

Security Vetting in Serbia

Security Vetting in Serbia

*Analysis by the Center
for Euro-Atlantic Studies*

June 2015

Title

Security vetting in Serbia

Publishers

Centre for Euro-Atlantic Studies – CEAS

Organization for Security and Cooperation in Europe
OSCE Mission to Serbia

Translation to English

Aleksandra Kukolj

Design and prepress

comma | communications design

Print

Fiducia 011 print

Copies

100

The implementation of the project “Adoption of Law on Security Vetting - Towards greater consistency with the Constitution” is supported by the OSCE Mission to Serbia, within the bigger project “Consolidating the democratization process in the security sector in Serbia”, which is financially supported by the Swedish International Development Cooperation Agency (Sida).

The views herein expressed are solely of the authors and do not necessarily reflect the official position of the OSCE Mission to Serbia and Swedish International Development Cooperation Agency.

“Security vetting interferes with the privacy of citizens and their immediate environment to such a great extent that it is absolutely necessary to regulate thoroughly the manner in which it is conducted and to establish redress mechanisms available in cases of abuse.”

Saša Janković, Protector of Citizens

TABLE OF CONTENTS

INTRODUCTION	9
GENERAL POLITICAL CONTEXT	11
OVERVIEW OF RECOMMENDATIONS AND EXAMPLES FROM PRACTICE ...	14
The Example of Finland	14
The Example of Germany	15
The Example of Croatia	15
CASE STUDY: Security Vetting and Critical Infrastructure – the Example of Slovenia	17
OVERVIEW OF REGULATORY PROVISIONS IN SERBIA	18
EXISTING REGULATORY FRAMEWORK	20
Law on Classified Information.....	20
Law on Police	25
Law on Armed Forces	27
Law on Military Security Agency and Military Intelligence Agency	27
Law on Security Information Agency	27
Law on Private Security	28
Law on Weapons and Ammunition – effective until April 2016.....	29
Law on Weapons and Ammunition – effective as of April 2016.....	31
Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes	32
Law on Citizenship	33
DRAFT LAWS	34
Draft Law on Police	34
Draft Law on Records and Personal Data Processing in the Field of Internal Affairs	37
CONCLUSIONS	38
Umbrella Law or Advancement of Thematic Regulations?	38
Separate Expert Opinion of Deputy Commissioner for Information of Public Importance and Personal Data Protection: Aleksandar Resanović	39
Separate Expert Opinion of Professor at the Faculty of Law, University Union: Saša Gajin, PhD.....	40
RECOMMENDATIONS	42
ABOUT THE CENTER FOR EURO-ATLANTIC STUDIES	43

INTRODUCTION

The matter of security vetting in Serbia is incompletely and imprecisely regulated by a number of mutually inconsistent laws and other regulations. They include the Law on Classified Information, the Law on Police, the Law on Armed Forces, the Law on Military Security Agency and Military Intelligence Agency, the Law on Security Information Agency, the Law on Weapons and Ammunition and the Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes.

Evidently, these are mostly the laws or other regulations governing the matter of employment in public authorities, especially in the army, police and security services, and the matter of educational institutions providing education required for employment in these public authorities. Thus, the current legislative framework focuses mainly on the individuals who are or will be employed in public authorities, while all other actors are marginalised. The existence of such legal gaps, both regulatory and procedural, indicates that a process is “legally invisible”; in other words, it is unknown whether the individuals are informed about being subjected to security vetting and collection of their data, what data is collected, by whom it has been collected and processed, who is responsible for keeping relevant records, and about many other issues. This gap is primarily inconsistent with the Constitution of the Republic of Serbia, whose Article 42 guarantees the protection of personal data and clearly stipulates that the collecting, keeping, processing and using of personal data shall be regulated by law; and also with a series of other laws and regulations.

CEAS believes that this situation carries a number of risks. First, the existing arbitrariness in conducting security checks when recruiting public security officers leaves room for crime and corruption, and allows a situation where discredited or “dirty”¹ public security officers continue being appointed and/or retain their positions. Detailed security checks of all police officers, announced by the Minister of Interior Nebojša Stefanović at the beginning of this year, were explained by the fact that detailed security checks of police officers were conducted only at the time of their recruitment and that corruption or close ties with people from crimi-

1 *“Most simply put, it happens that someone completely “clean” enters the police force, but gets “dirty” over the years of work, and it also happens that official records on suspicious contacts are used for mutual confrontations.”* ČEŠLJANJE Veliki pretres u policiji. 21.1.2015. Blic online.

nal circles had been the prevailing reasons for dismissal for years.² Furthermore, the lack of standardised procedures allows for the use of double standards in the various spheres of the security system, which in itself can pose a security risk. Also, the analysis of strategic documents reveals the lack of procedures for conducting security checks for natural persons or legal entities that are not public authorities.

Accordingly, a project of the Center for Euro-Atlantic Studies from Belgrade (CEAS) entitled *Adoption of Law on Security Vetting - Towards Greater Consistency with the Constitution*, supported by the Organisation for Security and Cooperation in Europe (OSCE) Mission to Serbia, aims at opening a wide public debate on security vetting, regulation of this area in other countries, legislative regulation and relevant practice in Serbia, as well as giving specific recommendations for improving the current situation.

2 ČEŠLJANJE Veliki pretres u policiji. 21.1.2015. Blic online.

GENERAL POLITICAL CONTEXT

At the beginning of 2015, the Minister of Interior Nebojša Stefanović announced a revision of the security checks of MoI personnel because, as he said, “of the fact that someone enters the police force completely ‘clean’, but gets ‘dirty’ over the years of work, and therefore it happens that official records on suspicious contacts are used for mutual confrontations”.³ The issue of the security vetting of public security officers was raised also a few months earlier, in September 2014, when during the Pride Parade a clash occurred between the members of the Gendarmerie and of the Military Security Agency.⁴ A year before, additional security checks had also been announced, on that occasion of all the members of the Gendarmerie, following a double murder committed by a Gendarmerie officer, after which the then Commander of the Gendarmerie, Milenko Božović, informed the public that out of 2, 900 members of the Gendarmerie as many as 400 had been employed without selective training that included security vetting, psychological tests and tests of physical endurance and flexibility.⁵

It is indicative that such checks of public security officers are often announced after an incident or at a politically convenient time. It must be concluded, as practice confirms, that, objectively speaking, the existing system of security vetting for public security officers does not function, that it is used for some wrong purposes, and therefore compromises the overall security of citizens. Moreover, the announced security vetting revisions because of the criminal behaviour of officers, for example, are equally arbitrary and insufficiently legally grounded, and do not provide any guarantee that they will be effective.

CEAS reminds that back in 2012, the Commissioner for Information of Public Importance and Personal Data Protection submitted to the Serbian Government an Initiative for the adoption of a special law on security vetting⁶, in which he stressed that the matter of security vetting in Serbia was not properly regulated and that the Law on Security Vetting should provide a unified, comprehensive and consistent legislative framework of security vetting, regulating in particu-

3 ČEŠLJANJE Veliki pretres u policiji. 21.1.2015. Blic online.

4 Žandarmerija na proveri. 13.10.2014. B92. – Usvojiti Zakon o bezbednosnim proverama - Povodom bezbednosnih provera pripadnika Žandarmerije. 13.10.2014. Centar za evroatlantske studije.

5 Bez provere primljeno 400 žandarma. 4.12.2013. RTS.

6 Initiative for adopting the Law on Security Vetting. 15/10/2012. Commissioner for Information of Public Importance and Personal Data Protection.

lar the following issues: definition of basic notions, especially security vetting and security impediment; types of security vetting procedures; which data is checked, who does it and in what situations; titles, positions and persons subjected to security vetting; purpose of conducting security vetting procedures; procedure of security vetting; deadlines for security vetting; consequences of completed security vetting; manner and periods of retaining the records of completed security vetting procedures, and other matters defined by representatives of competent ministries and/or public authorities, as appropriate.

Nevertheless, it should be emphasised that new regulations or proposed laws have been drafted in the meantime, greatly improving the regulation of security vetting - but, again, with a specific focus on employees of public authorities. Thus, the Draft of the new Law on Police, and the complementary Draft Law on Records and Data Processing in the Field of Internal Affairs, regulate rather comprehensively the levels of security vetting, the way of conducting it, and define who is responsible for keeping relevant records and in which way.

However, the issue that arises repeatedly and remains unregulated is *the level of security vetting for persons who are not public authority employees*, such as, for example, private security officers, who, under the Law on Private Security, are required to undergo security vetting to obtain a licence for the performance of security activities, and who must obtain security clearance before taking a professional exam.

Similar questions may arise from the media reports saying that on the eve of the Summit of China and 16 countries in Central and Eastern Europe, held in December 2014, 3, 500 individuals were recorded in the system of security vetting, including hotel employees engaged for the needs of the Summit, volunteers and even accredited journalists.⁷ Bearing in mind the nature of the Summit, high-level security measures are quite natural, but considering the existing legislation in Serbia, it is unclear to what type of security vetting these individuals were subjected. Who conducted it? Were these individuals informed about the fact that they were subjected to security vetting? Did they give a written consent? Were relevant records kept and who is responsible for them? If the answers to these questions are in the negative, Article 42 of the Constitution of Serbia has been violated.

7 Tajne službe proveravaju 3.500 ljudi pred samit u Beogradu. 12.12.2014. Blic online.

The issue of security vetting for natural persons and legal entities that are not public authorities has recently arisen from a tender procedure for the purchase of 282 tanks, over 1, 000 guns and other weapons being sold by the Serbian Army. The potential buyers will have to obtain a permission from the Ministry of Trade, on the basis of prior approval of three ministries and the Security Intelligence Agency (BIA). In this case, the Ministry of Defence will check the fulfilment of standards, qualifications of workers and the like, while the Ministry of Foreign Affairs will check where the bought weapons will end up, or whether perhaps the buyer is a country with which the trade in arms is prohibited and whether the weapons could end up in the hands of terrorist organisations. At the same time, it has been announced that the Ministry of Interior will check whether criminal charges have been filed against the employees of the company buying the weapons and whether they have violated laws, while the BIA will perform “*other security checks*.”⁸

It is not clearly defined in what way the said security checks will be carried out, at what level, by which authority and what the content of security questionnaires will be (who will prepare them) and whether those subjected to security vetting will be informed and give their written consent, and who will keep relevant records. There is neither an existing legal framework that could provide answers to these questions.

8 Ko može da kupi oružje Vojske Srbije? 12.2.2015. Press.

OVERVIEW OF RECOMMENDATIONS AND EXAMPLES FROM PRACTICE

The presented examples from practice have been selected on the basis of the existence of an umbrella law governing the matter of security vetting in order to highlight the benefits of its existence, i.e. to show how the umbrella law contributes to the regulation of this area, which actors it includes and what problems it can help prevent.

The Example of Finland

Finland regulated the matter of security vetting in 2002, by an act of the Ministry of Justice.⁹ This document introduces the basic procedures for conducting security checks, in accordance with the policy of protecting persons subjected to security checks and personal data, in order to prevent criminal offences that would pose a serious risk for (1) the external and internal security of Finland, national defence or emergency preparedness, (2) Finland's relationships with other countries or international organisations, (3) public finance, (4) a considerably valuable business or professional secret of a private party, or another corresponding very significant private interest of a financial nature, (5) data security that is very significant in view of the protection of the interests listed above.

Hence, by this umbrella law, Finland has regulated the basic principles of security vetting, first by determining the applicants. Thus, in addition to state institutions, security checks can be requested by state-owned companies, but also private companies whose seat is located in Finland or companies with a registered branch in Finland.

Security checks are usually conducted by the police, while the Ministry of Defence performs checks for its employees. The act has also introduced the concept of *limited security checks* that are performed for people who have access to a facility in order to perform their work (e.g. the border zone at the airport). In this case, security checks are carried out by the local branch of the police in the municipality where the concerned facility is located.

9 Act on Background Checks. 177/2002. Ministry of Justice. Finland.

In the era of free markets and multinational companies, corporate security has a growing importance and, therefore, it is necessary to bear in mind that economic operators, public or private, will consider that some data or objects used in their business operations are of sensitive nature and will, therefore, insist on the vetting of employees who have access to such data. The Finnish model is a good example of a general, umbrella law that, in addition to regulating security vetting in the traditional areas, such as state employment, takes into account the recent security challenges arising from the development of markets, in terms of privatisation and openness.

The Example of Germany

In Germany, this field is regulated by the Law on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government¹⁰. The Federal Office for the Protection of the Constitution is responsible for conducting security clearance checks.¹¹

The Law clearly separates the regulations concerning the employment of persons in public authorities and other persons. Thus, Germany has also regulated the matter of security vetting conducted for natural persons, focusing particularly on employment that requires access to security-sensitive data in the private sector. In this case, in addition to the Federal Ministry, the Ministry of Economics and Technology is responsible for conducting security checks.

Although there are differences as to the authority responsible for conducting security checks, other articles that regulate jurisdiction, security questionnaires and exchange of information in this area refer to the same principles concerning the security vetting of natural persons and of public employees.

The Example of Croatia

Croatia adopted the umbrella Law on Security Vetting¹² in 2008, with the latest amendments introduced in 2012. The Croatian law regulates the procedure of conducting security checks for both natural persons and legal entities. It covers

10 Law on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government (Security Clearance Check Act).

11 Federal Office for the Protection of the Constitution – BfV.

12 Zakon o sigurnosnim provjerama. Narodne Novine 85/08, 86/12.

the employment in public authorities, security and intelligence systems, specialised bodies for combating organised crime and corruption, the Ministry of Foreign Affairs, the bodies of the European Union and the bodies, facilities or plants of special importance for national security (critical infrastructure); members of the Council for the Civilian Oversight of Security and Intelligence Agencies; provision of physical and technical protection of protected persons and facilities; as well as the acquisition of citizenship. Security vetting is divided into three groups: (1) security vetting for access to classified information, (2) basic security vetting, and (3) security vetting for the protection of protected persons and facilities.

Thus, in adopting the Law on Security Vetting, Croatia took into account the issue of natural persons who provide private security services, as well as the services of physical and technical security of persons and facilities. By the adoption of the Law on Private Security in December 2013, Serbia also opened up this issue. However, the issue of conducting security checks for natural persons in Serbia, which is presently a legal requirement for private security officers who wish to obtain a necessary licence to work, is currently regulated by the Law on Police in one sentence, without any additional bylaws that would regulate this field more thoroughly.

The Croatian model also stipulates that security vetting shall be renewed every 5 years.

In order to prevent problems that may be caused by possible delays in responding to the requests of relevant institutions for conducting security checks – which, for example, can affect business of economic operators – the Croatian model has introduced clear deadlines for the competent security and intelligence agency to submit a report on security vetting:

- For 1st degree security vetting (access to data classified as “top secret”):
30-120 days
- For 2nd degree security vetting (access to data classified as “secret”):
20-90 days
- For 3rd degree security vetting (access to data classified as “confidential”):
10-30 days

CASE STUDY: Security Vetting and Critical Infrastructure – the Example of Slovenia

Slovenia, based on lessons learned from its experience, has developed various security vetting models, in accordance with the needs arising from new ways of business operations: new security needs and new security challenges. Specifically, in the case of the Slovenian nuclear plant in Krško, whose products are used by both Slovenia and Croatia, the need for a more comprehensive approach to security vetting of persons who have access to the facility has been identified. Accordingly, the process of conducting security checks is now viewed from the aspect of public-private, inter-ministerial and international cooperation.

Security vetting in Slovenia is regulated by several laws. In the case of the nuclear power plant in Krško, the relevant law is the one that regulates critical infrastructure, that is - the Law on Protection against Ionizing Radiation and Nuclear Safety. This Law regulates thoroughly the matter of security vetting of persons in this area; Article 120 regulates even the security vetting of foreign nationals who want to work in the area of critical infrastructure, conducted in cooperation with the Slovenian National Security Agency.¹³

Thus, as examples from practice show, in the era of free markets, international organisations and corporations, the issue of risk management and basic security vetting of natural persons employed by private entities must not be marginalised, because these entities may have a significant impact on the overall security situation of a state, for example, through providing services of the protection of facilities important to national security or, as said in this example, by having access to critical infrastructure.

13 Milan Tarman. 2015. Security Vetting in Relation to Critical Infrastructure. Published in Comprehensive Approach as „Sine Qua Non“ for Critical Infrastructure Protection. Denis Čaleta and Vesela Radovič (eds.). IOS Press.

OVERVIEW OF REGULATORY PROVISIONS IN SERBIA

In Serbia, the area of security vetting is regulated by several laws and bylaws, whereas each individual law regulates this issue strictly within the scope of its subject matter. These are: the Law on Police, the Law on Classified Information, the Law on Armed Forces, the Law on Military Security Agency and Military Intelligence Agency, the Law on Security Information Agency, the Law on Weapons and Ammunition and the Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes. Within this regulatory framework, and in accordance with each of these laws, individual bylaws have been adopted to regulate this matter more thoroughly. It can be said that the Law on Classified Information regulates most systematically the field of security vetting related to its subject matter, which is access to classified data, both in the text of the Law and in the supporting acts and prescribed forms, which, if adequately adapted, could be used as satisfactory forms in all other sectors.

However, the regulatory framework in Serbia fails to provide a prescribed procedure of security vetting conducted at the request of legal entity or natural person who is not a public authority - although such requests are legitimate and have been handled by the Ministry of Interior for decades.

The most obvious example of such practice is the security vetting of private security officers, conducted *ex officio* by the MoI - without a publicly known procedure. What is known is that field checks are conducted, during which a police officer visits the place of permanent/temporary residence of the person being checked, conducts an interview with the person being checked and other present persons, subjectively assessed as relevant to the required assessment of the existence of security impediments. This approach to the processing of any data is problematic. Private security officers represent only the most conspicuous example from practice, and it is, therefore, reasonable to ask which law prescribes security vetting procedures for legal entities or natural persons who are not public authorities.

At the time of writing this analysis, there is an ongoing public debate on the Draft of the new Law on Police, which has improved the regulation of security vetting, compared to the previous law; however, the procedures are clearly defined

exclusively for public authorities, although a request for security vetting can be submitted by a legal entity or natural person with respect to a legal entity or natural person who is not a public authority.

This part of the analysis gives an overview of the existing legal framework and current draft legislation covering the area of security vetting.

EXISTING REGULATORY FRAMEWORK

Law on Classified Information

Official Gazette of the Republic of Serbia, no. 104/2009

The Law on Classified Information defines three levels of secrecy, according to which appropriate security clearance shall be performed in order to allow access to data. These are:

- 1) basic security clearance, for data marked as “RESTRICTED” and “CONFIDENTIAL”;
- 2) full security clearance, for data marked as “SECRET”;
- 3) special security clearance, for data marked as “TOP SECRET”.

Security clearance for access to classified data and documents marked as “TOP SECRET” and “SECRET” shall be conducted by the Security Information Agency of the Republic of Serbia, while security clearance for access to classified data and documents marked as “CONFIDENTIAL” and “RESTRICTED” shall be conducted by the ministry responsible for internal affairs.

The Military Security Agency shall conduct security clearance for access to classified data and documents of any classification level for persons who need access to classified data and documents in order to discharge their functions and professional duties in the ministry responsible for defence and in the Army of the Republic of Serbia.

Exceptionally, security clearance for access to classified data and documents marked as “CONFIDENTIAL” and “RESTRICTED” for persons who need access to classified data and documents in order to discharge their functions or professional duties in the Security Information Agency, shall be conducted by the Security Information Agency.

Security clearance for access to classified data and documents marked as “SECRET” for persons who need access to classified data and documents of the

mentioned classification level in order to discharge their functions and professional duties in the ministry responsible for internal affairs, shall be conducted by the ministry responsible for internal affairs.

The authorities responsible for security clearance shall cooperate with each other in the security clearance procedure, particularly in the security clearance procedure for access to classified data marked as "TOP SECRET" and "SECRET".

The purpose of security clearance within the meaning of this Law is to assess security risks, in particular for access to secret data.

In order to conduct security clearance, the Council Office shall submit a security clearance questionnaire to the applicant. The applicant shall complete a basic security clearance questionnaire, and if a certificate is required for classified data marked as "TOP SECRET" and "SECRET", the applicant shall also complete a special security clearance questionnaire.

The following information about the applicant shall be entered in a basic security questionnaire:

- 1) name and surname, and previous names and surnames;
- 2) citizen's personal identification number;
- 3) date and place of birth;
- 4) citizenship, previous citizenships and dual citizenships;
- 5) permanent residence and temporary residence, and previous permanent residence;
- 6) marital and family status;
- 7) information about persons sharing a household with the person to whom the security clearance questionnaire relates (their names and surnames, together with previous names and surnames, their dates of birth and their relation to the person undergoing security clearance);
- 8) name and surname, date of birth and address of relatives to the second degree in the direct line and to the first degree in the collateral line, as well as of adoptive parents, guardians, step-parents or foster parents;
- 9) educational level and occupation;
- 10) information about previous employment;
- 11) information about military service;
- 12) information about punishments for criminal and misdemeanour offences, and ongoing procedures for criminal and misdemeanour offences;

- 13) medical reports concerning addictions (alcohol, drugs, etc.) or mental illnesses;
- 14) contacts with foreign security and intelligence services;
- 15) disciplinary procedures and disciplinary measures pronounced;
- 16) information about membership or participation in any organisations whose activities and objectives are prohibited;
- 17) information about responsibility for violating any regulations concerning classified information;
- 18) information about ownership rights or other proprietary rights over real estate, information about ownership rights over other assets entered in the public register, as well as information about the annual tax on the total income for the previous year;
- 19) previous security clearance checks.

The following information about the applicant shall be entered in a basic security questionnaire for legal entities:

- 1) company name and seat, as well as previous names and seats;
- 2) registration number of legal entity and tax identification number;
- 3) name and surname of representative;
- 4) date and place of incorporation;
- 5) information about organisational units, branches, subsidiaries and other forms of affiliation;
- 6) origin of foundation capital, including any changes in the last three years;
- 7) number of employees;
- 8) number of employees for whom the certificate is required and type of work duties they perform;
- 9) information about convictions for any criminal offence, economic offence and misdemeanour committed by a legal entity and responsible persons in the legal entity, as well as information about any ongoing procedures for criminal offence, economic offence or misdemeanour against the legal entity;
- 10) information about contacts with foreign security and intelligence services;
- 11) information about participation in any organisations whose activities and objectives are prohibited;
- 12) information about responsibility for violating any regulations concerning classified information;
- 13) information about a previous security clearance check;

-
- 14) information about ownership rights or other proprietary rights over real estate, information about ownership rights over other assets entered in the public register, as well as information about the annual financial statement for the previous year in accordance with the law regulating accounting and auditing.

The following information shall be entered in a special security questionnaire:

- 1) information about military service and service in paramilitary formations of a foreign country;
- 2) other information and facts, apart from the facts mentioned in Articles 58 and 59, making the legal entity or natural person susceptible to influence and pressure constituting security risks;
- 3) information about debts arising from financial liabilities or assumed guarantees.

Along with this completed questionnaire, the representative of legal entity shall submit a completed basic security questionnaire for natural persons.

Special security clearance shall be conducted when a certificate or permission is required for data marked as "TOP SECRET" and shall include, in addition to security check within full security clearance, the checking of facts, circumstances and events concerning the applicant's private life, at least in the last ten years from the day of applying for the certificate, which, if any, would constitute reason to doubt the applicant's trustworthiness and reliability, particularly if his/her activities are in contravention of the interests of the Republic of Serbia, or if he/she is connected with foreign nationals who might jeopardise the security and international interests of the Republic of Serbia.

In conducting security clearance, the competent authority shall assess, in terms of security, the information contained in the completed security clearance questionnaire, and according to this information it shall collect personal and other information from the person to whom the information is related, from other public authorities, organisations and persons, from registers, records, databases and data collections kept under law. The competent authority shall conduct security clearance within the following time periods, as of the day of the reception of a completed questionnaire:

- 1) up to 30 days, for basic security;
- 2) up to 60 days, for full security clearance;
- 3) up to 90 days for special security clearance.

As an exception, if there be justified reasons, these deadlines may be extended at most for the time period determined in these items, and in such a case the competent authority shall inform about the extension of deadline the head of the public authority that submitted a request for security clearance, as well as the Council Office.

If security clearance is not completed within the specified time periods, it shall be considered that the applicant's access to secret data poses no security risk.

The authorities responsible for security clearance shall submit to the Council Office a report on the results of security clearance or special security clearance, including a completed security clearance questionnaire, with a recommendation for issuing or denying the issuance of certificate.

The report shall not state the sources of security clearance.

The report and recommendation shall be marked as "CONFIDENTIAL".

The Council Office shall deny a request for issuing a certificate by passing a decision thereon, if it is established, based on a security clearance report or an additional security clearance report, that:

- 1) the applicant stated untrue and incomplete information in a basic or special security clearance questionnaire;
- 2) the applicant does not fulfil the conditions from Articles 48 to 50 of this Law for issuing a certificate or permission;
- 3) the applicant has not provided the conditions for undertaking the prescribed protection measures for classified data;
- 4) there is a security risk arising from access and use of classified data by the applicant.

The rationale for a decision denying a certificate shall not contain any information considered to be secret for the purposes of this Law, nor shall it state the sources of security clearance.

It can be considered that the Law on Classified Information best defines, prescribes, regulates and supports with bylaws the matter of security vetting in procedural terms, but only at the request of a public authority and for the purpose of access to classified information.

The question remains how private security officers will be checked, since they will have or may have access to classified information in performing their duties, in cases of protecting critical infrastructure or facilities of importance for the defence of the Republic of Serbia. The Commission for Public-Private Partnerships in the Security Sector of the Republic of Serbia (*that CEAS is a member of*) has discussed a model according to which the applicant for certification would be the Serbian Chamber of Commerce - on the basis of public powers - but such a solution has not been yet introduced in the regulatory framework.

Law on Police

Official Gazette of the Republic of Serbia, nos. 101/2005 and 92/2011

The police can collect data about the person who seeks to be employed in the Ministry, and for the purpose of performing police tasks, with the written consent of the person whose data is collected; the police can also collect data based on which they establish security impediments in the performance of police tasks.

Security vetting shall include the checking of data specified in the regulations on the requirements for obtaining a weapons licence, as well as the data provided by a candidate for employment in the employment procedure. Data about the person who seeks to be employed in the Ministry shall be collected in the procedure of security vetting with the prior written consent of that person and cannot be used for other purposes.

Security vetting pursuant to this Law constitutes a set of measures and activities aimed at establishing the existence or non-existence of security impediments. Security impediment is the fact that precludes employment in the Ministry in accordance with the conditions that provide that a person must:

- 1) be a citizen of Serbia;
- 2) have completed at least secondary education;
- 3) be younger than 27 for the position requiring secondary education or younger than 30 for the position requiring higher education and up to five years of work experience;
- 4) demonstrate such mental and physical abilities as required for the performance of work duties, stipulated by the act referred to in Article 4, paragraph 4 of this Law, as evidenced by the medical certificate of the Health Care Institute of the Ministry of Interior;

- 5) have completed military service or be exempt from military service as police officer, in accordance with law, if the candidate is a man;
- 6) not hold dual citizenship;
- 7) have been subjected to security vetting without security impediments being found.

The Ministry cannot employ a person who has been convicted for a criminal offence prosecutable *ex officio*; against whom a criminal procedure for such an offence is ongoing; who has been sentenced to an unconditional prison sentence of more than three months; or whose service in a public authority or legal entity with public powers has been terminated by a final decision of the competent authority, due to a serious breach of official duty.

It has been envisaged that the procedure of security vetting and the content of forms that are used in this procedure are to be regulated by an act adopted by the minister, but that obligation under the existing law has not been fulfilled.

Since December 2013, the Law on Private Security has been in force; it prescribes that natural persons (security officers) must receive a security clearance before taking the professional examination. This Law stipulates that security checks shall be conducted by the Ministry of Interior. However, neither the current law nor the Draft of the new Law on Police prescribe the procedure of security vetting that should be conducted in this particular case. Therefore, it is justifiable to remark that although security vetting for legal entities and natural persons who are not public authority is necessary in many cases, and even prescribed by law in this particular case, it is not regulated as such anywhere, except in Article 11 paragraph 1 item 6 of the Law on Weapons and Ammunition that becomes effective in April 2016 and stipulates that class B weapons may be purchased and held by natural persons with respect to whom it has been established, on the basis of security and operational checks in the place of their permanent/temporary residence and place of work, that their behaviour does not indicate that it may pose a danger to themselves or others and to public order. The Law on Private Security also refers to this Article, but the same issue remains - a procedures for conducting security checks of natural persons who are not public authority is not prescribed in any place. It is simply insufficient to say ***if his or her behaviour does not indicate that it may pose an impediment to security.***

Law on Armed Forces

Official Gazette of the Republic of Serbia, nos. 116/2007, 88/2009, 101/2010 – as amended and 10/2015

Professional military personnel may be citizens of the Republic of Serbia, who in addition to the general requirements, have been subjected to security checks that demonstrated the absence of security impediments to admission to professional military service, in accordance with the regulations governing the performance of security vetting at the Ministry of Defence, and the Rulebook on Security Vetting Conducted by the Military Security Agency (*Official Military Journal*, no.18/2010).

Law on Military Security Agency and Military Intelligence Agency

Official Gazette of the Republic of Serbia, nos. 88/2009 and 17/2013

The tasks and duties of the Military Security Agency include personnel security: security vetting and issuing of security clearance certificates to persons who have access to secret data, required for exercising their function or performing their job duties in the MSA and MIA, as well as conducting security checks of candidates for employment with the Ministry of Defence and for service in the Army of Serbia, and other persons important for the performance of activities in cooperation with the Security Information Agency and police.

Law on Security Information Agency

Official Gazette of the Republic of Serbia, nos. 42/2002, 111/2009 and 66/2014

The employment related rights, duties and responsibilities of the Agency staff shall be subject to the regulations that apply to the employees of the ministry responsible for internal affairs.

Having in mind that the Security Information Agency also performs security checks for third parties, at the request of public authorities, the Agency's Operation Booklet provides insight into its competences related to security checks for

others, referring to several laws: Law on Classified Information – Article 54; Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes - Article 16; Law on the Enforcement of Prison Sentences for Criminal Offences of Organised Crime – Article 12; Law on Defence – Article 81; Law on Foreigners – Article 11 and Law on Security Information Agency – Article 9.

Law on Private Security

Official Gazette of the Republic of Serbia, nos. 104/2013 and 42/2015

Article 12 of the Law on Private Security stipulates that a licence for performing activities of private security shall be issued to a natural person who meets the general requirements for obtaining each of the specified types of licences. One of these requirements is that a natural person has “undergone appropriate security vetting.”

However, the Law itself fails to define the meaning of “*appropriate security vetting*”, while the existing Law on Police (taking into consideration that the Ministry of Interior is defined as supervisory authority for the private security sector) fails to define procedures for the security checks of natural persons who should perform private security duties. The Draft of the new Law on Police also fails to regulate this matter more thoroughly, since there is no clear definition of a procedure of security checks for natural persons who perform private security activities and are not employed in public authorities.

Article 3 of the introductory provisions of the Law on Private Security defines security vetting as checks performed by the Ministry of Interior, in accordance with the law governing weapons and ammunition. However, neither the Law on Weapons and Ammunition prescribes any specific procedure for conducting security checks, but only lists the requirements that a person must meet in order to obtain a permit for carrying or possession of weapons.

Law on Weapons and Ammunition – effective until April 2016

Official Gazette of the Republic of Serbia, nos. 9/92, 53/93, 67/93, 48/94, 44/98, 39/2003, 101/2005 – as amended, 85/2005 - as amended, 27/2011 – CC Decision and 104/2013 - as amended

Although the existing Law does not mention security vetting explicitly, representatives of the Ministry of Interior often refer to certain parts of it, when the issue of security checks is raised during public debates on private security¹⁴; in particular, they refer to the provisions that define the acquisition, keeping and carrying weapons and ammunition.

A permit to acquire firearms shall not be issued to:

- 1) underage person or person deprived of legal capacity;
- 2) person sentenced for criminal offences against constitutional order, endangering territorial integrity, undermining military or defence strength, violence against representative of the highest state authorities, armed rebellion, terrorism, diversion, violation of territorial sovereignty, aircraft hijacking, threatening flight safety, murder, grave body injury, light body injury, participating in fights, endangering safety, endangering one with dangerous weapons in fight or roe, kidnapping, raping, unnatural lechery, grave theft, robbery, grave robbery, extortion, provoking general danger, illegal hunt, preventing official person in performing his/her duty, obstructing authorised person in performing security duties or maintaining public peace and order, preventing official person in conducting security duties or maintaining public peace and order, violent behaviour, manufacturing and acquisition of arms and means aimed at committing criminal offence, participating in a group committing violence and for the criminal offence defined by this Law;
- 3) person against whom a criminal procedure is instituted for criminal offences prosecutable *ex officio*, while the procedure is ongoing;
- 4) person who has been punished for the misdemeanour of violating public peace and order punishable with imprisonment or for a misdemeanour defined under this Law, in the period of three years prior to the day of submitting a request for obtaining the permit to acquire firearms;

¹⁴ When at the CEAS roundtable entitled *Training and Licencing in the Private Security Sector in Serbia* the CEAS researcher asked the representative of Police Directorate according to which principle private security officers would be subjected to security vetting, he referred to the provisions of the Law on Weapons and Ammunition.

- 5) person against whom a misdemeanour procedure has been ongoing for violating public peace and order punishable with imprisonment or for a misdemeanour defined under this Law, during the procedure;
- 6) person not trained for handling firearms.

A permit to acquire weapons shall not be issued even in case it is necessary to protect personal safety and property of other individuals, public peace and order or for the security and defence of the Republic.

When in the procedure of issuing a permit there is a justified suspicion that the submitter of request is not medically capable of handling firearms, the relevant authorities shall refer him/her to a medical examination.

The request for obtaining a permit to acquire firearms shall be accompanied by a certificate that no investigation has been initiated or charges raised against the applicant, and a certificate issued by the authorised organisation stating that the applicant has been trained in handling firearms.

It is obvious that there is a certain security vetting to which the persons are subjected in the procedure of issuing permits, and which is particularly based on the provisions stipulating that the **request will be rejected if there are other impediments that are not specified by the Law**, the evidence of which should be provided by the applicant or natural person. Therefore, once again we find gaps in the implementation of security checks - both procedural and in terms of records on collected data.

Since this process is “legally invisible”, it is unknown where the collected data ends up, which is not in compliance primarily with the Constitution of the Republic of Serbia, and then also with a number of other regulations that stipulate the protection of personal data and privacy.

Law on Weapons and Ammunition – effective as of April 2016

The new Law on Weapons and Ammunition was adopted in April 2015 and will become effective one year from the date of adoption. Article 11 of this Law specifies the requirements for obtaining a licence to carry category B weapons for natural persons.

The category B weapons may be acquired and held by natural persons:

- 1) who are legal adults;
- 2) who are citizens of the Republic of Serbia or permanently residing foreigners;
- 3) who are medically fit to hold and carry weapons;
- 4) who have not been finally sentenced to imprisonment for criminal offences against life and body, against human and civil rights and freedoms, against sexual freedom, against marriage and family, against property, against public health, against general security of people and property, against the constitutional order and security of the Republic of Serbia, against public authorities, against public order and peace, against humanity and other goods protected by international law, or persons against whom a procedure for these criminal offences is ongoing;
- 5) who have not been finally punished in the last four years for misdemeanours in the field of public order and peace punishable by imprisonment and for misdemeanours defined under this Law;
- 6) **whose behaviour does not indicate that they may pose a danger to themselves or others and to public order, as established on the basis of security and operational checks in the place of their permanent/temporary residence and place of work;**
- 7) who have been trained for handling firearms;
- 8) who have a justified reason, as follows:
 - (1) for category B personal safety weapons - if their personal safety is likely to be compromised due to the nature of work or other circumstances;
 - (2) for category B hunting weapons – if they provide proof that they meet requirements for the possession of hunting maps,
 - (3) for category B sporting weapons – certificate of active membership in a sport shooting organisation;
- 9) have conditions for the safe storage and keeping of weapons.

Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes

Official Gazette of the Republic of Serbia, nos. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 45/2005, 61/2005, 72/2009

Persons holding office or performing tasks and duties in public authorities and special organisational units under this Law, shall, before taking office or assuming work duties, submit to the Anti-Corruption Agency, in writing, complete and accurate information about their assets and the assets of their spouses and relatives in direct line, or in the collateral line - persons related to them by consanguinity to the third degree or affinity to the second degree.

The Anti-Corruption Agency shall record and verify the information, in accordance with a special law.

The security checks of the aforementioned persons shall be conducted by the ministry responsible for internal affairs, the Security Intelligence Agency and the Military Security Agency. Security checks can be carried out without the knowledge of these persons prior to the beginning of work or taking office, or during the discharge of office or performance of work duties, as well as one year upon the termination of office or performance of work duties.

The method of conducting security checks referred to in paragraph 3 of this Article, and the method of recording collected data, shall be regulated by the government's act – *Decree on recording the assets of persons holding office or performing tasks and duties in special organisational units under the Law on Organisation and Competences of Public Authorities in Combating Organised Crime*.¹⁵ Article 5a of this Decree provides that the security vetting of persons referred to in the Law on the Organisation and Competence of Public Authorities in Combating Organised Crime, Corruption and Other Particularly Serious Crimes shall be performed by the Security Information Agency, in accordance with the regulations on the manner of conducting activities within its purview.

The data from this Law shall be confidential, determined in accordance with the law governing classified information.

¹⁵ Official Gazette of the Republic of Serbia, nos. 72/2003 and 73/2007.

Law on Citizenship

Official Gazette of the Republic of Serbia, nos. 135/2004 and 90/2007

Although the Law on Citizenship does not mention explicitly security vetting, in the part regulating the procedure of acquiring and terminating the citizenship of the Republic of Serbia, Article 41 provides that the **ministry responsible for internal affairs can reject a request for acquisition of the citizenship of the Republic of Serbia by naturalisation or for termination of the citizenship of the Republic of Serbia, notwithstanding the fulfillment of all the requirements set forth by this Law, if it estimates that there are reasons in the interest of the Republic of Serbia for rejecting such a request for acquisition or termination of citizenship.**

In order to determine the existence of reasons for rejecting a request for citizenship, which by their nature cannot be anything but a security impediment, it is necessary to conduct security checks for a person who submits a request for citizenship.

In that context, the following questions arise: **Does a submitter of request for acquisition of citizenship sign consent for being subjected to security checks? Who is responsible for prescribing a form of consent? Who conducts security checks? According to which procedures?;** etc.

DRAFT LAWS

Draft Law on Police

In the Draft of the new Law on Police, security vetting is defined as a set of measures and actions determining the existence or non-existence of security impediments to the performance of particular activities. Security impediment involves a clear, accurate, precisely specified fact indicating that a candidate is not eligible for admission to employment in the Ministry.

Accordingly, the police shall be entitled to conducting security checks:

- 1) of candidates being admitted into employment in the Ministry;
- 2) of candidates for training at the Basic Police Training Centre;
- 3) of candidates enrolling in a tertiary-level educational institution for the needs of police education;
- 4) of employed police officers;
- 5) for admission to employment in other public authorities in accordance with the regulations governing that field, upon request of the authority;
- 6) of persons allowed access to particular facilities and/or locations under special security protection;
- 7) in other cases prescribed by law.

If security checks are conducted upon the request of a public authority or other person, the authorised applicant shall submit to the territorially competent organisational unit of the Ministry a written consent of the candidate referred to in paragraph 1, points 1)–7) of this Article, as well as other persons, for the purpose of conducting security checks.

Security vetting does not include the processing of particularly sensitive personal data, in accordance with the regulations concerning personal data protection.

This Draft Law on Police has introduced three different levels of security checks, depending on the scope of checked data.

-
- The first-level security check involves the processing of data from the official records of the Ministry and collection of data through direct operational-field work. The first-level security check shall be conducted for all employees of the Ministry for the period of five years.
 - The second-level security check shall be conducted for managers of smaller internal organisational units (middle-level management). The second-level security check involves the processing of data referred to in paragraph 3 of this Article, and complete verification of data from the records of other public authorities, public administration authorities, territorial autonomy, local self-government units and holders of public powers. The second-level security check shall be conducted for the period of three years.
 - The third-level security check shall be conducted for persons in managing positions, appointed persons and/or strategic-level managers at the Ministry, and in other cases prescribed by law. The third-level security check involves the processing of data referred to in paragraphs 3 and 6 of this Article, and data from the records of other security services. The third-level security check shall be conducted for the period of two years.

In the recruitment procedure, the person entering into employment with the Ministry shall complete and sign the questionnaire on identification data, as well as persons that the questionnaire relates to. If the candidate entering into employment refuses to complete and sign the questionnaire on identification data, he or she shall be considered to have abandoned the entry into employment, enrolment in training for the performance of police officer activities, enrolment in university for the needs of police education.

The request for conducting security checks shall be submitted by the organisational unit implementing the employment process to the competent authority in accordance with the permanent residence of the candidate / person who shall be checked.

Prior to checking, the police officer conducting the check shall inform the person about data processing, in accordance with law.

The content of the questionnaire referred to in paragraph 1 of this Article shall be prescribed by the Minister.

In the procedure of conducting the checking, the data from the questionnaire shall be collected and verified, as well as:

- 1) other data on persons that the candidate lives with in a joint household;
- 2) data from criminal and other records maintained by competent authorities;
- 3) data on bills of indictment, instituted criminal and misdemeanour procedures;
- 4) information on habits, inclinations and behaviour;
- 5) other data important for work at the Ministry.

Checks shall be conducted through direct conversation with the person being checked, inspection of official records and collections of data maintained by competent authorities, direct conversation with other persons according to the assessment of the competent officer conducting the checking, and/or direct observation of the officer conducting the checking.

Checks shall be conducted within 30 days of the day of receiving the request for checking. If the employment is not entered into within one year of the day of conducted checking, the competent organisational unit conducting the procedure of entry into employment shall ensure a repeated checking.

During the public hearing on the draft of this Law, the representatives of the working group within the Ministry of Interior answered **affirmatively** when asked whether “**other persons**” referred to in **Article 96, paragraph 3** included all natural persons and legal entities who were **not public authorities**, but the question concerning the procedure of security checks for those persons/entities remained unanswered. This situation is disconcerting, given that the Draft Law does not envisage any bylaws for further regulation of this matter, which means that the Law will be the only regulation that should be applied in practice - if the government adopts it in its current form.

Draft Law on Records and Personal Data Processing in the Field of Internal Affairs

This Law regulates the collection of personal data and performance of other actions related to personal data processing in the field of internal affairs, the purpose of processing, the rights and protection of the rights of persons whose data is processed, records in the field of internal affairs, the type and content of the records, data processing authorisations, time limits within which data is processed, the method of using data, the provision of quality assurance, protection, storage and oversight of data processing, as well as other issues of importance for data processing in the field of internal affairs.

The purpose of personal data processing is, *inter alia*, conducting security checks.

For the purpose of conducting security checks, the Ministry shall collect and process the following data: first name, last name, previous first and last names, citizen's personal identification number, place and date of birth, citizenship, previous citizenship and dual citizenship, permanent and temporary residence, previous permanent residence, marital and family status, data about persons living in the household with the person to whom the questionnaire relates (their first and last names, along with previous first and last names, their dates of birth, and relationship with the person subjected to checking), first and last name, date of birth and address of relatives to the second degree in the collateral line, spouse, adoptive parent, guardian, step-father, step-mother or foster parent, educational level and occupation, information about previous employment, information about military service, data on criminal and misdemeanour sanctions and ongoing criminal and misdemeanour procedures, medical information related to addictions or mental illness, disciplinary procedures and imposed disciplinary measures, as well as information on memberships or participation in the activities of organisations whose activities or goals are prohibited.

CONCLUSIONS

The analysis of the existing legal framework for security vetting clearly indicates that this field is regulated rigidly under several laws within their respective subject matters.

Currently, the only law that regulates this field thoroughly within its scope and purview is the Law on Classified Information, which systematically and comprehensively regulates the issues of who submits a request for security vetting, how and to whom, and also who conducts security vetting, how and within which deadlines, and finally who keeps and uses collected data, how and where.

The drafts of the Law on Police and the Law on Records and Data Processing in the Field of Internal Affairs regulate the field of security checking somewhat clearer and more comprehensively than the currently applicable laws, but there are still some shortcomings. First of all, they do not prescribe a procedure for conducting security checks at the request of persons/entities that are not public authorities and for persons that are not public authorities (legal entities and/or natural persons), nor do they provide for the possibility to regulate this matter in more detail in bylaws.

Article 42 of the Constitution of the Republic of Serbia stipulates that the collection, keeping, processing and use of personal data shall be regulated by law. Accordingly, the issues that must be regulated by law include at least: **the purpose of processing personal data, the types of personal data, the way of using personal data and data retention periods**. Regulating these issues with bylaws is not in compliance with the Constitution, which means that it is not a good solution to omit the issue of security vetting for legal entities and natural persons that are not public authorities in the applicable law (Law on Police) and leave it to be regulated in a bylaw.

Umbrella Law or Advancement of Thematic Regulations?

The Commissioner for Information of Public Importance and Personal Data Protection submitted to the Serbian government an initiative for the adoption of the Law on Security Vetting on 15 October 2012. The rationale behind the initiative is based on the fact that the matter of security vetting has for decades been regu-

lated in Serbia under several laws and regulations, but only partially, incompletely and imprecisely, and that most of these laws and regulations do not contain provisions on basic notions, entities/persons subjected to vetting, purpose and procedure of vetting, deadlines, etc., which leaves too much room for discretionary interpretation and actions of competent authorities, even individuals. In cases where relevant regulations do contain such provisions, they are almost always incomplete and/or relate exclusively to the subject matter of these regulations. The current situation leads to violations of human rights and freedoms, in particular the right to privacy and the right to protection of personal data.

Separate Expert Opinion of Deputy Commissioner for Information of Public Importance and Personal Data Protection: Aleksandar Resanović

Respecting the principle of the Constitution of Serbia and the Law on Protection of Personal Data saying that the processing of personal data must be regulated by law, the Commissioner, from the aspect of his work, points to the necessity of regulating the matter of security vetting by law instead of bylaws or internal regulations, which is presently not such a rare case.

We could discuss whether a comprehensive regulation of security vetting requires only the adoption of new sectoral laws and/or the significant improvement of the existing ones (for example in the field of employment in public authorities, especially in the police, military and security services, in the field of educational institutions that provide education required for employment in these public authorities, etc.) or the adoption of an umbrella law on security vetting in addition to these laws.

Choosing the first option would involve a realistic possibility that numerous provisions of these laws, especially the general ones, are similar and some of them even identical. This should be avoided so that each of these sectoral laws contains comprehensive, precise and specifically defined provisions, both substantive and procedural ones. Thus the matter of security vetting would be fully regulated in different sectors, which is currently not ensured practically by any sectoral law, apart from the Law on Classified Information to a certain extent.

The second option might solve some problems encountered in the first option, because an umbrella law on security vetting would regulate, in a uniform and comprehensive manner, all fundamental issues that, in the absence of an umbrella law, should be regulated by each sectoral law individually. The fundamental issues would be, for example: what are security impediments; what is security vetting and what types of vetting exist; which authorities are authorised to conduct security vetting; principles of conducting security vetting (purposefulness - results of vetting that can be used only for a specific, pre-defined purpose; proportionality - data collected through security vetting must be relevant and fit for purpose; awareness - it is necessary that persons should be informed in advance in which situations they undergo checks and to be acquainted with the questions, contained in the mandatory forms, to which they will have to respond, and if there are security impediments due to which they were not cleared, they should be notified of them); retention of security vetting results - periods, security measures, etc., and, where appropriate, other fundamental issues. These general provisions would still need to be developed in the sectoral laws, precisely regulating the procedure, in line with the needs of a given sector, and other issues.

However, whichever option is chosen - with or without an umbrella law, it is necessary to regulate the matter of security vetting by law and to ensure its consistent application.

Separate Expert Opinion of Professor at the Faculty of Law, University Union: Saša Gajin, PhD

Taking into consideration the unsatisfactory situation concerning the existing regulatory framework and the need to immediately improve the legal system in the area of security vetting, the question is raised whether it would be substantively, procedurally and legally & technically expedient to regulate this matter in a single law. Security vetting has never been and cannot be understood as an end in itself, but as a means of achieving other specific and precisely defined goals, determined by law and considered legitimate in a democratic society. In this regard, it is important to point out the substantive and procedural differences in the security vetting conducted in specific areas.

In fact, if we compare the particular situations that require the regulation of security vetting, we shall conclude that it is necessary to prescribe separate substan-

tive and formal requirements for security vetting for each area, such as access to classified information; employment and powers of employees and officials in security-sensitive authorities and services; authorisations of persons engaged to perform physical and technical security tasks; enrolment in certain schools and higher education institutions; licences for possessing and carrying weapons and ammunition, etc.

Substantive requirements primarily refer to the reasons and criteria for security vetting, not abstractly defined, but specifically focused on the goal or purpose for the collection and processing of personal data. In the context of security vetting in one of the aforementioned areas, it is important to note that these reasons and criteria significantly differ from the reasons and criteria dominating in other areas.

Similarly, procedural requirements refer to the competence for conducting security vetting and making decisions based on the security assessment, which includes the issue of using legal remedies against such decisions, and to the rules of security vetting procedure, in particular the issue of prescribing the form of security vetting, whose content is entirely conditioned by predefined substantive requirements. Given this specificity, it can be concluded that procedural requirements could not be uniformly prescribed for different areas in which security vetting is conducted, but it should be ensured that they reflect the characteristics of the area for which they are prescribed.

Hence, respecting the fact that the matter of security vetting relates to substantially different thematic units, an umbrella law would necessarily constitute only a simple collection or catalogue of purposes, forms, procedures, responsibilities of authorities, records, etc. related to particular areas. In other words, if the umbrella law included all of these issues, it would become a set of substantive and formal requirements lacking mutual legal communication. For that reason, it would be far more significant to work on the immediate advancement or upgrading of the special legal regimes of security vetting in certain areas, particularly in the areas where the prescribed regime of security vetting is not in compliance with the fundamental regulatory framework, primarily with the provisions of the Law on Personal Data Protection.

RECOMMENDATIONS

The benefits and risks of adopting an umbrella Law on Security Vetting should be considered against the possibility of filling the legal gaps within the existing thematic regulations.

Security vetting conducted for all natural persons and legal entities should be defined clearly and unequivocally, indicating also the authorities conducting security vetting and relevant procedures.

The new Law on Police should envisage the procedures of conducting security vetting for the legal entities and natural persons that are not public authorities or provide for the possibility of transferring public powers concerning the application for security certificates of private security operators, or leave space for further regulation of this area in a bylaw.

The new Law on Records and Data Processing in the Field of Internal Affairs should prescribe a set of data kept by the Ministry, specifically indicating that such data is collected by conducting security vetting for natural persons who are not a public authority.

The Law on Weapons and Ammunition should clearly specify the procedure of performing the security and operational checks referred to in Article 11, including the forms and manner of keeping records of collected data.

The Law on Citizenship should stipulate that applicants for citizenship are to be subjected to security vetting, and unless prescribed by another law or bylaw - the method of conducting security vetting and the authority conducting security vetting should be established.

All the existing regulations, which prescribe the conducting of security vetting in any way (explicitly or implicitly), should be aligned with the provisions of the Constitution that guarantee to the citizens of Serbia the right to privacy and personal data protection.

ABOUT THE CENTER FOR EURO-ATLANTIC STUDIES

The Center for Euro-Atlantic Studies (CEAS) is an independent, atheist, socio-liberal, policy research think tank, driven by ideology and values. It was established in 2007 by a small group of like-minded colleagues who shared an awareness of the inter-conditionality between global and regional trends, foreign policy orientation of the country, security and defense sector reform, and transitional justice in Serbia. With these linkages in mind, CEAS was established with the following mission:

- To accelerate the process of Serbian EU integration and to strengthen its capacities to confront global challenges through collective international action, resulting in full and active membership of the EU;
- To strengthen the cooperation with NATO and advocate for full and active Serbian membership in the Alliance;
- To promote regional cooperation and raise public awareness of its significance;
- To impose a robust architecture of democratic oversight of the security system;
- To support the development of transitional justice mechanisms, their enforcement in Serbia and the Western Balkans, and the exchange of positive experiences; to emphasize the importance of mechanisms of transitional justice for successful security sector reform in post-conflict societies in transition towards democracy.

To accomplish its mission, CEAS is targeting Serbian policy makers and the Serbian general public, as well as international organizations, governments and other actors dealing with Serbia and the region of Western Balkans, or dealing with the issues that CEAS covers, through the promotion and advocacy of innovative, applicable and practical policies aimed at:

- Keeping up with the trends and developments in socio-liberal studies and practice, and at strengthening of socio-liberal democracy in Serbia;

- Adopting the principle of precedence of individual over collective rights, without disregard for the rights which individuals can only achieve through collective action;
- Strengthening the secular state principle and promoting an atheistic understanding of the world;
- Contributing to the erection and preservation of a more open, safe, prosperous and cooperative international order, founded on the principles of smart globalization and equitable sustainable development.

With its high quality research and devoted work CEAS generates accurate and recognized analyses primarily in the fields of foreign, security and defense policies with recommendations based on its core values, with specific focus on:

- Acceleration of the processes of Serbian EU integration and strengthening of its capacities for confronting global challenges through collective international action, resulting in full and active Serbian membership of the EU;
- Strengthening cooperation with NATO and advocacy for full and active Serbian membership in the Alliance;
- Promotion of the significance of regional cooperation;
- Imposition of the robust architecture of democratic oversight of the security system;
- Supporting development of transitional justice mechanisms, their enforcement in Serbia and the Western Balkans, and the exchange of positive experiences; emphasizing the importance of mechanisms of transitional justice for successful security sector reform in post-conflict societies in transition towards democracy;
- Promotion of humanitarian and security norm Responsibility to Protect arguing that the state carries the primary responsibility for the protection of populations from genocide, war crimes, crimes against humanity and ethnic cleansing, that international community has a responsibility to assist states in fulfilling this responsibility and that the international community should use appropriate diplomatic, humanitarian and other peaceful

means to protect populations from these crimes if a state fails to protect its populations or is in fact the perpetrator of crimes;

- Promotion of Open Government Policy, aiming to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance.

CEAS is carrying out its mission through various projects within its five permanent programs:

- I Comprehensive monitoring of contemporary international relations and foreign policy of Serbia
- II Advocacy for full-fledged active membership of Serbia in the EU and NATO
- III Advocacy for comprehensive Security Sector Reform in Serbia
- IV Advocacy for development of the discourse of Energy Security in Serbia
- V Liberalism, Human Rights, Responsibility to Protect, Transitional Justice and Open governance in the globalized world

CEAS is an active member of the REKOM coalition which suggests that governments (or states) establish REKOM, an independent, inter-state Regional Commission for the Establishment of Facts on all the victims of war crimes and other heavy human rights violations undertaken on the territory of the former SFRY in the period 1991-2001.

During 2012, CEAS also became the first civil society organization from the region of South-Eastern Europe to have full membership in the International Coalition for the Responsibility to Protect – ICRtoP. The coalition brings together non-governmental organizations from all over the world to collectively strengthen normative consensus for the doctrine of Responsibility to Protect (RtoP), with the aim of better understanding the norm, pushing for strengthened capacities of the international community to prevent and halt genocide, war crimes, ethnic cleansing and crimes against humanity and mobilize the non-governmental sector to push for action to save lives in RtoP country-specific situations. Prominent members of the Coalition include Human Rights Watch and the International Crisis Group.

In April 2013, CEAS became the first civil society organization in Serbia that joined the Commission of Associations of the Serbian Chamber of Commerce for Public-Private Partnership in the security sector in Serbia. The Commission, alongside representatives of the private security sector, consists also of representatives of the MoI and other state bodies and institutions, which are responsible for cooperation between the public and the private security sector within the state administration.

In September 2013, CEAS also became a member of Sectorial civil society organizations – SEKO, for rule of law. The program of cooperation with civil society organizations in the planning of development aid distributed by the EU Integration Office, particularly programming and monitoring of use of the Instrument for Pre-Accession Assistance for 2011, envisaged the establishment of a consultative mechanism with CSOs implying Sectorial civil society organizations (SEKO) as key stakeholders. Under the sectorial organizations of civil society is a consortium of civil society organizations from the three partners most of which is the lead partner.

In September 2014 CEAS became a full-fledged member of the Policy Association for an Open Society – PASOS, an international association of think-tanks from Europe and Central Asia which supports the erection and functioning of an open society, especially in relation to issues of political and economic transition, democratization and human rights, opening up of the economy and good public governance, sustainable development and international cooperation. PASOS has 40 full-fledged and 10 associate members, including the prestigious European Council on Foreign Relations – ECFR.

