Guidelines on the Examination of Digital Data during On-Site Inspections

Adoption Date: 08.10.2020 Decision No:20-45/617

Guidelines on the Examination of Digital Data during On-Site Inspections

(1) With the Law No. 7246 dated 16.06.2020 has made significant amendments to Article 15.1(a) of the Act no. 4054 on the Protection of Competition, titled "On-Site Inspection". Within the scope of these amendments, general principles were established related to the examination of all data and documents of undertakings kept on electronic media and in information systems at the location of the on-site inspection, and/or the copying of these documents and data in order to take them to the Competition Authority headquarters for storage.

(2) In the light of the explanations above, the purpose of these Guidelines is to explain the procedure to be applied during the examination process for digital data pursuant to Article 15 of the Act.

(3) Duly charged Professional Staff[1] are authorized to inspect information systems such as servers, desktops/laptops and portable devices as well as storage devices such as CDs, DVDs, USBs, external hard disks, backup records and cloud services owned by the undertaking[2]. Professional Staff may make use of the keyword search tools installed on the systems owned by the undertaking or of forensic IT software and hardware that allow qualified searches in digital data. These forensic IT tools allow the Professional Staff to make searches in the digital data, copy them or retrieve previously deleted digital data during the inspection, while maintaining the originality and integrity of the data and systems owned by the undertaking.

(4) As a result of a quick review to determine whether portable communication devices (mobile phones, tablets, etc.) contain digital data belonging to the undertaking, it is decided whether these devices will be inspected or not. Portable communication devices that are determined to be completely specific to personal use are not subject to inspection. Portable communication devices that are found to contain data belonging to the undertaking are analyzed through forensic IT tools. Data that is considered to have an evidential value within the framework of the file is extracted and all other data that are not seen as evidence are permanently deleted in a way that cannot be recovered.

(5) Duly charged Professional Staff is authorized to inspect digital environments containing all kinds of data belonging to the undertaking. The digital environment containing the data to be inspected will be under the control of the Professional Staff throughout the

---

[1] "Professional Staff" include Chief Competition Experts, Competition Experts and Assistant Competition Experts.

[2] "Undertaking" includes associations of undertakings in addition to the undertakings.

course of the inspection. During the inspection, the undertaking is responsible for preventing interference with the data being inspected as well as with the environment where the data is stored. The officials of the undertaking are must provide full and active support in matters requested by the Professional Staff regarding IT systems. For example, the undertaking will be under certain obligations, such as providing information about the software and hardware related to the information technologies used, providing system administrator privileges, enabling remote access to the e-mail accounts of the undertaking personnel, isolating computers and servers from the network environment, limiting the access of users to their corporate accounts, and restoring backed-up corporate data.

(6) If deemed necessary by the Professional Staff during the inspection, the digital data to be inspected are partially or completely copied to separate data stores via forensic IT methods. The copy taken via forensic IT methods is a cloned copy obtained in a logical and physical way that ensures the authenticity of the data. The hash[3] values of the data are calculated to confirm that the data copied via forensic IT methods are calculating the hash values that the data copied by forensic methods are exactly the same as the originals.

(7) The forensic copy of the data is transferred to the computer allocated by the Authority to the duly charged Professional Staff, which has forensic IT software installed. The data copied is indexed[4] and inspected by the Professional Staff.

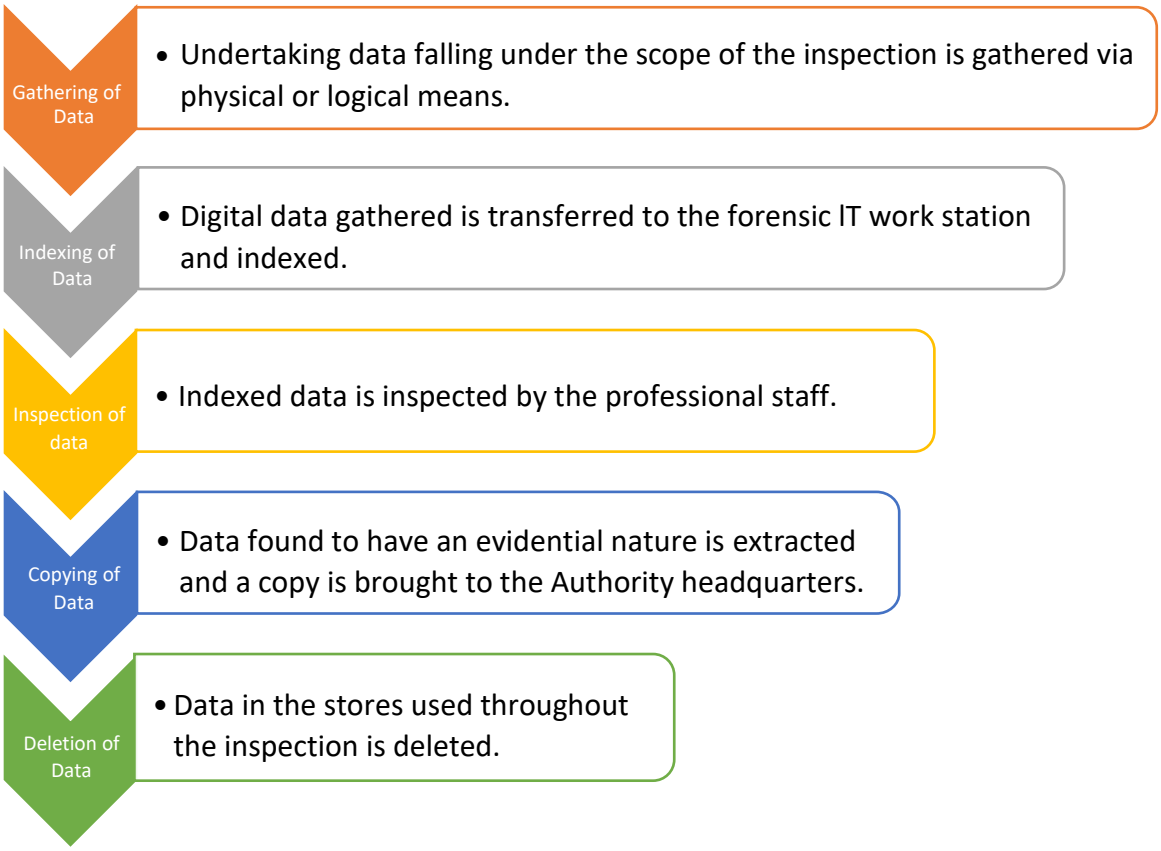
(8) When the inspection is complete, the digital data deemed to be necessary are copied to two separate data stores. One of the copies obtained is delivered to the undertaking. The hash values of the digital data in question are included in the attachment of the report to be prepared at the end of the inspection. The report is signed by the duly charged Professional Staff and the official of the undertaking. In the event that the undertaking official refuses to sign the report, this situation is indicated in the report and the report is signed by at least two Professional Staff. The report is drawn up in two copies, one of which is given to the official of the undertaking.

(9) At the conclusion of the inspection, all data stores used during the analysis are deleted in such a way as to ensure that their data cannot be restored, with the exception of the data stores which were submitted to the undertaking in the attachment to the report, a copy of which were taken by the Professional Staff.

---

[3] Hash is a mathematical computation method used to verify the integrity of digital files.

[4] The indexing operation makes the digital data obtained from the undertaking searchable by keywords through the use of forensic IT software.



(10) The inspection should be completed at the premises of the undertaking. However, if deemed necessary, the inspection may be continued in the forensic IT laboratory of the Authority. The inspection of the digital data obtained from mobile phones is always completed at the premises of the undertaking. The digital data to be inspected at the Authority headquarters are transferred to three separate data stores after their hash values are calculated and compared as cloned copies. One of the copies is left at the undertaking and the other two copies are put in an envelope and sealed by the Professional Staff in order to ensure their physical security. The undertaking concerned is invited in writing by the Authority to have a representative available at the time of opening of the sealed envelope and during the inspection that will continue at the Authority's forensic IT laboratory. If deemed necessary by the Board, a decision may be taken to return the sealed envelope to the undertaking concerned without being opened.

(11) If the undertaking concerned claims that trade secrets are contained among the digital data found to have an evidential nature and included in the file during the inspection conducted at the premises of the undertaking or at the headquarters of the Authority, action will be taken under the "Communiqué no 2010/3 on the Regulation of the Right of Access to the File and Protection of Trade Secrets".

(12) Data copied during on-site inspections are protected under the principle of professional privilege. Accordingly, any correspondence between a client and an independent lawyer with no employee-employer relationship with the client aimed at the exercise of the client's right to defense is accepted to belong to the professional relationship and are covered by the attorney/client privilege. However, correspondence that is not directly related to the exercise of the right to defense do not benefit from the privilege, especially if they involve giving assistance to an infringement of competition, or concealing an ongoing or future violation.