BUSINESSatOECD

Discussion Points

Presented by the *Business at OECD* Competition Committee to the OECD Competition Committee Working Party No. 3

Access to File and Protection of Confidential Information

December 3, 2019

I. Introduction

1. *Business at OECD* appreciates the opportunity to make this written contribution to the WP3 roundtable on access to the case file and protection of confidential information. The OECD's valuable work in this area should be understood in the context of its own broader examination of due process or procedural fairness in antitrust proceedings. As the OECD has noted, there is "broad consensus on the need for, and importance of, transparency and procedural fairness in competition enforcement, notwithstanding differences between prosecutorial and administrative systems, and other legal, cultural, historical, and economic differences among members."[1] The OECD has also stated that "transparent and fair processes are essential to achieving effective and efficient cooperation in competition law enforcement."[2]

2. The International Competition Network (ICN) has also "recognized the importance of fair and effective procedures and published various work products reflecting the broad consensus among its members."[3] In recognition, it has recently adopted a multilateral *Framework on Competition Agency Procedures*, which notes "[f]air and effective procedures are essential to sound competition law enforcement and can increase opportunities for international cooperation."[4] The ICN has also commented that "this includes availability and use of effective agency investigative tools, transparency and engagement with those subject to an investigation (investigated parties

---

1 OECD COMPETITION COMM., PROCEDURAL FAIRNESS AND TRANSPARENCY: KEY POINTS 5 (2012), *available at* https://www.oecd.org/daf/competition/abuse/50235955.pdf.

2 OECD, Recommendation of the OECD Council Concerning International Co-Operation on Competition Investigations and Proceedings 1 (Sept. 16, 2014), *available at* https://www.oecd.org/daf/competition/2014-rec-internat-coop-competition.pdf.

3 INT'L COMPETITION NETWORK, ICN FRAMEWORK ON COMPETITION AGENCY PROCEDURES 1 (June 2019), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2019/04/ICN_CAP.pdf [hereinafter ICN CAP FRAMEWORK].

4 *Id.* Although, as noted below, it is vital that access goes beyond merely "the evidence relied upon as the basis for the agency's allegations" as described by the ICN *Guidance on Investigative Process*. INT'L COMPETITION NETWORK, GUIDANCE ON INVESTIGATIVE PROCESS ¶ 5.4 (2018), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_Guidance_InvestigativeProcess.pdf. In fact, as the ICN *Guidance* also notes, a key purpose of access to file is to ensure that the parties under investigation have "an effective opportunity to respond" to the case, which is only possible with full access, including both inculpatory and exculpatory, and other relevant, material. *Id.*

and third parties), internal checks and balances on enforcement process, and protection of confidential information."[5]

3. The productive engagement with parties that comes with adequate access to file and robust protections of confidentiality "benefits competition enforcement agencies by enhancing their legitimacy, increasing efficiency and promoting accuracy and better-informed decisions. Indeed, the credibility of competition agencies is closely tied to the integrity and public understanding of the investigative process."[6]

4. *Business at OECD* has previously commented on the broader subject of procedural fairness, noting that "[p]rocedural fairness is critical to protect the interests of firms subject to competition law enforcement proceedings who face the risk of substantial sanctions, not least being increasingly onerous financial penalties, but which may also include the prohibition of or mandated changes to business practices and transactions. Importantly, such fairness also strengthens and streamlines agency decision-making, reducing the number of appeals, and increases public confidence in agency decisions and so is of general public benefit."[7]

5. In these comments, *Business at OECD* focuses on (i) the importance of access to file in the context of a broader examination of procedural safeguards, and to the efficiency and legitimacy of the investigatory process; (ii) the crucial need for access to file to be meaningful; (iii) the importance of agencies implementing adequate protections for confidential information; (iv) the need to balance the right to access a case file with the protection of confidential information within it; and (v) considerations of inter-agency sharing of confidential information.

6. We have in these comments focused on access to file being granted to parties under investigation (rather than access by third parties or potential claimants in follow-on damages actions, including in the context of access to leniency applications).[8]

II. The Importance of Ensuring Access to File

7. Access to file is fundamental to the rights of defence of parties under investigation. It is essential to enable the parties to respond effectively to allegations, by ensuring that they understand the case against them and the facts and arguments relied upon by the investigating authority. The right of defence flows from the fundamental principles of access to justice which is enshrined in

---

5 INT'L COMPETITION NETWORK, RECOMMENDED PRACTICES FOR INVESTIGATIVE PROCESS 1 (2019), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2019/05/RPs-Investigative-Process.pdf.

6 Paul Lugard, *IP and Antitrust: The Importance of Due Process and the ICC Best Practices*, CPI ANTITRUST CHRONICLE, Nov. 2017, at 1, *available at* https://www.competitionpolicyinternational.com/wp-content/uploads/2017/11/CPI-Lugard.pdf.

7 BIAC, SUBMISSION PRESENTED BY THE BUSINESS AND INDUSTRY ADVISORY COMMITTEE (BIAC) TO THE OECD COMPETITION COMMITTEE WORKING PARTY NO. 3 "PROCEDURAL FAIRNESS: TRANSPARENCY ISSUES IN CIVIL AND ADMINISTRATIVE ENFORCEMENT PROCEEDINGS" ¶ 1.2 (Feb. 16, 2010), *available at* http://biac.org/wp-content/uploads/2014/05/BIAC_2010_Oct_WP3_Procedural_Fairness_2010-02-05_FINAL.pdf [hereinafter BIAC FEB. 2010 PROCEDURAL FAIRNESS].

8 *Business at OECD* notes that the need to ensure that rights of defence are ensured through access to file and that disclosure and the protection of confidentiality are appropriately balanced apply equally to administrative and prosecutorial (and "hybrid") antitrust regimes. However, the way in which this is achieved between different types of regimes may differ. As the ICN *Report on Agency Effectiveness Project On Investigative Process – Competition Agency Confidentiality Practices* found, "Given the nature of prosecutorial systems, courts and court rules play a larger role in determining the appropriate disclosure of confidential information prior to a final decision on the merits of the conduct investigated." INT'L COMPETITION NETWORK, REPORT ON AGENCY EFFECTIVENESS PROJECT ON INVESTIGATIVE PROCESS – COMPETITION AGENCY CONFIDENTIALITY PRACTICES 12 (Apr. 2014), *available at* https://centrocedec.files.wordpress.com/2015/07/report-on-confidentiality-practices2014.pdf [hereinafter ICN 2014 REPORT]. Further, *Business at OECD* notes that where investigations move from an administrative stage to a prosecutorial one, it is important that any deficiencies in early access to file processes do not impact later stages in the investigative process.

the constitutional traditions of member countries and also reflected in binding international instruments, such as the European Convention on Human Rights and Fundamental Freedoms (and Article 6 of that Convention in particular) to which 47 member countries have signed up to. This is recognised in the ICN's principles, which include that parties under investigation should be granted "reasonable and timely access to the information related to the matter in the [Agency's] possession that is necessary to prepare an adequate defense, in accordance with the requirements of applicable administrative, civil, or criminal procedures and subject to applicable legal exceptions."[9] As the ICC succinctly noted that "[a]ccess to the complete case file is a core element of due process in the context of competition law investigations" underlining that it should not be for the agency to assess what material might be necessary for the defence.[10]

8. Ensuring that parties under investigation have adequate access to file also has significant benefits for competition agencies and the broader antirust community. It ensures that the investigation itself is robust and efficient, and it means that the engagement between the agencies and the parties is grounded in the facts, evidence and analysis gathered—and potentially not gathered—by the agency. This maximises the potential for meaningful dialogue between the agency and the parties under investigation, and with third parties, to effectively address the pertinent issues in the investigation. As a result, theories of harm and analysis are refined through that engagement process, of which access to file is a crucial part.

9. In addition, an investigation will invariably be more efficient for having allowed the parties to review and comment on the file. It may be perceived that allowing such access lengthens investigations and creates opportunities for the agency's evidence gathering process to be challenged, delaying progress towards a final decision. However, an investigation that has strong procedural safeguards can proceed with greater speed and efficiency. The refinement of theories of harm and analysis that comes with allowing access to, and commentary on, the agency's case file, invariably leads to the investigatory team focusing only on the elements of the case that would have the greatest impact, rather than expending time and resources on elements of the case not worth pursuing.

10. As the ICC has explained, "Only such a process [of complete access to file] ensures that investigated parties have sufficient knowledge of any potential allegations against them and have a full and effective opportunity to respond. This also ensures that agencies is [sic] informed of 'both sides of the story' and can form a better informed view of the facts of the case. This is particularly important in complex cases or where third parties may have a commercial interest which may not be immediately obvious to the agency."[11]

---

9 INT'L COMPETITION NETWORK, TEMPLATE PURSUANT TO SECTION 3 (A) OF THE ICN FRAMEWORK ON COMPETITION AGENCY PROCEDURES § II(h)(ii) (2019), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2019/04/CAP-Template.docx. *Business at OECD* notes that the term "reasonable" can be open to broad interpretation. As explained in the comments, it is essential that access be meaningful—this should be paramount—and any considerations of reasonableness should be objectively verifiable and cannot be guided by an agency's ability or willingness to devote internal resources to access to file requests.

10 INT'L CHAMBER OF COMMERCE, EFFECTIVE PROCEDURAL SAFEGUARDS IN COMPETITION LAW ENFORCEMENT PROCEEDINGS 5 (June 2017), *available at* https://iccwbo.org/content/uploads/sites/3/2017/07/ICC-Due-Process-Best-Practices-2017.pdf [hereinafter ICC EFFECTIVE PROCEDURAL SAFEGUARDS].

11 *Id.* at 5-6.

III. Ensuring That Access to File is Meaningful

11. In order to ensure that fundamental rights of defence are respected and, for an investigation and the regime, to reap the benefits described above, access to file must be meaningful.

12. As *Business at OECD* has observed previously, the starting point must be that "the agency should give the defendant access to all materials."[12] As such, access must be granted to the full scope of information collected during the investigation—regardless of whether it is defined as "evidence"—and that parties have ample time to review and respond to the information.

13. This means that access must be to the complete file—to all the information gathered relevant to the investigation. The European Commission defines an investigatory file as "consist[ing] of all documents obtained, produced and/or assembled by DG Competition during the investigation that has led the Commission to raise its objections."[13] Complete access requires that both potentially inculpatory and exculpatory evidence is made available. It cannot merely comprise information on which the allegations are based. As *Business at OECD* has noted previously, "The firms should also be given copies of all complaints and supporting materials and of all evidence, both inculpatory and exculpatory, subject only to protection of legitimate business secrets."[14]

14. The OECD has also noted that "right to access the evidence used to support the allegations against them ensures that parties to an antitrust proceedings have full knowledge of the case and details concerning the alleged violations against them, allowing them to substantially respond before a decision is taken,"[15] and the ICC has commented, "The agency should compile a record, or case file consisting of all evidence, arguments, analyses, expert opinions, correspondence with all interested parties, requests for information, minutes of any meetings (with the investigated parties, any interested parties, other stakeholders as well as meetings between the case team and other agency officials) relating to the investigation."[16] In this regard, access to file is not limited only to information received by the agency, but should encompass, for example, questions asked by the agency, meeting notes and analysis and reviews of evidence, including where wholly internal. This also means that in order to ensure due process the agency has an affirmative obligation to seek and place in the file potentially exculpatory evidence, particularly in jurisdictions where the party under investigation lacks independent rights of discovery.

15. Meaningful access to file also requires that access be timely—that access is granted sufficiently early in the investigation and that parties are given adequate time to review and to respond to the content of the investigation file. The volume and complexity of information on file should inform

---

12 BIAC, Submission Presented by the Business and Industry Advisory Committee (BIAC) to the OECD Competition Committee Working Party No. 3 "Procedural Fairness: Transparency Issues in Civil and Administrative Enforcement Proceedings" Additional Comments on Issues for Discussion ¶ 2.3 (June 15, 2010), *available at* http://biac.org/wp-content/uploads/2014/05/2010_June_WP3_Procedural_Fairness_FINAL_2010-06-09.pdf [hereinafter BIAC June 2010 Procedural Fairness].

13 Eur. Comm'n, Antitrust Manual of Procedures, Module 12, ¶ 11 (Mar. 2012), *available at* http://ec.europa.eu/competition/antitrust/antitrust_manproc_3_2012_en.pdf. The term "documents" includes all forms of information media.

14 BIAC Feb. 2010 Procedural Fairness, *supra* note 7, ¶ 3.13(ii). In this regard, it would not respect essential rights of defence for parties under investigation to receive access to only information that supports a statement of case (or statement of objections), with the broader case file, including potentially exculpatory evidence, only being made available after the parties have responded to the statement of case.

15 OECD, Competition Comm., Procedural Fairness: Transparency Issues In Civil And Administrative Proceedings 10 (2011), *available at* www.oecd.org/daf/competition/48825133.pdf [hereinafter OECD Transparency Issues].

16 ICC Effective Procedural Safeguards, *supra* note 10, at 5.

the amount of time that the parties have to review (such time allowing for review by its advisors and experts, as appropriate). Crucially, access should also be given on a timeframe that allows the parties under investigation to respond before any formal charges are levied. While a right to appeal an antitrust enforcement decision should always exist,[17] an appeal cannot be the first time that a party under investigation is able to access the agency's complete file.

16. In addition to full and timely access, parties should, from a practical perspective, be granted access in a form that allows for a meaningful review. As *Business at OECD* has noted previously, this, in part, relates to the gathering and organisation of the file itself: "Evidence should be recorded comprehensively and in a manner that can be made available to the defendant (e.g. an agenda and full record of all facts and matters discussed and provided to investigators during meetings and other discussions with complainants, witnesses and third parties should be made and kept on the investigation file)."[18] *Business at OECD* encourages agencies to adopt modern and secure tools wherever possible, such as encrypted electronic databases, to enable parties to review large volumes of information. Even more basic processes, such as well indexed and labelled "hard copy" material, can speed up the review to the benefit of the parties and the agency.

17. As such, for access to file to be meaningful—in particular, to meaningfully enable the parties under investigation to understand and respond to the allegations being made—that access must be complete and timely, and in a form that allows for a comprehensive review by the parties under investigation.

IV. The Importance of Confidentiality Protections

18. It is fundamental that confidential information in the hands of an agency is protected from disclosure. Invariably this is enshrined in the statute constituting or giving authority to the agency.[19]

19. In the course of any antitrust investigation, agencies will undoubtedly receive business confidential information. In particular, cases in which a company's business model itself is under investigation, whether that comprises a distribution system, a pricing model, core commercial contracts, technology or product design, will involve an investigating agency receiving highly sensitive business information, much of which may be protected by intellectual property or trade secrets. As the Secretariat's Call for Contributions notes, "It is in the agencies' interest to protect the confidentiality of sensitive information provided by their sources, both to prevent competitively sensitive information from being shared among competitors and to ensure that parties and third parties continue to be willing to cooperate with competition agencies and supply information."[20]

20. The importance of institutional safeguards to protect confidential information is recognised by the ICN. Its *Framework on Competition Agency Procedures* includes that agencies should "have publicly available rules, policies, or guidance regarding the identification and treatment of confidential

---

17 BIAC Feb. 2010 Procedural Fairness, *supra* note 7, ¶ 8.2.

18 BIAC June 2010 Procedural Fairness, *supra* note 12, ¶ 1.3.

19 *See, e.g.*, the duties of the UK Competition and Markets Authority under the Enterprise Act 2002 and its guidance "Competition Act 1998: Guidance on the CMA's investigation procedures in Competition Act 1998 cases Transparency and disclosure: Statement of the CMA's policy and approach" (Section 7), *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771970/CMA8_CA98_guidance.pdf.

20 Letter from Makan Delrahim, Chair, Working Party No. 3, to All Competition Delegates and Participants 2 (July 30, 2019) [hereinafter Call for Contributions].

information" and that each agency should "protect from unlawful disclosure all confidential information obtained or used by the [agency] during Investigations and Enforcement Proceedings."[21]

21. As with access to file, and, more generally, measures to ensure procedural fairness, adequate protections of confidentiality also serve the interests of agencies. They increase the likelihood of a constructive dialogue between the agency and the parties under investigation (and third parties). The more confident the business community is that confidential information, in particular knowhow and industrial secrets, will be sufficiently protected in the hands of the agency, the more open the engagement, within and outside an investigation.

22. It is therefore vital that agencies maintain robust legal and operational safeguards to protect confidential information shared in the course of an investigation. Such robust protections of confidentiality increase an agency's legitimacy and improve the ease with which industry can engage with the agency. These safeguards, however, normally cannot justify the denial of the right of access to file entirely. Rather, the safeguards should strive to grant access to file in a way that avoids significant risk of disclosure of confidential information.

V. Balancing Confidentiality Protections and Access to File

23. As the Secretariat's Call for Contributions identifies, the protection of confidential information is pertinent to any discussion of access to file since there will invariably be a balancing for the agency to achieve between granting full and complete access to file and withholding from disclosure confidential information.

24. As such, this balancing is between ensuring that the parties under investigation enjoy complete access to file and potentially withholding from disclosure confidential information provided to the agency by complainants and third parties.[22] This does not mean that confidentiality protections need not be robust, rather that "confidentiality concerns must be balanced carefully with the right to access evidence as a matter of due process."[23]

25. The starting point for identifying what is confidential information is often the legislative or procedural rules that define , at a high-level, non-public, business confidential, or commercially sensitive, information.[24] However, as the OECD has noted, "Few jurisdictions have a clear statutory definition of 'confidential information' and the concept has been given meaning through agency practice and case law."[25] The OECD has suggested that "[b]usiness secrets, trade secrets or commercially sensitive information are universally recognised by competition agencies as constituting confidential information. This will generally cover price information, commercial know-how, production quantities, market shares and commercial strategies of undertakings.

---

[21] ICN CAP FRAMEWORK, *supra* note 4, at 5-6. The ICC has also noted that "[a]gencies should have specific safeguards in place to protect the confidentiality of information gathered as part of the investigation." ICC EFFECTIVE PROCEDURAL SAFEGUARDS, *supra* note 10, at 3.

[22] The need for such balancing does not arise in the opposite situation—the protection of confidential information provided to the agency by the parties under investigation outweigh any claim from complainants or third parties for access. Note that we have not addressed here disclosure of leniency applications, since such disclosure in more often sought by third parties, for the purposes of "follow-on" private actions, rather the parties under investigation to exercise their rights of defence.

[23] ICC EFFECTIVE PROCEDURAL SAFEGUARDS, *supra* note 10, at 3.

[24] *Business at OECD* has focused here on business confidential information. However, in the context of cartel investigations, a leniency application is confidential and withheld from disclosure on a separate basis.

[25] OECD TRANSPARENCY ISSUES, *supra* note 15, at 12.

Other types of recognised confidential information include sensitive personal information, such as private telephone numbers and addresses, medical or employment records, or information that would place the provider under considerable economic or commercial pressure from competitors."[26] Even with such definitions there may be debate over whether specific information falls within the category and it is important that procedural rules allow recourse to independent review, within and/or outside the agency.

26. In *Business at OECD*'s view, this balancing exercise should almost always be conducted in favour of disclosure to the parties under investigation.[27] In other words, the rights of the parties under investigation to see all the information relevant to the case, in particular evidence on which the allegations are based, is fundamental and invariably outweighs information being withheld entirely from disclosure although not necessarily to third parties (where the interest in favour of disclosure—the right to participate in the process—is less fundamental than the interests in favour of disclosure to the parties directly involved).

27. Further, there exist a range of means and tools for agencies to grant access to confidential information that guards against the provider of information suffering commercial harm as a result of disclosure, or to prevent separate concerns arising from the sharing of competitively sensitive information among competitors. Firstly, as followed by the European Commission and a number of other agencies, the case file itself should only include information related to the investigation. As noted above, both inculpatory and exculpatory evidence must be included. However, removing entirely unrelated information (which may have been caught by overly broad information requests or which become unrelated because of a narrowing of the issues under investigation) reduces the risk of confidential information being disclosed.

28. Secondly, for information that is both relevant and confidential, agency case teams should develop the expertise, and devote the resources necessary, to critically appraise confidentiality claims. The ICC has suggested, by way of "procedures to avoid unacceptable or over-inclusive confidentiality claims" for a "senior official—acting in an independent role—to carry out an impartial and objective review of the confidentiality claim and to make a ruling on the issue."[28]

29. There are now also a variety of best practices by which agencies can strike that balance between ensuring complete access to file and protecting highly sensitive commercial information.[29] These include redacting documents, creating "confidentiality rings" or protective orders, and setting up

---

[26] *Id.* A possible exception may be in the case of national security interests. *Business at OECD* also notes that the confidentiality of information may change over time. In particular, information provided to an agency early in a multi-year investigation may no longer be confidential at the time that access to file is granted. Given the importance of ensuring adequate access to file, it is important that agencies continue to reassess confidentiality claims throughout an investigation.

[27] *Business at OECD* notes that the Call for Contributions suggests that the balance is generally in favour of non-disclosure—that the protection of confidential information is a limit on the right of access to file. However, as noted, in *Business at OECD*'s view the balancing should almost always be in the favour of disclosure. The Call for Contributions notes that "[t]he right to access the file is not unlimited, however, and must be balanced against the need to protect confidential information in the file." Call for Contributions, *supra* note 20, at 2.

[28] ICC EFFECTIVE PROCEDURAL SAFEGUARDS, *supra* note 10, at 6.

[29] *See* ICN 2014 REPORT, *supra* note 8, at 10 ("[t]echniques and tools such as redaction, non-confidential summaries, aggregation and anonymisation of information are commonly used to limit the disclosure of confidential information. In litigation or investigative hearings, courts and competition agencies may use tools such as protective orders, closed hearings, sealed filings, and other restrictions on access to confidential information via 'confidentiality rings'").

"data rooms."[30] The European Commission has described data rooms as "an exceptional tool which can – depending on the circumstances of the individual case – safeguard the rights of defence while respecting the legitimate interests of confidentiality of the undertakings or persons from which the Commission has obtained the information."[31]

30. In fact, given the range of mechanisms by which agencies can allow disclosure of confidential information to parties under investigation in a controlled way, it is important that agencies apply those mechanisms in an appropriate hierarchy, taking into account the importance of the information to the case. In particular, allowing disclosure through restricted access (e.g. through confidentiality rings, protective orders and/or data rooms) often offers the best way to minimise harm to the information provider while ensuring that such rights of defence are respected. Where this is not possible, making information available in redacted, aggregated, or summarised form, may be appropriate. As *Business at OECD* has noted previously, limiting access within the defendant team and subjecting disclosure to obligations to only use any disclosed confidential information only for the purposes of the investigation (backed up by sanctions) can (in exceptional circumstances) be highly effective ways of reducing the risk of harm to the information provider.[32] There is extensive experience of such methods within the competition law community, and best practices are readily available.[33] *Business at OECD* urges agencies to adopt and share such best practices, and in doing so, build up the expertise among, and resources available to, investigatory teams.

VI. Confidentiality Protections and Interagency Disclosure

31. The Secretariat's Call for Contributions, in addition to seeking comments on the balancing between ensuring complete access to file and confidentiality protections, notes the tension between protecting confidentiality and facilitating interagency disclosure.[34]

---

[30] "Confidentiality rings" allow the disclosure of confidential information only to specific individuals (for example, only to the in-house legal counsel, to certain business executives, and/or to external legal or economic advisors, of a party under investigation). Those recipients are bound by obligations not disclose the information outside of the "ring," often backed up by sanctions for non-compliance.

[31] EUR. COMM'N, DG COMPETITION, BEST PRACTICES ON THE DISCLOSURE OF INFORMATION IN DATA ROOMS IN PROCEEDINGS UNDER ARTICLES 101 AND 102 TFEU AND UNDER THE EU MERGER REGULATION ¶ 9 (June 2, 2015), *available at* https://ec.europa.eu/competition/mergers/legislation/disclosure_information_data_rooms_en.pdf [hereinafter EU DATA ROOMS BEST PRACTICES]. The EU Data Rooms Best Practices helpfully describe the "restricted manner" in which access is granted, namely "by limiting the number and/or category of persons having access and the use of the information being accessed to the extent strictly necessary for the exercise of the rights of defence." *Id.* To the extent antitrust agencies do not have so already, in *Business at OECD*'s view, there is significant benefit in agencies having the power to issue or seek protective orders as a means of facilitating access to file and balancing the interests of the parties under investigation with those of the information provider, where such a balancing is necessary.

[32] *See* BIAC JUNE 2010 PROCEDURAL FAIRNESS, *supra* note 12, ¶ 2.3 ("In exceptional circumstances, i.e., where there is compelling commercial sensitivity surrounding the sharing of certain confidential information such that it would be demonstrably harmful to allow a defendant's employees full access to it even under . . safeguards . . . it may be appropriate to request that parties agree to special procedures for dealing with the manner in which defendant's employees are provided with access to such exceptionally sensitive elements (without prejudice to the defendant's right to access materials)."). Severe practical problems can also arise if the access team consists only of lawyers. Teams should also include representatives of the business (bound by appropriate non-disclosure agreements).

[33] *See, e.g.*, EU DATA ROOMS BEST PRACTICES, *supra* note 31.

[34] The Call for Contributions asks, "Does your jurisdiction allow the sharing of confidential information with foreign agencies or courts? Does it allow the sharing of confidential information with other domestic agencies or government and legislative bodies. If so, what factors are taken into consideration to decide whether the information is shared (e.g. the approach of that agency or body to the protection of confidential information)." Call for Contributions, *supra* note 20, at 6.

32. In *Business at OECD*'s view, these are two fundamentally different considerations. The tension between access to file and confidentiality protections is relevant to ensuring that the parties under investigation are able to adequately defend themselves, a core requirement of due process. Interagency disclosure aims at a wholly different consideration, namely facilitating the investigatory process, in particular in complex and cross border cases.

33. In the context of interagency disclosure, sharing confidential information (invariably of the parties under investigation) can in fact hinder the exercise of rights of defence and due process. There is currently such diversity among the safeguards applied by agencies and domestic rules on, for example, legal privilege, that broad powers to share confidential information would mean that procedural safeguards are circumvented. As *Business at OECD* has previously recommended, "confidential information should be exchanged through waivers and information gateways only in situations where there are necessary, appropriate and proportionate for the proceedings. Agencies should not exchange confidential information that goes beyond the scope of or it is not related to the investigation or proceeding concerned."[35]

VII. Conclusion

34. As noted above, *Business at OECD* welcomes the OECD's examination of procedural fairness—and in doing so, the acknowledgement of its importance—of which access to file forms a crucial part. It is vital that agencies adopt robust procedures on access to file and ensure that such access is complete, timely, and meaningful. Parties under investigation must be given the opportunity to understand and respond to the allegations being made and have recourse to an independent review of an agency's decision on access to file.

35. On the balancing between access to file and the protection of confidentiality, while confidentiality protections must be strong, that balance must weigh in favour of disclosure unless that would cause significant harm to the information provider or the market. There is a range of means by which agencies can grant disclosure while mitigating any such harm. As *Business at OECD* has noted previously, "There should be a strong presumption in favour of disclosing the facts, documents, theories and legal authority to firms under investigation as early in the investigative process as is practicable."[36] This is fundamental to ensuring that rights of defence are respected and standards of procedural fairness are upheld.

---

[35] BIAC, COMMENTS TO REVISION OF THE OECD 1995 RECOMMENDATION OF THE COUNCIL CONCERNING CO-OPERATION BETWEEN MEMBER COUNTRIES ON COMPETITION INVESTIGATIONS AND PROCEEDINGS ¶ 21 (Feb. 25, 2014), *available at* http://biac.org/wp-content/uploads/2014/05/1-200214_BIAC_Comments_on_Revsions_of_the_OECD_1995_Council_Reccomendation_on_Cooperation_between_Competition_Authorities.pdf.

[36] BIAC FEB. 2010 PROCEDURAL FAIRNESS, *supra* note 7, ¶ 3.11.