MOROĞLU ARSEVEN

Guideline on Digital Data Review During On-Site Inspections of Turkish Competition Authority

22 Oct 2020

What it Brings and How it Resonates from Privacy and Data Protection Perspective

Turkish Competition Authority ("**TCA**") has published its Guideline on Digital Data Review During On-Site Inspections ("**Guideline**") on its website on 11 October 2020 which was approved by the TCA on 8 October 2020.

The recent amendments[1] introduced to Article 15 of the Law on Protection of Competition Law ("**Law**") constitutes the basis of the Guideline. These amendments were aiming to detail the documents and information that the TCA can obtain from the undertakings or associations of undertakings during the on-site inspections it carries out. In practice, the TCA has already been examining and taking copies of electronic media and information systems of the investigated undertakings over the past years and this practice was deemed legal as the precedent of the Council of State suggests. Obviously, the amendment provided a solid legal basis to the examination powers of the TCA and extended the TCA's authority in a clear manner so that the TCA can examine the data retained in physical and electronic media and also in information systems.

The Guideline elaborates how the TCA will implement its examination powers which are akin to practices of the European Commission ("**Commission**"); set in the "*Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003*" ("**Explanatory Note**") dated 11 September 2015, as it was also signaled in the public announcement of the TCA dated 5 June 2020[2].

In this article, we aim to provide information on the examination powers vested on the TCA in the Guideline and its repercussions from a personal data protection perspective.

1. Overview of the Guideline

1.1. According to the Guideline, the Chief Competition Expert, the Competition Expert and the Assistant Competition Expert ("**Case Handlers**") are authorized to examine information systems such as a server, desktop/ laptop, portable device, and storage devices such as CD, DVD, USB, external hard disk, backup records, cloud services belonging to an undertaking or an association of undertakings.

Also, it is foreseen in the Guideline that the Case Handlers can now benefit from e-discovery tools belonging to the undertaking or forensic information software and hardware that allow qualified searches in digital data.

1.2. The Guideline points out that portable communication devices (mobile phones, tablets, etc.) can be quickly reviewed by the Case Handlers to determine whether the relevant device contains digital data belonging to the undertaking. Portable communication devices that are found to contain data belonging to the undertaking will be examined through forensic information tools. As a result of the examination, the data considered to be evidence within the scope of the file will be parsed and all other data that are not seen as evidence will be permanently deleted so that they cannot be recovered.

The review of the personal devices appears as one of the most controversial aspects of the Guideline. The legal basis of the Guideline, Article 15 of the Law, clearly states that the TCA is authorized to review any document, electronic media, etc. that belongs to an undertaking or an association of undertakings. That being said, the Guideline refrained from making such separation between personal devices and those belonging to undertakings. Therefore, within the provisions of the Guideline, the personal portable communication devices (mobile phones, tablets, etc.) can be subjected to quick review of the Case Handlers to determine whether they contain digital data belonging to the undertaking.

The specific criteria set by the Guideline in respect of the portable devices are whether the data in the devices pertain to the undertaking or the association of undertakings, not to whom the device itself belongs as it is regulated under Article 15 of the Law.

Accordingly, the scope of the respective provision of the Guideline and the examination powers vested in the Case Handlers on portable devices will be under scrutiny vis-à-vis the administration's lawfulness principle which is protected under Article 123 of the Constitution of the Republic of Turkey (the "**Constitution**").

The legislative process of the amendment law may shed light into how the TCA was expected to use its new authorities arising out of Article 15. It was recorded in the 8 June 2020 dated Report[3] of the Industrial, Commercial, Energy, Natural Resources, Information Technologies Commission that discusses the law proposals for the Grand National Assembly of Turkey that the portable devices belonging to a company can be subjected to the examination of the Case Handlers with the exclusion of personal portable devices. On the contrary, it was emphasized in the Commission Report that in the European Union practice, the portable devices can also be confiscated, documents and information can be sealed and yet a more subtle and free implementation has been introduced with the amendment proposal. Although the legislative history of the amendments in Article 15 of the Law provides a more subtle approach to the personal portable devices, it is apparent that the TCA favored the European Union practice, which can also be verified by observing its similarities with the Explanatory Note of the Commission.

It is also possible for the "quick review" *-as suggested in the Guideline-* to turn into an intervention to personal rights; such as the right to privacy (protection of personal data), the freedom of communication, the property right which are also protected under respective provisions of the Constitution. The "quick review" approach, in the absence of its clear basis under the Law and lacking of a technical and methodological framework that will be applied by the Case Handlers in similar circumstances has a potential to *quickly* become a pitfall in the practice of the TCA for on-site inspections as it may be hooked up in the judicial review process of the TCA's decisions. The Case Handlers should show due care in these reviews considering that communications, personal data and privacy of individuals are in the core of these reviews and the principle of proportionality set out under Article 13 of the Constitution should always be sought.

1.3. The Case Handlers are authorized to conduct inspections in digital environments containing all kinds of data belonging to the undertaking. The digital environment in which the data to be examined will be kept under control by the Case Handlers throughout the inspection.

The Guideline also sets forth that the authorities of the undertaking are obliged to provide full and active support in the matters requested by the Case Handlers regarding the information systems. In this regard, the Guideline provides certain examples; the undertaking is obliged

- to provide information about software and hardware related to the information technologies used,
- to provide system administrator privileges,
- to provide remote access to the e-mail accounts of the employees of the undertaking,
- to isolate computers and servers from the network environment,
- to limit the access of users to their corporate accounts,
- to restore backed up corporate data.

1.4. The Case Handlers will be able to partially or completely copy the digital data that is going to be analyzed to a separate data storage by applying forensic methods. The copy taken with the forensic method is a duplicate copy obtained in a logical and physical way that ensures the authenticity of the data which is confirmed by calculating the hash (which is a mathematical calculation method used to verify the integrity of digital files) values ??that the data copied with forensic methods are exactly the same as the original. The copied data will be indexed to make it searchable by using forensic software and analyzed by the Case Handlers.

1.5. Digital data that is deemed necessary at the end of the analysis are copied to two separate data storage. One of the copies obtained is delivered to the undertaking.

At the end of the examination, all data stores used during the examination will be deleted in a way that their data cannot be restored, except for the data stores that contain digital data submitted to the undertaking and a sample of which will be taken by the Case Handlers.

1.6. The Guideline also points out that it is essential that the examination is completed on the premises of the undertaking. However, if deemed necessary, it may be decided to continue the examination in the forensic informatics laboratory within the TCA. In any case, the analysis of digital data obtained from mobile phones is completed at the plant/office of the undertaking. Accordingly, Case Handlers are not empowered to take copies of portable devices.

In case the Case Handlers decide to examine the digital data on the premises of the TCA, the undertaking concerned should be invited in writing by the TCA to have a representative available during the examination.

1.7. The relevant undertaking has the right to claim that the digital data included in the file, as a result of the examination conducted at the undertaking's premises or the premises of the TCA, to be treated as a trade secret within the scope of the "Communiqué on the Regulation of the Right to Enter the File and the Protection of Trade Secrets" numbered 2010/3.

1.8. Finally, the Guideline states that the data copied during on-site inspection benefits from protection under the principle of attorney-client confidentiality. Accordingly, it is being accepted that correspondence between the client and an independent lawyer, who does not have an employee-employer relationship with his/her client, made for the purpose of using the client's right to defense will benefit from the protection within the scope of the lawyer-client confidentiality principle.

However, it is pointed out in the Guideline that the correspondence on matters that are not directly related to the exercise of the right to defense, especially to assist in an infringement of competition, or to conceal an ongoing or future violation, cannot benefit from this protection.

2. Review of the Guideline in Personal Data Protection View

The Guideline does not provide any direct reference to the protection of personal data nor any explanations regarding the impacts of the inspections on the personal data processed. Unlike the Guideline, in the Explanatory Note, it is clearly stated that the GDPR provisions apply to all personal data collected by the Commission during anti-trust investigations and personal data of individuals are not the target of the investigations and inspections. However, personal data of the employees of undertakings (such as their names, telephone numbers, email addresses) may be contained in business documents and data related to such investigations and may therefore be copied or obtained during an on-site inspection and may become part of the Commission file. It is finally stated that all data should only be used for the purpose for which they were collected, and data protection rules should be followed at each step of processing.

In the European Union practice, the protection of personal data with competition law perspective was heavily discussed and the European Data Protection Supervisor ("**EDPS**") has published a document discussing this issue.

According to the EDPS;

- The GDPR does not prevent the submission of information containing personal data to the EU institutions, either in response to a legal obligation to do so or voluntarily, as long as you act within your powers and sphere of competences.
- Economic operators do not have the legal obligation to inform people about the disclosure of their personal data to the EU institutions in case such data is submitted to your services to carry out a particular inquiry within their powers under European Union law.
- GDPR is not an obstacle to auditing / financial verification clauses.

It can be seen that a similar approach with Turkey is adopted in the European Union practice with a special emphasis on the protection of proportionality principle and ensuring all necessary technical measures in order to prevent any data incidents are also compulsory in the European Union approach.

In the TCA's practice, the onsite inspections have so far captured all devices that belong to an undertaking or an association of undertakings or that are provided to the individuals by the same. In these devices, any correspondences had been made subject to the inspection including text messages, WhatsApp messages, e-mails, and all other communication applications as well as other data in the portable device.

In several precedent cases, the TCA imposed administrative fines on several undertakings for the prevention of on-site inspections as they refused to access certain data with privacy concerns:

- In the Groupe SEB decision[4] dated 2020, the TCA imposed an administrative fine on Groupe SEB which refused access to a former manager of the undertaking for data protection purposes.
- In an earlier decision[5], the TCA imposed an administrative fine on Unilever who refused access to certain data for the reason that the system contains both Unilever Turkey's and Unilever Global's data as they are not separated.
- Similarly, in Siemens Healthcare decision[6] dated 2019, the TCA imposed an administrative fine on Siemens Healthcare which refused access to employee data as the systems not only contain personal data of employees of Siemens Healthcare Turkey, but also data of global employees.

The TCA's comprehensive powers (*including administrative fines as described above*) on the information systems of the undertaking, including the portable devices, bring many privacy concerns with respect to personal data as described under Law on Personal Data Protection no. 6698 ("**DP Law**"). Although it is pointed out in Paragraph (4) of the Guideline that the "*devices confirmed to be dedicated to personal use will not be inspected*", the respective paragraph is also expected to be the focal point of criticism from different angles, if not only from personal data protection law perspective.

Personal data is defined under the DP Law as "*all the information relating to an identified or identifiable natural person*", and the DP Law applies to natural persons whose personal data are processed as well as to natural or legal persons who process such data fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means. Processing of personal data is also defined under the DP Law as "*any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means*". In this respect, in case the data inspected and copied by the TCA are personal data, the process by the TCA will be personal data processing as defined under DP Law.

As the TCA processes personal data during onsite inspections, the provisions prescribed under the DP Law must be followed at all times. At this point, it must be determined which provisions apply to these processing activities.

As per Article 28 of the DP Law, besides others;

- DP Law does not apply in case personal data is processed within the scope of preventive, protective, and intelligence activities carried out by public institutions and organizations duly authorized and assigned to

maintain national defense, national security, public security, public order, or economic security;
- Article 10 regarding the data controller's obligation to inform, Article 11 regarding the rights of the data subject, excluding the right to demand compensation, and Article 16 regarding the requirement of enrolling in the Registry of Data Controllers shall not apply in case personal data processing is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of the public institution, assigned and authorized for such actions, in accordance with the power conferred on them by the law.

Article 28 of the DP Law provides a full or partial exemption from the DP Law provisions. Accordingly, it should be determined whether TCA's on-site inspections are exempted from the DP Law fully or partially. Although the scope of each exemption is not completely clear, it can be said that full immunity from the DP Law requires heavier causes such as prevention of any interventions to national security or intelligence activities.

On the other hand, partial exemption explicitly refers to the regulatory duties and inspections of public institutions. The purpose of the Law is defined in the first article as "*to prevent agreements, decisions and practices preventing, distorting or restricting competition in markets for goods and services, and the abuse of dominance by the undertakings dominant in the market, and to ensure the protection of competition by performing the necessary regulations and supervisions to this end*". Obviously, the purpose of the TCA's inspections is not to ensure national defense, national security, public security, public order, or economic security, but to perform its respective regulatory and supervisory administrative powers as defined under the Law. In this regard, the TCA's inspections are more likely to be exempted (partially) from the DP Law in other words exempted from the obligation to inform, the obligation to enroll in the registry, and the data subject's rights except the right to demand compensation.

According to the Personal Data Protection Board ("**Board**"), in any case, no matter fully or partially exempted from the DP Law, all personal data processing activities should be in line with the basic principles of data processing as described under Article 4 of the DP Law[7]. Also, as the protection of personal data is a right protected by the constitution, the constitutional principles regarding fundamental rights and freedom should be followed. There are several precedent decisions[8] of the Constitutional Court for the protection of personal data before the DP Law was enacted.

As per the above-mentioned principles under Article 4 of the DP Law should be followed in each processing activities;

- Lawfulness and conformity with rules of *bona fide*.
- Accuracy and being up to date, where necessary.
- Being processed for specific, explicit, and legitimate purposes.
- Being relevant to, limited to, and proportionate to the purposes for which they are processed.
- Being retained for the period time stipulated by relevant legislation or the purpose for which they are processed

Article 4 of the DP Law requires personal data to be processed for specific, explicit, and legitimate purposes. Also, the personal data should be processed proportionately to the purposes for which they are processed. The proportionality principle is a key principle that determines the lawfulness of all data processing activities. In this sense, the intensity of processing must be proportional to the importance of the aim wished to be achieved and only data strictly necessary for the achievement of the purpose must be processed. If the same result can be achieved by processing less data, the extensive processing would be regarded as unlawful.

The data processing activities of the TCA during inspections should be assessed with regards to the lawfulness and proportionality principle. It should be noted that the right to privacy is not absolute and can be restricted by a greater right of society in certain cases. In this case, it should be determined whether the aim wished to be achieved, which is the protection of competition in any given market, in this case, is greater than the individuals' right to privacy. Second, it should be assessed in each individual case whether the processing is extensive, in other words, the same results could be achieved by following the data minimization principle.

According to Paragraph (4) of the Guideline, all information systems of the undertaking including portable devices, which in fact may be provided to the employees by the undertaking to be used for business purposes can be examined by the Case Handlers as explained above under Section 1.2, above. The wording of the Guideline enables the interpretation as if the Case Handlers are allowed for a quick review on employee's personal devices, which are not provided by the undertaking. It is stated in Paragraph (4) of the Guideline that the portable devices will be run through *(quick review)* and confirmed whether they consist of any information concerning the undertaking or association of undertakings. At this point, an assessment from personal data protection view should be made for personal and company-owned devices separately.

In principle, explicit consent is the rule for processing personal data. However, there are certain exemptions brought by the DP Law which are stated above. As a general principle of law, exemptions are interpreted narrowly. The Law, which is explained in detail under Section 1.2., does not specifically allow the Case Handlers to inspect personal devices. In this case, it can be argued that the processing of personal data is not arising from any particular provision of the "law". As such, only in the presence of the employee's explicit consent, employee's device can be inspected. However, under the pressure of investigation, the validity of explicit consent is also suspicious.

On the other hand, devices provided to the employee by the undertakings are also very likely to contain personal data of the employee or third persons. Although it is stated that the devices confirmed to be dedicated to personal use will not be subjected to the inspection, how this confirmation will be achieved, unfortunately, is not clear and the term, i.e. the "quick review" used in the Guideline is not clearly defined.

In any case, unlike personal devices, the Law allows the Case Handlers to inspect undertaking owned devices. It might, therefore, be justifiable to inspect devices provided to the employees by the undertaking. The principle of proportionality as stated under Article 4 of the DP Law, however, should be followed in all steps very carefully otherwise this processing can be excessive, thus, unlawful with respect to the DP Law. For instance, as the inspections can be carried out based on searching for certain keywords as explained in the Paragraph (3) of the Guideline, the keywords to be searched must be chosen by giving respect to the specifics of the case, which can be easily finding its way from authorization letter as provided to the Case Handlers, and not allow extensive personal data processing. Another example is that personal emotions should not be chosen as keywords as much as possible. In case the devices are detected to contain information regarding the investigation, only the data concerning the undertaking and the investigation should be copied.

It is also explained in Paragraph (5) of the Guideline that the Case Handlers should be vested with administrator authorities in the digital systems and remote access to the employee e-mails should be enabled. The explanations regarding keyword search hereinabove are also applicable in these cases. On the other hand, having administrator authorities in all digital systems and accessing all employee e-mails remotely can be excessive in certain situations.

Relativity and scope of the investigations should be considered in order to follow the principle of proportionality and limitedness as prescribed under Article 4 of DP Law. For example, in a cartel investigation regarding customer sharing, accessing all files or e-mails of the human resources department can be regarded as excessive. Also, the human resources department may be containing special category personal data such as criminal records or pregnancy leaves etc. and accessing these data would not have any legal ground. Additionally, access to e-mail accounts of certain employees which cannot be related to the investigated issues, thus, exceeding the scope of the authorization letter of the Case Handlers, due to their positions in the investigated undertaking can be regarded as excessive. In these cases, as processing personal data is not strictly required to enlighten the case or draw a conclusion in the investigation, the process of these data does not comply with Article 4 of the DP Law. A case by case analysis should be made for each individual situation. Also, the protection of the data must be ensured with adequate security measures taken by the Case Handlers.

If the TCA's inspections are accepted to be partially exempted from the DP Law, Article 5 and Article 6 of the DP Law should also be followed:

- As per Article 5 of the DP Law, the personal data can only be processed in the presence of explicit consent of the data subject or otherwise on a certain legal basis prescribed under Article 5 without the data subject's consent. These legal bases include being provided by the law and being mandatory for the controller to be able to perform his legal obligations. In this sense processing personal data during on-site inspections can be regarded as lawful.
- On the other hand, Article 6 brings specific protection for the special category of personal data. As per Article 6 of the DP Law, personal data, excluding those relating to health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. It should be noted that the Board tends to interpret this provision narrowly and regard only the explicit and clear reference by the law that enables the processing of special category of personal data. In this case, the Law does not explicitly refer to any special category data to be processed, the process of this data for the inspection is unlikely to be regarded as lawful by the Board.

Personal data relating to health and sexual life, on the other hand, may only be processed, without seeking explicit consent of the data subject, by any person or authorized public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing. Processing of personal data concerning health and sexual life cannot be regarded as lawful in any case.

[1] The amended Article 15/1/a reads as follows *"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,*".

[2] "…*With the 20th article of Council Regulation No 1/2003 in the EU implementation, the investigative powers of the Commission officials regarding the information systems have been significantly expanded. With the Law Proposal, powers similar to the powers granted to the EU Commission officials are granted to the experts of the Authority, in this way, it is aimed to effectively tackle the hidden cartel structures just like in the EU practice. While the legal infrastructure for strengthening the examination of information systems with the new regulation is strengthened, the protection of personal data and the confidentiality of attorney-client communications will be secured in detail by the regulations to be issued by the Competition Board, as it is in the EU practice.*"

[3] Industrial, Commercial, Energy, Natural Resources, Information Technologies Commission Report, page 17-18, https://www.tbmm.gov.tr/sirasayi/donem27/yil01/ss215.pdf

[4] TCA, Decision Date: 09.01.2020, Decision Number 20-03/31-14

www.rekabet.gov.tr/Karar?kararId=b7085aec-faf9-4023-8be7-3cb7801cbcf2

[5] TCA, Decision Date: 07.11.2019, Decision Number 19-38/584-250

http://www.rekabet.gov.tr/Karar?kararId=f36e9c11-c48a-43dc-8c07-e6b1297f06ed

[6] TCA, Decision Date: 07.11.2019, Decision Number 19-38/581-247

http://www.rekabet.gov.tr/Karar?kararId=38800013-e0f0-4375-9f16-ce520b83e25c

[7] Örneklerle Ki?isel Verilerin Korunmas?, Ki?isel Verileri Koruma Kurumu, 2019, Ankara, s. 50. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.pdf

[8] Constitutional Court, Decision Date: 03.03.206, Decision Number: 2013/5356

https://kararlarbilgibankasi.anayasa.gov.tr/Ara?BasvuruNoYil=2013&BasvuruNoSayi=5653&KararTarihiBaslangic=03%2F03

Related Practices

- Privacy and Data Protection
- Antitrust and Competition

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- CEYLAN NEC?PO?LU, Ph.D, LL.M.