ECN RECOMMENDATION ON THE POWER TO COLLECT DIGITAL EVIDENCE, INCLUDING BY FORENSIC MEANS

By the present Recommendation the ECN Competition Authorities (the Authorities) express their common views on the power to collect digital evidence, including evidence obtained forensically and forensic copies of evidence. It contains the general principles which the Authorities consider relevant to ensure the effective enforcement of the EU competition rules within the ECN.

This Recommendation may serve as guidance to all those involved in shaping the legal framework for enforcement of Articles 101 and 102 TFEU. It is without prejudice to the legal frameworks of those ECN jurisdictions which already provide for these general principles or which go beyond the scope of the present Recommendation.

I. INTRODUCTION

1. Inspections and requests for information are key tools for Authorities to gather documentary and other evidence about alleged anticompetitive practices and thus detect infringements of competition law (see further the ECN Recommendation on investigative powers, enforcement measures and sanctions in the context of inspections and requests for information). It is a prerequisite for effective inspections that Authorities are able to gather all relevant evidence at business and non-business

premises. Similarly, Authorities must be able to gather all relevant evidence through requests for information or other investigative tools. Given the important role information technology ("IT") plays as both a means of storage and a communication tool, it is essential that the Authorities have effective powers to gather digital evidence.

2. Digital evidence includes all information gathered in digital form, and encompasses the content itself (e.g. text documents, correspondence, drawings, photos, databases, etc.) including deleted content, and information about this content, which is the so-called metadata (information regarding file names, pathnames, the date and time that a document has been created or edited or a message has been sent, received or opened, the creator/ sender of a document or a message, etc.). The notion of digital evidence also covers evidence obtained forensically and forensic copies of the original evidence, that is, digital evidence gathered during an inspection in the form of unaltered duplicates of the digital data, e.g. a desk-top computer's hard-disk (desktops or laptops) or other types of storage media. Storage media are any devices that may contain or transport digital information and include physical hard drives, floppy disks, Personal Digital Assistants (PDAs), tablets, Universal Serial Bus devices (USBs), SIM cards of mobile phones, mobile devices, flash memory sticks or cards, CD-ROMs, DVDs, Blu-Ray Discs (BD), networks and servers etc.

3. The gathering of the digital evidence may be carried out either by the seizure of the storage media or the making of digital copies including forensic images (for example, a bit-for-bit copy of all data in a piece of media which includes all allocated files, as well as file slack, unallocated space, deleted files and non-partitioned space), file copies etc.

4. Currently all Authorities are able to gather digital evidence. Experience shows that digital evidence is gathered in virtually all inspections conducted by the Authorities in the ECN. However, the powers to gather digital evidence vary, for example, some Authorities cannot gather digital data stored on mobile phones or cannot take forensic images. It is desirable that all Authorities have effective powers to gather digital evidence, in particular, to ensure the effectiveness of inspections, as well as to enhance convergence

within the ECN which would facilitate co-operation. The Authorities have to be able to search effectively the IT environment and storage media. Accordingly, the power to gather digital evidence must apply irrespective of the medium on which it is stored and the technological evolution of the storage media. Effective powers to gather digital evidence necessarily also comprise the power to collect digital information during inspections, either by taking digital copies of the data held (e.g. file copies or forensic images) and/or through the seizure of storage media.

5. Practice shows that undertakings may store, access or otherwise use business related information on external servers or other storage media such as so-called cloud services (networked online storage where data is stored on multiple virtual servers) which are located outside the territory of the competent national competition authority or outside the European Union. To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union.

6. The exercise of the powers outlined in this Recommendation should be in accordance with the general principles of EU law (such as the principle of proportionality, respect for the rights of defence and legal certainty), the rules and principles of international law, as well as the observance of fundamental rights, including those enshrined in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights where applicable. Such safeguards should also include the respect of the relevant legislation and case law on Legal Professional Privilege and the processing of personal data, as interpreted under the law of the respective ECN jurisdiction.

7. The majority of the Authorities have the power to gather digital information at the premises being inspected and to continue making searches of this information which is typically done at the premises of the Authority, or at the premises of the police or an

equivalent enforcement authority, to the extent that the latter are assisting the Authority (the so-called continued inspection procedure). In some jurisdictions, the selection of the digital evidence may be conducted on a prima facie basis at the premises being inspected (for example, by performing searches using key words) with further review and selection taking place at the premises of the Authority. Some Authorities routinely take a forensic image of storage media at the premises being inspected and carry out the review of the data at their premises, whereas others do so on a case by case basis.

8. Experience has shown that given the increasing amount of digital information to be searched, the continued inspection procedure is an effective means of gathering digital evidence. In practice, this is used in the majority of inspections carried out by the Authorities. It is therefore desirable that all Authorities have effective powers to carry out a continued inspection procedure. Convergence in the ECN in this respect would facilitate cooperation pursuant to Articles 12 and 22 of Regulation 1/2003.

9. It is important that the effectiveness and efficiency of the procedures for gathering digital evidence is ensured. In particular, it is desirable that the Authorities have sufficient time to gather and to continue making searches of digital evidence, notably within the framework of a continued inspection procedure, and in light of the technical difficulties that may arise. It is also essential that the Authorities are adequately equipped to gather digital evidence and have at their disposal appropriate technical means and expert resources, as well as access to regular training.

10. In order to ensure the effectiveness and efficiency of inspections, it is desirable that undertakings are obliged to ensure that digital evidence can be gathered effectively, for example, by providing appropriate representatives or members of staff to assist during the course of an inspection, not only to give explanations about the organisation of the undertaking and its IT environment and storage media, but also by carrying out specific tasks as requested, such as the temporary blocking of individual e-mail accounts, temporarily disconnecting running computers from the network, removing and re-

installing hard drives from computers and by making data effectively accessible, such as by providing the Authority 'administrator access rights'-support to the IT environment and storage media (including passwords for decryption). Where such actions are taken, undertakings should be obliged not to interfere in any way with such measures. Non-compliance with this obligation should be subject to effective sanctions (see further the ECN Recommendation on investigative powers, enforcement measures and sanctions in the context of inspections and requests for information).

11. Currently, some Authorities make available their procedures for gathering digital evidence, e.g. through the publication of guidelines, best practices etc. and/or through the provision of information at the beginning of an inspection. This can contribute to ensuring that the gathering of digital evidence functions smoothly and effectively.

II. ECN RECOMMENDATION

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.

3. The power to gather digital evidence, including evidence obtained forensically, should include the right to continue making searches of the information gathered at the premises being inspected by means of a continued inspection procedure.

4. The procedures for gathering digital evidence, including evidence obtained forensically, should be effective and efficient, in particular, the Authorities should have sufficient time to gather digital evidence, notably within the framework of a continued inspection procedure. The Authorities should also be adequately equipped to gather digital evidence and have at their disposal appropriate technical means and expert resources, as well as access to regular training.

5. Undertakings should be obliged to ensure that digital evidence, including evidence obtained forensically, can be gathered effectively, inter alia, by providing appropriate assistance, for example, by giving explanations about the organisation of the undertaking and its IT environment and storage media and by carrying out specific tasks upon request such as providing 'administrator access rights'-support.