OLAF Digital Forensic Operations Information Leaflet

http://ec.europa.eu/anti-fraud/

What is a digital forensic operation?

A digital forensic operation is a technological inspection, acquisition, and examination of digital media and/or their contents, carried out by OLAF Digital Evidence Specialists (DES) using forensic equipment and software tools. The objective is to locate, identify, collect and/or acquire data which may be relevant to an investigation, and may be used as evidence in administrative, disciplinary and judicial procedures. Data which have not been forensically copied by OLAF may also be collected during such an operation.

What is OLAF's legal basis for conducting a digital forensic operation in internal investigations?

Article 4 of Regulation (EU, Euratom) 883/2013 empowers OLAF to take a copy of, and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies, and if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearance. All officials, other servants, members of institutions or bodies, heads of offices or agencies, or staff members have a duty to cooperate fully with OLAF. It also empowers OLAF to obtain access to information relevant to the matter under internal investigation at the premises of economic operators under the same rules and conditions as provided for in its Article 3.

What is OLAF's legal basis for conducting a digital forensic operation in external investigations?

Articles 3 of Regulation (EU, Euratom) 883/2013, empowers OLAF to have access, to all information and documentation held by economic operators, including computer data, necessary for the proper conduct of the inspection. It also empowers OLAF to access any relevant information and data, irrespective of the medium on which it is stored, held by the

institutions, bodies, offices and agencies, connected with the matter under investigation. Other sector specific provisions may also apply.

What if my digital device contains personal data not relevant to the investigation?

Digital forensic operations will respect the principles of legitimacy, necessity, and proportionality in the context of the investigation. OLAF investigators are empowered to assume custody of /forensically acquire data from the electronic devices or media which they have identified as potentially relevant to the investigation, even if they contain personal data which are not relevant. However, as explained below, OLAF will access and only further process the data which are relevant to the investigation.

What procedures will be followed during the digital forensic operation?

OLAF's procedures are specified in the Guidelines on Digital Forensic Procedures, which are available on the OLAF Europa site (http://ec.europa.eu/anti_fraud). In brief, they are the following:

- The OLAF investigator will provide you with a copy of the Investigation Authority, which has been signed by OLAF's Director General or a Director by delegation, and with a copy of this leaflet.
- The OLAF DES will take photographs and make an inventory of the devices/media that will be subject to the digital forensic operation.
- The OLAF DES will create a digital forensic copy (a "forensic image") of the data, which is stored in binary format with a unique hash value, which guarantees the integrity of the copy while respecting the integrity of the digital medium and the data thereon.

- If, for technical reasons, it is not possible to make a digital forensic copy, the DES may instead assume custody of the electronic device/medium or make a partial copy of the data.
- The DES will draw up a Digital Forensic Operation Report documenting all activities relating to the access, acquisition, collection and storage of the data. All persons actively involved in the Digital Forensic Operation, including officials of national authorities, will be listed. The report shall be signed by the DES who carried out the Digital Forensic Operation and if applicable by the on-site technical staff that assisted OLAF staff in the execution of their duties. The report will be placed in the OLAF case file, and you will receive a copy of the report.

What will OLAF do with the data which have been acquired / collected?

- OLAF will securely store the data.
- Any data relevant to the investigation will be identified by keyword searches and other search methods. Only these data will be placed in the case file.
- Upon completion of the examination, the DES will prepare a report and place it in the case file.
- OLAF will retain the data for a maximum of 15 years after the closure of the investigation.
- Where potentially relevant in a subsequent investigation, the data may be re-acquired for that investigation. Should that occur, you will be informed of the date and place of the re-acquisition.

Privacy Notice

Pursuant to Articles 15 and 16 of Regulation No 2018/1725 on the protection of natural persons with regard to the processing of personal data by Union Institutions, bodies, offices and agencies and of the free movement of such data, please be informed that your personal data are stored in OLAF's electronic and paper files concerning this matter for the purposes of or in relation to the activities carried out in order to fulfil OLAF's tasks referred to in Article 2 of Decision 1999/352/EC, ECSC, Euratom and Regulation (EU, Euratom) 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF). The categories of your personal data being processed are contact data, identification data, professional data, and case involvement data. Your data may originate from various sources, including publicly accessible information. Your data may be transferred to other EU institutions, bodies, offices and agencies, competent Member State and third country authorities and international organisations. There is no automated decision process by OLAF concerning any data subject. Your data will be stored for a maximum of 15 years.

You have the right to request access to, rectification or erasure, or restriction of processing of your personal data and to object to their processing on grounds relating to your particular situation. If you wish to request access to your personal data processed in a specific file, please provide the relevant reference or description in your request. Any such request should be addressed to the Controller (OLAF-FMB-Data-Protection@ec.europa.eu).

The complete privacy statement for this and all other OLAF personal data processing operations are available at http://ec.europa.eu/anti_fraud. If you have questions as regards the processing of your personal data or your rights you may contact the OLAF Data Protection Officer (OLAF-FMB-DPO@ec.europa.eu)

You may lodge a complaint concerning the processing of your personal data with the European Data Protection Supervisor (edps@edps.europa.eu) at any time.