Organisation for Economic Co-operation and Development

DAF/COMP/WP3(2019)6

Unclassified English - Or. English

15 October 2019

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Working Party No. 3 on Co-operation and Enforcement

Access to the case file and protection of confidential information – Background Note

by the Secretariat

3 December 2019

This document was prepared by the OECD Secretariat to serve as background paper for Item 4 of the 130th meeting of Working Party 3 on Co-operation and Enforcement on 3 December 2019.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

More documentation related to this discussion can be found at www.oecd.org/daf/competition/access-to-case-file-and-protection-of-confidential-information.htm

Ms Despina PACHNOU
Email: Despina.PACHNOU@oecd.org

JT03452827

Access to the case file and protection of confidential information[1]

Providing access to all relevant evidence in a timely manner is indispensable to protect the rights of defence.

Access to the evidence in the agency's case file is ensured differently across jurisdictions. Some grant parties in the process a very broad access, almost to the whole file. Some others provide access to specific documents only. Access is provided following the issuance by the agency of the document outlining its allegations or, in some cases, before.

Other interested parties and the general public may also be granted access to specific documents in the agency's case file. Jurisdictions provide a limited access to the general public.

The protection of confidential information sets a limit to the right to access the case file. Although the vast majority of jurisdictions protect confidential information, the definition of 'confidential information' varies across jurisdictions. Commercially sensitive information and sensitive personal information are typically considered confidential.

The fact that information is confidential means that, in principle, it will not be disclosed. Still, disclosure can occur in a number of circumstances. First, confidential information might be shared with parties in the process in order to protect their rights of defence. Secondly, confidential information may be disclosed to other domestic and foreign agencies. Disclosure to foreign agencies generally occurs pursuant to a waiver signed by the party having submitted the information. More rarely, disclosure also occurs on the basis of information gateways. Finally, information may be disclosed for the purposes of private enforcement.

[1] This paper was prepared by Jordi Calvet Bademunt, OECD Competition Division. The document benefitted from comments from Antonio Capobianco, Despina Pachnou, and Pedro Caro de Sousa, and research assistance by Gabriella Erdei, Harry Hong, and Fumihiko Okumura (all OECD Competition Division).

Table of Contents

Boxes

1. Introduction

1. Access to the case file and protection of confidential information are two competing aspects of competition law enforcement.

2. For the purposes of this paper, access to the case file is the right of parties – including, in some jurisdictions, third parties – to examine evidence in possession of the agency pertaining to a competition proceeding. Access to this evidence is typically granted in the context of the administrative proceedings (in administrative competition enforcement systems) or at the litigation stage (in judicial competition enforcement systems).

3. As explained in Section 2.1, access to the case file is essential to protect the rights of defence of the parties, given that it provides them with the opportunity to examine the basis on which the agency or court, depending on the competition enforcement system, will adopt its decision.

4. The protection of confidential information[1] sets a limit to the right to access the case file. Confidential information is not disclosed unless this is necessary to protect legitimate interests, for instance, to safeguard the rights of defence. Where disclosure is necessary, confidential information may be shared under conditions, e.g. by restricting disclosure to the external legal counsel of the party requesting access.

5. Competition agencies need to foster a reputation for respecting the confidentiality of the information they receive, in order to ensure the continued supply of information from parties and third parties. Agencies should also avoid that the parties that have submitted the information or from which information has been seized are unduly prejudiced due to its disclosure to other parties.

6. Currently, the OECD is in the process of discussing a draft Recommendation on Transparency and Procedural Fairness, which includes clauses on access to the case file and the protection of confidential information.

7. The first part of this paper discusses access to the case file. It begins by explaining why access to file is relevant to ensure the fairness and transparency of competition enforcement. Then, it discusses what type of information is accessible by which parties and when this information can be accessed.

8. The second part of the paper examines the protection of confidential information as a limit to the right to access the case file. It examines the notion of confidential information and how this is identified and protected in practice. Then, the paper addresses various exceptions to the non-disclosure of confidential information: to parties in the process; to other agencies, domestic and foreign; and for the purposes of private enforcement. The paper concludes by providing the common denominators and key challenges across jurisdictions.

2. Access to the case file

2.1. Overview

9. Competition agencies typically have an obligation to act fairly in the collection and disclosure of evidence (both incriminating and exculpatory) (OECD, 2012[1]). Evidence should be recorded and made available to investigated parties (ICC, 2010[2]) and merging parties.

10. For the purposes of this paper, 'case file' is the ensemble of evidence gathered by an agency in the context of competition proceedings. The case file of the agency may include:

- documents provided by or seized from the parties, such as leniency applications and supporting documents, replies to requests for information or documents obtained by the agency in the context of dawn raids;
- information provided by third parties, such as complaints and supporting documents or replies to requests for information;
- documents in the public domain;
- documents prepared by the relevant agency, such as statement of objections; and
- documents shared by other domestic or foreign agencies.

11. The Recommended Framework for International Best Practices in Competition Law Enforcement Proceedings of the International Chamber of Commerce[2] recommends that the file also includes, among others, the underlying data (including the source of that data) and methodology used to prepare charts, tables and other analysis.

12. The opportunity to access the case file –at least some of the documents it contains– is provided in both merger and non-merger matters. Access is particularly relevant where sanctions or remedies may be imposed (OECD, 2012[1]). In this regard, the Supreme Court of the United States (US) has pointed out that "[t]*he extent to which procedural due process must be afforded the recipient is influenced by the extent to which he may be condemned to suffer grievous loss*."[3]

13. Access to evidence in possession of the agency before an adverse decision is adopted is provided in both administrative and judicial systems. The extent of access, however, varies from one jurisdiction to another.

14. As the International Competition Network (ICN) points out in its Recommended Practices for Investigative Process,[4] the closer a process is to the adoption of the decision, the more transparency –and, hence, disclosure of evidence– there should be.

Box 1. Access to exculpatory evidence

The importance of providing access to exculpatory evidence was addressed by the Court of Justice of the European Union (EU) in the *Intel* case.

Following a complaint, the European Commission launched a round of investigations in 2004 and 2005 in Intel's premises and the premises of some of its customers. In 2009, the Commission found that Intel had abused its dominant position in the market for processors and decided to fine the company.

Intel challenged the decision adopted by the Commission before the General Court. Subsequently, it appealed the judgment of this court before the Court of Justice. In both proceedings, Intel claimed –among other things– that its rights of defence had been breached. In particular, the company argued that the Commission had held a meeting with one of the most senior executives of its largest customer (Dell), but Intel had not been provided with the transcript of the discussion. The company claimed that some of the evidence provided in that meeting could have been used as exculpatory evidence. Instead of the transcripts, the Commission had provided a non-confidential internal note with the

subjects addressed at the meeting (but not the content) and Dell's written answers to the oral questions asked to the interviewee during the meeting.

The Court of Justice considered that, based on the EU legal framework,[*] the Commission must record in full all interviews held for the purpose of collecting information relating to the subject matter of an investigation. The Court claimed that the internal note provided by the Commission was not sufficient, given that it did not contain "*any indication of the content of the discussions that took place during* [the interview]*, in particular as regards the nature of the information that* [the interviewee] *provided during that interview.*"

Despite the above, the Court considered that, in the case at stake, Intel's rights of defence had not been breached. Intel did not establish that the non-disclosure was able to influence, to its detriment, the course of the procedure and the content of the decision. In particular, it is for the company to establish, "*first, that it did not have access to certain exculpatory evidence and, secondly, that it could have used that evidence for its defence.*"

Intel had been granted access to Dell's written answers to the oral questions and, in the context of the challenge before the General Court, to the confidential version of the internal note of the meeting, which contained indications as to the content of the discussions. In spite of this, Intel did not adduce any evidence to suggest that the Commission had failed to record exculpatory evidence. Further, the company did not make use of the possibility to request that the interviewee be summoned before the General Court.

In view of the above, the Court decided to reject Intel's plea based on a possible breach of its rights of defence.

Source: Judgment of the Court of Justice of the EU in Case C-413/14 P Intel v Commission.
Notes: [*] Article 19(1) of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (EU Regulation 1/2003), and Article 3 of Commission Regulation (EC) No 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty (EU Regulation 773/2004).

15. The main objective of providing access to evidence in possession of the agency is protecting the rights of defence of the parties, providing interested parties with the possibility to rebut the facts on which the agency or the court relies to adopt the decision (Ginsburg and Owings, 2015[3]).[5] The concerned parties should be able "*to examine all the documents in the investigation file, which may be relevant for* [their] *defence.*" (Wils and Abbott, 2019, p. 10[4]) The right to access the case file complements the right to be heard (Kowalik-Bańczyk, 2015[5]).

16. A further objective of providing access to evidence, in this case to interested third parties, is making sure that they are aware of the basis on which decisions that may affect them are adopted.

17. Finally, the principle of open justice –and, more generally, transparency– is a reason to grant access to evidence to the general public (OECD, 2012[1]). Transparency assists stakeholders and the general public "*in understanding how the competition laws are administered*", and enhances public confidence in, and the credibility of, the competition agencies (First, Fox and Hemli, 2012, p. 46[6]).

2.2. Who accesses what?

18. The extent of the information that can be accessed depends on the type of party requesting access. Investigated parties in behavioural proceedings and merging parties are granted wider access than other interested parties and the general public.

2.2.1. Investigated parties and merging parties

19. Agencies must provide access to all the information on which an adverse decision may be based.

20. In some jurisdictions, investigated and merging parties are granted access to the case file as a whole, with limited exceptions. This is the case, for instance, of the EU[6], Spain, Portugal, and Hungary.[7]

21. The main exception to the general right to access the case file is the protection of confidential information. There are, however, other exceptions. Internal documents of the agency and correspondence with other agencies are not disclosed, for instance, in the EU and Hungary.[8]

22. In other jurisdictions, agencies do not provide access to the case file, but only disclose the specific documents that are relevant to establishing the infringement (OECD, 2012[1]). For instance, the Korean Fair Trade Commission (KFTC) attaches the relevant evidence to the proposed decision and shares it with the investigated party. The KFTC does not need to share with the investigated party either data irrelevant to establishing the facts or confidential information.[9] Similarly, the Japan Fair Trade Commission is obligated to disclose only evidence that is relevant to establishing the infringement.[10]

23. Similarly, the Competition and Markets Authority (CMA) typically provides "*copies of the documents that are directly referred to in the Statement of Objections*" and "*a schedule containing a detailed list of all the documents on the file.*" The parties then have the opportunity to inspect the documents on the schedule upon request.[11]

24. In the US, disclosure occurs under discovery rules in the course of judicial proceedings. According to the rules applicable to civil proceedings, access must be granted to "*all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses*," the identity of expert witnesses and their written reports, information allowing to identify the witnesses expected to be called, and the documents and exhibits expected to be introduced into evidence.[12]

25. The extent of access in the same jurisdiction might be different for criminal and civil or administrative proceedings. For instance, in criminal proceedings in the US, the Department of Justice (DoJ) needs to disclose "*any evidence favourable to an accused that is material to guilt or punishment as well as any evidence tending to impeach any potential witnesses. Moreover, the defendant has the right to inspect the government's case file*". The Antitrust Division Manual of the DoJ[13] requires broader disclosure than that required by the Supreme Court and the Federal Rules (Yoo and Wendland, 2019, p. 12[7]).

26. Depending on the jurisdiction and the circumstances of the case, information may be accessed in different ways. Information may be shared in electronic data storage units, such as USB sticks or DVDs; by email; as a hard copy of the document in the file and sent by mail; by inviting parties to examine the accessible file in the agency's premises; or through a virtual data room.

27. Regardless of the extent of access to evidence, there might be limitations concerning the use that can be made of the information. In the EU, documents obtained through access to the file in the context of behavioural proceedings can only be used by the investigated parties for the purposes of exercising their rights in these types of proceedings.[14] This includes not only challenging the decision adopted by the European Commission, but also using the documents in the context of related damages actions. As an exception, leniency corporate statements and settlement submissions can only be used for the exercise of the rights of defence in relation to the specific proceedings concerned.[15] In the case of mergers, documents can only be used for the purposes of the concerned proceedings (Wils and Abbott, 2019[4]).[16]

28. In Portugal, there are restrictions, specifically, as regards the use of confidential information. This type of information can only be used to exercise the rights of defence in the concerned proceedings and to challenge the decision before court.[17]

2.2.2. Other interested parties

29. For the purposes of this paper, other interested parties are subjects that have some sort of legal interest in the proceedings, such as complainants in behavioural proceedings or the company selling the target undertaking in merger proceedings.

30. In some jurisdictions, other interested parties are granted more limited access to the case file than investigated and merging parties are. For instance, in the EU, complainants do not have a general right to access the file as investigated and merging parties do. However, if the European Commission decides to initiate proceedings based on a complaint, it provides the complainant with a copy of the non-confidential version of the statement of objections (except in cases where the settlement procedure applies).[18] If the European Commission decides to reject the complaint, the complainant may request access to the documents on which the Commission bases its provisional assessment, in order to present its views on the preliminary decision. The complainant cannot have access to confidential information belonging to other parties involved in the proceedings, as opposed to investigated parties.[19]

31. In other jurisdictions, the extent of access granted to other interested parties is similar to the one for investigated and merging parties. This is the case, for instance, of Hungary, Portugal and Spain.[20] In these jurisdictions, parties need to show that they have a legitimate interest in the proceedings. However, as a rule, these parties do not have access to confidential information.

2.2.3. General public

32. The general public has very limited access to the evidence in the case file.

33. The main way the public can access information included in the case file is through the publication of agencies' and courts' decisions and their public statements. Agencies and courts typically redact confidential information from the documents they publish (see Box 9).

34. Some jurisdictions, such as Hungary, allow access to the case file to all third parties –not only interested third parties– once the proceedings have been closed. However, access may be refused if disclosure of such documents would jeopardise the activity of the agency.[21]

35. Third parties may also attempt to access documents in the case file under general transparency rules. Information accessed on the basis of general transparency rules and information included in public decisions and public statements enter the public domain and may be used for any purpose.

Box 2. Access to the case file under transparency rules

Like many other jurisdictions, Canada, the US, and the EU have general transparency rules. These rules allow, with certain limits, that natural and legal persons access the documents held by the public institutions and agencies. Transparency rules aim to enhance the transparency and accountability of the public administration.

In Canada, the Access to Information Act establishes that, as a rule, Canadian citizens have the "*right to and shall, on request, be given access to any record under the control of a government institution.*" Similarly, in the US, the Freedom of Information Act provides the public "*the right to request access to records from any Federal Agency*." Finally, EU Regulation 1049/2001[1] establishes a general right to "*access the documents of the* [EU] *institutions.*"

In all three jurisdictions, however, this general right comes with exemptions, which protect other interests such as personal privacy, national security or law enforcement. These exemptions generally cover all the information contained in competition agency's files or, at least, the confidential information therein.

In Canada, the Access to Information Act provides that certain records of the Competition Bureau pertaining to proceedings are not to be disclosed. Crucially, this exemption covers "*all third party confidential information contained in Bureau records.*"[2]

In the US, the Freedom of Information Act establishes nine exemptions to the general obligation to disclose agencies' records. Importantly, one of these exemptions covers trade secrets, and commercial or financial information obtained from a person that is confidential or privileged. Further, agencies do not need to disclose materials obtained through civil investigative demands (such as documents, interrogatory responses, and transcripts of oral testimony) or materials obtained as part of the merger process.[3]

In the EU, the European Commission has so far denied access to information pertaining to competition proceedings on the basis that the documents in the case file are not to be disclosed. However, it cannot be ruled out that, under certain arguments (such as an overriding public interest) the disclosure is justified (Wils and Abbott, 2019[4]).

Notes:
[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, in the EU.
[2] Information Bulletin on the Communication of Confidential Information Under the Competition Act of the Canadian Competition Bureau (Bureau's Bulletin), paragraph 7.5.1. The Bureau's Bulletin is available here: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/cb-bulletin-confidential-info-2013-e.pdf/$file/cb-bulletin-confidential-info-2013-e.pdf.
[3] DoJ's Antitrust Division Manual, Chapter VII, page 43.

2.3. When can the evidence be accessed?

36. The moment at which the evidence can be accessed typically differs across jurisdictions. In general terms, it is important that access to evidence is provided following

the issuance by the agency of the document outlining its allegations, if this has not been done before. A discussion of the relevant facts and evidence early on can allow the parties and the agency to focus on the most relevant issues (ICN, 2019[8]). It may, for instance, allow for the early closure of the proceedings through the adoption of commitments. However, the extent of the information shared at each moment needs to be carefully considered to avoid putting the investigation at risk (ICN, 2014[9]).

37. In practice, in administrative systems, access to the case file is typically granted during the investigative stage. The specific moment at which access is granted, however, varies. Italy and – in the case of infringement proceedings – Spain grant access to the file throughout the whole investigation stage, starting from the formal initiation of the proceedings.[22] This means that parties have access to the case file even before the issuance of the statement of objections.

38. However, other jurisdictions only allow parties to access the file after a certain stage and for a limited time. For instance, in the United Kingdom (UK), the CMA's file can only be inspected following the notification of the statement of objections. The time given to addressees to inspect the file depends on factors like the size of the file and the nature of the documents.[23] As an exception, in the case of settlement proceedings, parties may have access to the "*documents on which the CMA is relying as well as a list of the documents on the CMA's file*" before the issuance of the statement of objections. Access to additional documents can be requested, but the request will influence the CMA's assessment on whether the settlement achieves procedural efficiencies and, hence, is suitable.[24]

39. Similarly, the European Commission also grants access to the case file following the issuance of the statement of objections and does so during a limited period. Access may be granted again if new incriminating or exculpatory evidence is included in the case file.[25] In the case of settlement proceedings, the Commission may disclose certain documents – generally of incriminating nature – before the adoption of the statement of objections.[26]

40. In Hungary, access to the case file is not granted until the investigatory phase has finished and the agency has adopted a preliminary position. As an exception, parties are granted access to documents that are essential to exercise their rights of defence against an injunction. Further, upon the parties' request, the agency has discretion to grant access to documents when it deems that this will not jeopardise the effectiveness of the proceedings.[27]

41. In judicial systems, disclosure of evidence typically takes place at the litigation stage before the decision is adopted by the court. In the US, in the context of court proceedings with the Federal Trade Commission (FTC), investigated parties obtain discovery from the agency and third parties following the issuance of an initial complaint laying down the charges (ICC, 2010[2]).

42. In these systems, access to the evidence in the case file during the investigation stage is typically limited. For instance, in Canada, there is no right to inspect the records of the authority. As an exception, companies are able to examine the information they have provided to the Bureau.[28]

Box 3. Access to the case file in commitments procedures

An important question in the context of access to the case file is whether the parties involved in commitment procedures should enjoy the same degree of due process and procedural safeguards as in the context of infringement decisions (OECD, 2016[10]).

There is a tension between the objective of speedier procedures –which is achieved, among others, by restricting access to the case file– and full due process protection. Some competition authorities have stressed the significance of granting the parties full and adequate access to the case file within the authority, while others have indicated that these would lessen the efficiency gains and should be required in adversary infringement procedures only (OECD, 2016[11]).

By way of example, the right of access to the file is only partly granted in France. In commitments procedures, the *Autorité de la Concurrence* is only required to share with the party its preliminary assessment of the case and the comments submitted by third parties in the context of the market test of the commitments. If the party that accepted the commitments seeks to annul the decision, it is for the courts to determine whether the lack of disclosure of certain elements harmed its interests.[1]

The limitation of the right to access the file (in combination with the large degree of discretion of some agencies) may lead to disadvantageous commitments for the company involved. This can be the case for agencies that are only under an obligation to make known their preliminary concerns, but not to fully disclose the evidence they have in the file. Commitment negotiations may therefore take place in an asymmetric context where the company has only a partial view of the agency's case. This may not be problematic in straightforward cases, but might result in overreaching commitments if the facts of the case are complex or disputable (OECD, 2016[10]).

Notes:
[1] Notice on procedure of 2 March 2009 on commitments in competition proceedings (*Communiqué de procédure du 2 mars 2009 relatif aux engagements en matière de concurrence*), paragraphs 27 and 28. Available here: http://www.autoritedelaconcurrence.fr/doc/cpro_autorite_2mars2009_engagements_antitrust.pdf.

3. Protection of confidential information

3.1. Overview

43. The right to access evidence in the case file is not without limits. It must be balanced against the need to protect confidential information in the file. There are a number of reasons that justify this. First, competition agencies need to foster a reputation for respecting confidentiality of the information they receive to ensure the continued supply of information from parties and third parties (OECD, 2012[1]). This reputation may also encourage other agencies (domestic or foreign) to share confidential information in parallel cases, if this is appropriate and allowed under the applicable legislation. Secondly, agencies should ensure that undertakings do not have access to confidential information of other companies when accessing the case file to the extent possible. Disclosing this information may harm information providers, for instance, by exposing their commercial strategy or

personal details. Disclosing confidential information may also harm competition by facilitating co-ordination.

44. The need to protect confidential information is a principle accepted by the vast majority of jurisdictions and is included in many relevant recommendations by international organisations.[29] Most jurisdictions have statutory provisions on the protection of confidential information obtained during investigations. There seem to be no significant differences between administrative and judicial systems in the protection of confidential information (ICN, 2014[9]).[30]

45. Confidential information should not be made public, in principle. However, the disclosure of confidential information is possible under exceptional circumstances; for instance, when disclosure is necessary to ensure the rights of defence or, more rarely, in the context of international co-operation among agencies.

46. When assessing whether potentially confidential information should be disclosed, agencies and courts typically use the following two-step process. First, they establish whether the information in question is confidential under the applicable law. Second, they determine whether, on balance, disclosure to a party other than the provider should nevertheless be made (OECD, 2012[1]). The specific factors used to decide whether confidential information should be disclosed are addressed in Section 3.4.

47. It is important that jurisdictions publish the applicable rules and practices for the protection of confidential information (for instance, as guidelines). Many jurisdictions do so, often through the agency website (e.g. Canada, Greece, the EU, the UK, and the US). The rules and practices should include what information is considered confidential, how confidential treatment should be requested, how the agency or court assesses requests for confidential treatment or disclosure, and how to challenge relevant decisions. This can contribute to reduce the workload that can result from the excessive designation of information as confidential, a practice in which parties have a natural tendency to engage (OECD, 2012[1]).

3.2. What is confidential information?

48. Despite the widespread protection of confidential information, few jurisdictions have a statutory definition of what confidential information is. On many occasions, this concept has been given meaning through agency practice and case law (OECD, 2012[1]). Some jurisdictions use the definition set in other legal frameworks, like definitions in civil or criminal law, or other jurisdictions, like the EU national agencies that use the European Commission's guidance.

49. According to the OECD Secretariat Report on the OECD/ICN Survey on International Enforcement Co-operation,[31] jurisdictions define information as 'confidential' according to one or more of the following criteria:

- The nature and type of the information. For these purposes, jurisdictions typically look at whether disclosure would harm the commercial interests of the source that provided it. Some jurisdictions also examine whether disclosure would: affect future supply of information; jeopardize an investigation; or be contrary to the public interest. Information in the public domain is not confidential.

Box 4. Specific types of information that are considered confidential

An analysis of the applicable legal frameworks and practices across jurisdictions provides a sense of what type of information may be deemed confidential (OECD, 2012[1]):

- Business secrets and other commercially sensitive information are universally recognised by competition agencies as constituting confidential information. This typically covers price information, commercial know-how, production quantities, market shares and commercial strategies of undertakings.
- Sensitive personal information, such as private telephone numbers and addresses, medical or employment records, is typically considered confidential as well. Agencies may obtain this type of information in the context of competition proceedings. In the EU, the European Data Protection Supervisor has confirmed that the EU General Data Protection Regulation[1] does not prevent the submission of information –voluntarily or in response to a legal obligation– containing personal data to the European Commission in the context of competition matters.[2] In many jurisdictions, general data protection rules regarding the disclosure of this type of information already exist.
- Some jurisdictions deem as confidential information that, if disclosed, could expose the submitting party to retaliation from other market participants. For instance, the EU considers confidential the information submitted by an undertaking which might negatively affect its supplier.[3] In these cases, it is often not the information itself, but the identity of the information provider that requires protection.
- Other types of information considered confidential include information concerning the public interest (e.g. national security) or information which cannot be disclosed due to international law obligations (e.g. information exchanged by agencies). The CMA may consider confidential "*information whose disclosure* [it] *thinks is contrary to the public interest.*"[4]

Notes:
[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[2] The letter of the European Data Protection Supervisor is available here: https://edps.europa.eu/sites/edp/files/publication/18-10-30_letter_investigative_activities_eui_gdpr_en.pdf.
[3] European Commission's Guidance on confidentiality claims during Commission antitrust investigation (Commission's Guidance on Confidentiality), paragraph 10. Available here: https://ec.europa.eu/competition/antitrust/business_secrets_en.pdf.
[4] Transparency and disclosure: Statement of the CMA's policy and approach, paragraph 4.14. The document is available here: https://www.gov.uk/government/publications/transparency-and-disclosure-statement-of-the-cmas-policy-and-approach.

- The way in which the information is collected. Some jurisdictions consider confidential any information obtained by the agency in the course of the performance of its official duties and functions. Others deem confidential only information obtained by power of compulsion, or by other agencies. For instance, in the US, information obtained through civil investigative demands (CIDs, tools that can compel the production of documents, written responses and oral testimony) is considered confidential and can only be disclosed under specific circumstances.

In general, information obtained by the DoJ through CIDs "*cannot be disclosed to state, foreign, or other Federal agencies (except for the FTC), nor can* [it] *be disclosed during the course of interviews with other parties, without the consent of the producing party.*" Conversely, information provided in the context of voluntary information requests is not protected in the same way.[32]

- The purpose for which the information was collected or submitted, so that information collected or submitted for a particular defined purpose will be protected as confidential. For instance, in Spain, consultations with companies prior to the notification of a merger are considered confidential.[33]
- The way the parties define it, so that any information that the source has defined as such is considered confidential.

50. Apart from the above, many jurisdictions also consider whether parties have shared the information with the agency in confidence or –if the information has been seized by the agency–whether the data is secret (OECD, 2012[1]).

51. A relevant factor to assess the confidentiality of information is the age of the data. For instance, in the EU, commercial information that is five years old or more is in principle not confidential.[34] In the UK, financial information or other data relating to a business which is more than two years old is unlikely to be considered confidential.[35]

52. Information may be considered confidential regardless of the party that provides it (e.g. investigated party, third party).

53. Confidential information should be distinguished from legally privileged information. Legal professional privilege refers to the protection of confidential communications between clients and their legal advisors from forced disclosure to domestic or foreign public bodies and third parties (OECD, 2018[12]). Legally privileged information is, thus, protected also as regards the agency or court,[36] and not only as regards other parties accessing the case file and the general public. Hence, agencies and courts have access to confidential information, but do not have access to legally privileged information. If privileged information is unlawfully collected, it should be excluded from the case, not used as evidence, and returned to the party (OECD, 2018[12]).

54. Confidential information must also be distinguished from merely non-public information. The OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings (the Recommendation on International Co-operation)[37] refers to information that the agency "*does not routinely disclose and for which there is no statutory prohibition or restriction on disclosure, and which does not specifically identify confidential information of individual enterprises.*" Similarly, in the US, the DoJ and the FTC refer to 'agency non-public information', which they define as "*information that the* [a]*gencies are not statutorily prohibited from disclosing, but normally treat as non-public*." In the US, non-public information includes "*staff views on market definition, competitive effects, and remedies.*"[38]

3.3. How is confidential information identified and protected?

55. In most jurisdictions, parties (including parties from which information has been seized) need to identify the confidential information in the documents they provide and provide non-confidential versions of such documents (OECD, 2012[1]). This is the case, for instance, of the EU, Spain, and the UK.

56. Generally, submitting parties are required to provide explanations such as the nature of the information, the harm that could be caused if the information were disclosed, and the likelihood of this harm. These parties may also be requested to briefly describe the information in order to allow parties accessing the file to assess whether the information treated as confidential is relevant for their defence.

57. Early bilateral discussions between parties and authorities can enable a quicker agreement on what information should be considered confidential (OECD, 2012[1]).

58. Where parties fail to identify the confidential information, the agency may assume that no confidentiality is claimed. This is the case, for instance, of the UK if parties do not indicate to the CMA that information is confidential.[39] It is also the case in Portugal and Hungary.[40] However, even in cases where parties fail to claim confidentiality, agencies may need to consider granting confidential treatment to particularly sensitive information (e.g. recent prices or future strategies) to avoid anti-competitive outcomes resulting from the disclosure (e.g. price alignment).

59. In some instances, the agency may also carry out an initial *ex officio* assessment of the confidentiality of the information (OECD, 2012[1]). In Chile, confidential treatment can be granted by the *Fiscalía Nacional Económica* both at the request of the parties or *ex officio*.[41] In some jurisdictions, all the information submitted in the course of an investigation is considered confidential (OECD, 2018[13]). For instance, in the US, as a rule, materials provided to the DoJ or the FTC in the context of merger control are treated as confidential.[42]

60. Many jurisdictions provisionally accept confidentiality claims and, where appropriate, decide whether to deny the claim at a later stage in the context of a request for access or when the information is to be disclosed for another reason (ICN, 2014[9]).

61. Once a confidentiality claim has been made, the decision on whether confidential treatment should be granted is often taken, in administrative systems, by the agency officials involved in the case. Some agencies allow that parties contest the decision of these officials before an independent body within the agency. For instance, in the EU, the Hearing Officer –independent from the enforcer in their decision-making– decides on disputes between the parties to the proceedings, the parties providing the information and the case team. Similarly, in the UK, if parties disagree with what has been decided by the case team, they may refer the case to the CMA's Procedural Officer.

62. At the litigation stage, courts typically have the discretion to determine whether confidential treatment should be granted.

63. Generally, there is an obligation on all those having access to the evidence throughout the proceedings to not reveal the information. This includes agency officials, but also any other party to whom confidential information has been disclosed. The Spanish Competition Law, for instance, prohibits that any of these subjects reveal the confidential information they access in the context of proceedings.[43]

64. The Recommendation on International Co-operation advises that an adequate sanctions system be in place for breaches of the confidentiality provisions. Many jurisdictions have measures in place to investigate and punish unlawful disclosure or improper handling of confidential information (ICN, 2014[9]).

65. Many agencies develop internal rules dealing with how to handle confidential information. If information is unduly revealed, some agencies have procedures to investigate it. Depending on the jurisdiction, investigation may be carried out internally by

the agency or externally by another entity such as a prosecutor. The punishment for improper disclosure may be imposed by the agency itself or by a court and may consist in criminal fines or disciplinary procedures, including the dismissal of the employee (ICN, 2014[9]).

66. Revelation of information by parties who have accessed information in the case file should also be discouraged. As mentioned above, in Spain, the duty of secrecy covers all persons having access to the file (including the agency's staff, but also the parties). The breach of this duty may result in civil and criminal liability and can constitute a serious disciplinary offence.[44] In the UK, the CMA's Guidance on Procedure points out that disclosure of information accessed by way of a confidentiality ring or data room is a criminal offence, punishable by fine and/or imprisonment.[45]

3.4. Exceptions to the non-disclosure of confidential information

3.4.1. When and on which basis

67. The fact that information is confidential means that, in principle, it will not be disclosed. Still, disclosure may take place in a number of circumstances. Generally, disclosure is allowed (i) to the parties in the context of the proceedings (Section 3.4.2), (ii) for co-operation purposes with other agencies (Section 3.4.3), or (iii) in relation to damages actions concerning a competition infringement (Section 3.4.4).

68. Disclosure of confidential information may be ordered by the agency or the court, as a discretionary decision. It may also happen with the consent of the submitting party, as is often the case in merger control proceedings with a cross-border aspect. Exceptionally, the legal framework may require that agencies disclose confidential information. For instance, the DoJ must disclose evidence to the US Congress when requested to do so. When such a request is made, however, the DoJ "*tries to respond to congressional inquiries in a manner that does not disclose* [confidential] *information.*"[46]

3.4.2. To parties in the process

General framework

69. Investigated parties and merging parties may be granted access to confidential information in order to guarantee their rights of defence. Other interested parties do not typically have access to confidential information, as explained in Section 2.2.

70. Most jurisdictions do not allow for the disclosure of confidential information during the investigative phase, with limited exceptions when this is necessary to ensure the rights of defence. Disclosure becomes more common –and may be necessary to ensure the rights of defence– during the course of the enforcement proceedings.

71. Agencies may consider *ex officio* that the disclosure of confidential information is necessary for enforcement purposes (e.g. to prove an infringement). Further, investigated and merging parties may be allowed to request disclosure. These parties may claim that the information at stake is not confidential or argue that their rights of defence will be breached if the information is not disclosed or that general procedural fairness or natural justice justify disclosure. The decision may be adopted internally by the agency (directly by the team dealing with the case or by an independent body) or by a court (ICN, 2014[9]).

72. In Greece, the President of the agency, following a request, can grant access in whole or in part to documents containing confidential information. These documents are

disclosed only to the person for whom the access has been considered as necessary. At a litigation stage, courts can also disclose confidential information if this is deemed necessary in order to protect an overriding interest. Where that is the case, the adjudicating court grants permission to access to the necessary extent, at the party's request (OECD, 2018[14]).

73. In many jurisdictions, the authorities will notify submitters when they contemplate disclosing confidential information either because there is a legal requirement to inform them or as a common practice. In the UK, the CMA generally seeks to inform the party claiming confidentiality or the party to whom the information relates of its intention to make a disclosure.[47] In the US, the DoJ points out that, "[i]*n appropriate circumstances, staff may agree to provide defendants with notice of the intention to disclose such documents to third parties.* […] *The agreement should be drafted to avoid committing the Division to procedures that would significantly affect the use of such information at trial or in pretrial depositions with third parties that are important to the Government's case.*"[48]

74. In other jurisdictions, the notice is given after the information has been disclosed or no notice is given at all. For instance, in Canada, the agency does not typically provide notice of intent to disclose confidential information in the context of competition proceedings, as this is considered to unreasonably hinder the investigative process.[49]

75. The factors that agencies and courts consider when deciding whether confidential information should be disclosed include (OECD, 2012[1]):

- The degree of harm that could be caused to the submitting party and the person to which the information relates.
- The value of this information as inculpating or exculpatory evidence.
- The availability of alternative non-confidential documents that can be used to prove or disprove the alleged infringement.
- And the availability of methods to desensitise information without undermining its value, such as non-confidential summaries (see below).

76. The key factor in most jurisdictions is the administration of justice, i.e., the ability of agencies to prosecute and the ability of the accused to defend themselves (OECD, 2012[1]). For instance, the Canadian Competition Bureau does not disclose confidential information in proceedings before the Competition Tribunal or the courts unless the non-disclosure hinders the administration or enforcement of the competition act. In addition, the Bureau considers alternatives to outright disclosure such as the use of mechanisms to protect confidential information.[50]

Box 5. Access to leniency documents

Most jurisdictions have rules in place to protect the identity of leniency applicants and the confidentiality of materials associated to the leniency application. These rules aim to ensure the effectiveness of the leniency programme. They are sometimes so broad that all of the documents and information submitted by a leniency applicant may be undisclosable, not just information of a confidential nature (OECD, 2015[15]).

Korea has rules that, in principle, prevent the disclosure to third parties of the identity of the leniency applicant and of any information and materials submitted under the leniency programme. Exceptionally, the KFTC may disclose the identity and/or material submitted

by the leniency applicant to other persons if either the leniency applicant agrees or if the information is necessary to file a lawsuit in relation to the case concerned (OECD, 2015[15]).

In the EU, access to leniency corporate statements is only granted at the premises of the Commission. The parties and their counsel are not allowed to copy the statement by any mechanical or electronic means.[1] Finally, in relation to private enforcement, the EU has exempted leniency statements –including verbatim quotations– from disclosure of evidence (see section 3.4.4).

Canada, as a rule, grants confidential treatment to the information received by a party requesting leniency. Disclosure is allowed, however, when necessary for the purpose of the administration or enforcement of the Competition Act and in other limited circumstances, including where it is required by law, where the party agrees to disclosure or has disclosed the information itself, or when disclosure is necessary to secure assistance of other Canadian law enforcement agencies or to obtain or maintain the validity of a judicial authorisation. Further, the Bureau does not disclose the information to any foreign law enforcement agency without the consent of the applicant or unless this is required by law. Finally, with respect to private enforcement, the Bureau only provides confidential information in response to court orders and commits to take "*all reasonable steps to protect the confidentiality of the information.*"[2]

In the US, the DoJ has a strict confidentiality policy concerning the disclosure of the identity of leniency applicants and the information obtained from them. The DoJ only discloses this information when the applicant has previously made such a disclosure, or when it is authorised to make such a disclosure by the applicant or by court order.[3]

Notes:
[1] Article 15(1b) of the EU Regulation 773/2004.
[2] Bureau's Bulletin, paragraphs 7.1.2 to 7.1.5.
[3] DoJ's Antitrust Division Manual, Chapter III, page 102.

77. In most jurisdictions, submitting parties have the right to appeal the decision allowing for the disclosure of information. This may result from the fact that the agency or court having adopted the original decision did not consider the information to be confidential or that, despite being confidential, it should nevertheless be disclosed. It is important that when confidential treatment is denied the agency or court justify their decision to ensure that parties can appeal the decision.

78. Some jurisdictions require that challenges be brought directly before a court (ICN, 2014[9]). Others allow or require the party to question the confidential treatment before the agency first.

79. Parties opposing disclosure may apply for interim measures to avoid disclosure while the challenge is being reviewed. In the EU, the application for interim measures requires, first, that the applicant alleges that "*the information whose publication he wishes provisionally to prevent constitutes business secrets*" and, secondly, that the allegation "*satisfies the condition that there is a prima facie case*", so that the judge can start from the premise that the information is confidential.[51]

Mechanisms to disclose to parties documents containing confidential information

80. Jurisdictions typically have mechanisms to protect confidential information, while ensuring that parties have access to the documents that are relevant for the purposes of their

defence. Parties may be able to request the use of a particular mechanism, such as confidentiality rings or data rooms. The factors to be considered when deciding which mechanism to use include: the nature and degree of sensitivity of the information (e.g. prices, customer names); the extent of the requested disclosure (i.e. the number of documents to be disclosed); the relationship between the parties (e.g. whether the disclosing party is a direct competitor of the party requesting access); the circle of individuals allowed to access the information (e.g. external legal counsel only); and the risk of inadvertent disclosure (European Commission, 2019[16]).[52] Some of these factors –namely, the nature and degree of sensitivity of the information and the relationship of the parties– can be used both to determine whether information is confidential and, if so, how it should be disclosed (e.g. using non-confidential versions or confidentiality rings).

81. As mentioned below, on some occasions, confidential information is not shared at all and only the non-confidential parts of the documents are shared. On other occasions, confidential information is shared but the disclosure is limited, for instance, to external counsel only.

82. Below the main mechanisms used to disclose confidential information to parties are provided.

Non-confidential versions

83. The most widespread mechanisms consist in the preparation of a non-confidential version of the document from which all confidential information is deleted. Typically, the submitting party is requested to provide the redacted version, but in some jurisdictions the preliminary assessment is carried out by the agency itself (OECD, 2012[17]). Depending on the jurisdiction and the circumstances, confidential information may need to be blacked-out, or replaced with anonymised data or aggregate figures.

84. Many jurisdictions keep two sets of files, one confidential (with the original documents) and the other one non-confidential (with the redacted documents). This is the case, for instance, of Spain and Greece. Other jurisdictions act on a case-by case basis (e.g. by "*taking out pages*" when access to file is requested) (ICN, 2014[9]). Some jurisdictions provide a brief description of the confidential documents to help identify the information that was removed.

85. Similarly, many agencies produce two versions of decisions and provide different versions of statements of objections to parties and third parties, redacting confidential information as appropriate. Likewise, in some judicial systems some parts of the final judgment may remain confidential. The preparation of non-confidential versions of decisions and judgments can be burdensome in terms of time and resources. These non-confidential versions can be relevant for the purposes of private enforcement (see Box 9).

Confidential summaries

86. Some jurisdictions grant access to documents containing confidential information by allowing for the preparation of non-confidential summaries. This is the case, for instance, of France, where these non-confidential summaries accompany and complement the non-confidential versions of documents.[53] Depending on the jurisdiction and the circumstances, summaries may be prepared by the parties themselves or by an expert.

87. The use of an expert to prepare a summary is appropriate when the information is "*commercially very sensitive and quantitative or technical in nature.*" In this case, the expert may prepare a confidential summary to be shared with the external counsel of the

requesting party and/or a non-confidential version to be shared with the requesting party. (European Commission, 2019, p. 17[16]).

Confidentiality rings

88. A number of jurisdictions use confidentiality rings, including the EU and the UK. This method can be described as "*a form of restricted disclosure by which a party entitled to access to the file arranges,* [with a submitting party]*, that that information be received on party's behalf by a restricted circle of persons (typically decided by negotiation on a case-by-case basis)*" (Wils and Abbott, 2019, p. 44[4]). Hence, this method allows for the disclosure of confidential information, but does so under a tight control. It is possible that different access rights are granted to different persons (European Commission, 2019[16]). For instance, external counsel may be granted wider access than in-house counsel.

89. Confidentiality rings can be used as a 'filtering mechanism' which allows persons having access to large sets of confidential information request a non-confidential version of the relevant documents. They may also allow external counsel to obtain further understanding of the case and prepare confidential submissions for the clients, without the need of preparing non-confidential versions.[54] In the latter case, special arrangements may be sought to protect the confidential nature of the information from disclosure to the addressee of the proceedings and others in the reply to statement of objections and the potential hearing, as well as any possible subsequent court submissions.[55]

90. Some systems limit disclosure of confidential information to outside counsel and experts, thus excluding in-house counsel and business employees of the party having access to the data (ICN, 2014[9]). In the UK, the group of persons to which information is disclosed "*is determined on a case-by-case basis but, generally, disclosure is made to the relevant parties' external (legal and/or economic) advisers.*"[56]

Data rooms

91. A few jurisdictions, such as the EU and the UK, also use data rooms. Data rooms can be described as "*a form of restricted disclosure by which material is disclosed to a limited number of specified advisers for a limited period of time in a secure room*", "*subject to a number of restrictions and safeguards designed to prevent confidential information being disclosed beyond* [the data room]" (Wils and Abbott, 2019, pp. 42, 43[4]) Data rooms, therefore, provide enhanced security measures compared to confidentiality rings and may be used where information is considered particularly confidential.[57]

92. Data rooms are generally used for the disclosure of quantitative data relevant for econometric analysis. The advisers having access to the data room generally are external legal counsel and economic advisers. These advisers may need to sign undertakings committing not to disclose the confidential information to which they have access. The European Commission, for instance, requires that they sign a no-disclosure agreement prior to getting access to the data room.[58] The advisers generally prepare a 'data room report', in non-confidential terms, for the party concerned (Wils and Abbott, 2019[4]).

Box 6. Disclosure of documents containing confidential information

In 2014, the CMA issued a document on its policy and approach on transparency and disclosure. This document provides a good example of how agencies may deal with the different mechanisms they have available. It considers the shortcomings of confidentiality rings and data rooms and clarifies that the CMA considers their use on a case-by-case basis. An excerpt of this document is provided below:

> *"When the CMA considers it appropriate to disclose information it will consider how best to protect confidential information. For example, the CMA may redact, anonymise or aggregate confidential information, such as by providing ranges in relation to market share data.*
>
> *Sometimes, the CMA may use confidentiality rings or data rooms as a means of making disclosure of confidential information while recognising the restrictive nature of the disclosure […]. Their use will be restricted to when it is necessary to make the disclosure for the purpose of facilitating the CMA's functions by ensuring due process although in [competition] investigations, the CMA may also use confidentiality rings at access to file stage to handle the disclosure of confidential information where there appear to be identifiable benefits in doing so.*
>
> *[…]*
>
> *Requests for the use of confidentiality rings and data rooms will be considered on a case-by-case basis. The CMA has discretion as to whether to agree to such requests, and is likely to do so only where it is proportionate, there are clear benefits in doing so, and potential legal and practical difficulties can be resolved swiftly in agreement with the parties concerned. The CMA will also take into account whether it is appropriate to provide access at the time the request is made, having regard to the progress of the case, the resource implications of operating confidentiality rings and data rooms, and of risks of human error and information leaks."*

Source: Transparency and disclosure: Statement of the CMA's policy and approach, Paragraphs 4.28 to 4.34.

Closed hearings

93. Courts and agencies may also restrict the persons that can attend hearings (e.g. external counsel only) in order to protect confidential information. Closed hearings can be useful to cross-examine confidential information disclosed through a confidentiality ring (European Commission, 2019[16]). In some jurisdictions, parties must demonstrate the harm that might occur absent the closed hearing (ICN, 2014[9]).

94. Alternatively, jurisdictions may allow for public hearings, but restrict the information that can be discussed (European Commission, 2019[16]). Otherwise, they may opt to exclude from the public record references to confidential information. The legal framework of the US, for instance, provides for the *in camera* treatment of documents and testimony under certain circumstances. In particular, Administrative Law Judges, when handling FTC cases, can keep "*documents and testimony confidential and not part of the public record of the hearing.*" This is possible when the public disclosure of this evidence would "*likely result in a clearly defined, serious injury to the person, partnership or corporation requesting their in camera treatment; only respondents, their counsel,*

authorized Commission personnel, and court personnel concerned with judicial review shall have access thereto." The court order shall provide the date on which *in camera* treatment will expire. [59]

95. These mechanisms should be used carefully, as they limit the "*vital public interest in open judicial proceedings.*"[60]

3.4.3. To domestic and foreign agencies

General framework

96. Many jurisdictions allow for the disclosure of confidential information to other domestic government agencies in their jurisdictions. Typically, disclosure is made to tax authorities and criminal prosecutors, but it may also occur with other agencies. For instance, in Canada, the Competition Bureau may disclose confidential information "*to any federal or provincial authority that enforces acts or regulations that provide for criminal, civil or administrative sanctions.*" The authority to do so is discretionary and, as rule, the Bureau only discloses information under specific circumstances, including when a domestic agency "*has expressly requested confidential information for the purpose of carrying out its mandate.*" The Bureau communicates confidential information "*only after it is satisfied that the receiving agency will respect the confidentiality of the information to be communicated.*" [61]

97. Other jurisdictions are more reluctant to disclose confidential information. For instance, the US DoJ does not, in general, disclose "*documents, answers to interrogatories, and transcripts of oral testimony*" obtained pursuant to a CID to state or other Federal agencies (except for the FTC).[62]

98. Disclosure of information to other domestic government authorities does not generally require providing notice to the submitting party (ICN, 2014[9]). Authorities may still attempt to minimise the amount of confidential information that is shared and require that the receiving authority respects the confidentiality of the information.

99. Disclosure to foreign competition agencies is also possible in many jurisdictions. The Recommendation on International Co-operation advises that exchange of information be undertaken on a case-by-case basis and cover only the information that is relevant to the proceedings at stake. Jurisdictions should clarify the requirements with which both the transmitting and receiving jurisdiction have to comply in order to allow for information sharing. The agency requesting the information should explain the purpose for which the information is sought and commit to limit its use or further dissemination, unless the transmitting agency has explicitly granted prior approval. The transmitting agency should retain full discretion when deciding whether to transmit the information and the ability to choose to provide it subject to restrictions on use or disclosure.[63]

100. As regards the disclosure of information that is not public, the Recommendation on International Co-operation distinguishes between two situations: (i) information that the agency does not routinely disclose but which does not comprise information that is considered –strictly speaking– confidential information; and (ii) confidential information.

101. As regards the former, the agency may disclose the information, but choose to impose conditions restricting further dissemination, without the transmitting agency's consent. As regards the latter, information should only be shared when public information and non-confidential information is not sufficient for effective co-operation in a matter.

102. The Recommendation on International Co-operation encourages agencies to consider, among others, the following factors when deciding whether to share confidential information:

- The nature and seriousness of the matter, the affected interests of the receiving jurisdiction, and whether the investigation or proceeding is likely to adequately safeguard the procedural rights of the parties concerned.
- Whether the disclosure is relevant to the receiving agency's investigation or proceeding.
- Whether the receiving jurisdiction grants reciprocal treatment.
- Whether the information can be used by the receiving jurisdiction in a criminal proceeding.
- Whether the level of protection granted by the receiving agency would be at least equivalent to the confidentiality protection in the transmitting jurisdiction (including considerations on electronic protection or whether access to the information is granted on a need-to-know basis). Special care should be taken when considering whether to transmit particularly confidential information, such as pricing plans.

103. Where agencies have discretion over whether to share confidential information, the risks of doing so should be carefully considered prior to any disclosure. Apart from the risk of leakage, third parties in the receiving jurisdiction may request that information received from foreign agencies be disclosed. The reputation that the agency has built as regards the protection of confidential information can be relevant for other agencies to decide whether to share information or not. The OECD Recommendation on Merger Review[64] and the Recommendation on International Co-operation encourage countries to establish safeguards concerning the treatment of confidential information obtained from another competition authority.

Box 7. Disclosure of confidential information to foreign agencies by the Canadian Competition Bureau

Agencies can greatly benefit from exchanging information when assessing mergers and conducting behavioural investigations with a cross-border aspect. This is recognised by many agencies, including the Canadian Competition Bureau.

The Bureau's Bulletin on the Communication of Confidential Information outlines the agency's approach when sharing confidential information with other agencies, either on its own initiative or on that of the foreign agencies. An excerpt of this document is provided below:

"[T]he Bureau is committed to enhancing the effectiveness of Canadian enforcement efforts through cooperation with foreign authorities enforcing similar legislation. In conducting these cooperative activities, the Bureau may need to communicate confidential information to a foreign authority, either on its own initiative or on that of the foreign authority. The decision to communicate confidential information to foreign authorities is not taken lightly.

[…]

> *In all cases where confidential information is communicated to a foreign authority, the Bureau seeks to maintain the confidentiality of the information through either formal international instruments or assurances from the foreign authority. The Bureau also requires that use of the confidential information by the foreign authority be limited to the specific purposes for which it is provided.*
>
> *[…]*
>
> *In assessing whether to communicate confidential information in [cases requiring international co-operation], the Bureau will consider the laws protecting confidentiality in the requesting country, the purpose of the request, and any agreements or arrangements with the country or the requesting authority. If the Bureau is not satisfied that the information will remain protected or be used only for its intended purpose, the information will not be communicated."*
>
> Similarly, when the Bureau receives the information, it is prepared to provide assurances that the information will be treated confidentially and used for the purposes of competition enforcement. Before using the information for any other purpose, the Bureau commits to seek consent from the foreign authority.
>
> *Source*: Bureau's Bulletin, section 4.2.2.

Basis for disclosing confidential information to other agencies

Confidentiality waivers

104. Most of the time, disclosure of confidential information to foreign agencies occurs following a waiver signed by the party providing the information. The Recommendation on International Co-operation encourages the use of waivers in all enforcement areas as it allows for enhanced co-operation among agencies. In particular, it reduces the likelihood of inconsistent decisions and allows agencies to assess cases more adequately.

105. The Recommendation on International Co-operation points out that the information should be exclusively used by the agency that received the information pursuant to the waiver (unless the waiver provides for further disclosure) and that this agency should only use the information received in accordance with the terms of the waiver.

106. When dealing with information exchanges, agencies may take into account the discrepancies in the way different jurisdictions qualify the same type of information. For instance, the Best Practices on Co-operation in Merger Investigations adopted by the DoJ, the FTC, and the European Commission provides that: "[a]*s the rules governing legal professional privilege are different in the EU and the US, in particular with regard to in-house lawyers, the agencies will accept a stipulation in parties' waivers given to DG Competition that excludes from the scope of the waiver evidence that is properly identified by the parties as and qualifies for the in-house counsel privilege under US law.*"[65]

107. When seeking a waiver, it is important that agencies make parties aware of the benefits of the exchange of information between agencies (ICN, 2002-2018[18]), while making clear that declining to sign a waiver will not prejudice the outcome of the investigation (OECD, 2014[19]). In the US, the Frequently Asked Questions document accompanying the model waiver created by the DoJ and the FTC specifies that: "[w]*hile the Agencies may request waivers from an Entity, the decision whether to provide a waiver*

is at the Entity's discretion. A decision not to provide a waiver will not prejudice the outcome of the DOJ's or FTC's investigation. However, […] *this may have practical effects. For example, it may impact an investigation's timing and/or increase the risk of inconsistent outcomes.*" [66]

108. The use of waivers is particularly common in merger control proceedings. The OECD Recommendation on Merger Review encourages merging parties to consider a waiver of confidentiality where possible. At the same time, however, it stresses the need for competition authorities to have the necessary safeguards for handling the exchange of confidential information.

109. The Australian Competition and Consumer Commission's (ACCC) practice in mergers is to seek waivers from relevant parties to permit the exchange of information that may be of a confidential nature with other regulators. A few years ago, the ACCC realised that at times the process of obtaining waivers could be somewhat onerous. This was the case, in particular, when the parties were not familiar with dealing with the ACCC on such processes or when waivers were required in relation to multiple jurisdictions. To assist in remedying this issue, the ACCC introduced a standard form confidentiality waiver (OECD, 2011[20]). Other jurisdictions have also adopted model waivers for the same reason, including the Czech Republic, the EU, and the US or use the ICN Model Confidentiality Waiver[67] (OECD, 2011[20]).

110. Waivers are increasingly used in the context of leniency applications as well. Simultaneous leniency applications in several jurisdictions often include waivers of confidentiality rights. Such waivers create more opportunities for multi-jurisdiction co-operation by enabling the competition authorities involved to share information they have received via the leniency applications and conduct co-ordinated investigations. In particular, as summed up by a former Deputy Assistant Attorney General of the DoJ, waivers allow authorities to "*routinely discuss investigative strategies and co-ordinate searches, service of subpoenas, drop-in interviews, and the timing of charges with* [other agencies] *in order to avoid the premature disclosure of an investigation and the possible destruction of evidence*"[68].

111. In Chile, the *Fiscalía Nacional Económica* (FNE) may request, in the context of international cartels, that leniency applicants sign a waiver regarding one or more jurisdictions in which they have requested leniency in order "*to exempt said agencies from the confidentiality obligation with regards to the FNE in connection with such requests or negotiations, and provided that they refer to the conduct described in the application filed before the FNE.*"[69]

112. Some competition authorities have considered making leniency conditional on waivers being granted by the applicant precisely because of their usefulness. Even if not formalised in leniency policies, the trend among the more established cartel enforcers is to require waivers and for these to be expansive, enabling the exchange of evidence (OECD, 2012[17]). However, some voices hold that waivers should not be mandatory or a condition for granting leniency. To support this point it has been argued that confidentiality is a key aspect of leniency programmes and that applicants may have valid reasons to refuse to waive their right to confidentiality, such as the risk of damages actions or of information leaks (OECD, 2018[21]).

Information gateways

113. Confidential information may also be disclosed through information gateways, i.e. legal provisions allowing for the exchange of confidential information between competition agencies without the need to obtain prior consent from the source of the information (OECD, 2014[19]). These information gateways typically contain the applicable confidentiality safeguards.

114. Disclosure through information gateways is far less frequent than via waivers. For instance, in the US, absent a waiver, "*most of the information submitted by the merging parties or third parties during an antitrust investigation cannot be disclosed, including the HSR forms and materials responsive to a request for additional information.*" (OECD, 2011, p. 298[20]). Similarly, as a rule, information obtained through CIDs "*cannot be disclosed to state, foreign, or other Federal agencies (except for the FTC)*",[70] as mentioned in Section 3.2.

115. Although disclosure of confidential information may occur on the basis of an Antitrust Mutual Assistance Agreement under the US International Antitrust Enforcement Assistance Act of 1994, this happens rarely. "*This law allows the United States government to enter into agreements with other governments that enable its antitrust agencies to share otherwise confidential antitrust evidence (although not HSR material) with non-U.S. antitrust authorities, to use their investigative powers to collect evidence for use by the non-U.S. authority, and to withhold from public disclosure any antitrust evidence obtained from the other authority. The United States currently has only one such agreement, with Australia, which has been used rarely*" (OECD, 2011, p. 298[20]).

116. Information gateways may be found in:

- International agreements: Most agreements concluded to date are first generation agreements which allow only the exchange of non-confidential information. However, some second generation instruments contain information gateway provisions, which cover ways of information exchange (e.g. the ability to discuss, transmit or obtain information), and include confidentiality safeguards and limitations on use or further disclosure of the information (OECD, 2015[22]). For instance, the following agreements include information gateways: Australia and the US (1999), the EU and Switzerland (2013), New Zealand Commerce Commission and the Australian Competition and Consumer Commission (2013), and the Nordic countries (Sweden, Norway, Finland, Iceland and Denmark) (2017).
- National legislation allowing agencies to share confidential information under certain circumstances. Australia (Section 155AAA), Germany (§50) and the UK (Section 243) all have provisions in this line (Jenny, 2017[23]). Article 12 of EU Regulation No 1/2003 also contains an information gateway for exchange of confidential information within the EU.[71]

Box 8. Examples of information gateways

This box provides examples of international agreements, and national and supra-national rules allowing for the exchange of confidential information.

International agreement on Cooperation in Competition Cases between the Nordic Countries (2017)[1]

Article 3 – Exchange of information:

"For the purpose of applying competition rules and merger control rules the competition authorities of the Parties shall have the power to provide one another with and use in evidence any matter of fact or of law, including confidential information.

Information exchanged shall only be used in evidence and in respect of the subject matter for which it was collected by the transmitting authority."

Co-operation Arrangement between the New Zealand Commerce Commission and the Australian Competition and Consumer Commission in relation to the provision of compulsorily-acquired information and investigative assistance (2013)[2]

"4. The Participants agree that the mutual sharing of information and investigative assistance will increase the efficiency of their respective investigations and facilitate effective outcomes.

5. The provision of protected information from the ACCC to the NZCC is permitted subject to the provisions of section 155AAA of the CCA. The ACCC has provided protected information to the NZCC from time to time prior to this Arrangement coming into force. This Arrangement allows for the ACCC to continue to provide such protected information in accordance with section 155AAA.

6. Amendments made in 2012 to New Zealand's Commerce Act, Fair Trading Act, Credit Contracts and Consumer Finance Act and Telecommunications Act allow the NZCC to provide compulsorily-acquired information and investigative assistance to overseas regulators with whom a co-operation arrangement is in place (subject to the safeguards set out in those statutes). This Arrangement is intended to give effect to those amendments in relation to the provision of compulsory acquired information and/or investigative assistance to the ACCC."

Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty[3]

Article 12 – Exchange of information:

"1. For the purpose of applying Articles 81 and 82 of the Treaty the Commission and the competition authorities of the Member States shall have the power to provide one another with and use in evidence any matter of fact or of law, including confidential information."

German Act against Restraints of Competition[4]

Article § 50b – Other Cooperation with Foreign Competition Authorities

"(1) The Bundeskartellamt shall have the powers pursuant to § 50a(1) also in other cases in which it cooperates with the European Commission or with the competition authorities of other states for the purpose of applying provisions of competition law. [Article § 50a(1) establishes a broad power to share confidential information with the European Commission and the competition agencies of the other Member States of the EU. Article § 50b refers explicitly to cases in which the Bundeskartellamt "co-operates" with other agencies, not necessarily EU agencies]

(2) The Bundeskartellamt may only forward information pursuant to § 50a(1) with the proviso that the receiving competition authority

uses the information in evidence only for the purpose of applying provisions of competition law and in respect of the subject-matter of the investigation for which it was collected by the Bundeskartellamt, and

maintains the confidentiality of the information and transmits such information to third parties only if the Bundeskartellamt agrees to such transmission; this shall also apply to the disclosure of confidential information in court and administrative proceedings.

Confidential information, including operating and business secrets, disclosed in merger control proceedings may only be transmitted by the Bundeskartellamt with the consent of the undertaking which has provided that information."

Sources and Notes:
1 Available here: https://www.kkv.fi/en/current-issues/press-releases/2017/8.9.2017-finland-signs-cooperation-agreement-with-other-nordic-competition-authorities/.
2 Available here: https://www.accc.gov.au/system/files/Cooperation%20arrangement%20between%20the%20New%20Zealand%20Commerce%20Commission%20and%20the%20Australian%20Competition%20and%20Consumer%20Commission.pdf
3 Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02003R0001-20090701.
4 Available here: http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0670.

3.4.4. For private enforcement

117. Allowing a claimant an easier access to information in the case file can be a useful way to facilitate private antitrust litigation, especially in follow-on damage actions. The file of the competition authority can include useful information not only on the antitrust violation itself but also on the amount of damages and the causation link between the infringement and the damage (OECD, 2015[15]).

118. In Canada, the Bulletin on the Communication of Confidential Information of the Competition Bureau points out that it is possible that the agency possesses information, such as information obtained in the course of an investigation, which may be relevant for claimants. However, to ensure that the Bureau's mandate can be carried out effectively and to protect the investigative process and the confidential information in its possession, the Bureau does not voluntarily provide access to its records. If served with a subpoena, the Bureau informs the information provider and, if compliance with the subpoena could potentially interfere with an ongoing investigation or otherwise adversely affect its administration or enforcement activities, it opposes the subpoena. If the opposition is unsuccessful, the Bureau seeks a protective court order to maintain the confidentiality of the information.[72]

119. The EU is in the process of consulting with stakeholders a Communication on the protection of confidential information for the private enforcement of EU competition law by national courts. The Communication deals with the relevant considerations for disclosure of confidential information and the available measures to protect this type of information (such as confidentiality rings or closed hearings).[73]

120. The degree of legal protection against disclosure may differ depending the types and nature of the information and the documents. The EU Directive on Antitrust Damages Actions provides an example of how disclosure rules can vary for categories of documents to balance the interest of leniency applicants and those of potential follow-on claimants for

damages. The Directive distinguishes between three categories of documents (OECD, 2015[15]):

- Leniency statements and settlement submissions, which are never disclosable by court order.
- Documents prepared for the purpose of the investigation, such as replies to requests for information, which are disclosable by court order only after the relevant agency has taken a decision in the case or closes the proceedings.
- Pre-existing materials not prepared in connection with the investigation, such as texts of emails or minutes of meetings, which are disclosable by court order at any time.

121. Most of the mechanisms discussed in Section 3.4.2 can be used as well in the context of private enforcement in order to disclose documents containing confidential information. Mechanisms such as non-confidential versions of documents, confidentiality rings, closed hearings, and the preparation of summaries are particularly suitable (European Commission, 2019[16]).

Box 9. The publication of the Air Cargo decision in the context of damages claims

The decisions of agencies and courts are typically greatly valuable for parties wishing to submit a damages claim. The information they contain can provide a basis for the claimant's arguments.

Conversely, the parties that have provided the information or from which the information has been seized have the incentives to hold up the publication of non-confidential decisions and fuller versions of these decisions. This may pursue legitimate interests, in particular, protecting the company's confidential information. However, this may also be a tactic to push back the publication beyond the limitation period of the damages claims or to force claimants to file claims with an insufficient basis (Howard, 2015[24]).

In practice, the publication of decisions might take several months. The cartel decisions adopted by the European Commission between 2010 and 2014 were published an average of almost 29 months after the press release. Summary decisions were published much earlier: approximately, 11 months after the press release (PaRR, 2015[25]).

The *Air Cargo* case, in the UK, provides an example of the conflicting interests existing as regards the disclosure of infringement decisions. In 2010, the European Commission imposed fines of nearly EUR 800 million on 12 air cargo carriers, including British Airways.[74] The Commission found that these carriers had participated in a price-fixing cartel in the airfreight services market. Eventually, the General Court annulled the Commission's decision on procedural grounds, not ruling out the existence of a cartel. The Commission re-adopted a decision in 2017 and fined the companies with a similar total fine (European Commission, 2017[26]).

Following the Commission's decision, follow-on damages claims were filed before the British courts. The case involved hundreds of complainants (Fieldfisher, 2016[27]). British Airways was the anchor defendant and brought the rest of the addressees of the Commission's decision and another 11 airlines into the proceedings. These 11 additional airlines were not addressees of the decision and had not been found to participate in the

infringement, but the decision contained confidential information concerning them (Howard, 2015[24]).

In the context of the follow-on litigation, the claimants sought a copy of the non-confidential version of the decision. This decision had not yet been published by the European Commission. In March 2014, the High Court ordered the preparation of a non-confidential version of the decision from which all airlines, including the 11 non-addressees, would redact confidential information. Unsurprisingly, all these redactions resulted in a non-confidential version which was not intelligible. In view of this, the High Court ordered the disclosure of the confidential version of the decision within a confidentiality ring (except for the leniency material and legally privileged information) (Fieldfisher, 2016[27]). The decision was adopted despite the *Pergan*[*] case in which the European Court of Justice had not allowed the disclosure of a non-confidential version of an infringement decision that contained prejudicial references to a non-addressee (Howard, 2015[24]).

The resolution to allow for the disclosure of the decision was appealed by the non-addressee airlines. They argued that disclosing the decision –which contained allusions to their liability– would breach the principle of presumption of innocence. These airlines had not had the chance to rebut these allusions in the context of the infringement proceedings carried out by the European Commission. In October 2015, the Court of Appeal overturned the High Court's order and indicated that the *Pergan* protection did not allow the disclosure of the decision. In May 2016, the Supreme Court upheld the decision of the Court of Appeal. In the meantime, the Commission had published a non-confidential version of the decision (May 2015) and the first Commission's *Air Cargo* decision had been annulled as regards the vast majority of addresses (December 2015) (Fieldfisher, 2016[27]).

Note: [*] Case T-462/12R Pilkington Group Limited v Commission, upheld in case C-278/13 Commission v Pilkington

4. Conclusions and challenges

122. Jurisdictions ensure in different ways that parties have access to the evidence in the agency's case file. While some provide a very broad access –encompassing almost the whole file– others provide access to specific documents only. For the purposes of protecting the rights of defence, it is essential that parties have access to all relevant incriminating and exculpatory evidence. Determining which information is exculpatory and making sure that parties are granted access in a suitable manner can be challenging, as illustrated by the *Intel* case (see Box 1). It is also indispensable that parties have access to all relevant evidence in due time, so they can adequately defend themselves.

123. Other interested parties and the general public may also be granted access to specific documents in the agency's case file. Jurisdictions provide a rather limited access, especially to the general public.

124. The protection of confidential information sets a limit to the right to access the file. Although the vast majority of jurisdictions protect confidential information, the exact definition of 'confidential information' varies across jurisdictions. Commercially sensitive information and sensitive personal information are typically considered confidential. In practice, there may be significant discrepancies between what the agency, on the one hand, and the parties, on the other, consider confidential.

125. The fact that information is confidential means that, in principle, it will not be disclosed. Still, disclosure can occur in a number of circumstances. First, confidential information might be shared with parties in the process, in order to protect their rights of defence. There are a number of mechanisms that allow agencies to share documents containing confidential information. Non-confidential versions of documents –from which all confidential information has been redacted– are the most widespread mechanism. Others, such as confidentiality rings, data rooms and closed hearings, allow for the disclosure of confidential information, while controlling who has access to it.

126. Secondly, confidential information may be disclosed to other domestic and foreign agencies. Some jurisdictions have adopted a rather open approach as regards disclosure to domestic agencies. Some others are stricter. Disclosure to foreign agencies generally occurs pursuant to a waiver signed by the party having submitted the information. Waivers are used in mergers and, increasingly, in the context of parallel leniency applications. More rarely, disclosure to foreign agencies also occurs on the basis of information gateways.

127. Finally, information may be disclosed for the purposes of private enforcement. Granting claimants access to information in the case file can be useful to promote damages actions. However, the disclosure of leniency and settlement materials could discourage parties to use these mechanisms.

Endnotes

[1] The definition of confidential information is discussed in Section 3.2.

[2] This document is available here: https://iccwbo.org/content/uploads/sites/3/2017/06/ICC-International-Due-process-08-03-10.pdf.

[3] Case *Goldberg v Kelley*, 397 US 254, 263 (1970). Based on (Ginsburg and Owings, 2015[3]).

[4] This document is available here: https://www.internationalcompetitionnetwork.org/wp-content/uploads/2019/05/RPs-Investigative-Process.pdf.

[5] For instance, the Charter of Fundamental Rights of the EU, in its Article 41, indicates that "[e]*very person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union*", which among other things includes "*the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy*." Based on (Wils and Abbott, 2019[4]).

[6] See the European Commission's Notice on the rules for access to the Commission file in cases pursuant to Articles 81 and 82 of the EC Treaty, Articles 53, 54 and 57 of the EEA Agreement and Council Regulation (EC) No 139/2004 (2005/C 325/07) (Commission's Notice on Access to File). Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005XC1222(03)-20150806.

[7] See: in Spain, Article 31 of the Regulation on the Defence of Competition, passed by Royal Decree 261/2008; in Portugal, Article 33(1) of Law 19/2012; in Hungary, Article 55(1) of Law LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices.

[8] Apart from having been prepared by the agency, internal documents must be "*neither incriminating nor exculpatory*", according to EU case law, i.e. they "*cannot contribute to establishing whether an infringement has or has not been committed*" (Wils and Abbott, 2019, p. 31[4]).

[9] Article 29(12) of the Rules on the KFTC's Committee Operation and Case Handling Procedure.

[10] Article 52(1) of the Act on Prohibition of Private Monopolization and Maintenance of Fair Trade, Act No. 54 of April 14, 1947.

[11] Competition Act 1998: Guidance on the CMA's investigation procedures in Competition Act 1998 cases, paragraphs 11.20 and 11.21 (CMA's Guidance). Available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771970/CMA8_CA98_guidance.pdf.

[12] Rule 26 of the Federal Rules of Civil Procedure. Based on (Calvani and Mellott, 2015[28]) and (Yoo and Wendland, 2019[7]).

[13] The Manual is available here: https://www.justice.gov/atr/file/761141/download.

[14] Article 16a(1) of EU Regulation 773/2004.

[15] Article 16a(2) of EU Regulation 773/2004.

[16] Article 17(4) of Commission Regulation (EC) No 802/2004 of 7 April 2004 implementing Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings.

[17] Article 33(4) of Law 19/2012.

[18] Article 6(1) of EU Regulation No 773/2004.

[19] Article 8(1) of EU Regulation 773/2004.

[20] See: in Hungary, Article 55(3) of Law LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices; in Portugal, Article 33(3) of Law 19/2012; in Spain, Article 31 of the Regulation on the Defence of Competition, passed by Royal Decree 261/2008.

[21] Article 55(3) and (4) of Law LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices.

[22] Article 31 of the Regulation on the Defence of Competition, passed by Royal Decree 261/2008 and Article 13 of Decree number 217 on competition proceedings of the Italian *Autorità garante della concorrenza e del mercato*.

[23] CMA's Guidance, paragraph 11.19.

[24] CMA's Guidance, paragraph 14.14.

[25] Commission's Notice on Access to File, paragraph 27.

[26] Articles 10a(2) and 15(1a) of EU Regulation 773/2004.

[27] Article 55(5) and (6) of Law LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices.

[28] Bureau's Bulletin, paragraph 7.4.1.

[29] The importance of the protection of confidential information is clear in the OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings. See, also ICN's Recommended Practices for Investigative Process and Recommended Practices for Merger Notification and Review Procedures, and the ICC's Recommended Framework for International Best Practices in Competition Law Enforcement Proceedings.

[30] The statements in this paragraph concerning the protection of confidential information are based on a survey carried out by the ICN in 2014. All respondents answered that their legal framework provided for the protection of confidential information obtained during investigations. 39 jurisdictions submitted responses, including 21 OECD jurisdictions.

[31] The survey was addressed to 120 competition agencies from around the world, including agencies from the 34 OECD member countries, the 15 OECD observer countries, and all other member agencies of the ICN. The response rate among OECD members and observers was around 90%. The OECD report is available here: https://www.oecd.org/daf/competition/InternEnforcementCooperation2013.pdf.

[32] DoJ's Antitrust Division Manual, Chapter III, pages 19 and 62.

[33] Article 59(6) of the Regulation on the Defence of Competition, passed by Royal Decree 261/2008.

[34] Commission's Guidance on Confidentiality, paragraph 15.

[35] Transparency and disclosure: Statement of the CMA's policy and approach, paragraph 4.15.

[36] According to the Secretariat's research of public resources, the only OECD Members that do not recognise legal privilege are Japan and Korea (OECD, 2018[12]).

[37] Available here: http://www.oecd.org/daf/competition/2014-rec-internat-coop-competition.pdf.

[38] Model Waiver of Confidentiality For use in civil matters involving non-U.S. competition authorities: Frequently Asked Questions, page 2. This document is available here: https://www.ftc.gov/system/files/attachments/international-waivers-confidentiality-ftc-antitrust-investigations/waivers_faq.pdf.

[39] CMA's Guidance, paragraph 7.10.

[40] See: in Portugal, Article 30(4) of Law 19/2012; in Hungary, Article 55/A(2) of Law LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices.

[41] Article 39 of Decree-Law 211.

[42] DoJ's Antitrust Division Manual, Chapter III, pages 31 and 32.

[43] Article 43 of Law 15/2007, of 3 July, on the Defence of Competition.

[44] Article 43 of Law 15/2007, of 3 July, on the Defence of Competition.

[45] CMA's Guidance, paragraph 11.30.

[46] DoJ's Antitrust Division Manual, Chapter III, page 64.

[47] Transparency and disclosure: Statement of the CMA's policy and approach, paragraph 4.27.

[48] DoJ's Antitrust Division Manual, Chapter IV, page 47.

[49] Bureau's Bulletin, paragraph 3.7.

[50] Bureau's Bulletin, paragraph 3.6.

[51] Order of the Court of Justice of the EU in Case C-318/19 P(R) *Lantmännen v Commission*.

[52] The draft Communication of the European Commission refers to disclosure by courts, but the factors are applicable *mutatis mutandis* to disclosure by agencies.

[53] Article L463-4 of the Commercial Code.

[54] CMA's Guidance, paragraph 11.27.

[55] European Commission's Guidance on the use of (voluntary) confidentiality rings, paragraph 22(b). Available here: https://ec.europa.eu/competition/antitrust/conf_rings.pdf.

[56] Transparency and disclosure: Statement of the CMA's policy and approach, paragraph 4.30.

[57] CMA's Guidance, paragraph 11.26.

[58] European Commission's Best Practices on the disclosure of information in data rooms in proceedings under Articles 101 and 102 TFEU and under the EU Merger Regulation, paragraph 30. Available here: https://ec.europa.eu/competition/mergers/legislation/disclosure_information_data_rooms_en.pdf.

[59] See: https://www.justice.gov/atr/mutual-antitrust-enforcement-assistance.

[60] US 28 CFR § 50.9.

[61] Bureau's Bulletin, paragraphs 4.1.1 to 4.1.3.

[62] DoJ's Antitrust Division Manual, Chapter III, page 62.

[63] The Recommendation on International Co-operation points out that it is not intended to affect any special regime adopted with respect to the exchange of information received from a leniency or amnesty applicant or an applicant under specialised settlement procedures.

[64] Available here: https://www.oecd.org/daf/competition/oecdrecommendationonmergerreview.htm.

[65] This document is available here: https://www.ftc.gov/system/files/111014eumerger.pdf.

[66] Model Waiver of Confidentiality For use in civil matters involving non-U.S. competition authorities: Frequently Asked Questions, page 3.

[67] This document is available here: https://www.internationalcompetitionnetwork.org/portfolio/model-confidentiality-waiver-for-mergers/.

[68] Speech by Scott Hammond, former Deputy Assistant Attorney General of the US DoJ, 2003. (OECD, 2012[17])

[69] Internal Guidelines on Leniency in Cartel Cases, paragraph 83. The Guidelines are available here: https://www.fne.gob.cl/wp-content/uploads/2017/10/Guidelines_Leniency_Cartel_Cases-1.pdf.

[70] DoJ's Antitrust Division Manual, Chapter III, pages 19 and 62.

[71] EU Regulation 1/2003 can be considered as a hybrid between an international agreement and national legislation, as it has been adopted by a supranational organisation.

[72] Bureau's Bulletin, paragraphs 7.6.1 to 7.6.3.

[73] The draft Communication is available here: https://ec.europa.eu/competition/consultations/2019_private_enforcement/en.pdf.

[74] Case AT. 39258 *Airfreight*.

References

(n.a.) (n.d.), *X*. [45]

Autorité de la concurrence (2009), *Communiqué de procédure du 2 mars 2009 relatif aux engagements en matière de concurrence*. [32]

Calvani, T. and J. Mellott (2015), "Discovery of European Commission materials in U.S. civil antitrust litigation: An update", *Concurrences*, Vol. 1. [28]

CMA (2019), *Competition Act 1998: Guidance on the CMA's investigation procedures in Competition Act 1998 cases*. [30]

CMA (2014), *Transparency and disclosure: Statement of the CMA's policy and approach*. [40]

Competition Bureau (2013), *Information Bulletin on the Communication of Confidential Information Under the Competition Act*. [31]

DoJ (2019), *Chapter III. Investigation and Case Development*. [42]

DoJ (2019), *Chapter IV. Litigation*. [43]

DoJ (2019), *Chapter VII. Antitrust Division Relationships with Other Agencies and the Public*. [44]

DoJ, FTC (2015), *Model Waiver of Confidentiality For use in civil matters involving non-U.S. competition authorities: Frequently Asked Questions*. [39]

DoJ, FTC, European Commission (2011), *Best Practices on Cooperation in Merger Investigations*. [38]

European Commission (2019), *Draft communication on the protection of confidential information for the private enforcement of EU competition law by national courts*. [16]

European Commission (2018), *Guidance on confidentiality claims during Commission antitrust investigation*. [34]

European Commission (2018), *Guidance on the use of (voluntary) confidentiality rings*. [35]

European Commission (2017), *Antitrust: Commission re-adopts decision and fines air cargo carriers €776 million for price-fixing cartel*, https://europa.eu/rapid/press-release_IP-17-661_en.htm. [26]

European Commission (2015), *Best Practices on the disclosure of information in data rooms in proceedings under Articles 101 and 102 TFEU and under the EU Merger Regulation*. [36]

European Commission (2005), *European Commission's Notice on the rules for access to the Commission file in cases pursuant to Articles 81 and 82 of the EC Treaty, Articles 53, 54 and 57 of the EEA Agreement and Council Regulation (EC) No 139/2004*. [37]

Fieldfisher (2016), *Air Cargo follow-on damages action – no disclosure of the Commission's cartel decision*, https://competitionlawblog.fieldfisher.com/2016/air-cargo-follow-on-damages-action-no-disclosure-of-the-commissions-cartel-decision. [27]

First, H., E. Fox and D. Hemli (2012), "Procedural and Institutional Norms in Antitrust Enforcement: The U.S. System", *New York University Law and Economics Working Papers*. [6]

Fiscalía Nacional Económica (2017), *Internal Guidelines on Leniency in Cartel Cases*. [41]

Ginsburg, D. and T. Owings (2015), "Due Process in Competition Proceedings", *Competition Law International*, Vol. 11/1. [3]

Howard, A. (2015), "Disclosure of Infringement Decisions in Competition Damages Proceedings: How the UK Courts Are Leading the Way Ahead of the Damages Directive", *Journal of European Competition Law & Practice*, Vol. 6/4, pp. 256-259. [24]

ICC (2010), *Recommended framework for international best practices in competition law enforcement proceedings*. [2]

ICN (2019), *ICN Recommended Practices for Investigative Process*. [8]

ICN (2014), *ICN Agency Effectiveness Project on Investigative Process: Competition Agency Confidentiality Practices*. [9]

ICN (2002-2018), *ICN Recommended Practices for Merger Notification and Review Procedures*. [18]

Jenny, F. (2017), *International cooperation on competition: achievements and challenges*. [23]

Nihoul, P. and T. Skoczny (eds.) (2015), *An Elusive Convergence – Rights of Defence in Competition Matters in the Jurisprudence of the CJEU*, Edward Elgar Publishing. [5]

OECD (2018), *Background Paper by the Secretariat: Treatment of Legally Privileged Information in Competition Proceedings*. [12]

OECD (2018), *Detailed Summary of the Discussion: Challenges and co-ordination of leniency programmes*. [21]

OECD (2018), *Issues Note by the Secretariat: Due Process in relation to Evidence Gathering*. [13]

OECD (2018), *Peer Reviews of Competition Law and Policy: Greece*. [14]

OECD (2016), *Background Paper by the Secretariat: Commitment Decisions in Antitrust Cases*. [10]

OECD (2016), *Executive Summary of the Roundtable on Commitment Decisions in Antitrust Cases held at the 125th meeting of the Competition Committee of the OECD.* [11]

OECD (2015), *Background Note by the Secretariat: Relationship between Public and Private Antitrust Enforcement*. [15]

OECD (2015), *Competition co-operation and enforcemen: Inventory of Co-operation Agreements*, https://www.oecd.org/daf/competition/competition-inventory-provisions-exchange-of-information.pdf. [22]

OECD (2014), *Recommendation of the OECD Council concerning International Co-operation on Competition Investigations and Proceedings*. [19]

OECD (2013), *Secretariat Report on the OECD/ICN Survey on International Enforcement Co-operation*. [33]

OECD (2012), *Improving International Co-operation in Cartel Investigations*. [17]

OECD (2012), *Procedural Fairness and Transparency*. [1]

OECD (2011), *Cross-Border Merger Control: Challenges for Developing and Emerging Economies*. [20]

OECD (2005), *Recommendation of the OECD Council on Merger Review*. [29]

PaRR (2015), *EC six months slower in publishing cartel decisions than before 2010*, https://app.parr-global.com/intelligence/view/prime-1946130. [25]

Wils, W. and H. Abbott (2019), "Access to the File in Competition Proceedings before the European Commission", *World Competition*, Vol. 42/3. [4]

Yoo, C. and H. Wendland (2019), "Procedural Fairness in Antitrust Enforcement: The U.S. Perspective", *Faculty Scholarship at Penn Law*. [7]