Jelena Kostić, PhD
Institute of Comparative Law
Terazije 41, Belgrade, Serbia
suputjelena@yahoo.com

Sanja Jelisavac Trošić, PhD
Institute of International Politics and Economics
Makedonska 25, Belgrade, Serbia
sanja@diplomacy.bg.ac.rs

DIGITAL FORENSIC PROCEDURES OF EUROPEAN ANTI-FRAUD OFFICE AND PROTECTION OF PERSONAL DATA[1]

ABSTRACT

The European Anti-Fraud Office is established in order to step up the fight against fraud, corruption and other illegal activity affecting the financial interests of the European Union. In that fight essence of investigation makes a digital forensic procedure. Digital forensic procedure implies a technological inspection, acquisition, and examination of digital media or their contents using forensic equipment and software tools. The objective of digital forensic procedure is to locate, identify and collect data which may be relevant to an investigation and use it as evidence in administrative, disciplinary and judicial procedures. These operations can include acquiring personal data what may be perceived as privacy invasive. In this paper, the authors will try to analyze the legislation of European Union in this field and the European Anti-Fraud Office legislation in order to explain the conditions of use and protection of personal data.

Key words: *digital forensic procedure, European Anti-Fraud Office, investigations, privacy, protection, EU.*

[1] This paper was created within the two projects: "Serbian and European Law: Comparison and harmonization", Ministry of Education and Science of the Republic of Serbia, number 179031, for the period 2011-2017 and is implemented in the Institute of Comparative Law and "Serbia in contemporary international relations: Strategic directions of development and firming the position of Serbia in international integrative processes – foreign affairs, international economic, legal and security aspects", Ministry of Education and Science of the Republic of Serbia, number 179029, for the period 2011–2017 and is implemented in Institute of International Politics and Economics.

1. INTRODUCTION

The right to privacy falls into the rights of a new generation. Privacy is a fundamental right that protects the private sphere of life of an individual. The protection of the right to privacy allows the life and development of a human without arbitrary interference of the state and other parties. In recent years, there is an increasing need for protection of the right to privacy, because the development of science and technology opens up large opportunities for endangering the private sphere of a human life.[2] In this Digital Age, faster exchange of personal data, especially on-line, creates the possibility of easy access and abuse to a large number of individuals and companies. When it comes to data relating to private life they are part of the private sphere, i.e. human right to live how they want, protected from the public to some extent.[3] Therefore, the right to respect a private life limits the extent to which the individual himself brings his private life into contact with public life or in close connection with other protected interests.[4] But, sometimes it is necessary to use some data, which fall into the category of personal data, in order to carry out certain activities to satisfy public interest by both national and international institutions. One of those interests is controlling the EU budget expenditure.

The responsibility for spending of financial resources of the Union is an issue that is on the list of priorities for both its institutions and EU Member States.[5] The European Anti-Fraud Office (OLAF), based in Brussels, is established at the European Union level in order to ensure effective protection of its financial interests. It has been established in 1999, based on the Decision of the European Commission, as an independent body with power to investigate possible financial offenses that could endanger the financial interests of the European Union.[6] OLAF carries out investigations into the existence of irregularities, regardless of whether such irregularities deserve criminal or other kind of prosecution. Its jurisdiction is the prevention of irregularities relating to the expenditure of European Union funds.[7]

---

2 Dimitrijević, V.; Popović, D.; Papić, T.; Petrović, V.; *Međunarodno pravo ljudskih prava*, Beogradski centar za ljudska prava, Beograd, 2007, p. 203.

3 Dimitrijević, V.; Paunović, M.; Đerić, V.; *Ljudska prava*, Beogradski centar za ljudska prava, Dosije, Beograd 1997, p. 286.

4 *Ibid.*

5 Rabrenović, A., *Odgovornost za trošenje finansijskih sredstava Evropske unije*, in: 50 godina Evropske unije, Institut za uporedno pravo, Vlada Srbije - Kancelarija za pridruživanje Evropskoj uniji, Beograd, 2007, p. 186.

6 Commission decision of 28. April 1999 establishing the European Anti Fraud Office (OLAF) (notified under document number SEC (1999) 802) 1999/352/EC, ESC, Euroatom) [1999] OJ L136/20.

7 Article 1 of Decision No 352/1999. Cited by Šuput, J., *Zaštita finansijskih interesa Evropske unije-uspostavljanje AFCOS sistema*, Pravni život, No 7-8, 2014, p. 24.

It is part of the European Commission and conducts fraud investigations in all European Union countries and within the European institutions themselves. It can also conduct investigations in non-EU countries with which it has agreements.

OLAF is not competent to fight fraud that does not concern the budget of the European Union. In other words, EU money has to be involved. The same goes for the fight against corruption: OLAF can only investigate cases where EU staff appears to be involved.[8] When OLAF control is carried out in the territory of the Member State, authorities in that territory are obliged to provide all necessary assistance to its inspectors during controls and inspections.[9] The control is done by examining the books and records, invoices, contracts, receipts, bank statements and computer databases. It includes physical verification, check of the quantity and nature of goods ordered or the quality of service, taking and checking of samples, control of completed works and investments from the European Union funds, as well as insight into the technical implementation of subsidized projects.[10] The information gathered during the control are representing a business secret, in accordance with national regulations of the country in whose territory the inspection was conducted, and may only be used for the protection of the financial interests of the Union. Materials and documentation collected in the process of inspection may be used as evidence in administrative or judicial proceedings in the territory of the State where the irregularity was detected at the expense of the financial interests of the European Union.

The European Anti-Fraud Office is not a judicial authority or law enforcement agency. The punishment of the perpetrators of any violations or criminal offenses against the financial interests of the European Union is the responsibility of the police and judicial authorities of the countries on whose territory OLAF performs its financial investigations. Accordingly OLAF collects data and submits them to relevant institutions at the national level.[11] In that way, relevant institutions are able to use the information and data that OLAF collects during its investigation.

---

8 IAACA, *European Anti-Fraud Office*, URL=http://www.iaaca.org/AntiCorruptionAuthorities/ByInternationalOrganizations/InterGovernmentalOrganization/201202/t20120215_805457.shtml. Accessed 31 January 2017.

9 Article 4, Paragraph 1 of the Council Regulation (Euroatom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks inspections carries out by the Commission in order to protect the European Communities´ financial interests against fraud and other irregularities. Cited by Šuput, J. *op.cit*. note 7 , p. 25.

10 *Ibid.* Article 4.

11 Reljanović, M.; Ivanović, Z.; *Evropska kancelarija za borbu protiv finansijskih prestupa* in: Borba protiv korupcije, iskustva i poređenja, Ćirić, J. (ed.), Beograd, 2013, p. 113.

The European Anti-Fraud Office has the right of access under the same conditions as national administrative inspectors to all the information and documents concerning economic activities, including computer data necessary to conduct proper inspections.[12] A special kind of evidences is data on a digital media, i.e. the information contained in the digital form. They are further processed and prepared for the purpose of a possible proof of certain facts in court proceedings. However, also in a digital media you can found a large number of personal data, and that always raises the question of the efficiency of their protection, both in general and at the institutional level.

During development of the legal protection of personal data in the European Union, emerged the need for more specific protection of personal data from abuse. Legal regulations are developed gradually, and some institutions have established their own rules of procedure relating to the collection and disposal of personal data in a digital form. Under personal data we consider any information that can point to a particular person, such as name, phone number or photo. Personal data can be collected directly from individual person or from the database. Thus, the data collected may be made available to a larger number of entities and may be used for other purposes.[13] Privacy as an ethical concept and as a fundamental human right is not static. The privacy concerns and expectations of research participants are likely to evolve in the upcoming years.[14]

Although, at the level of the European Union, there are a number of regulations that provide effective mechanisms of personal data protection, certain institutions adopted internal acts for employees regulating the manner of handling in order to protect personal data. The same approach in this regard is also present at the European Anti-Fraud Office.

2. LEGAL PROTECTION OF PERSONAL DATA

The Universal Declaration on Human Rights (Universal Declaration) was the first legal document which provides protection of personal data at the international level.[15] Besides Universal Declaration, the International Covenant on Civil

---

12 Council Regulation (Euroatom, EC) No 2185/96, *op. cit.* Article 7.

13 Nikodinovska-Stefanovska, S., *Lisbon Treaty and the Protection of Personal Data in the European Union*, in: Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske unije (II), Dimitrijević, D.; Miljuš B. (ur.), Beograd, 2012, p. 717.

14 Joly, Y.; Dyke, S.O.M.; Knoppers, B.M.; Pastinen, T., *Are Data Sharing and Privacy Protection Mutually Exclusive?*, Cell 167, Elsevier Inc, November 17, 2016, p. 1153.

15 The Universal Declaration on Human Rights, adopted by the **UN** General Assembly on 10 December 1948, in Paris, General Assembly Resolution 217A, United Nations. Universal Declaration was pro-

and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) also has provisions for the protection of personal data.[16] According to Article 12 of the Universal Declaration no one shall be subjected to arbitrary interference with her/his privacy, family, home or correspondence, or to attacks upon her/his honor and reputation. Everyone has a protection provided by the law against such interference or attacks. The same right to protect privacy is guaranteed by Article 17 of the International Covenant on Civil and Political Rights. The European Convention on Human Rights mentions the right to respect private and family life, home and correspondence. The term implies the respect and protection of the individual against arbitrary interference with privacy by public authorities, but requires the state to actively participate in the provision of the mentioned law.[17] It is therefore necessary both at national and international level to establish effective mechanisms for prevention of a behavior that can be arbitrary interference in the private life of individuals.

Modern development of science and technology opens up previously unimagined possibilities of interference in the most intimate parts of human life.[18] One of the first documents that provide protection of personal data in digital form in the European Union is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981.[19] It envisages the obligation

---

claimed as a common standard of achievements for all peoples and all nations. Text of the Declaration can be found at: URL=www.un.org/en/universal-declaration-human-rights/. Accessed 02 February 2016.

16 The International Covenant on Civil and Political Rights (ICCPR) was adopted and opened for signature, ratification and accession by United Nations General Assembly resolution 2200A (XXI) of 16 December 1966. That document entered into force on 23 March 1976. Law on ratification of ICCPR, Službeni list SFRJ-Međunarodni ugovori (Official Gazette SFRY-International Agreements), No 7/1971. The European Convention for the Protection of Human Rights and Fundamental Freedoms was ratified by the Law on Ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol 11, Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, Protocol No. 4 to the Convention for the Protection of human rights and Fundamental freedoms securing certain rights and freedoms that are not included in the Convention and the first Protocol thereto, Protocol No. 6 to the Convention for the protection of human rights and Fundamental freedoms concerning the abolition of the death penalty, Protocol No. 7 to the Convention for the protection of human rights and Fundamental freedoms, Protocol No. 12 to the Convention for the protection of human rights and Fundamental freedoms and Protocol No. 13 to the Convention for the protection of human rights and Fundamental freedoms concerning the abolition of the death penalty in all circumstances, Službeni list SFRJ-Međunarodni ugovori (Official Gazette SCG-International Agreements), No. 9/2003 and 5/2005.

17 Paunović, M.; Krivokapić, B.; Krstić, I.; *Osnovi međunarodnih ljudskih prava*, Megatrend univerzitet, Beograd, 2007. p. 217.

18 Dimitrijević *et al., op. cit*. note 2, p. 203.

19 The Convention for the Protection of Individuals with regard to automatic processing of Personal data.

of every country to respect the rights and fundamental freedoms of every person, especially the right to privacy during the automatic processing of personal data.[20]

When it comes to the Community institutions and bodies of the European Union, the first time the protection of personal data is referred to was in Article 286 of the Treaty establishing the European Community. According to that provision, the Community is taking measures for the protection of personal data during data processing and exchanging of Community institutions and bodies.[21] The mechanisms to achieve this objective are contained in the Regulation on the protection with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data No. 45 of 2001 (hereinafter the Regulation).[22] When collecting personal data in digital form the OLAF employees are obliged to comply with the provisions of the Regulation. Given that a large number of financial data is nowadays in digital form, such data are often subject to digital forensics, which is carried out in special OLAF laboratories. Since often among the financial data can also be found personal data, they must be processed in accordance with applicable regulations of the European Union. That is why the European Anti-Fraud Office issued special instructions to be followed by employees during digital data processing.[23]

3. OLAF - COLLECTING DIGITAL EVIDENCE AND PROTECTION OF PERSONAL DATA

Since OLAF is the European Commission institution, it is required in conducting their investigations, i.e. when collecting data in digital form, to primarily obey the provisions of Regulation No 45/2001. However, this does not mean that when

---

The Convention was adopted and opened for accession in Strasbourg 28.01.1981. Convention entered into force in 1985. Text of the Convention can be found at: URL=www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007b37. Accessed 07 February 2016.

20 *Ibid.* Article 1.

21 The Consolidated version of the Treaty establishing the European Community [1997] OJ C340 and [2002] OJC325. Text of the Treaty can be found at: URL=www.eu-lex.europa.eu/legl-content/EN/TXT/?uri=CELEX%3A12002E%2FTXT. Accessed 03 February 2016.

22 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Text of the Regulation can be found at: URL=http://secure.edps.europa.eu/EDPSWEB/webday/site/my/Site/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf. Accessed 04 February 2016.

23 Guidelines on Digital Forensic Procedures for OLAF Staff,15. February 2016, Text can be found at: URL=https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf. Accessed 08 February 2016.

performing investigations the European Anti-Fraud Office does not apply internal rules and procedures. OLAF has the right during inspection to access all information relevant to the investigation, including digital data and databases. It is authorized to check the accounts and financial records of institutions, bodies, offices and agencies. In order to take adequate inspection measures inspectors or auditors employed by OLAF may take a copy of any document. They have the same rights in this respect, as well as national inspectors in accordance with the regulations of the country where the controls or inspections are conducted. Also, there is an obligation of the employees of the institution in which inspection is carried out to provide OLAF personnel the data necessary to carry out their activities.[24]

The data that are taken in the process of inspection, which can serve as evidence in subsequent proceedings, must be protected as a confidential data in the same manner as the data that are in similar situations provided protection at the national level. These data can not be disclosed to anyone, except the person or institution in the Member State whose function requires that such data to be used in their work. They can be used solely for the purpose of protecting the financial interests of the European Union. If irregularities are detected in the work of the institutions whose operations is being investigated, the Commission should immediately inform the competent authorities of the Member State in question. In any case it is necessary to inform the competent authorities in relation to the reported results of the inspection. The Commission has an obligation to prepare a draft report which is an integral part of the collected materials and evidence in the future to be used as evidence in a possible misdemeanor or criminal proceedings, in the same way as in the case where the materials and evidence collected by the competent national authority.[25] If the national inspectors participated in the inspection and control, they are also obliged to sign the report.[26] Bearing in mind that OLAF represents the kind of budget inspection of the European Union, it should be noted that it is also responsible for providing evidence for future legal proceedings with regard to violations of the financial interests of the Union.

When the digital evidence began to be accepted as equal to the other evidence in the court, digital forensic has developed, as part of forensic science, whose subject

---

[24] Council Regulation (EUROATOM, EC) No 2185/96 of 11 November 1996 concerning on the spot checks and inspections carried out by the Commission in order to protect the European Communities´ financial interests against fraud and other irregularities, Article 7., OJ L 292/96, URL=https://publications.europa.eu/en/publication-detail/-/publication/adc86f79-268e-4ac4-8ae5-85c70ade888f/language-en. Accessed 07 February 2016.

[25] The Commission is responsible for ensuring that Member States respect European Union laws.

[26] *Ibid.* Article 8.

is legal analyzes of the obtained evidence found in computer and digital media.[27] Sometimes in order to provide relevant evidence the large amount of personal data are also collected. Therefore, there are the possibilities of violations of right to privacy, not only during data collection and processing, but also in delivering these data to other relevant institutions. In order to avoid violations of right to privacy, when performing digital forensics, OLAF employees have an obligation to comply with that provision of Regulation No 45/2001 and Guidelines on Digital Forensic Procedures for OLAF Staff.

3.1. Protection and free movement of personal data

The provisions of Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data are obliged to adhere to all institutions and bodies which are established in accordance with the provisions of the Treaty establishing the European Community.[28] One such body is the European Anti-Fraud Office. It has the obligation, during digital forensic operations, to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and to allow the free exchange of such data with other EU bodies and Member States.[29] The Regulation also applies to the processing of personal data wholly or partly by automatic means (automatic data processing).[30]

Data provided by OLAF delivered to the Member States in order to carry out the responsibilities of entities on their territories can be delivered only if it is necessary to exercise the powers in the public interest, or if it is a public institution providing data to perform its obligation from its jurisdiction, or if the recipient proves that these data are really necessary and if it proves that there is no possibility to harm legally protected personnel interests of persons whose data are submitted.[31]

When institutions or bodies of the European Union, or countries that have national legislation in accordance with Directive 95/46 /EC are not in question

---

27 Korać, V.; Prlja D.; Gasmi, G., *High Technology Criminal and Digital Foresics*, in: Preventing and Combating Cybercrime, Cluj_Napoca, Accent, 2016, p. 93.

28 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L008 pp. 0001 – 0022.

29 *Ibid.* Article 1.

30 *Ibid.* Article 3.

31 *Ibid.* Article 7-8.

special conditions shall be applied.[32] Under these conditions, personal data may be submitted only if the protection of personal data is provided at an adequate level, and if the submission of these data is done solely for the purpose of performing legal powers by the person requesting the information. When it comes to an adequate level of protection at the level of countries that are not members of the European Union or international organizations, they should be treated depending on the particular circumstances, such as: nature of the information that is provided, the duration of the procedure of processing such data, respect for the rule of law in the country where the information is provided on both the general and at the institutional level as well as the security measures that are taken to protect data. If it is concluded that the level of protection of personal data in the country of international institutions is not adequate, the data will not be send, and OLAF should inform about that decision the Commission and data protection officer. In this case the Commission, not OLAF, exclusively informs the third party of a refusal. Exception from that rule is only if the person, to whom the personal data are relating, give explicit consent, as well as other conditions prescribed in the Regulation. In such situations it is also necessary to inform data protection officer at EU level.[33]

The collection, processing and exchange of special categories of data such as ethnic origin, political opinions, religious or philosophical beliefs, membership in business associations or data relating to health and sex life is strictly prohibited. However, there is a possible deviation in the case of one of the exceptions set out in the Regulation. The exception is the explicit consent of the person whose personal data is processed during the investigation.[34] Any person who considers that her or his privacy rights are violated as a result of taking action by OLAF can lodge a complaint to the European data protection supervisor or to the European Ombudsman.[35]

---

[32] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In accordance with mentioned Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

[33] *Ibid.* Article 9.

[34] *Ibid.* Article 10.

[35] The European data protection supervisor (EDPS) in an independent supervisory authority established by the Regulation No 45/2001 devoted to protecting personal data and privacy and to promoting good practice in the EU institutions and bodies. More information about mentioned authority can be found on the website: http://secure.edps.europa.eu/EPDSWEB/edps/EDPS The European Ombudsman is an independent and impartial body that holds the EU administration to account. Mentioned body investigates complaints about maladministration in EU institutions, bodies, offices and agencies. The Ombudsman may find maladministration if an institution fails to respect fundamental rights, legal

3.2. Rights and obligations when processing personal data

When it comes to the use of personal data we saw rights and obligations of the institution and employees that collect them. But also a person whose data is used by OLAF has certain rights.

When taking personal data OLAF employee is obliged to communicate to person in question she/he identity, the purpose for which such data is collected and the name of the institutions and bodies that will be allowed to use this information. In addition, it is required that person in question should be informed when answering certain questions mandatory, and when voluntarily, as well as the consequences of failure to give answers, to be informed of the right of access to data concerning she/he personality, the right to revise these data. The person in question should also be given additional information, such as the legal basis for the collection of data, the time limit for storing the data, the right to contact at any time the supervisor for personal data protection in the European Union. Also the person from whom the personal data are collected will be given any additional information, bearing in mind the special circumstances under which the data were collected, in order to ensure protection of the right to privacy.[36]

In some cases, personal data have not been obtained from the data subject. Then it is necessary that a person who collects information at the time of taking, if a disclosure to a third party is envisaged, inform the person to whom they relate about the purpose for which they are collected, the data category, the category of recipients, the existence of the right of access or modification of data concerning data subject, as well to offer additional information concerning a legal basis for an action for which the data is collected, the time period of storing such data, the right to apply to the supervisor for the protection of personal data at the European level Union, the origin of the data (how to reach these data) unless that person is unable to disclose the information due to professional secrecy, as well as any other information that depending on the circumstances is necessary to ensure legality of such data.[37]

Also, a subject whose personal data are used in the process of digital forensics, has the right to access this information, right of correction, the right to block

rules or principles, or the principles of good administration. Any citizen or resident of the European Union or business, association, or other body with a registered office in the Union can lodge a complaint. Ombudsman only deal with complaints concerning the EU administrations. Complaint can be sumitted electronicaly or printed out and sent by post. More information about mentioned body can be found on the web-site:URL=http://www.ombudsman.europa.eu/home.faces

36 *Ibid.* Article 11.

37 *Ibid.* Article 12.

their use, deletion, right to request the modification and deletion of data that are communicated to a third party (unless it does not require additional efforts), and have requested that she/he identity not mentioned in the decision. However, these rights may be denied, and if necessary, take the necessary measures in order: prevention, investigation, detection and prosecution of criminal offenses, if it is an important economic or financial interest of a Member State or the European Community, by which it means a circumstance which belongs to monetary, budgetary or tax matter.[38]

When it comes to personal data which are the subject of digital forensics by experts employed in OLAF, that organization in compliance with the provisions of Regulation, is obliged to deny access unauthorized persons to computerized systems used for the processing of personal data, and to prevent unauthorized reading, copying, modification or transfer of data stored on digital media, as well as unlawful destruction, modification or deletion of data stored on digital media. Obligations of OLAF in connection with the above consists in preventing unauthorized persons to use the system for processing data, ensuring that at any time can be checked when, where and who participated in the processing of personal data, ensuring that data can only be delivered, in accordance with the relevant legal documents, to the other institutions. During transport of media in which personal data are kept, personal data can not be read, copied or erased by unauthorized persons.[39] Therefore, in accordance with the provisions of the Regulation, Guidelines on Digital Forensic Procedures for OLAF Staff provides for monitoring entry and exit of authorized persons in the laboratory for digital forensics, as well as the obligation of recording the persons involved in the processing which are authorized to access personal data. The Regulation provides for certain measures for recording any damage related to the digital media where personal data are stored, as well as measures for recording communication between persons involved in the process of personal data processing.

3.3. Data protection officer

The European Anti-Fraud Office in accordance with Article 24 of Regulation appoints officers for the protection of personal data. Data protection officer commitments are: to ensure that persons who process personal data, as well as persons whose data is processed should be made aware of their rights and obligations pertaining to them in accordance with the Regulation, to respond to requests to monitor protection of personal data at the level of the European Union, to

[38] *Ibid.* Article 20.

[39] *Ibid.* Article 21.

cooperate with supervisors to ensure the internal application of the provisions of the Regulation to lead register of activities related to data processing, to inform the manager for the protection of personal data in the European Union if certain operations pose a particular risk to the violation of privacy rights, and to ensure that data processing respect all the rights of the individuals whose personal data are subject to processing.[40]

Data suspected to contain a high level of risk in terms of potential violation of privacy rights are, for example, information with respect to whom there is a suspicion of certain criminal offenses, violations, as well as data contained in court rulings, or information on safety measures relating to the assessment of the personal qualities and abilities of a specific person. After receiving the notification data protection officer in the European Union gives its opinion and recommendations to OLAF in order to most effectively protect personal data in their processing procedure. The European Anti-Fraud Office also has an obligation to submit proof on the implementation of the recommendations to a data protection officer. Given that this is a very sensitive data and a specific situation, the person responsible for the protection of personal data at the level of OLAF is obliged to seek opinion from the data protection officer before the start of the processing of such data. Apart from these situations, it is possible that the case file contains information on a large number of people, which are not relevant to the investigation conducted by the European Anti-Fraud Office. Notification to such persons that their data are stored in the file would be too much time consuming and burden for OLAF. However, bearing in mind that these are personal data, it is essential that the person responsible for the protection of personal data seek the opinion of the data protection officer for the protection of personal data at EU level. In order to ensure in the internal level that measures necessary for the protection of personal data are conducted in accordance with Regulation 45/2001, EU issued a Guideline which defines the manner of employees in relation to personal data in the process of digital forensics.

3.4. Protection of personal data in accordance with OLAF Guidelines

Guidelines on Digital Forensic Procedures for OLAF Staff were adopted in 2016.[41] Its provisions are applied in the process of identification, collection, processing, analysis and storage of digital evidence, while their goal is to establish rules for conducting digital forensics, to ensure the integrity and quality of the

[40] *Ibid.* Article 24.

[41] *Guidelines on Digital Forensic Procedures for OLAF Staff*, European Commission, European Anti-Fraud Office, 15 February 2016.

evidence that is admissible in court proceedings. Adoption of these rules achieves two objectives. One is to provide valid evidence in eventual court proceedings, and the other is the protection of personal data from abuse. The provisions of the Guidelines defines that the digital forensics laboratory, in the framework of OLAF, should be physically separated from other rooms and equipped with means for monitoring the entry and exit of authorized persons. Also, they are required to record communication between persons who access data and those involved in data processing. A person who carries out the procedure of digital forensics before undertaking any activities informs the person whose data are subject to processing, by submitting "OLAF digital forensic operations information leaflet". In addition, it is also obliged to provide answers to questions to persons whose data are subject to processing, concerning the specific procedures of digital forensics.

In order to ensure compliance with the provisions of all relevant legislation, a person who conducts digital forensics has the obligation to draw up a written report in which will be described method, the process of collection and storage of data being processed. The same report describes possible damage incurred in connection with digital data. Also, the report should indicate the complaints related to personal data. In addition, the report should include data on all persons involved in the process of collection and processing of evidence which are the subject of digital forensics.[42] A special part of the Guidelines relates to the special protection of personal data. Accordingly, information concerning marital status and information about children can only be included in the case file if they are relevant to the investigation.[43]

During the preparation and implementation of activities that fall into digital forensics, conducted at the level of OLAF, persons employed in the mentioned institutions are required, when it comes to personal data, to comply with the provisions of Regulation No 45/2001. Guidelines on Digital Forensic Procedures for OLAF Staff were adopted to facilitate the application of these provisions. Therefore, in situations that are not defined in the Guidelines directly applicable are provisions of the aforementioned Regulation.

4. CONCLUSION

Digital Forensics by the European Anti-Fraud Office is carried out mainly for the purpose of producing evidences for court proceedings. Considering the fact that among digital data investigator can found a large number of personal data it is

42 *Ibid*. Article 4.

43 *Ibid*. Article 9.

important for OLAF to act in accordance with the provisions regulating the protection of privacy rights. Such provisions are prescribed by Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. However, that Regulation, in addition contains a large number of exceptions to the rules. It is therefore of a great importance, for the legality of the OLAF activities, the adequate selection of officials within the institution. Those officials are authorized to monitor the application of Regulation No 45/2001 and cooperation with supervisors for personal data protection in the European Union.

Bearing in mind that in the process of digital forensics personal data should be handled in a special way, at the level of the OLAF was adopted Guidelines on Digital Forensic Procedures for OLAF Staff. Application of the Guidelines has two objectives. One is to protect the integrity of digital data in order for these data to be used in the future as evidence by the competent authorities of the Member States. The second is to increase the effectiveness of protection of personal data at the level of institution. The special quality of the Guidelines provide measures that are prescribed, relating to the submission of the "OLAF digital forensic operations information leaflet" to a person whose data are subject to processing; the provisions on monitoring the entry and exit from the laboratory; recording communication of a person who processes data with other persons; and the obligation of drawing up reports on the method of collecting and storing data; as well as specific information on possible damage that occurs during the processing of these data; also a data on complaints submitted by authorized persons and data related to information on all persons who have been involved in the process of digital forensics. Guidelines that is compatible with the provisions of Regulation constitutes a kind of written procedures that all employees involved in the process of digital forensics are required to apply. Bearing in mind that Guidelines is a mean for effective implementation of the provisions of the Regulation on the level of the institution, its practical application oversees data protection officer at the European Anti-Fraud Office.

REFERENCES

BOOKS AND ARTICLES

1. Dimitrijević, V.; Paunović, M.; Đerić, V.; *Ljudska prava*, Beogradski centar za ljudska prava, Dosije, Beograd, 1997.
2. Dimitrijević, V.; Popović, D.; Papić, T.; Petrović, V.; *Međunarodno pravo ljudskih prava*, Beogradski centar za ljudska prava, Beograd, 2007.
3. Joly, Y.; Dyke, S.O.M.; Knoppers, B.M.; Pastinen, T., *Are Data Sharing and Privacy Protection Mutually Exclusive?*, Cell 167, Elsevier Inc, November 17, 2016.
4. Korać, V.; Prlja D.; Gasmi, G., *High Technology Criminal and Digital Foresics*, in: Preventing and Combating Cybercrime, Cluj_Napoca, Accent, 2016.
5. Nikodinovska-Stefanovska, S., *Lisbon Treaty and the Protection of Personal Data in the European Union*, in: Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske unije (II), Beograd, 2012.
6. Paunović, M.; Krivokapić, B.; Krstić, I.; *Osnovi međunarodnih ljudskih prava*, Megatrend univerzitet, Beograd, 2007.
7. Rabrenović, A., *Odgovornost za trošenje finansijskih sredstava Evropske unije*, in: 50 godina Evropske unije, Beograd, 2007.
8. Reljanović, M.; Ivanović, Z.; *Evropska kancelarija za borbu protiv finansijskih prestupa* in: Borba protiv korupcije, iskustva i poređenja, Ćirić, J. (ed.), Beograd, 2013.
9. Šuput, J., *Zaštita finansijskih interesa Evropske unije-uspostavljanje AFCOS sistema*, Pravni život, No 7-8, Beograd, 2014.

EU LAW

1. Commission Decision of 28. April 1999 establishing the European Anti Fraud Office (OLAF) (notified under document number SEC (1999) 802) 1999/352/EC, ESC, Euroatom) [1999] OJ L136/20, p. 20–22.
2. Council Regulation (EUROATOM, EC) No 2185/96 of 11 November 1996 concerning on the spot checks and inspections carried out by the Commission in order to protect the European Communities´ financial interests against fraud and other irregularities,1996 OJ L 292/96.
3. Commission Decision of 27 September 2013 amending Decision 1999/352/EC, ECSC, Euratom establishing the European Anti-fraud Office (2013/478/EU) [2013] OJ L 257/19
4. *Guidelines on Digital Forensic Procedures for OLAF Staff*, European Commission, European Anti-Fraud Office, 15 February 2016.
5. Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11. September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 [2013] OJ L248, p. 1.

6. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L008,pp. 0001 – 0022
7. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L008.
8. Council Regulation (Euroatom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks inspections carries out by the Commission in order to protect the European Communities´ financial interests against fraud and other irregularities [1996] OJ L292, p. 2–5.
9. The Consolidated version of the Treaty establishing the European Community [1997] OJ C340 and [2002] OJ C325.
10. The Convention for the Protection of Individuals with regard to automatic processing of Personal data, Councle of Europe, European Treaty Series - No. 108, 28 January 1981.
11. The International Covenant on Civil and Political Rights (ICCPR), Law on ratification of ICCPR, Službeni list SFRJ-Međunarodni ugovori (OfficialGazette SFRY-International Agreements), No 7/1971.
12. The Universal Declaration on Human Rights, adopted by the UN General Assembly on 10 December 1948, Paris, General Assembly Resolution 217A, United Nations.

WEBSITE REFERENCES

1. IAACA, *European Anti-Fraud Office*.
URL=http://www.iaaca.org/AntiCorruptionAuthorities/ByInternationalOrganizations/InterGovernmentalOrganization/201202/t20120215_805457.shtml. Accessed 31 January 2017.