



A Framework for Examination of Personal Devices under the Turkish Competition Authority's New Guidelines – How it Converges with and Differs from the EU Practice

Authors: Gönenç Gürkaynak, Esq., O. Onur Özgümüş and Fırat Eğrilmez, ELIG Gürkaynak Attorneys-at-Law

(1) Introduction

The Guidelines on Examination of Digital Data during On-site Inspections (“*Guidelines*”),¹ which was recently published by the Turkish Competition Authority (“*Authority*”), specifically refer to the procedure to be followed when the case handlers encounter situations calling for the examination of the personal devices during on-site inspections. The procedure referred in the Guidelines is an outline of general principles; there are no exhaustive explanations, various potential scenarios, nor an indication when such review (or the possibility of review) may come into play. To that end, this article aims to cover the decisional practice of the Authority prior to the Guidelines, as well as the approach in the EU, with regard to their investigative powers pertaining to the portable devices and devices allocated for personal use.

(2) The Authority's Approach Regarding the Examination of Personal Data/Devices

As per the recent amendment made to Law No. 4054 on Protection of Competition (“*Law No. 4054*”) by way of Law No. 7246 on Amendments to the Law on Protection of Competition, which entered into force on June 24, 2020, during on-site inspections the Authority is entitled to conduct their examinations on “*the books, all types of data and documents of undertakings and associations of undertakings kept on physical or electronic media and in information systems, and take copies and physical samples thereof.*”² Following this amendment to Law No. 4054, the Guidelines were published to set forth the principles governing the examination

¹ The Guidelines were approved by the Turkish Competition Board (“*Board*”) with its decision dated 08.10.2020 and numbered 20-45/617.

² Before the amendment by the Law No. 7246 on Amendments to the Law on Protection of Competition, the former version of the sub-paragraph read as follows: “[To] Examine the books, any paperwork and documents and take their copies if needed.”

of digital data, including references to the handling of portable devices (*e.g.*, mobile phones, tablets etc.).

As per the Guidelines, the case handlers shall first decide whether the relevant portable device should be subjected to review within the scope of the on-site inspection, after a quick browse of the subject portable device to determine whether it contains any data pertaining to the relevant undertaking. The Guidelines expressly provide that, those portable devices allocated entirely for personal use cannot be brought under the scope of an on-site inspection. On the other hand, the personal portable devices that did contain data pertaining to the relevant undertaking would still be subject to the review of the case handlers, through the use of digital forensic tools.

At this point, it should be noted that the examination of personal devices and data have been a practice employed by the Authority, even prior to the Guidelines. In the Koçak Petrol decision,³ the on-site inspection was hindered by an executive of the undertaking under scrutiny, on the grounds that the laptop subject to the examination was allocated for personal use and the warrant issued by the Board did not cover such inspection. The Board decided to impose an administrative fine against the relevant undertaking, since the executive was seen to delete certain documents from the laptop, which he alleged had been personal documents, and the case handlers could not commence the on-site inspection at the time intended.⁴

In a similar fashion, it is understood from the Board's Nuhoğlu İnşaat decision⁵ that the case handlers were prevented from conducting an on-site inspection on the premises of the relevant undertaking, on the ground that the corporate e-mail account also contained the relevant employee's personal e-mail correspondence. Despite the relevant undertakings' efforts to prevent the on-site inspection, the case handlers conducted the on-site inspection with one day delay, with a warrant granted by the criminal justice of peace to the case handlers for

³ *Koçak Petrol Decision* of the Board, dated 05.08.2009 and numbered 09-34/837-M.

⁴ *Koçak Petrol Decision* of the Board was upheld by the Decision of Council of State's Plenary Session of Administrative Law Chambers, dated 18.01.2016 and numbered E. 2013/3389, K. 2016/23.

⁵ *Nuhoğlu İnşaat Decision* of the Board, dated 21.12.2017 and numbered 17-42/669-297.

conducting the on-site inspection, and an administrative monetary fine was imposed on the relevant undertaking for preventing the on-site inspection.

In the Askaynak decision,⁶ wherein the case handlers were prevented from examining the personal e-mail account of an employee of the undertaking under scrutiny, the Board decided that such an action amounted to prevention of the on-site inspection and thus imposed upon the relevant undertaking an administrative monetary fine. In this particular case, the case handlers became aware of the personal e-mail account and suspected that the messages therein may pertain to the merits of the case, since they had already found an e-mail message sent from that account, which seemed relevant to the conduct under scrutiny. In a similar vein, in the Ege Gübre decision,⁷ the case handlers noted that upon the examination of a corporate e-mail account, certain e-mail messages that may pertain to the merits of the case were sent from the personal e-mail account of the relevant undertaking's general manager. Accordingly, the case handlers requested to examine the personal e-mail account of the general manager but were prevented from conducting such an examination by the representatives of the undertaking. A day later, the case handlers continued the on-site inspection and examined the personal e-mail account of the general manager, based on a court judgment granting a warrant to the case handlers. Subsequently, an administrative monetary fine was imposed on the undertaking under scrutiny, for preventing the on-site inspection.

In a similar vein, the Authority also assumes investigative powers on WhatsApp communications on company mobile phones and considers any pertinent finding to have evidential value.⁸ To that end, the *Burdur Akaryakit* decision of the Board includes even explicit references to the Explanatory note on European Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003 ("**Commission's Explanatory Note**"), the Bring Your Own Device ("BYOD") policy⁹ exemplified within the scope of Commission's

⁶ *Askaynak Decision* of the Board, dated 26.12.2019 and numbered 19-46/793-346.

⁷ *Ege Gübre Decision* of the Board, dated 07.02.2019 and numbered 19-06/51-18.

⁸ *Ege Konteyner Decision* of the Board, dated 02.01.2020 and numbered 20-01/3-2 and *Burdur Akaryakit Decision* of the Board dated 09.01.2020 and numbered 20-03/28-12.

⁹ BYOD refers to a policy regulating the use of personal devices for work-related purposes at the workplace. BYOD policy would also often entail principles regarding the employees' access to confidential company information and software via their personal devices.

Explanatory Note, as well as the Almendra y Miel case discussed below, to justify the reasoning for the review of the personal mobile phones.

(3) Assessments of the European Union Authorities Regarding the Inspection of Personal Devices/Data

The guidance for the European Commission’s (“*Commission*”) investigative powers was laid down with the Explanatory Note,¹⁰ which clearly provides that the Commission’s inspectors are empowered to “...*examine any books and records related to the business, irrespective of the medium on which they are stored, and to take or obtain in any form of copies of or extracts from such books or records...*”¹¹ They may search the IT-environment (*e.g.* servers, desktop computers, laptops, tablets and other mobile devices) and all storage media (*e.g.* CD-ROMs, DVDs, USB-keys, external hard disks, backup tapes, cloud services) contained in the private devices and media that are used for professional reasons, when they are found on the premises (BYOD policy).¹² However, the Commission’s Explanatory Note does not set out any specific principles as to how the inspectors of the Commission should determine whether the private devices and media are “used for professional reasons.” To that end, the Commission’s Explanatory Note does not spell out any further details, *e.g.* whether the Commission must have a reasonable suspicion beforehand that professional documents are likely to be found in personal devices.

In this context, the Almendra y Miel case of the Spanish Markets and Competition Commission (“*CNMC*”) (which was subsequently approved by judicial review, as well)¹³ highlights that mobile phones could be subject to examination during on-site inspections. During the appeal of this decision, the relevant employee claimed that the CNMC inspection order did not entitle the inspectors to check his mobile phone. However, the court rejected that

¹⁰ The Commission’s Explanatory Note introduction paragraph emphasizes that: “The note is for information only and is without prejudice to any formal interpretation of the European Commission’s powers of investigation.”

¹¹ Explanatory Note, Paragraphs 4 (b) and 4 (c).

¹² Explanatory Note, Paragraph 10.

¹³ CNMC Council Decision of 7 April 2016, Nougat producers, S/DC/0503/14, Audiencia Nacional, Judgment of 21 July 2016, D. Claudio, Almendra y Miel SA y Confectionary Holding SL v CNMC, No 136/2014, ES:AN:2016:2986

claim on the basis that the order authorized the inspectors to inspect the company's employees' physical and electronic logs, "which included their mobile phones." The court also dismissed the relevant employee's claims regarding privacy, by referring to the inspection report that indicated that the relevant employee had been consulted on which documents were personal, so they could be left out of the review. The court also set forth that in order to decide whether a particular document is confidential or not, the inspection team has the right to take a cursory look at the document in question. This cursory look does not amount to an infringement of the right to privacy, because without such a brief review of the document, an effective inspection would not be possible.

Furthermore, in its Akzo Nobel and Ackros judgment, the Court of First Instance stated that "a mere cursory look by the Commission officials at the general layout, heading, title or other superficial features of the document will enable them to confirm the accuracy of the reasons invoked by the undertaking and to determine whether the document at issue was confidential, when deciding whether to put it aside."¹⁴ Accordingly, taking into account the references to a cursory look by the case handlers within the scope of on-site inspections in the EU (despite the absence of a reference within Commission's Explanatory Note), the reference to a quick browsing might be deemed as relatively justified within the Guidelines.

(4) Conclusion

In both jurisdictions, the secondary legislation (*i.e.*, the Guidelines of the Authority and the Commission's Explanatory Note) specifies that, the relevant rules enabling both competition authorities conducting on-site inspections also allow for the examination of private/personal devices, provided that such devices contain business-related information and are found on the premises during the on-site inspection. That being said, there is an explicit reference to the BYOD policies/practices within the Commission's Explanatory Note, whereas the Guidelines adopt a so-called quick browsing method by the case handlers during on-site inspections. All in all, the question will still boil down to whether, in the absence of a specific BYOD

¹⁴ Joined Cases T-125/03 and T-253/03, Akzo Nobel Chemicals and Akros Chemicals/European Commission, Judgment of 17 September 2007, § 77, confirmed in appeal by Case C-550/07, Akzo Nobel Chemicals and Akros Chemicals/European Commission, Judgment of 14 September 2010.



policy/practice by the relevant undertakings, the personal devices of the employees would still be subject to a quick look/browsing by the case handlers, as a standard practice to ensure that nothing falls through the cracks and no stone is left unturned. In a similar vein, it will also remain to be seen whether a reasonable doubt/suspicion or a prior finding would be deemed as a pre-requisite for the case handlers of the Authority to go through the personal devices/data of the employees with a quick browse or cursory look. Although various antitrust authorities are empowered to review and copy data from a wide range of IT-environment and storage media, including the private mobile phones that are used for professional purposes, they also aim to strike a balance when it comes to the review of personal devices/data during on-site inspections. In that context, the Board`s case-by-case assessments will be invaluable and provide further insight on the actual implementation of the Guidelines on this front.

Article contact: Gönenç Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published by November 13, 2020)