Practice Name:

Digital forensic operations with OLAF

Country:

Bulgaria

Practice category:

- System and tools

Contact:

- AFCOS Bulgaria and Public Financial Inspection Agency
- www.afcos.bg
- afcos@mvr.bg

Fraud risk(s) countered

- Conflict of interest
- Avoidance or manipulation of public procurement procedures
- Double funding
- Collusion
- Manipulation of project costs
- Others – **all other**

Context and objective(s)

Regulation 2185/96 *concerning on-the-spot checks and inspections carried out by the EC in order to protect the European Communities' financial interests against fraud and other irregularities* requires that national authorities provide the necessary assistance to the European Commission (EC), in particular – the European Anti-Fraud Office (OLAF), during on-the-spot-checks (OTSC) on the territory of the country.

During the OTSC, the investigators' main objective is to gather evidence to prove the case. In light of the current electronic information age, the **digitalisation of all processes** and the implementation of **digital forensic operations** is more essential now than ever before. In many cases the OTSC involves the collection **of computer data.**

Therefore, the objective of this good practice is to demonstrate how national authorities in Bulgaria secure and gather computer data to be used by the European Anti-Fraud Office (OLAF).

Description of the practice

This practice was implemented after the accession of Bulgaria to the European Union, with amendments to the Law of the Public Financial Inspection Agency (PFIA), in order to tackle two major problems that the OLAF investigative teams may encounter during an OTSC which aims to collect digital data:

1. If the economic operator denies access to premises, where the computer data is stored, such as an office, car, archive etc., or

2. If the economic operator allows the investigators to enter the premises, but does not give permission to the investigators to take the necessary computer data (USB drives, hard disks, SSDs, CDs, DVDs, computers etc.)

With the amendments of the Law (Official Journal of Bulgaria № 98/2008) Chapter 3a was created, called ***"Rendering assistance to the inspectors of the European commission for granting access to premises and/or documentation for carrying out on-the-spot inspections and checks under council regulation (EURATOM, EC) № 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."***

The law now targets exactly these two potential problems with the following text:

"The Public Financial Inspection Agency of Bulgaria shall provide assistance to the inspectors of the Commission for carrying out on-the-spot inspections and checks, in case of:

1. Denied access to premises, means of transport, and also other places used for keeping documents, **recordings of computer information data**, carriers of computer information data of the checked organisation or of a person who received funds under international treaties or programs of the European Union;

2. Denied provision of documents, **recordings of computer data relevant to the investigation, carriers of computer information data**, necessary for the check, where access under Item 1 has been granted."

What are the main steps to gather digital evidence for the purposes of an OLAF Investigation in the area of ESI funds? 10 step model.

1. In order to collect and safeguard digital evidence and present it to the OLAF investigators, the adapted procedure in Bulgaria envisages assistance to be rendered by the Director of the PFIA based on a reasoned written request by the Director of Directorate "Protection of the Financial Interests of the European Union AFCOS" at the Ministry of the Interior (Bulgarian Anti-Fraud Service, AFCOS, contact point for OLAF).

2. The request for assistance to OLAF's investigators shall contain information on the checked organisation or person (economic operator, beneficiary), the object and purpose of the OTSC or inspection and the grounds for seeking assistance.

3. AFCOS shall present copies of the authorisation of OLAF's investigator and of the document stating the object and purpose of the OTSC.

4. The financial inspector from PFIA shall establish if there are grounds to render assistance to OLAF's investigators in the two possible instances of non-cooperation – denied access to premises or denied access to digital data.

5. The financial inspector from PFIA visits the address of the economic operator and if the latter **still does not cooperate**, the financial inspector draws up a protocol of findings. At the same time, the Director of PFIA immediately submits a written request to the police (Ministry of the Interior) to access the premises.

6. If the financial inspector is concerned that the economic operator may hide or delete digital data, they **seal off** the premises or documentation until the arrival of police authorities to enter the premises.

7. If sufficient information is available that there are documents and/or computer information data, or carriers thereof in them, which are necessary for the check and are of such importance as to justify their seizure in order to secure evidence within the premises, the Director of PFIA shall write a motivated request to the regional court at the seat of the address. The regional court decides on the request **immediately** within the same day of its submission in a closed session on a motivated ruling not subject to appeal.

8. After receiving the same-day permission by the Court, the Director of PFIA or officials authorised by the director shall request assistance from the authorities of the Ministry of the Interior for the search and/or seizure of the premises and/or digital data.

9. The search and the seizure shall be carried out by the financial inspector assisted by a representative of the Ministry of the Interior in the presence of:

- a representative of the checked organisation or person, financed by funds under international treaties or programmes of the European Union;
- OLAF's investigator/s;
- two witnesses.

10. The financial inspector shall provide copies of the computer data seized to OLAF's investigator by compiling a protocol of delivery and acceptance. The originals and the seized records of computer information data shall be kept in the PFIA until conclusion of the OTSC.

Unique features

Many EU Member States have highlighted the **lack of procedures to safeguard and collect digital evidence** when it is needed for the purposes of an investigation of OLAF, as opposed to the purposes of a national investigation. This practice shows a good approach where OLAF, the national contact point AFCOS, the police and the PFIA work together to resolve issues regarding non-cooperation by the economic operator, namely access to premises or collection of digital data as evidence.

Outcomes and results

The results are very positive, especially in the preventative function of such a practice. The reason to introduce this practice was a case in 2008 where an economic operator in the centre of Sofia did not cooperate with an OLAF investigation. At the time, there was no existing legal capacity to grant OLAF's team access to the premises, which was the motivation to amend the law. Having a coercive way to collect evidence, regardless of the resistance of the economic operator, has prevented almost all instances where the economic operator could have obstructed an investigation in the period between 2008 and 2020 in Bulgaria.

Key success factors

The key success factors are as follows:

- Necessity to amend the national law in order to implement the practice.
- Necessity to identify the best-suited competent institutions in rendering assistance to OLAF. In the case of **Bulgaria,** these are AFCOS (contact point and operational cooperation); PFIA, Police and District court – access to premises and collection of evidence.
- Sufficient awareness of this practice so that economic operators do not attempt to obstruct OLAF's investigations.

Challenges encountered & lessons learned

The challenge to adopt such a legal practice is hidden within the requisite to have institutional and political support to amend an existing law or adopt a new law concerning rendering assistance to OLAF in obtaining computer data in the territory of the Member State. This procedure is needed as stated in Regulation 2185/96 that OLAF's investigators (named in the regulation Commission's inspectors) shall have access, under the same conditions as national administrative inspectors and in compliance with national legislation, to all the information and documentation on the operations concerned which are required for the proper conduct of OTSC and inspections. According to research executed by OLAF with AFCOS, the majority of EU Member States do not have specific Digital Forensic Operations legislation in place.

Potential for the transferability

This good practice was implemented in Bulgaria through the Law on the Public Financial Agency and the Rules of implementation of the Law.

It is perfectly transferable into any continental-law-based EU Member State. Notably, amendment of the law is key to successfully implementing the practice in view of the described steps above.