Organisation for Economic Co-operation and Development

DAF/COMP/GF/WD(2018)19

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 Austria

- Session IV -

30 November 2018

This contribution is submitted by Austria 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.

JT03439936

Investigative Powers in Practice

Breakout session 1 - Unannounced inspections in the digital age

- Contribution from Austria –

1. The investigative powers of the Austrian Federal Competition Authority (FCA) are enshrined in the Austrian Competition Act (ACA), but also stem from Council Regulation (EC) No 1/2003 on the implementation of the rules on competition. The FCA is an independent and autonomous authority, in particular mandated to conduct investigations into suspected infringements of Austrian and European competition law. Austria follows a purely prosecutorial enforcement system, which is also reflected in the setup of its investigative powers.

2. As the Austrian FCA started to carry out a considerable number of dawn raids in 2011, practical problems thereto became evident. They were addressed by **adoptions in the Cartel and Competition Act** 2013 and 2017. Besides, a number of legal questions were litigated and hence a broad body of **jurisprudence** developed.

3. In October 2017, the FCA published a **guidance paper on dawn raid practice** to further increase transparency for addressees as well as to advocate compliance.[1] This guideline specifies the procedure of the dawn raids itself as well as the rights and obligations of the company, their employees and the members of the FCA. It is a summary of the legal framework and the practical handling with special focus on securing electronic data.

4. The present submission will first describe the actual legal framework in detail, then focus on questions related to electronic data and finally mention challenges encountered and, as a background, how they were solved by changes in the Cartel and Competition Act.

1. Unannounced Inspections in the Digital Age: Current Legal framework and procedure

5. Where there is reasonable suspicion of anti-competitive conduct, the FCA is entitled to carry out a search following an order of the Cartel Court pursuant to Section 12 Competition Act (WettbG). A search of premises may also, pursuant to Article 22 of Regulation (EC) No 1/2003, be carried out at the request of another competition authority or of the European Commission.

6. The FCA starts the process based on a **search warrant issued by the Cartel Court (KG)**. As a rule, the search warrant is handed over to a company representative at the beginning of the search.

7. When conducting a search, any sensation, nuisance and disturbance will be limited to the absolute minimum, and any ownership and personal rights of the party concerned protected as much as possible (Section 12 para. 4 WettbG). The search will be carried out

[1] https://www.bwb.gv.at/fileadmin/user_upload/Englische_PDFs/Standpoints%20and%20Handbooks/Guidance_on_dawn_raids_final.pdf.

in a manner that is as unobtrusive as possible in order not to interfere in daily business dealings, and for the required duration only. Depending on the individual circumstances of the case (e.g. company size, type and extent of suspicion, type of IT-infrastructure used, a search may take place from a few hours to several days. The FCA is not bound by the company's business hours in terms of when it conducts its search.

8. The FCA is entitled to inspect and examine all **business documents** during searches. This includes the right to check whether documents found on the premises are business documents after all within the meaning of the law. In this context, the FCA is entitled to inspect both **physical** documents (paper documents, notebooks etc.) and **electronically stored** documents. The search right includes all documents legally and economically related to the suspected infringement.

9. Searches are not only carried out on the premises of a company suspected of anti-competitive conduct. A search warrant may also be issued for the **premises of third companies** or private homes, reasonable suspicion provided evidences of a third party antitrust law-breach might be found on those premises.

10. The FCA is entitled to **seal** rooms or individual items (such as filing cabinets or laptops) for the duration of the search. To this end, the FCA uses official seals. Damaging or removing such a seal constitutes a criminal offence.[2]

11. The FCA is entitled to **seize evidence**, too. However, the FCA prefers to take copies. The seizure of a laptop or a smartphone, for instance, might be required to ensure that data can be properly copied by supporting forensic police. Copying electronic data does not constitute a seizure.[3] The FCA will collect all seizure details in an official record and provide a copy to the company.

12. The company concerned may **appeal** to the Supreme Cartel Court (KOG) against a warrant issued by the KG.

13. The FCA records the whole search procedure in an **official record**. This record covers all details relevant to the search such as company address, contact persons within the company, time of the warrant being served, start and end time of the search, information about copied paper documents and any electronically collected IT data, noteworthy incidents during the search, as well as any comments and statements made by company representatives during the search. The company may make a copy of the official record at the end of the search. The official record will subsequently be submitted to the KG.

14. The FCA is entitled to **request any relevant information** from the company and its staff which is needed to carry out the search unhindered. Questions can, for instance, be related to the corporate structure, the location of relevant employees' workstations, document archives or corporate IT landscape.

15. The FCA is also entitled to request documents and explanations from all staff about facts or documents that are related to the subject and purpose of its investigation (Section 11a para. 1 no. 3 WettbG) such as, for example, explanations about the meaning of

[2] *Section 272 para. 1 of the Austrian Criminal Code (StGB): "Any person who damages or removes a seal that a government official has attached in the execution of his or her official duties in order to keep a thing under lock, confiscate or label a thing, and who in whole or in part renders the purpose of the seal useless is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units."*

[3] Cf. Supreme Court of Justice of 20 December 2011, 16 Ok 7-13/11.

abbreviations used in email communication or to grant access to sales representatives' laptops (passwords).

In addition, since the Amendments of the Cartel and Competition Act 2013 the FCA is also authorised to question about matters beyond sole explanations of facts or documents access.

16. As will be explained in more detail under section 3, the company has the **right to object** to the examination, inspection or seizure of certain specified documents (Section 12 para. 5 WettbG). However, this right of objection is **limited to specific grounds**.

17. If necessary, searches can be executed by coercion. The FCA can ask police officers for assistance (Section 14 WettbG).

18. At the end of the investigation the authority organises a **final debrief** with the company. During this debrief the FCA provides the official record, explains the further procedure and answers questions. The company may copy the official record as well as the physical and electronically collected documents at its own expenses.

2. Access to electronic data

19. Companies are more frequently communicating via digital technologies. Paper documents and physical archives are replaced by emails and electronic data files. The FCA must adapt to these technological and social changes to be able to fulfil its statutory order.

20. The FCA is entitled to inspect or examine business documents irrespective of their form, to have them inspected or examined with the help of suitable experts and to make copies and extracts from those documents (Section 11a para. 1 no. 2 WettbG). This covers both **physical** documents (e.g. paper documents, notebooks) and **electronically stored documents** (e.g. on laptops, USB flash drives, smartphones, external servers, in the cloud). It is not relevant whether the electronic data is actually stored on a storage medium at the inspected premises or on external storage sites (including cloud services).[4] The authority can take any data which is **accessible from the premises**, **no matter where the data is stored**.[5]

21. In cases when **electronic devices** are not to be found **on site** (e.g. sales representatives), the FCA is entitled to **demand** production of those devices. This document production request is made by the FCA in its capacity as an independent administrative authority and is not part of the enforcement of the search warrant.

22. Companies are obliged to tolerate a search. It is therefore recommended that companies instruct their employees to use their electronic devices only after consulting with the FCA team leader.

23. The company is **obliged to provide electronic data access** upon FCA request. Upon request, this obligation also includes the disclosure of passwords and the provision of a copy of the relevant electronic data in a FCA-compatible electronic format.[6]

[4] See also Administrative Court of 22 April 2015, Ra 2014/04/0046 to 0051.

[5] See the amendment of Section 11a para. 1 no. 2 WettbG, enacted by the KaWeRÄG 2017, which now refers to business documents as those that "can be accessed at the company or from its premises".

[6] See the related amendment of Section 11a para. 2 WettbG, enacted by the KaWeRÄG 2017.

24. The Amendments of the Cartel and Competition Act 2017 introduced a new offence on **penalty payments** in Section 35 para. 1 lit c KartG[7] to be imposed by the KG. Daily penalties can be imposed on undertakings, if in the course of a dawn raid, they **fail to grant access to electronic data** that is accessible from the premises concerned. The fines can amount to up to 5% of the average daily turnover for each day of delay. In this context, penalty payments are not imposed to sanction a certain conduct or failure to act but to force a company to provide access to evidence.[8] The penalty payment is imposed upon request and after giving the party concerned the opportunity to carry out their duty to comply. A company may be deemed to be in default no earlier than one day after the search warrant has been served.[9]

3. Steps to follow when gathering electronic data; Procedural safeguards for the right of defence and the right to privacy

25. In accordance with the subject of the investigation and the search warrant, the FCA **restricts the relevant areas** (e.g. certain employees or PCs) for the period of the search. Depending on the local situation it may be necessary, for instance, to copy whole shared folders or a complete Outlook mailbox. The FCA is entitled to use **forensic software** when dealing with relevant electronic documents.[10] Relevant data is copied on hard drives provided by the FCA. Both, the party concerned and their person of trust are entitled to be present during each investigative step of the FCA.

26. Information about the collected electronic data is included in the official record. The FCA makes **two copies of the electronic data** collected on site. One copy serves as a working copy for analyzing the electronic data on the FCA's premises. The other copy is sealed into seal bags and stored on the FCA's premises for evidence reasons. The company can make a copy of the entire collected data at the end of the search at its own expenses.

27. Subject to the provisions of Section 12 para. 5 WettbG, the company has the **right to object** to the examination, inspection or seizure of certain specified documents. However, this right of objection is **limited to specific grounds**. These specific grounds include professional secrecies or the right to refuse to testify (Section 157 para. 1 nos. 2 to 5 StPO). In case a person invokes to its rights, the FCA seals the documents concerned and submits them to the KG, which decides on whether there is a lawful reason to object.[11] If the person concerned is not able to specify single documents because of the sheer volume of documents, the FCA will seal categories of documents and keep them separate from its general case file. The FCA will grant an appropriate time limit (at least two weeks) to inspect and indicate a copy of the relevant documents. (see paragraph 31). In case the period

[7] These may amount to no more than 5% of the daily turnover achieved on average during the previous business year for every day of the delay from the deadline stipulated in the administrative decision.

[8] Cf. in general on the purpose of penalty payments: Supreme Court of Justice of 21 January 2008, 16 Ok 8/07.

[9] Explanatory notes on the KaWeRÄG 2017 (government bill in annex 1522 to the shorthand verbatim records of the National Council, 25th legislative period) on no. 6 (Section 35 para. 1).

[10] Cf. Administrative Court of 22 April 2015, Ra 2014/04/0046 to 0051.

[11] Cf. Supreme Court of Justice of 6 March 2014, 16 Ok 2/14.

prescribed expires without indication of relevant documents, the objection will become void and the documents will become part of the general case file of the FCA.

28. Due to what is frequently a high volume of data, with electronic data also often being closely interlinked, it is not always possible to collect only the electronic data that is of immediate and obvious relevance to the subject of the dawn raid. This is why the FCA sorts the relevant data on its own premises after the end of the dawn raid. Any personal and non-relevant data will be deleted at the end of the sorting process. The sorting process is conducted after the end of the inspection and is a mere internal procedure; no company representatives are allowed. After the sorting process the FCA informs the company which data has been taken to the case file (= relevant data). The company can submit a statement in accordance with the right to be heard (cf. Section 11 para. 1 WettbG). The company has also the possibility to appeal against excessive FCA-conducts during inspection, like excessive copying of non-relevant data. Any other data that is not relevant to the investigation will be irrevocably deleted by the BWB from the working copy, and the company informed accordingly. The sealed backup copy will be deleted after a final court judgement has been reached, the latest.

4. Legislative milestones

29. When the FCA started to carry out a considerable number of dawn raids in 2011, a number of **questions and contentious issues** came up:

30. Companies began to appeal against the search of physical documents and electronic data. **Huge amounts of copies were sealed** and referred to the KG. This left the KG with an enormous amount of data it had to sort out and decide on which documents the FCA could look at and which it could not. In addition to the enormous amount of work for the KG this consequently led to a considerable delay in handling the cases. This was in particular problematic as fines could only be imposed if the FCA filed an application with the Cartel Court less than five years after the determination of the anticompetitive behavior without being able to suspend this limitation period by investigations.

31. Many of the controversial issues were **solved due to several important amendments to the Cartel and the Competition Act in 2013 and 2017**. The FCA conducted 109 dawn raids between 2011 and 2016 and the legal amendments helped the enforcement to be more efficient. The most important changes are the following:

- In 2012 it was made clear that the FCA **can seal rooms** to the extent necessary.
- Before the amendment of the Cartel Act in 2013 a **rejection of access to documents** during dawn raids was in principle a discretionary power of the document owner. This was changed to **narrowly defined preconditions** and therefore a very limited possibility to take advantage of sealing documents during dawn raids: Since the changes in 2013 the rejection of access to certain documents is only possible in case of 1) a statutory duty of secrecy or 2) a right to refuse the statement according to Section 157 para 1 item 2 to 5 of the Code of Criminal Procedure (i.e. in case of self-incrimination, for certain cases for specific professions like lawyers, public accountants etc.). Only in these cases these specific documents will be secured in an appropriate manner against unauthorized inspection and submitted to the Cartel Court which decides which documents the FCA can look at. While companies made partly massively use of the possibility to

seal documents in former times, hardly any documents were sealed after this change in law up to now.

- In 2017 also two amendments regarding gathering electronic data during dawn raids came into force: **Daily penalties** can be imposed on undertakings, if in the course of a dawn raid, they fail to grant access to electronic data that is accessible from the premises concerned. The fines can amount to up to 5% of the average daily turnover for each day of delay. Also it was clarified that the authority can **take any data which is accessible from the premises**, no matter where the data is stored.

32. Another important **change** concerned the **limitation period** in 2017: Until 1st May 2017 the application for fines has had to be submitted to the Cartel Court within 5 years from the end of anticompetitive behaviour without any possibility to interrupt this period. As of the amendments in 2016 this period is suspended in case the FCA informs at least one of the cartel members of an investigatory activity, e.g. a dawn raid or a request for information. Furthermore, an absolute limitation period of 10 years - not counting the time of procedures before courts - after the determination of the anticompetitive behavior was introduced. This change in the former, intensively criticized provision will further increase the efficiency of antitrust enforcement.

5. Conclusion

33. The FCA is entitled to inspect and examine any and all business documents during searches. It is entitled to inspect both physical documents (paper documents, notebooks etc.) and electronically stored documents. The search right includes all documents legally and economically connected to the suspected infringement.

34. The Austrian authority has invested meaningful resources in the past years in building up its forensic know-how, an expert team and the necessary technical equipment. In addition, legislative changes have helped dealing with the challenges involved. Besides, a number of legal questions were litigated and hence a broad body of **jurisprudence** developed.

35. As the Austrian FCA started to carry out a considerable number of dawn raids in 2011, practical problems with respect to dawn raids became evident. They were solved by changes in the Cartel and Competition Act 2013 and 2017. This was important to help the considerable amount of dawn raids and the enforcement as such to be efficient.

36. With regard to gathering electronic data during dawn raids also two amendments came into force in 2017: Sanctions can be imposed on undertakings, if in the course of a dawn raid, they fail to grant access to electronic data that is accessible from the premises concerned. The fines can amount to up to 5% of the average daily turnover for each day of delay. Also it was clarified that the authority can take any data which is accessible from the premises, no matter where the data is stored.

37. In October 2017 the FCA published a guidance paper on its dawn raid practice to increase transparency and legal security for addressees as well as to advocate compliance.[12] This guideline specifies the procedure of the dawn raids itself as well as the rights and obligations of the company, their staff and the members of the FCA. It is a summary of the legal framework and the practical handling with a special focus on securing electronic data.

[12] https://www.bwb.gv.at/fileadmin/user_upload/Englische_PDFs/Standpoints%20and%20Handbooks/Guidance_on_dawn_raids_final.pdf.