Organisation for Economic Co-operation and Development

DAF/COMP/GF/WD(2018)65

Unclassified

English - Or. English

20 November 2018

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Global Forum on Competition

INVESTIGATIVE POWER IN PRACTICE - Breakout session 1 - Unannounced Inspections in the Digital Age - Contribution from Hungary

- Session IV -

30 November 2018

This contribution is submitted by Hungary under Session IV of the Global Forum on Competition to be held on 29-30 November 2018.

More documentation related to this discussion can be found at: oe.cd/invpw.

Please contact Ms. Lynn Robertson [E-mail: Lynn.Robertson@oecd.org], if you have any questions regarding this document.

JT03439938

Investigative Powers in Practice

Breakout session 1 - Unannounced Inspections in the Digital Age

- Contribution from Hungary –

1. The contribution provides a general overview on digital evidence gathering practice of the Hungarian Competition Authority ('GVH') in the course of unannounced inspections with particular emphasis on the related practical and procedural issues.

1. Digital evidence gathering – relevance and general framework

2. In the cartel detection and investigative work of the GVH, information and evidence gathering – considering the hidden and secret nature of cartels – is of utmost importance. Therefore, the GVH decided to set up – beyond the Cartel Unit – a separate unit, the Cartel Detection Unit, in order – inter alia – to perform these tasks more efficiently. The Cartel Detection Unit is responsible for the detection of cartels and also gathers, analyses, and processes all the information that is necessary for the initiation of competition supervision procedures; furthermore, it carries out unannounced inspections ('dawn raids').

3. Over the last few decades, due to the sudden evolution of information technology (IT) and digitisation, paper-based data storage is increasingly being replaced by data storage on a variety of electronic devices, such as computers, tablets, mobile phones and servers accessed from the internet (so-called 'clouds'). In response to these tendencies, an amendment to Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices' (hereinafter referred to as Hungarian Competition Act, 'HCA') came into effect on 1 November 2005. This amendment enabled the case handlers to make copies of not only paper-based documents, but also data stored on electronic devices. Pursuant to the respective provisions of the HCA currently in force, the case handler is entitled to make a forensic copy (also known as a 'mirror copy' or a 'bit-by-bit copy') of the data storage device and to inspect its contents using that forensic copy if it is likely to contain data in connection with the conduct under investigation that cannot be retrieved in course of the proper use of the computer. Additionally, the respective provisions of the HCA state that in the process of making an electronic copy of the data stored on the data storage device, the data shall be recorded in a way that prevents the subsequent manipulation of the data or – if this is not possible due to the type of the data storage device – the data shall be recorded using a technology that ensures that it is possible to control the unchanged nature of the data at a later stage.

4. Procedures that allow the creation of a 'mirror copy' / 'bit-by-bit copy' of specific digital data, identical to the original, which also ensure the authenticity and integrity of the copy are together referred to as forensic-IT procedures. Forensic-IT procedures enable, for example, the current status of a computer's hard drive to be recorded and a certified copy to be made, while the original hardware remains in the owner's possession with its proper use unhindered. Moreover, these procedures enable the retrieval of deleted data. The software that makes a copy generates a certificate and a code (so-called 'HASH code') that unambiguously certifies that the 'mirror copy' is identical to the original. In case of

manipulation of the copy (i.e. minor changes to any of the files) the HASH code will consequently change. At the end of a competition supervision procedure, the code of the copy generated with the use of forensic-IT procedures is exactly the same as the certificate issued at the beginning of the procedure on the spot, thus the copy verifies that the evidence contained therein was derived from the original computer. The forensic copy or parts thereof can neither be deleted nor modified, therefore it is a much more reliable means of proof, than the seizure and removal of a computer, since if the status of the computer has not been recorded at the time of the seizure, the authority cannot prove that the data stored on the computer has not been modified.

2. Forensic-IT procedures in the practice of the GVH

5. The use of forensic-IT procedures is a special area of expertise of the Cartel Detection Unit, the development of which is strongly promoted by the GVH, including the development of tools, software and the training of the staff. An employee of the GVH is a member of the Forensic IT working group set up by the European Competition Network (hereinafter referred to as 'ECN').

6. By using forensic-IT procedures, the case handlers of the GVH are able to make forensic copies of the servers, computers, data storage devices, mobile devices and data stored in clouds, and are also able to search for evidence in these copies by using special analytical software. It is important that the tools used ensure that the copies made with them and the evidence obtained therefrom are suitable for judicial use, and that the authenticity thereof can be proven. This is ensured by the closed chain of proofs, the nature of the hardware and software tools used and the certification provided by the HASH code.

7. During unannounced inspections the case handlers are required to make copies of varying amounts of electronic data, ranging from mailboxes containing a few hundred emails to hundreds of gigabytes (GB) of data, including data stored on mobile devices, the significance of which is continuously growing. Consequently, the types software used must allow the case handlers to carry out searches easily and systematically. A number of common features of the software programmes used by the GVH are that they enable comprehensive and in-depth analyses, are able to process the mirror / bit-by-bit copies made in the course of unannounced inspections, as well as provide various export options. The entire process is of course conducted on a forensic basis, according to which the data source may only be read and not modified.

8. In the course of unannounced inspections it may occur that the data is not stored on the servers of the undertaking subject to the proceeding but on remote servers or in clouds. In such a case, pursuant to Article 18 (1) of the *Convention on Cybercrime, Budapest, 23.XI.2001*[1] as well as to the *ECN Recommendation on the power to collect digital evidence*

[1] ***Convention on Cybercrime**, Budapest, 23.XI.2001. Article 18 - Production order*

"1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control."

including by forensic means[2], the physical or geographic location of the data is irrelevant. If the data is accessible from the headquarters or the premises of the undertaking subject to the unannounced inspection, the authority can make copies of such data. According to GVH's experience, sending requests for information to host providers is slow and usually unsuccessful.

9. Access to data stored on the servers of the parent companies of the parties subject to the proceeding varies on a case-by-case basis. Corporate policies and procedures usually determine whether a company has direct access to the data stored on the servers of the parent company or not. If the GVH cannot have direct access to the data during the unannounced inspection, a request for information will be sent to the party concerned to provide the data in question.

10. In case of mobile devices, such as smartphones, it often unclear in which cases the device is considered as a private/personal device and how private vs corporate use can be delimited. In principle, the GVH examines the data content of the phone, the call list, and if work-related information, such as SMS, e-mails, chat messages, is found on the phone, the GVH will certainly make a copy.

11. If due to the amount of data it is not feasible to inspect and select the relevant data during the unannounced inspection, the GVH only examines on the spot whether the data is relevant to the conduct investigated and decides whether or not to make a copy. The data will be selected and processed at the premises of the GVH at a later date.

12. If there is a possibility that the copy may contain any document prepared for the purpose of defence – communications between client and attorney (*legal professional privilege, 'LPP'*)[3] – the GVH deposits the data, including data stored on data storage device, in a container in order to prevent access to the data and their subsequent

https://rm.coe.int/1680081561

[2] *ECN RECOMMENDATION on the power to collect digital evidence including by forensic means: "It is recommended that:*
1) All Authorities should have effective and efficient powers to gather digital evidence, including evidence obtained forensically, through inspections of business and/or non-business premises, requests for information and other investigative tools. To that end, the Authorities should have the power to gather all information in digital form related to the business(es) under investigation, ***irrespective of the medium on which it is stored and the technological evolution of the storage media.*** *The Authorities should also have powers to gather digital information by taking digital copies, including forensic images, of the data held and/or through the seizure of storage media.*
2) The power to gather digital evidence, including evidence obtained forensically, as set out in Recommendation 1, ***should include the right to access information which is accessible to the undertaking or person whose premises are being inspected and which is related to the business(es) under investigation."***
http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

[3] Pursuant to Article 65/C (2) of the HCA *a document prepared for the purpose of defence shall mean a document or a part thereof that was created in the course of communications between the person acting as a lawyer and the party as the client of the former, for the purposes or in the framework of the exercise of the rights of defence in the proceeding of any public authority, or that is a record of the contents of such communications, provided that such character of the document is apparent from the document itself. A document not in the possession of the party or the person acting as a lawyer concerned shall not qualify as a document prepared for the purpose of defence unless such party or lawyer is able to prove that the document was removed from their possession illegally or in the course of criminal proceedings.*

manipulation, which is then sealed and signed by the party concerned and the case handler in a manner that prevents it from being opened without the seal being damaged (hereinafter referred to as 'sealed container'). The sealed container will be opened in the presence of the party concerned. If according to the statement of the party the data contains documents prepared for the purpose of defence, a working copy that does not contain the documents prepared for the purpose of defence shall be made.

3. Procedural safeguards in the course of unannounced inspections and electronic evidence gathering

13. In case of digital evidence gathering carried out during unannounced inspections, a number of procedural safeguards ensure the rights of the client, including in particular the right to due process. The related procedural rules are closely linked to the rules on unannounced inspections, thus for a better understanding of the topic – to the extent necessary – these rules will be presented together below.

14. ***Judicial warrant is required for unannounced inspections.*** Pursuant to Article 65/A (3) of the HCA, an unannounced inspection shall only be carried out if a judicial warrant has previously been obtained. The application of the GVH for such a warrant shall be authorised in a non-litigious procedure by the Budapest-Capital Regional Court within seventy-two hours of receipt of the application. Pursuant to Article 65/A (4) *"the court shall authorise the unannounced inspection requested if in its application the Hungarian Competition Authority proves presumptively that other investigative measures would be unlikely to produce results, and there are reasonable grounds to presume that a means of proof relating to the infringement under investigation is in the location indicated in the application and that it would not be surrendered voluntarily, or it would be made unusable. The court may authorise an unannounced inspection to be taken partially, specifying the target persons and the type of investigative measures allowed."*

15. **Competition supervision proceeding shall be started no later than the beginning of the unannounced inspection.** Pursuant to Article 65/A (6) "the competition supervision proceeding shall be started simultaneously with the commencement of the unannounced inspection at the latest. The injunction ordering the investigation shall be serviced at the scene to the party present, including the party's employee present, and shall be serviced to other parties also by telephone or fax, in addition to the start of the service pursuant to the general rules governing the mode of the service of decisions". Pursuant to Article 65/A (7) the party concerned, including the party's employee present shall be informed about the unannounced inspection at the time of the beginning of the search, and about the court order authorising the unannounced inspection as well as the purpose of the investigative measure before the investigative measure is started.

16. **Unannounced inspection should take place in the presence of the party concerned.** Pursuant to Article 65/A (7a) "whenever possible, the unannounced inspection shall be carried out in the presence of the party affected. If the presence of the party affected cannot be ensured, the participation of an official witness in the unannounced inspection shall be requested". The unannounced inspection – pursuant to Article 65/A (8) – shall be carried out on working days between 8:00 am and 8:00 pm, unless another time is necessary to assure the success thereof.

17. **Unannounced inspection of real estate, vehicles, or data storage device used for private purposes.** Pursuant to Article 65/A (2) "an unannounced inspection of the real estate, vehicles or data storage serving or used for private purposes which are not registered at the registered office or establishment of the party and are not used for economic activity by the party in any manner, is only possible if they are used by a person who is, or was in the period investigated, the party's executive officer, employee or agent or a person exercising actual control over such party". In this case the unannounced inspection shall be carried out in such a manner that it does not cause a disproportionate disturbance to the privacy of the person concerned and causes the least possible disruption to the work and regular activity of the person concerned.

18. **The making of electronic copies.** Pursuant to Article 65 (1) "on the request of the case handler or the competition council, data recorded in a computing system or on an electronic data storage device shall be made available by the possessor of such data storage device in a format enabling reading and copying". Point (2) of this article states that "the case handler and the competition council shall be entitled to make copies of documents and data stored on a data storage device. The case handler shall be entitled to make a forensic copy of the data storage device and to inspect its contents using that forensic copy if it is likely to contain data in connection with the conduct under investigation that cannot be retrieved in the course of the proper use of the computer". Point (3) of this article states that "in the process of making an electronic copy of the data stored on the data storage device the data shall be recorded in a way that prevents the subsequent manipulation of the data or — if this is not possible due to the type of the data storage device — the data shall be recorded using a technology that ensures that it is possible to control the unchanged nature of the data at a later stage". Pursuant to Article 65/B (1) "if during the unannounced inspection it is impossible to inspect the data storage device on-site without interfering with the normal course of activities of the person affected for a disproportionate length of time, or otherwise if the person affected agrees, the case handler shall make a copy of the data and documents found on the data storage device (hereinafter: search copy)".

19. **Process of taking minutes**. The case handler shall prepare minutes of the unannounced inspection. Additionally, Article 65/B (2) states that "the minutes of the unannounced inspection shall contain the type of data storage used to record the copy with the data necessary for its individual identification, the nature of the data and of the documents copied as well as other necessary data which enable both the individual identification of the copy and the subsequent control of the unchanged nature of the data". Point (3) of this Article states that the case handler shall conduct the search of the means of proof using a working copy made of the data and documents on the search copy (hereinafter referred to as 'investigation working copy'). The case handler shall prepare a separate electronic or paper copy of the evidence intended to be used (hereinafter: 'evidence brief') and send the description enabling the individual identification of the data and documents therein to the party who previously had possession of the data storage or who is connected to the site where the search copy was made or to the data owner, ordering them to make a statement within a time limit of eight days as to whether the evidence in the evidence brief contains any business secret or private secret.

20. **Legal Professional Privilege (LPP).** In principle, any document prepared for the purpose of defence shall not be used as evidence in competition supervision proceedings. If, in the context of a search copy, there is a possibility that the copy may contain any document prepared for the purpose of defence, pursuant to Article 65/C (5), the search copy containing the document shall be deposited in a sealed container which prevents access to the data and their subsequent manipulation and which is signed by the person concerned

and the case handler in a manner which prevents the container from being opened without the seal being damaged. Point (6) of this Article states that the party affected shall be invited to make a statement about whether any of the documents taken into physical possession should be qualified as a document prepared for the purpose of defence, and to clearly indicate the document or part of document affected. Point (9) of this Article states that if according to the statement of the party the documents include documents prepared for the purpose of defence, such documents shall be separated in the presence of the party affected. In the case of search copies this shall be carried out by using a copy enabling the separation of data (hereinafter referred to as 'interim working copy'), and an investigation working copy not containing the document prepared for the purpose of defence shall be made of the interim working copy and subsequently the interim working copy shall be destroyed without delay by the physical destruction of the data storage containing the copy or by the erasure of the data using a procedure rendering the data irrecoverable.[4]

21. **Disputes on the qualification of a document as LPP.** If, contrary to the statement of the party, the case handler considers the document not to have been prepared for the purpose of defence, the disputed document as well as the interim working copy containing the document in question shall be deposited in a sealed container. Pursuant to Article 65/C (10) the dispute shall be decided, upon the request of the GVH and having heard the party affected, by the Budapest-Capital Regional Court in a non-litigious procedure within fifteen days. The GVH shall attach to its request the sealed container containing the document and the interim working copy made thereof. Point (11) of this Article states that if the court establishes that the document or the part thereof does not qualify as a document prepared for the purpose of defence, it shall release it to the GVH. If the court decides to the contrary, it shall release the document or the part thereof to the party affected.

22. **Servers of the Cartel Detection Section, internal procedures.** Internal procedures related to the storing, processing and archiving of copies of electronic data storage carried out by the Cartel Detection Unit during unannounced inspections, having regard to *Act L of 2013 on* the *Electronic Security of State and Municipal Bodies*, is regulated by Notice No. 11/2015. (V.12.) of the GVH on the IT system security and safety rules of the Hungarian Competition Authority (hereinafter referred to as 'Notice No. 11/2015'). According to Notice No. 11/2015, the Cartel Detection Unit operates a separate electronic information system for storing, processing and archiving the copies of electronic data, which consists of a separate network, a dedicated server storing the data and dedicated workstations assigned to that purpose. Furthermore, data stored at the servers of the Cartel Detection Unit can only be accessed by the case handlers from the dedicated workstations, on which the data processing is carried out using forensic software. The workstations are not connected to the local network of the GVH and can be connected to the servers of the Cartel Detection Unit only from the offices of the Cartel Detection Unit. Access to the workstations is restricted for those who have been registered and granted access.

[4] The rules are different for paper-based copies. If the party concerned states that there is a document prepared for the purpose of defence, such document shall be separated in the presence of the party concerned and the document prepared for the purpose of defence must be handed back to the party concerned.