, 83) emphasizes the difference between tax secrecy as a type of data collection restriction, from confidentiality of taxpayer information from disclosure to the third parties and states: "U principu, granice između poreske tajne i poreske poverljivosti mogu biti povučene naznačenjem da se prva tiče granica u prikupljanju informacija dok se druga odnosi na ograničen pristup njima." Tax secret is a official secret hold and by tax administration and the other state authorities, who are obliged to its protection against cognition and disclosure to the third parties. Bank secret has the characteristics of the professional secret because of its availability to a specific circle of authorized persons. Bank secrecy implies high level and a specific confidential relationship (Svedrović, 2005, 575).

Protection of personal data in Bosnia and Herzegovina

According to the Article 3 provisions of the Law on personal data protection, personal data indicates any information regarding the natural person who has been identified or whose identity can be established. Data subject is a natural person whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (taxpayer or client of the bank). Third party is a natural or legal person, public authority, agency or any other body except data subject, controller, processor or persons authorized by them for the purpose of data processing. Controller is any public authority, natural person or legal entity, agency or any other body, which, independently or together with another party, manages processes and determines the purpose and the manner of personal data processing on the basis of laws or regulations. Processor is a natural or legal entity, public authority, agency or any other body which processes personal data on behalf of the controller. Tax authorities and banks appear in the roles of controllers and data processors.
One of the most important articles of the Law is article 6 in the order to regulate data processing without consent of a data subject if one of the following conditions has been fulfilled:

- if he is carrying out personal data processing as it is provided by law or which is required to comply with the duties specified by law;
- if it is necessary for the data subject to enter into negotiations on a contractual relationship or to fulfil the obligations agreed upon with the controller;
- if it is necessary for the protection of interests of the data subject when the consent of the data subject has to be obtained without undue delay or the processing has to be terminated and collected data destroyed;
- if the personal data processing is required in order to complete the task carried out in the public interest;
- if it is necessary for the protection of rights and interests exercised by the controller or user, and if such processing is not in contradiction with the right of the data subject to protection of personal privacy and personal life;
- if it is necessary for carrying out legitimate activities of political parties, political movements, civic associations, trade union organizations, religious communities, except in the cases where interests for human rights and freedoms of data subject are prevailing comparing to these activities with special regard to the right to privacy.

Keeping the secret data employees collected to perform tasks at work does not end by the termination of employment with the controller or data processor as an employer. Employees in the office of the controller or processor are required to maintain confidentiality of personal data they process even after they complete certain task or after termination of employment (Art. 16). The personal data controller is authorized to provide personal data to the third party based on his written request if this is necessary for carrying out tasks within the competence specified by law or for exercising of lawful interests of the user.

According to provisions of the Law, Article 28, exceptions regarding providing of information about personal data processing and providing of access to the personal data are foreseen if that action could cause significant damage to legitimate interests of: state security, public security, defence, prevention, investigation, detection of crimes and prosecution of perpetrators as well as violations of ethical regulations of the profession, economic and financial interests (including monetary, budgetary and tax issues[8]),

[8] For example, let us take the case in which the Agency for the Protection of Secret Data in BH, acting under the complaint launched against the Tax Administration of FBH and against business banks, reached the Decision in December 2018 by which it rejected the complaint from the appellant as unfounded in the case of activities implemented by the Tax Administration of FBH in relation to taxation of natural persons – citizens who generate income from abroad and charge them via electronic online payment or directly via foreign

inspection and duties related to control, protection of data subjects or rights and freedoms of other people. The data controller submits an annual report to the Agency on rejected requests of data subjects. In accordance to Law on personal data protection and according to the Rulebook on the implementation of the Law on personal data protection inspectors of the Agency for personal data protection of BH conduct *supervision inspection*[9]. If the inspector finds out that the violation[10] of the Law or other regulation concerns the breach of the job duty, the misdemeanour[11] or crime, he/she

currency accounts, or other types of accounts opened in business banks. The Decision established that there was no violation of privacy or of the Law on Protection of Personal Data when submitting the request to business banks to deliver data about inflow of funds on their transaction accounts via PayPal system and further processing of data by the Tax Administration. The legal obligation of business banks is to deliver personal data to the Tax Administration even without the consent of the user of the account given the fact that the Tax Administration, in accordance with the Law on Tax Administration of FBH and the Law on Income Tax, is competent for the processing of taxpayers' personal data. The Agency has determined that by delivering the data of business banks to the Tax Administration, and by further processing of data by the Tax Administration, no violation of relevant regulations occurred.

[9] Supervision inspection may be regular and special. The regular supervision inspection conducts in accordance with the annual and monthly programs of work. The special supervision inspection could be conducted: on the basis of a complaint data subject lodged or based on request by the Agency Director and in the other justifiable cases if suspect in legality of activities related to processing personal data. They make a direct insight in the legality of work and treatment by controllers and processors, they eliminate illegal processing of data and order implementation of certain administrative measures. Inspectors conduct revision after expiration of 30 days upon administrative measure pronouncing in order to verify the implementation of required administrative measures.

[10] For the Law on personal data protection violation foresees monetary fines: for controllers are between KM 5.000 - 100.000, fines for responsible person in controller are between KM 200 - 15.000, and fines for controller's employee are between KM 100 to 10.000 (Art. 48-52). A person who processes the personal data contrary to the conditions and extent determined by the controller or data processor shall be fined between 500 KM and 5,000 KM. Same fine is foreseen for responsible person within the public authority who fails to issue a regulation aimed at enforcing this Law and who fails to extend the support to the Agency in carrying out its duties. EU GDPR from 25, May 2018 upper level of fines for a firm infringes of its provisions are up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. Bosnia and Herzegovina signing (2008) and entering into force (2015) the Stabilization and Association Agreement with European Union, has undertaken the obligation to harmonize domestic legislation with the acquis communautaire (deadline is June 1, 2021), so that encompass the harmonization of the Law on Personal Data Protection with the General Regulation on Protection data

[11] The largest number of misdemeanor orders was issued to the banks, as well as the highest amounts of fines. Due to the limited capacity of the Agency (for example there are only 45 employees), the volume of undertaken activities at the annual level is not large. During 2017 the Agency undertook 83 inspections (that is approximately equal to the average number of annual inspections), issued 180 opinions, received 96 complaints and issued 15 orders in total (which represents less than average number of their annual activities).

will submit a request for establishing responsibility for the job duty violation or misdemeanour commitment or report the crime.
The inspector may undertake appropriate preventive measures in order to prevent the possible damaging consequences due to faults and irregularities in the enforcement of the Law such as: warning to the controller or the data processor about the duties indicated by law, briefing on damaging consequences; suggesting measures for removal of their causes etc., and other preventive activities. Unsatisfied data subject could exercise his rights through administrative suit before the Court of Bosnia and Herzegovina[12].

Bank(ing) secret

Banking secret represents the obligation of the bank not to give any explanation to third parties about the funds on their client's account, or any other facts it learned about the client based on business relations with them. Bank's obligation to keep the banking secret results from personal rights of citizens guaranteed by the constitution, from legal regulations, contracts, and banking practices and the content of this obligation may be restricted or changed by the will of the client (Pravna enciklopedija, 1985, 92-93). The obligation to protect the banking secret is limited by the statutory authority

[12] The dispute launched by a lawsuit by the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina (IDDEEA) **and Bosna Bank International (BBI) d.d. Sarajevo** over the decision issued by the Agency for Personal Data Protection (APDP) before the Court of BH was concluded in December. The Agency for Personal Data Protection in BH, in accordance with its legal competences, conducted an extraordinary inspection supervision in the IDDEEA in terms of enforcement of the Law on Protection of Personal Data. It was determined that the IDDEEA, on the basis of the implementing regulation, reached the Decision and concluded the Agreement on free access to data from the records (permanent and temporary place of residence, and unique master citizen number) of users of services of banking organizations and other legal persons that provide the services of telecommunication and utility services contrary to their legal competences and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (it approved and enabled access to personal data of citizens contained in electronic records to 35 legal persons that provide financial, telecommunication, and utility services). Upon determining the violation of the Law on Protection of Personal Data, the APDP has permanently banned the IDDEEA from approving and enabling permanent access to personal data contained in electronic records to legal persons, ordering that the relevant administrative measure is to be carried out within 15 days from the day of receipt of the Decision, and the Court has determined that the **contested Decision is based on correct and fully established factual state, as well as correct enforcement of the substantive regulation, and that the APDP** made the right decision when it pronounced an administrative measure to IDDEEA on permanent ban on approving and enabling permanent access to personal data contained in electronic records to unauthorised legal persons.

of public authority bodies, most often the court, prosecutor's office, and the police. It is also the right of the bank to refuse to give information on clients and their business operation.
Although banking secrecy is the professional secret of a banking profession, nevertheless it is sometimes viewed as identical to a business and official secrets. Some of the authors see bank secrecy as a composite professional-business secret. The similarity of bank secrecy to the business secrecy is reflected in the scope of the bank's right "to be wrapped in secret veil" and to deny notification to anyone if there is no legal obligation to inform (Svedrović, 2005, 578). Svedrović also explains that professional obligation of banks and their associates to remain silent, (bank secrecy) and official secrecy arise, exist and are extinguish side by side, independent on each other.

Switzerland is one of the most famous countries in terms of banking secrecy. Article 47 of the Federal Act on Banks and Savings Banks (Swiss Banking Act) from 1934 established a code of secrecy for banking and account information. Song (2015, 691-692) claims: "Under the current Swiss law, banking secrecy is protected under both civil and criminal codes. Civil law on bank secrecy exists in the Swiss Civil Code and the Code of Obligation. Article 28(1) of the Swiss Civil Code provides that a customer can petition a judge to bar a bank from releasing private information. Article 27 of the Swiss Code of Obligation gives a customer a cause of action against a bank for damages for violation of secrecy and disclosure of private information. The Swiss Penal Code complements the civil law by providing that bankers face criminal prosecution if they divulge confidential information about their customers. Swiss Penal Code Article 271 prohibits financial institutions from acting on behalf of a foreign government, and Article 273 makes it a crime for a person to divulge secret business information to a foreign government authority." Keeping a bank secrecy enabled the free and unhindered transfer of income and profits to countries with a high level and multilayered system of protection financial information and data of an individual's. The exception of the rule that banker can refuse to provide tax information to the tax authority of any country, is when a taxpayer falsifies documents in order to mislead the Switzerland revenue service (the Federal Tax Administration - FTA). In the mentioned case criminal liability rises from tax evasion to the level of tax fraud and then bank secrecy will be annulled (Stauter, 1988, 626).
Protection of banking secrecy is a significant factor in determining the destination in the international movement of capital, especially if the origin of funds does not have a legal basis, and the state of the business headquarters, supervision and management of the bank does not set the

barriers and limits for deposit and placement of funds. In this sense, the offshore zone also appears as tax havens and places of high-level respect for bank's client data secrecy. Cindori mention them as areas of liberalized legislation in terms of operating and opening up banks and companies, with a very small percentage of tax liabilities, and a very notable banking secret. These zones offer advantages in terms of investment, electronic banking, international trade, property protection and confidentiality of bank accounts data, whose delivery on demand concerns different obstacles, requirements and restrictions (2010, 22-23).

The United States of America adopted Patriot Act in 2001 that spread jurisdiction of the courts in the matter of money laundering for the terrorism financing. Svedrović noted that the Act increased the eventuality of courts to review bank accounts and obtain documentation of bank transactions, expanded the role: of the Federal Reserve System (FED), The Office of Foreign Assets Control (OFAC) and the US Department of the Treasury's powers to report and pursue suspicious money laundering activities (2005, 582). The fight to prevent money laundering and terrorism financing, both regional[13] and international/global[14], leads to a narrowing of the space for the application of banking secret. Song (2015, 696) states: "The Swiss and U.S. perspectives on banking secrecy came to a headon collision with the UBS scandal. The U.S. Department of Justice's investigation into UBS AG, a titan in Swiss private banking[15], revealed that the bank's clients used undeclared Swiss Bank accounts to avoid reporting $20 billion of income to the IRS.[16]" That was one of the most powerful triggers for an introduction of the Foreign Account Tax Compliance Act (FATCA) in 2009 by U.S. Senate. The FATCA incurs certain costs to the foreign financial intermediaries and may require from them to violate national privacy and banking secrecy laws (Anđelković, 2014, 162). Implementation of the U.S. 's Foreign Account Tax

[13] Moneyval; Convention CE; Directives and Recommendations EU.

[14] The Financial Action Task Force (FATF) sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. http://www.fatf-gafi.org/about/

[15] In 2009, UBS and Credit Suisse together occupied about half of Switzerland's private banking market. KPMG SWITZ & UN1V. OF ST. GALLEN, PRIVATE BANKING IN SWITZERLAND: Quo VADIS? 5 (2009), *available at* https://www.alexandria.unisg.ch/export/DL/57055.pdf.

[16] *See* Pascal Fletcher & Lisa Jucca, *UBS, U.S. Settle Tax Evasion Case,* Reuters, Aug. 12, 2009, *available at* http://www.reuters.corn/article/2009/0S/l2/us-ubs-tax-idUSTRE57B2CF20090812.

Compliance Act (FATCA)[17] began in 2014. Switzerland's participation in U.S.[18] and international regimes for greater exchange of information has lead way to an unprecedented amount of disclosure, assistance, and cooperation by Swiss banks (Song, 2015, 718). Switzerland and Japan 2012 entered Model II FATCA that implies exchange of information between financial institutions and IRS instead of collection of data through the governments or an agent, intermediator.

Consideration of banking secrecy, data and information on bank's client accounts and business activities, very often are intertwined with tax issues such as tax haven disclosure issues, offshore business, capital escapes, double non-taxation etc. This decade in the context of the confidential and the secret information on the one side, and the exchange of information and public (state and interstate) and global interest on the other side, is marked by several initiatives[19] and acts[20] [21]. Anđelković notes that the bank secrecy

[17] Despite the fact that the United States has had a several agreements and protocols on elimination of double taxation and prevention from tax avoidance and evasion (related to the bank secrecy issues) with Switzerland (1951, 1996, 2003, 2009, 2011), an effective mechanism for the exchange of tax information has not been established until 2014 when FATCA was adopted. FATCA sought to create a "powerful incentive for foreign financial institutions to provide the IRS with the information it needs to identify persons seeking to evade U.S. tax." - statement of Stephen E. Shay, Deputy Assistant Sec'y of the Treasury, quoted according to Song (2015, 698).

[18] Discussing the issue of hiding an bank client's information Song mentions that the closing of Switzerland's oldest bank Wegelin in early 2013 was a symbolic moment for the Swiss banking industry. Add to Wegelin fourteen other Swiss banks under fire by the U.S. Department of Justice for aiding tax evasion, and Swiss banks no longer seem to be shrouded in a cloak of mystery (2015, 687).

[19] In 2012 the OECD delivered to the G20 the report "Automatic Exchange of Information: What it is, How it works, Benefits, What remains to be done", which summarizes the key features of an effective model for automatic exchange. The main success factors for effective automatic exchange are: (1) a common agreement on the scope of reporting and exchange and related due diligence procedures; (2) a legal basis for the domestic reporting and international exchange of information; and (3) common technical solutions(OECD, 2013, 7). http://www.oecd.org/tax/exchange-of-tax-information/automaticexchangeofinformationreport.htm

[20] On the basis of a report prepared by the Committee on Economic and Monetary Affairs (ECON), the European Parliament adopted its resolution on the proposal for a Council directive amending Directive on Administrative Cooperation2011/16/EU as regards mandatory automatic exchange of information in the field of taxation on 11 December 2013. The amendment to the DAC adopted on 9 December 2014 (Directive 2014/107/EU) implements at EU level the automatic exchange of financial account information, which is envisaged in the 'global standard' (Automatic Exchange of Information, AEOI) of the Organisation for Economic Co-operation and Development (OECD). This global standard (referred to as a 'common reporting standard' and a 'model competent authority agreement') prepared by the OECD and the Global Forum (including OECD and non-OECD members)

as a particularly sensitive segment of the international tax cooperation process, and explains that Switzerland, in order to protect the interests of clients of domestic financial institutions, through Rubik Agreements offers to the other states that Swiss as an intermediator, calculates income taxes and capital gains for their residents in exchange for maintaining the anonymity of individual account holders (2014, 163).[22]

---

was endorsed by both the G8 and G20. Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC) provides the basis for exchange of information (on request, administrative enquiries, mandatory exchange of information and spontaneous exchange of information), and other forms of administrative cooperation. Countries began the signature of the 'multilateral competent authority agreement to automatically exchange information under the standard' in autumn 2014. Member States started exchanging information automatically for the first time under the revised directive at the end of September 2017. See: http://www.europarl.europa.eu/legislative-train/theme-deeper-and-fairer-internal-market-with-a-strengthened-industrial-base-taxation/file-extended-automatic-exchange-of-information

"A major step towards greater transparency marking the end of bank secrecy in tax matters in the EU", Combating tax evasion: Council agrees to extend automatic exchange of information, 15 october 2014. https://www.europa-nu.nl/id/vjo155sqb8z9/nieuws/combating_tax_evasion_council_agrees_to?ctx=vg9pil5lzczq&s0e=vhdubxdwqrzw

25/05/2018: ECOFIN adopted Council Directive 2018/822/EU amending Directive 2011/16/EU as regards automatic exchange of information on reportable cross-border arrangements.

https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en .

[21] According to the Global forum 2019 Report many jurisdictions are committed to automatic exchange of information (AEOI) according to the growing demands for tax transparency, that result that under AEOI Standard in 2017 and the first widespread exchanges amongst almost 100 jurisdictions in 2018 and 2019. It has been a step change in the international community's ability to improve tax compliance and to fight against tax evasion through individuals and entities holding undeclared financial accounts abroad. A peer review process of legislative gap analysis is undertaken to ensure all the key elements of the AEOI Standard are reflected in each jurisdiction's domestic legal framework (98% jurisdictions put in place legal framework). Successful implementation of AEOI by each jurisdiction of several legal and technical requirements which entail: (i) the introduction of detailed domestic and reporting rules requiring financial institutions to collect and report the data to be exchanged and ensuring they are complied with in practice, (ii) the putting in place of international agreements with each partner to deliver exchanges with all interested appropriate partners, and operationalising them. This includes the assessment of each jurisdiction's specific lists of non-reporting financial institutions and excluded accounts to ensure their conformity with the AEOI Standard. The emphasis in the coming years will therefore be on assessing the effectiveness of the implementation of the AEOI Standard in practice, including through examining the administrative compliance frameworks each jurisdiction has in place to ensure that financial institutions comply with their obligations and providing mechanisms for exchange partners to highlight issues with the quality of the information received (2019; 5,9,15,16).

[22] See UK and Switzerland Rubik Agreement on bilateral tax matters:

Public space expands as privacy diminishes under the influence of tax and banking transparency requirements. Here, we can observe the emerges of the public or general interest and its positioning above the individual, because of the need to prevent crimes, which entails limiting the rights to the confidentiality and secrecy of personal data of individuals related to their accounts and financial transactions.

If the general interest and security circumstances, the area, the environment and interstate/international cooperation on prevention and revelation of financial frauds and exchange of information, and other factors that determine the scope of data protection that banking secrecy is providing, are taken into consideration, banking secret will be under the numerous challenges.

Banking secret in Bosnia and Herzegovina

In relation to the regulation and protection of banking secret data in Bosnia and Herzegovina, the following laws are enforced: The Law on Banks, the Law on Internal Payment Transactions, The Law on Foreign Exchange Operations, The Law on the Banking Agency (at the level of entities); Law on State Investigation and Protection Agency, Law on Prevention of Money Laundering and Financing of Terrorism (at the state level), Criminal Law and Law on Criminal Procedure (both State and entities). The Law on Protection of Personal Data applies in Bosnia and Herzegovina since 2006.
The Law on Banks of Federation of Bosnia and Herzegovina, in the Articles 102-105 regulates the issue of banking secret and defines secret as an information, facts or knowledge acquired and aware by the shareholders members of the bank's body and bank employees while performing tasks and discharge of duties within their responsibilities, as well as persons working for the company that perform the audit of the bank, and other persons who, due to the nature of their work, have access to these data whose disclosure to the unauthorized person would or could cause harm or could have detrimental consequences for the bank and its clients. The bank secrecy[23] shall be considered in particular as to:

---

https://www.ustaxfs.com/wp-content/uploads/2013/05/Pages-from-Solving-The-Puzzle-Equity-International-JG-Excerpt.pdf

[23] Bank secrets shall not deemed to be:
a) public data and data accessible to interested parties with legitimate interest from other sources;
b) bulk information, summary data where it is not possible to identify personal or business data about the individual persons to whom these data relates,

a) the data known to the bank, related to: a personal data, financial status and transactions, as well as the ownership or business links of individuals and legal entities that are clients of that or another bank,
b) information on the balances and turnover through individual accounts of natural persons and legal entities opened with the bank.

There are differences between: using and processing data, and delivering data. Persons who have access to the data and information that represents bank secrecy are obliged to keep these data as a bank and professional secret, may not use it for personal gain and benefit, nor to communicate and disclose them to the third parties. They are obliged to keep the bank secret even after the termination of employment, termination of engagement in the bank, and outage of the status upon which they obtained access to the data. These provisions (Article 103, paragraph 2) indicate a interlaces between the bank secret and the official secret that a bank employees shell keep.

Legal exceptions to keeping bank secrets refer to the information communicated to a third party:
- with the written consent of the client,
- in order to safeguard the interest of the bank in the sale of the client's pledge,
- to the competent court, the prosecutor or persons acting under their orders,
- to the court or administrative body related with the enforcement or bankruptcy administrator,
- to the Agency, the Ombudsman for the banking system, the Deposit Insurance

Agency, at written request of tax authorities, inspection and control bodies; insurance companies; a Central bank, a foreign competent regulatory authority that issues and revokes operating permits to the financial sector persons or to exercise controls and supervisions of these persons - in accordance with terms of an agreement on cooperation between the Agency and that authority and in the other cases when these data are necessary for the proceedings conducted within their jurisdiction foreseen by Article 104 (points a-t).

---

c) data on the bank's shareholders, and the amount of their participation in the bank's share capital, as well as data on other persons, irrespective of whether they are bank clients,
d) public data from the single account registry.

In addition to the consent of a bank client, the Law therefore provides lists of the exceptions of banking secrecy in cases where state authorities (courts and prosecutor's offices, investigative agencies), administration bodies (internal affairs bodies, tax administration), financial institutions (central bank, regulatory agencies), and certain companies (insurance) that, in order to carry out activities within their jurisdiction (which are related to the protection of the public interest), should have access to customer information and data on their transaction accounts. According to the article 86 of the Code of Criminal Procedure of the Federation of BiH Prosecutor[24] might issues an order to a bank or an other legal entity if there are grounds suspicions that a person has committed a criminal offense related to the obtaining of a material or property gain. The court may, based on prosecutor's proposal, order to the bank or to the other legal person that performs financial operations to provide information on bank deposits and other financial transactions and activities of that person, as well as of persons for whom it is believed to be involved in those financial transactions or the affairs under suspicion, if such information could be an evidence in a criminal proceedings.

An important role in detecting financial fraud and money laundering in Bosnia and Herzegovina is played by the State Investigation and Protection Agency (SIPA). Law on the State Investigation and Protection Agency[25] of Bosnia and Herzegovina in article 3 establishes its jurisdiction as it is: prevention, detection and investigation of criminal offenses within the jurisdiction of the Court of Bosnia and Herzegovina, collecting information and data on crimes, observance and analyses of security situation and phenomena conducive to the emergence and development of crime, implementation of international agreements on police co-operation and of other international instruments that are within the scope of its jurisdiction,

[24] Prosecutor's rights and duties defines Article 45 of the Code of Criminal Procedure of the Federation of BiH: a) requesting the provision of information from state bodies, enterprises, individuals in the Federation; b) to issuing the calls and the ordering and to propose issuing calls and orders in accordance with this Law; c) ordering to the authorized official to execute an order issued by the court in accordance to the Code of Criminal Procedure. All authorities involved in the investigation shall be obliged to inform the Prosecutor of any action taken and to act upon any request of the Prosecutor.

[25] This Law defines SIPA as an operationally independent administrative organization within the Ministry of Security of BiH whose competencies include prevention, detection, and investigation of criminal offenses that under-falls within jurisdiction of the Court of BiH, particularly organized crime, terrorism, human trafficking and other criminal offenses against humanity and values protected under international laws, serious financial crimes, protection of endangered and threatened witnesses as well as other duties that entered within its competence as established by the Law. http://www.sipa.gov.ba/en/about-us/general-info

assistance to the Court and the Prosecutor's Office of Bosnia and Herzegovina in obtaining information, and execution of the orders of the Court and of the Head of Prosecutor of BiH, Criminal expertise, and the other. The Financial Intelligence Unit (FOO) of SIPA is established by Article 13 of the Law, and the Unit performs following tasks: a.) receives, collects, records, analyzes, investigates and transmits to the Prosecutor information, data and documentation received in accordance with the law and other regulations of BiH on the prevention of money laundering and financing of terrorist activities; b) it is engaged in international cooperation in the field of prevention and investigation of money laundering and financing of terrorist activities; c) provide professional support to the Prosecutor in the field of finance.

Law on Banking Agency of Federation of Bosnia and Herzegovina regulates business secret in the chapter IV Article 39 - 42. Confidential information is information, facts and circumstances that the Agency's authorized persons have find out performing their duties within its jurisdiction and/or received by the Agency from the competent authority of another state, including supervisory bodies established by the decisions of the European Parliament and the Council of the European Union. Confidential information is considered as a business secret. The authorized persons of the Agency must keep all information received during the supervision or performing their duties at the Agency as confidential.

Confidential information shall not be disclosed to any other person or government authority except in a aggregate or summary form based on which it is not possible to identify specific banks and other financial entities that are controlled by the Agency to which such confidential information pertains.
The ban of the disclosure of confidential information mentioned above shall not apply in the following cases:

a) if confidential information is necessary for the conduct of criminal proceedings, or
b) in the event of bankruptcy or liquidation, the confidential information necessary to resolve the creditor claims and other claims relating to the bankruptcy or liquidation proceedings of a bank or other controlled entity or a civil proceeding relating to that

The duty to keep confidential latter information shall also apply to information received by the Agency or authorized persons when exchanging information with other supervisory bodies, including the European Central

Bank, the European Banking Authority, the European Banking Agency and the European Committee for systemic risk. This Law permits disclosure of confidential information to the legal entities and natural persons in Bosnia and Herzegovina, EU Member States and third countries.[26]

Conclusion

In the context of protection of personal data that represent or may represent banking secret and/or tax secret, it is necessary to undertake appropriate steps to inform the public and citizens about the right to protection of personal data and methods of protection. It is then necessary to work on additional education of staff in public institutions and services such as tax administration bodies, internal affairs bodies, police, and State Investigation and Protection Agency who apply the laws, and particular enforce criminal legislation and undertake activities in discovering the acts of tax evasion, money laundering, financing of terrorism, and especially when it is the case of their power, competences, rights and obligations, as well as the scope and range of their competences which, if exceeded, would lead to the violation of the right to personal data protection and at the same time would not contribute to the exercise of public interest. It is necessary therefore to have in mind that sometimes the border between individual and public interest is very thin and it is not easy to determine it clearly. Public servants and employees in authority bodies, in their work and contacts with the controllers

[26] a) supervisory authorities responsible for the supervision of financial sector entities (banks, micro-credit organizations, leasing companies, insurance companies, investment funds, voluntary pension funds, etc.) and the bodies responsible for conducting the bank restructuring process; b) courts and other bodies that carrying out activities under the liquidation or bankruptcy process or similar proceedings; c) auditors in charge of auditing the financial statements of banks and controlled entities; d) authorized persons or bodies responsible for deposit insurance, including the Deposit Insurance Agency; e) the bodies responsible for supervising the authorities involved in the liquidation or bankruptcy proceedings of a bank or a controlled entity or other similar proceedings; f) to courts, to the prosecutor's office or to legitimated persons acting under their orders if such information is necessary for the proceedings they carry out within their jurisdiction; h) competent authorities in Bosnia and Herzegovina responsible for financial stability, including crisis situations and systemic risk; i) the central banks of the European System of Central Banks, including the Central Bank and other bodies with similar tasks and responsibilities as central monetary authorities, when the information is relevant for the implementation of their respective statutory tasks, including the implementation of monetary policy and related liquidity provisions, payment, clearing and settlement systems and the preservation of the stability of the financial system or, j) the ministry responsible for the finance or the state body of a particular country responsible for the implementation of laws governing the supervision of banks and controlled entities or insurance companies,

and data processors, have a duty to respect the provisions of the Law on Protection of Personal Data, taking into account the instrument of official secret specified by the criminal legislation whose violation stipulates fines and punishment of imprisonment for a term of up to ten years. Further, we must not ignore the role of the media and journalists in forming the public opinion by revealing and disclosing the information on taxpayers and bank clients, as well as the potential pressure on employees of controllers and personal data processors who, if they are not thoroughly familiar with the provisions of the law, may, without any intent to do so, disclose information and data of personal nature and bear sanctions for it. On the other hand, pretty highly set fines for the violations of the Law on Protection of Personal Data should influence a higher degree of adherence to the Law. The Agency for Personal Data Protection, meaning its director, is called to provide an opinion in concrete cases of personal data protection in relation to presence of personal and/or public interest. If the opinion given by the Agency is not satisfactory, the person, or third (interested) party, can turn to the Human Rights Ombudsman of Bosnia and Herzegovina and ask for recommendations in the specific case, which enables a higher degree of objectivity in assessing the existence and protection of personal and public interest.

Bibliography

1. ”A major step towards greater transparency marking the end of bank secrecy in tax matters in the EU”, Combating tax evasion: Council agrees to extend automatic exchange of information, Europa Nu, 15 october 2014. https://www.europa-nu.nl/id/vjo155sqb8z9/nieuws/combating_tax_evasion_council_agrees_to?ctx=vg9pil5lzczq&s0e=vhdubxdwqrzw
2. Anđelković Mileva (2014). Međunarodne inicijative u domenu sprečavanja poreskih prevara,U: Usklađivanje prava Srbije sa pravom EU: tematski zbornik radova. Niš : Pravni fakultet.
3. Anđelković Mileva (2017). Poverljivost *versus* transparentnost u savremenom poreskom pravu, Strani pravni život, broj 3.
4. Bajec Jurij & Joksimović Ljubinka, (2004). Savremeni privredni sistemi, V - izdanje, Beograd: Ekonomski fakultet.
5. Birman Igor (1981). Secret Incomes of the Soviet State Budget. Dordrecht: Kluwer Academic Publishers Group.
6. Bozeman Barry (2007). Public Values And Public Interest: Counterbalancing Economic Individualism. Washington, D.C.: Georgetown University Press.
7. Cindori Sonja (2010). Sustav spriječavanja pranja novca, Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

8. Cohen Steven & Eimicke (2008). The Responsible Contract Manager - Protecting the Public Interest in an Outsourced World. Washington, D.C.:Georgetown University Press.
9. Global Forum on Transparency and Exchange of Information for Tax Purposes (2019): The 2019 AEOI Implementation Report, Paris: OECD.
10. Gregory Paul R, Stuart Robert C. (2014). The Global Economy and Its Economic Systems, Mason: South-Western Cengage Learning.
11. http://www.europarl.europa.eu/legislative-train/theme-deeper-and-fairer-internal-market-with-a-strengthened-industrial-base-taxation/file-extended-automatic-exchange-of-information
12. http://www.oecd.org/tax/exchange-of-tax-information/automaticexchangeofinformationreport.htm
13. https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en
14. Krivični zakon BiH (Službeni glasnik Bosne i Hercegovine" br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15 i 35/18).
15. Krivični zakon Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", br. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 i 75/2017)
16. OECD (2013). A Step Change In Tax Transparency, OECD Report for the G8 Summit Lough Erne, Enniskillen, June 2013.
17. Pravna enciklopedija 1 (1985), Beograd: Savremena administracija.
18. Prvulović Vladimir (2010). Ekonomska diplomatija, IV- izdanje, Beograd: Megatrend univerzitet.
19. Song G. Jane (2015). The End of Secret Swiss Accounts?: The Impact of the U.S. Foreign Account Tax Compliance Act (FATCA) on Switzerland's Status as a Haven for Offshore Accounts. Northwestern Journal of International Law & Business, Vol. 35, No. 3.
20. Stauter Robert Luis (1988). Swiss Bank Secrecy Laws and the U.S. Internal Revenue Service - Are the Swiss to Blame for Tax Dollars That the U.S. Internal Revenue Service Cannot Collect When U.S. Citizens Hide Their Money in Swiss Banks. Case Western Reserve Journal of International Law, Volume 20, Issue 2.
21. Steiner Andreas (1995). "Customer focus in ABB Switzerland's communication policy: An Ethical Challenge", in Facing Public Interest - The Ethical Challenge to Business Policy and Corporate Communications, ed. Ulrich P. & Sarasin Ch., Dordrecht: Kluwer Academic Publishers Group.
22. Svedrović Marijan (2005). Bankarska tajna i njezina normativna ograničenja prema ZUSKOK-u, Hrvatski ljetopis za kazneno pravo i praksu, vol. 12, broj 2/2005.
23. Trost Christine & Gash L. Alison (2008). Conflict of Interest and Public Life, Cross-National Perspectives. New York: Cambridge University Press.
24. UK and Switzerland Rubik Agreement on bilateral tax matters:

https://www.ustaxfs.com/wp-content/uploads/2013/05/Pages-from-Solving-The-Puzzle-Equity-International-JG-Excerpt.pdf
25. Ulrich Peter (1995). Business in Nineties: Facing Public Interest, in Facing Public Interest - The Ethical Challenge to Business Policy and Corporate Communications, ed. Ulrich P. & Sarasin Ch., Dordrecht: Kluwer Academic Publishers Group.
26. Zakon o Državnoj agenciji za istrage i zaštitu ("Službeni glasnik BiH", br. 27/04, 63/04, 35/05, 49/09 i 40/12)
27. Zakon o izmjenama i dopunama Zakona o zaštiti ličnih podataka ("Službeni glasnik BiH", broj 76/11 i 89/11)
28. Zakon o izmjenama i dopunama Zakona o zaštiti tajnih podataka ("Službeni glasnik BiH", broj 12/09)
29. Zakon o krivičnom postupku BiH ("Službeni glasnik BiH", broj 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13 i 65/18)
30. Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti ("Službeni glasnik BiH", broj 47/14 i 46/16)
31. Zakon o zaštiti ličnih podataka ("Službeni glasnik BiH", broj 49/06);
32. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", broj 54/05);