

Recently Published Guidelines of the Turkish Competition Authority on Examination of Digital Data during On-site Inspections

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

(1) Introduction

The Turkish Competition Authority (“**TCA**”) recently published its Guidelines on Examination of Digital Data during On-site Inspections (“**Guidelines**”),¹ which set forth the general principles with respect to the examination, processing and storage of data and documents held in the electronic media and information systems, during the on-site inspections to be conducted by the TCA. According to the recitals of the Guidelines, the TCA deemed that it was necessary to determine and set out these relevant principles, in light of the recent amendment to Article 15 (“On-Site Inspections”) of the Law No. 4054 on the Protection of Competition (“**Law No. 4054**”).²

The Guidelines essentially (i) clarify the procedures to be abided by when the data on the electronic media or information systems are required to be examined by the case handlers during on-site inspections, in a way that relatively echoes the recent enforcement practices of the TCA, and (ii) introduce a new method for the examination of digital data, which is akin to the methodology and principles set forth within the European Commission’s (“**Commission**”) Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003 (“**Commission’s Explanatory Note**”).

(2) What do the Guidelines bring: An uncharted territory or statutory safeguard with new formalistic principles?

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

² Law No. 7246 on the Amendment of Law No. 4054 was promulgated on 24.06.2020 via the Official Gazette numbered 31165. In this respect, the wording of Article 15(a) of Law No. 4054 is amended as follows: “[To] examine 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.”

In terms of the legislative justification of the Guidelines, it should be noted that the Board's decisional practice³ had, in effect, already been emphasizing that the previous wording⁴ of Article 15(a) of the Law No. 4054 did not preclude the TCA from exercising its investigative powers on the data and documents held in electronic media and information systems, during its on-site inspections. That being said, the TCA's approach was merely shaped with the case law of the Board and thus, a guidance based on secondary legislation was most welcomed on this front. In this respect, the Guidelines essentially concretise the Board's decisional approach and explicitly set forth the scope of investigative powers of the Authority during the on-site inspections, while also pinpointing which acts of undertakings might be deemed as non-compliant with the relevant principles.

Following from the above, the Guidelines underline that during an on-site inspection, the TCA case handlers are entitled to conduct their examination on the relevant undertaking's IT systems such as servers, desktop or laptop computers and portable devices, as well as all data storage apparatus and mechanisms, such as CDs, DVDs, USB sticks, external hard disks, backup records and cloud services. In a similar vein, the Guidelines note that the case handlers may utilize digital forensics software or hardware during their on-site inspection, to search, retrieve and duplicate the digital documents or data, as well as recover any deletions.

The Guidelines also emphasize the principles governing the examination of portable devices (e.g., mobile phones, tablets etc.), where the case handlers shall decide whether the relevant device should be subject to the review within the scope of the on-site inspection, after a quick browse to determine whether the subject portable device contains any digital data pertaining

³ *Gediz/Aydem Decision* of the Board dated 01.10.2018 and numbered 18-36/583-284, para. 1034 and *Chemotherapy Drugs Decision* of the Board dated 02.01.2020 and numbered 20-01/14-06, para. 204. Additionally, in the *Chemotherapy Drugs Decision*, the Board indicated that certain decisions of administrative courts rendered with regard to applications for judicial review of the Board's decisions, had upheld the TCA's powers to inspect digital data and electronic documents: *see Turkcell Decision* of the 10th Chamber of Council of State dated 25.11.2002 and numbered E: 2000/5592, K: 2002/4506; *Turkcell Decision* of the Plenary Session of Administrative Law Chambers, Council of State dated 16.06.2005 and numbered E: 2003/315, K: 2005/21 77; *Koçak Petrol Decision* of the 13th Chamber of Council of State dated 26.03.2013 and numbered E:2009/5890, K: 2013/847 and *Reysaş Decision* of the 13th Chamber of Council of State dated 26.03.2013 and numbered E: 2010/543 K:2013/844.

⁴ The wording of Article 15(a) of the Law No. 4054 prior to the amendment has been as follows: "*To this end, it is entitled to: (a) Examine books, any paperwork and documents and take their copies if needed.*"

to the relevant undertaking. The Guidelines specify that those portable devices which are allocated entirely for personal use, cannot be brought under the scope of an on-site inspection. That being said, personal portable devices which also include digital data pertaining to the relevant undertaking, would still be subject to the review of the case handlers through the use of digital forensic tools. It should be noted that the Guidelines do not introduce a completely brand new approach to the examination of personal devices or accounts, as there are recent decisions wherein the Board decided that personal devices⁵ or e-mail accounts⁶ can also be examined within the scope of on-site inspections, if they contain information pertaining to the relevant undertaking.

The Guidelines also draw a framework for the undertakings' obligation to cooperate with the TCA case handlers during the on-site inspections. Accordingly, the undertaking under scrutiny is obliged to prevent any interferences to the data itself or the medium wherein it is stored, as well as to fully and actively assist the case handlers where needed with regard to the IT systems, such as by (i) providing the case handlers with information regarding the IT software and hardware, (ii) authorizing the case handlers as system admins, (iii) providing remote access, (iv) isolating the computers and servers from the network, (v) limiting user access to corporate accounts and (vi) restoring backed-up/stored business data. In this respect, the undertakings' obligation to cooperate, as stipulated within the Guidelines, also closely reflects the Board's current decisional practice, wherein the relevant undertaking's failure to provide the case handlers access to its IT infrastructure (*e.g.* Office365 and eDiscovery) due to reasons of technical impossibility or concerns about potential breach of the relevant undertakings' data protection policy, was deemed to be non-compliant with the cooperation obligation.⁷

⁵ *Koçak Petrol Decision* dated 05.08.2009 and numbered 09-34/837-M and *Nuhoğlu İnşaat Decision* dated 21.12.2017 and numbered 17-42/669-297 of the Board.

⁶ *Askaynak Decision* dated 26.12.2019 and numbered 19-46/793-346 and *Ege Gübre Decision* dated 07.02.2019 and numbered 19-06/51-18 of the Board.

⁷ *GROUPE SEB Decision* dated 09.01.2020 and numbered 20-03/31-14 and *Siemens Decision* dated 07.11.2019 and numbered 19-38/581-247 and *Unilever Decision* dated 07.11.2019 and numbered 19-38/584-250 of the Board.

As another significant point, the Guidelines emphasize that the attorney-client privilege shall be respected when an on-site inspection is conducted. To that end, the Guidelines indicate that, in order to benefit from the attorney-client privilege, two cumulative conditions shall need to be met, which is again, in line with the recent decisional practice of the Board.⁸ Accordingly, for digital data or documents to fall under the protective cloak of the attorney-client privilege, the Guideline criteria are: (i) the correspondence shall be between the undertaking and an independent/outside legal counsel, who has no employment relationship with the relevant undertaking and (ii) the correspondence shall be made with the purpose of exercising the undertaking's right to defence. The Guidelines explicitly set forth that communications that are not directly related to the use of undertaking's right to defence and particularly communications that are made with the purpose of facilitating any conduct that violates competition rules or for concealing an on-going or future violation of the competition rules are out of the scope of attorney-client privilege.

In addition to bringing the recent enforcement trends of the TCA under a statutory safeguard, the Guidelines also introduce a brand-new procedure, which grants the TCA the discretion to continue its inspection of the digital documents or data, in the computer forensics laboratory of the TCA, if deemed necessary.⁹ The relevant paragraph of the Guidelines echoes paragraph 14 of the Commission's Explanatory Note, which sets forth that if the selection of documents relevant for the inspection is not yet finished at the end of the envisaged on-site inspection at the undertaking's premises, the copy of the data can be collected to continue the inspection process at the Commission's premises.¹⁰ Similar to the principles set forth within the Commission's Explanatory Note, the Guideline also states that the Authority will invite the investigated undertaking, in writing, to have a representative present during the opening of the

⁸ *Enerjisa Decision* of Ankara Regional Administrative Court, 8th Administrative Law Chamber dated 10.10.2018 and numbered E.2018/658 K.2018/1236; *Çiçeksepeti Decision* dated 02.07.2020 and numbered 20-32/405-186, *Huawei Decision* dated 14.11.2019 and numbered 19-40/670-288, *Warner Bros Decision* dated 17.01.2019 and numbered 19-04/36-14 of the Board.

⁹ Having said this, the Guidelines provide that the inspection of the digital data contained in mobile phones shall be completed at undertaking's premises, in any event.

¹⁰ In such instances, the Commission may create an authentic copy and secure it in a sealed envelope for further examination - either at the Commission's premises, or if there is a new announced visit at the premises of the undertaking. The Commission's Explanatory Note is also aligned with the Commission's practice of requesting from the undertaking to keep the sealed envelope, where relevant. In that case, the undertaking keeps its data under control but also bears a responsibility for keeping it safe.



sealed envelope and the examination to be carried out at the Authority. To that end, the Guidelines also suggest that if the Board deems it necessary, it may decide to return the sealed envelope containing the digital data to the relevant undertaking, without being opened. This new procedure might be the harbinger of continued inspections by the TCA in the future and it also bolsters the necessity of robust on-site inspection compliance procedures by the undertakings in light of the increasing complexity of the processes within the scope of on-site inspections.

(3) Conclusion

In conclusion, taking into account the recent decisions of the Board concerning on-site inspections, it can be stated that the Guidelines actually reflect the previously established practices and current approaches of the TCA, along with further clarifications and a newly introduced formalistic methodology similar to the Commission's Explanatory Note. That being said, since the Guidelines also take a snapshot of the Board's recent approach, this could result in a formalization that allows relatively less room to manoeuvre going forward, from a case-law stand point. All things considered, the Board's case-by-case assessments will still shed further light on the actual implementation of the Guidelines and be most welcomed.

Article contact: Gönenç Gürkaynak, Esq.

Email: gonenc.gurkaynak@elig.com

(First published by Mondaq on October 15, 2020)