



Brussels, **XXX**
[...](2019) **XXX** draft

COMMUNICATION FROM THE COMMISSION

**Communication on the protection of confidential information for the private
enforcement of EU competition law by national courts**

COMMUNICATION FROM THE COMMISSION

Communication on the protection of confidential information for the private enforcement of EU competition law by national courts

I. Scope and purpose of this Communication

1. Access to evidence is an important element for enforcing the rights that individuals derive from Articles 101 or 102 of the Treaty on the Functioning of the European Union ("TFEU") in civil proceedings before national courts. Through the disclosure of evidence, national courts play an essential role in remedying information asymmetries between claimants and defendants.
2. Private enforcement of EU competition law can take different forms such as, among others:
 - (i) declaratory actions which can be understood as actions by which the claimants seek the court to declare that the defendant has infringed EU competition law and that they were harmed by such infringement. In these cases, the quantification of the harm suffered is decided by national courts in separate subsequent proceedings;
 - (ii) actions for injunctive relief which can be understood as actions to stop behaviour contrary to EU competition rules; or
 - (iii) damages actions which can be understood as actions by which the claimants seek compensation for harm caused by an infringement of EU competition law by an undertaking or by an association of undertakings. Damages actions could be follow-on or standalone actions. Follow-on actions are civil actions brought after the European Commission ("Commission") or a national competition authority has found an infringement. Stand-alone actions are civil actions that do not follow from a prior finding by a competition authority of an infringement of competition law. In such a case, the court will, assess, first, whether competition law has been infringed before evaluating whether the claimant has suffered harm, and quantifying such harm and ordering compensation.
3. In actions for private enforcement of EU competition law, national courts are likely to receive requests for disclosure of evidence containing confidential information. This applies in particular to damages actions.
4. In damages actions, national courts should be able to order the disclosure of specified items or categories of evidence, upon request of a party, with due regard to the necessity and proportionality of the disclosure measures.¹ To this end, national courts should have at their disposal a range of measures to protect confidential information in a way that does not impede the parties' effective access to justice or the exercise of the right to full compensation. At the same time, national courts should take into account

¹ Article 5(1), (2) and (3) of Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349, 5.12.2014, p.1. ("Damages Directive")

the safeguards necessary for the protection of evidence containing confidential information.²

5. This Communication seeks to assist national courts when they deal with disclosure requests of confidential information in proceedings for the private enforcement of EU competition law, and in particular when dealing with damages actions.³ The Communication specifically seeks to assist national courts in selecting effective protective measures considering the specific circumstances of the case, the type and degree of sensitivity of the confidential information, as well as other relevant considerations set out in Section III below. Such measures may be used to the extent that they are available under and compatible with national procedural rules, including the right to a fair trial and the right of defence as recognised under EU and national law.
6. As a reference for inspiration and guidance, this Communication is not binding for national courts and does not alter existing rules under EU law or the laws of the Member States. This Communication does not modify or bring about changes to the procedural rules applicable to civil proceedings in the different Member States. Accordingly, there is no obligation for a national court to follow the Communication. This Communication is also without prejudice to the case law of the EU courts.
7. Furthermore, nothing in this Communication should be interpreted as allowing the disclosure of evidence protected under the legal professional privilege, i.e., the principle of confidentiality of communications between a legal representative and his/her client.⁴ This Communication does not cover and is without prejudice to the rules and practices on public access to documents held by the European institutions under Regulation (EC) No 1049/2001⁵ and on the processing of personal data under Regulation (EC) No 2018/1725 and Regulation (EU) 2016/679.⁶

² See recital 18 and Article 5(4) of the Damages Directive.

³ Article 2(1) of the Damages Directive defines "infringement of competition law" as an infringement of Article 101 or 102 TFEU or of national competition law. Article 2(3) of the Directive defines 'national competition law' as provisions of national law that predominantly pursue the same objective as Articles 101 and 102 TFEU and that are applied to the same case and in parallel to Union competition law pursuant to Article 3(1) of Regulation (EC) No 1/2003, excluding provisions of national law which impose criminal penalties on natural persons, except to the extent that such criminal penalties are the means whereby competition rules applying to undertakings are enforced.

⁴ Article 5(6) of the Damages Directive; see also, judgment in Case 155/79, *AM & S Europe v Commission*, EU:C:1982:157 and Case C-550/07 P, *Akzo Nobel Chemicals and Akros Chemicals v Commission*, EU:C:2010:512.

⁵ 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, OJ L 145, 31.5.2001, p.43. "*The purpose of this Regulation is to give the fullest possible effect to the right of public access to documents [...] (recital 4). The access to documents regulation concerns transparency and is intended for disclosure of information to the wider public. As the General Court recently clarified [...] the purpose of Regulation No 1049/2001 is to give the general public a right of access to documents of the institutions, and not to lay down rules designed to protect the particular interest which a specific individual may have in gaining access to one of them*" (see Case T 623/13 *Unión de Almacenistas de Hierros de España v Commission*, ECLI:EU:T:2015:268, paragraph 86). Therefore, this Regulation does not cater for the specific needs of claimants of damages due to EU competition law violations. Instead, those claimants can fully rely on the national rules transposing Articles 5 and 6 of the Damages Directive.

⁶ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, OJ L 295, 21.11.2018, p. 39–98, and 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 ("General Data Protection Regulation"), OJ L 119, 4.5.2016, p.1.

8. Finally, this Communication builds upon certain aspects treated by the Notice on the co-operation between the Commission and the national courts.⁷ This Communication also takes into account and is fully in line with relevant aspects of the Trade Secrets Directive.⁸

II. Disclosure of evidence containing confidential information before national courts

A. Relevant considerations for disclosure of evidence

9. In the context of private enforcement of EU competition law, the ability of the parties to exercise effectively their rights often depends on the possibility to access the evidence necessary to substantiate their claim or defence.
10. For the claimants, such access to evidence will be necessary, among others, to prove an infringement in a stand-alone action, to prove whether there is a causal link between the infringement and the alleged harm and, if so, the quantum of that harm. However, such evidence may not always be in the possession of or readily accessible to the party that bears the burden of proof.
11. For instance, in the context of follow-on damages actions, claimants may have to request access to evidence to prove the existence or the extent of the harm suffered as the necessary evidence is often held by the defendant. Moreover, if, for example, a defendant argues that the claimant has passed on to its own customers the overcharge from the infringement (so-called passing-on defence), the defendant might require access to evidence that is in possession of the claimant or third parties.⁹
12. In most cases, one of the parties will hold the evidence requested. In some instances, the evidence sought (e.g., for finding the infringement or defining the temporal scope of the infringement) will be in documents submitted to or obtained by the defendant from a competition authority through access to the competition authority's file (e.g. pre-existing documents, responses to requests for information, etc.). In other instances, the defendant or claimant might possess additional evidence that is relevant to a damages' claim (e.g. quantification of the harm, establishing the causal link, estimating a possible "passing-on" of an overcharge by the defendants, etc.) and that was not included in the competition authority's file. This is particularly the case for information concerning customer-specific prices, profit margins, revenues or other data such as the pricing behaviour of the purchasers, etc.
13. Disclosure of evidence shall be sought from parties to the civil proceedings or third parties in so far as they are information holders, that is, if they have evidence under their control. The concept of control does not mean that the documents have to be in the physical possession of the information holder. For example, if evidence were to be

⁷ Commission Notice on the co-operation between the Commission and the courts of the EU Member States in the application of Articles 81 and 82 EC, OJ C 101, 27.4.2004 p. 54, as amended by the Communication from the Commission - Amendments to the Commission Notice on the cooperation between the Commission and courts of the EU Member States in the application of Articles 81 and 82 EC, OJ C 256, 5.8.2015, p.5. ("Notice on Cooperation with National Courts")

⁸ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know how and business information (trade secrets) against their acquisition, use and disclosure, OJ L 157, 15.6.2016, p.1-18.

⁹ Communication from the Commission on quantifying harm in antitrust damages actions, OJ C 167, 13.6.2013, p.19, and Practical Guide, quantifying harm in actions for damages based on breaches of Article 101 or 102 of the Treaty on the Functioning of the European Union (11.6.2013). See also, Guidelines for national courts on how to estimate the share of cartel overcharges passed on to indirect purchasers and final consumers (*Note: not yet published*).

located in the hard drive of a defendant's subsidiary, such evidence would be considered to be under the control of the defendant.¹⁰

14. Upon request of a party, national courts may decide to order disclosure of evidence to a party or a third party. As a residual measure, if the parties to the civil proceedings or any other third party cannot reasonably produce the identified evidence and the request concerns a document in the file of the Commission or the relevant national competition authority, the national court may address the order to them.¹¹ This could be the case when the party in question cannot find a specific document (e.g. the file is corrupted, there was a fire in the premises and old physical files were destroyed).
15. In particular, the Damages Directive obliges Member States to provide for the right for claimants and defendants to obtain disclosure of evidence relevant to their claim or defence under the following conditions.¹²
16. First, national courts shall determine whether the claim for damages is plausible and whether the disclosure request concerns relevant evidence and is proportionate¹³. The Damages Directive stipulates that the assessment of proportionality should consider the scope and cost of disclosure, especially for any third parties concerned, including preventing non-specific searches for information that is unlikely to be of relevance for the parties in the procedure. Very broad or generalised disclosure requests will likely fail to meet such requirements.¹⁴
17. Second, disclosure requests shall identify specified items of evidence or relevant categories of evidence "as precisely and as narrowly as possible" on the basis of reasonably available facts.¹⁵ Categories of evidence might be identified by the reference to common features of its constitutive elements such as the nature, object or content of the documents sought to disclose, the time during which they were drawn up or other criteria. For example, a request for categories of evidence could refer to sales data of product Y exchanged by companies A and B between years 2000 and 2005.
18. Third, regarding disclosure of information included in the file of the Commission or of a national competition authority, the Damages Directive specifies that, when assessing the proportionality of a disclosure order, a national court must, among others, consider whether "the request has been formulated specifically with regard to the nature, subject matter or contents of documents submitted to a competition authority or held in the file thereof, rather than by a non-specific application concerning documents submitted to a competition authority".¹⁶ However, as regards these types of

¹⁰ For the notion of undertaking in private enforcement see Case C-724/17 *Vantaan kaupunki v Skanska Industrial Solutions Oy and Others*, EU:C:2019:204, paragraph 47.

¹¹ See, Article 4(3) TEU on the principle of sincere cooperation between the Union and the Member States and Article 15(1) of Regulation No 1/2003 as regards requests for information to the Commission as well as Case C-2/88, *Zwartveld*, EU:C:1990:315, paragraph 22. See also Article 6(10) of the Damages Directive which provides that disclosure from a competition authority is only a measure of last resort ("*Member States shall ensure that national courts request the disclosure from a competition authority of evidence included in its file only where no party or third party is reasonably able to provide that evidence*").

¹² See, recital 15 and Article 5(1) of the Damages Directive.

¹³ See, Article 5(1) and (3) of the Damages Directive; See also, observations of the Commission to the UK High Court of Justice of 27 January 2017 pursuant to Article 15(3) of Regulation (EC) No 1/2003, in the EURIBOR case, paragraph 24, available at http://ec.europa.eu/competition/court/antitrust_amicus_curiae.html

¹⁴ See, recital 23 of the Damages Directive regarding the principle of proportionality and the prevention of fishing expeditions, i.e. non-specific or overly broad searches of information that is unlikely to be of relevance for the parties to the proceedings.

¹⁵ See, recital 16 and Article 5(2) of the Damages Directive.

¹⁶ Article 6(4)(a) of the Damages Directive.

documents, it must be recalled that the Damages Directive provides that leniency statements and settlements submissions can never be disclosed (so called "black list documents").¹⁷ Moreover, if the Commission or a national competition authority has not yet closed its proceedings, the national court cannot order the disclosure of information that was prepared by a natural or legal person specifically for the proceedings of a competition authority; information that the competition authority has drawn up and sent to the parties in the course of its proceedings; and settlement submissions that have been withdrawn (so called "grey list documents").¹⁸

B. Disclosure of confidential information

19. In proceedings for the private enforcement of EU competition law, national courts shall ensure the effective exercise of the claimants and defendants' rights by granting access to the relevant information for substantiating the respective claims (if the conditions for its disclosure are met), while at the same time protecting the interests of the party or third party whose confidential information is subject to disclosure.
20. Moreover, in the context of national proceedings, the fact that information is of a confidential nature is no absolute bar to its disclosure.¹⁹ The same applies also to the disclosure of trade secrets in the context of the Trade Secrets Directive.²⁰
21. However, when disclosing confidential information, such information should be, to the extent possible, protected. Indeed, the protection of business secrets and other confidential information is a general principle of EU law.²¹
22. As regards private enforcement, the Trade Secrets Directive provides for an EU notion of trade secret. Article 2(1) of the Trade Secrets Directive defines trade secret as information which meets all of the following requirements:
 - (i) It is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
 - (ii) It has commercial value because it is secret; and
 - (iii) It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.
23. Trade secrets as defined above are, per definition, to be considered confidential information. However, other types of information could also be considered confidential.
24. What may constitute confidential information might be assessed on a case-by-case basis. For instance, parties to the administrative proceedings may have made

¹⁷ Article 6(6) of the Damages Directive.

¹⁸ Article 6(5) of the Damages Directive.

¹⁹ Case T-353/94, *Postbank*, EU:T:1996:119, paragraphs 66 and 89; see also, for inspiration, Notice on Cooperation with National Courts, cited above, paragraph 24; and Commission 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, OJ C 325, 22.12.2005, p. 7, as amended, OJ C 144, 23.4.2016, p. 29 ("Access to File Notice"), paragraph 24.

²⁰ See Articles 3 and 9 of the Trade Secrets Directive.

²¹ See, Article 339 TFEU. See also, Case C-53/85, *Akzo Chemie v Commission*, EU:C:1986:256, paragraph 28; Case C-36/92 P, *SEP v Commission*, EU:C:1994:205, paragraph 37 and Case C-15/16, *Baumeister*, EU:C:2018:464, paragraph 53. The protection of confidential information is also a corollary of everyone's right to respect for his or her private and family life laid down in Article 7 of the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407 (see, Case C-450/06, *Varec S.A. v Belgian State*, EU:C:2008:91, paragraphs 46–54).

confidentiality claims vis-à-vis other parties to the administrative proceedings but may not make the same claims vis-à-vis the parties requesting disclosure before the national court in civil proceedings. This also applies to third parties from whom the Commission might have obtained information during the administrative proceedings.

25. Moreover, national courts should consider national rules or relevant national case law defining confidential information. Therefore, this Communication does not provide a definition of confidential information for the private enforcement of EU competition law by national courts. However, inspiration can be taken from the jurisprudence of the EU courts,²² which qualifies as confidential information the evidence that meets the following cumulative conditions:

- (i) it is known only to a limited number of persons;²³ and
- (ii) its disclosure is liable to cause serious harm to the person who provided it or to third parties; this is usually the case where the information has commercial, financial or strategic value. In this sense, the confidential nature of information may depend on the persons to whom it will be disclosed (e.g. whether a competitor, a customer or a supplier).²⁴ To assess the potential for causing harm it is also relevant to consider how recent the information is. Sensitive information concerning an ongoing or future business relationship, internal business plans and other forward looking commercial information could often qualify (at least partially) as confidential information. However, even such information may lose its confidential nature when it has "lost its commercial importance due to the passage of time";²⁵ and
- (iii) the interests liable to be harmed by disclosure are, objectively, worthy of protection. In this regard, the interest of a party to protect itself or its reputation against any order for damages made by a national court because of its participation in an infringement of competition law is not an interest worthy of protection.²⁶

²² Case T-198/03, *Bank Austria v Commission*, EU:T:2006:136, paragraph 71; Case T-474/04 *Pergan Hilfsstoffe für industrielle Prozesse v Commission*, EU:T:2007:306, paragraph 65; Case T-88/09, *Idromacchine v Commission*, EU:T:2011:641, paragraph 45; Case T-345/12, *Akzo Nobel and Others v Commission*, EU:T:2015:50, paragraph 65; and Case C-162/15 P *Evonik Degussa v Commission*, ECLI:EU:C:2017:205, paragraph 107.

²³ However, information may lose its confidential nature as soon as it becomes "available to specialist circles or capable of being inferred from publicly available information"; see, for instance, Order in Joined Cases T-134/94 etc., *NMH Stahlwerke v Commission*, EU:T:1996:85, paragraph 40; Order in Case T-89/96, *British Steel v Commission*, EU:T:1997:77, paragraph 29; Order in Case T-271/03 *Deutsche Telekom v Commission*, EU:T:2006:163, paragraphs 64 and 65; and Order in Case T-336/07 *Telefónica v Commission*, EU:T:2008:299, paragraphs 39, 63 and 64; See also, Access to File Notice, paragraph 23.

²⁴ This is also relevant concerning the protection of third parties from the risk of retaliation by a competitor or trading partner that can exercise significant commercial or economic pressure on them. See, for example, Case C-310/93, *BPB Industries and British Gypsum v Commission*, EU:C:1995:101, paragraphs 26 and 27.

²⁵ Information that was confidential but dates from five years or more ago must be considered historical unless exceptionally the applicant shows that it still constitutes an essential element of its commercial position or that of a third party; see in this respect Case C-162/15 P, *Evonik Degussa v Commission*, EU:C:2017:205, paragraph 64; and Case C-15/16, *Baumeister*, EU:C:2018:464, paragraph 54. See also, Access to File Notice, paragraph 23.

²⁶ See *Bank Austria*, cited above, paragraph 78, and *Evonik Degussa*, cited above, paragraphs 107 to 110 and 117. See also judgment of the European Court of Human Rights in *Gillberg v Sweden* [GC], No. 41723/06, paragraph 67, according to which "Article 8 cannot be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence."

C. Cooperation between the Commission and national courts in the context of disclosure of evidence

26. In civil proceedings for the application of Articles 101 and 102 TFEU, a national court may decide to ask the Commission for an opinion on questions concerning the application of EU competition law or to transmit any legal, economic or procedural information in its possession in line with the principle of loyal cooperation of Article 4(3) of the Treaty on European Union.²⁷ The national court might, for example, request documents from the Commission's file if no other (third) party can reasonably provide them.²⁸ In this regard, it is important to recall that, as set out above, the Commission will not transmit black listed documents or, if its proceedings are not closed, grey listed documents (see paragraph 18).²⁹
27. Moreover, the Commission's assistance to national courts must not undermine the guarantees that natural and legal persons have following the principle of professional secrecy pursuant to Article 339 TFEU and Article 28 of Regulation (EC) No 1/2003.³⁰
28. When the Commission is of the view that the information requested by the national court contains confidential information, before transmitting the information concerned, it will ask the national court whether it can guarantee the protection of confidential information and will consider the measures put in place by the national court to this end. The national court should provide the person whose confidential information is subject to disclosure with the necessary guarantees for the protection of this information.³¹
29. If the Commission considers that the rights of natural and legal persons to protect confidentiality can be appropriately safeguarded by the national court, it will transmit the requested information to the national court. The latter may then disclose the information in national proceedings by applying the measures to protect the confidentiality of information communicated to the Commission and taking into account any observations provided on this matter by the Commission.

III. Measures for protection of confidential information

A. Introduction

30. As a source of inspiration and non-binding guidance, this Communication seeks to assist national courts to evaluate, in a specific disclosure request, what measures may need to be put in place before confidential information is disclosed.
31. By way of example, the Damages Directive refers to a few measures such as the possibility of redacting sensitive passages in documents, conducting hearings in

²⁷ Article 15(1) of Regulation (EC) No 1/2003; Notice on Cooperation with National Courts, paragraphs 21, 27 and 29; Postbank, paragraph 65; see also *Zwartveld*, paragraphs 21-22.

²⁸ See Article 6(10) of the Damages Directive.

²⁹ See Article 16a 2. 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 as amended, OJ L 123, 27.4.2004, p.18. See also paragraph 26 of the Notice on cooperation with national courts for refusal to transmit information due to overriding reasons relating to the need to safeguard the interests of the Union or to avoid any interference with its functioning and independence.

³⁰ *Postbank*, paragraph 90.

³¹ Notice on Cooperation with National Courts, paragraph 25. See also, paragraph 12 of Commission Opinion of 22 December 2014 following a request under Article 15(1) of Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, *The Secretary of State for Health and others v Servier Laboratories Limited and others*, C(2014) 10264 final, available at http://ec.europa.eu/competition/court/confidentiality_rings_final_opinion_en.pdf.

camera, restricting the persons allowed to see the evidence and instructing experts to produce summaries of the information in an aggregated form or otherwise non-confidential form.³² Naturally, the choice of measure used to protect confidential information when ordering disclosure would depend on the specific national procedural rules including to what extent certain measures are at all available.

32. The choice of one or more effective measures to protect confidentiality in disclosure proceedings will be a case-by-case assessment which may depend on several factors, such as, *inter alia*:

- (i) the nature and degree of sensitivity of the information subject to disclosure (e.g. customer names, prices, structure of costs, profit margins, etc.) and whether for the purpose of the exercise of the rights of the party requesting disclosure, access to such information can be given in an aggregated or anonymised form or not;
- (ii) the extent of the requested disclosure (i.e. volume or number of documents to be disclosed);
- (iii) the number of parties concerned by the litigation and disclosure. Certain measures for protection of confidentiality might be more effective than others, depending on whether there is more than one requesting party and/or disclosing parties;
- (iv) the relationship between the parties (for example, whether the disclosing party is a direct competitor of the party seeking disclosure,³³ whether the parties have an ongoing supply relationship, etc.);
- (v) whether the owners of the information subject to disclosure involved in the litigation before the national court are third parties.³⁴ The rights of third parties to the civil proceedings in the protection of their confidential information must also be taken into account.³⁵ The disclosing party may have in its possession third party documents the content of which may be confidential towards the requesting party or other parties to the proceedings.³⁶
- (vi) the circle of individuals allowed to access the information (i.e. whether disclosure should be granted only to external legal representatives or whether the requesting party (company representatives) would also be allowed to access the information);

³² See, recital 18 of the Damages Directive.

³³ For example, if the parties are direct competitors, the measure chosen must ensure that the way the information is disclosed will not enable the parties to collude or give a competitive advantage to the party requesting disclosure.

³⁴ The disclosing party may not necessarily be the information owner. For example, a party may have accessed information from third parties during the administrative proceedings before the Commission or a national a competition authority. Having had access to the information does not make this party the information owner.

³⁵ See in particular, Article 5(7) of the Damages Directive ("Member States shall ensure that those from whom disclosure is sought are provided with an opportunity to be heard before a national court orders disclosure [...]").

³⁶ For example, in relation to non-confidential versions of documents regarding a data collection process that was prepared specifically for access to the file purposes, see Commission Opinion of 29 October 2015, in application of Article 15(1) of Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, *Sainsbury's Supermarkets Ltd v Mastercard Incorporated and Others*, (C(2015) 7682 final), paragraph 23, where the Commission stated that, at that stage, it had not been necessary to take a position as to whether the information was confidential vis-à-vis other parties, but that third parties who provided the information might object to sharing the information with the claimant. The opinion concluded that "[...], the fact that Mastercard might be satisfied with particular arrangements made, such as a confidentiality ring, would not necessarily satisfy third parties who submitted the information." The opinion is available at http://ec.europa.eu/competition/court/sainsbury_opinion_en.pdf.

- (vii) the risk of inadvertent disclosure;
 - (viii) the ability of the court to protect confidential information throughout the civil proceedings and even after the proceedings are closed: national courts may conclude that, to effectively protect the confidential information, a single measure will not suffice and other measures may need to be adopted throughout the proceedings; and
 - (ix) any other constraints or administrative burdens associated with the disclosure such as increased costs or additional administrative steps for the national judicial system, costs for the disclosing parties, potential delays to the proceedings, etc.
33. Finally, the choice of the most effective measure(s) may depend on the existence of and ability to impose and enforce sanctions for failure or refusal to comply with measures ordered by courts to protect confidential information. National courts should be able to impose sufficiently deterrent penalties for non-compliance with obligations to protect confidential information, in particular to avoid that parties use confidential documents outside the proceedings in which they have been disclosed.³⁷ Pursuant to Article 8 of the Damages Directive, national courts must be able to effectively impose penalties on parties, third parties and their legal counsels.³⁸
34. The precise nature and scope of the sanctions will depend on the national rules. Pursuant to the Damages Directive, sanctions for the failure to comply with a disclosure order, the destruction of relevant evidence; the failure or refusal to comply with the obligations imposed by a national court order protecting confidential information; and the breach of the limits on the use of evidence provided for, shall include the possibility to draw adverse inferences, such as presuming the relevant issue to be proven or dismissing claims and defences in whole or in part, and the possibility to order the payment of costs.³⁹ External legal counsels or experts may also be subject to disciplinary sanctions by their professional associations (e.g. suspension, fines, etc.).
35. In conclusion, the choice of a disclosure measure may require a comprehensive evaluation of multiple factors. To assist national courts in this assessment, and based also on the Commission's experience in administrative and judicial proceedings, this Communication provides an overview of the most common measures that – subject to their availability under Member States' procedural rules – may be used to protect confidential information and of relevant considerations as regards their effectiveness.

B. Confidentiality rings

36. A confidentiality ring is a disclosure measure whereby specified categories of information, including confidential information, are made available by the disclosing party only to defined categories of individuals.⁴⁰

³⁷ See e.g. Article 16 of the Trade Secrets Directive that provides for the possibility of imposing sanctions on any person who fails or refuses to comply with measures ordered to preserve the confidentiality of trade secrets in the course of legal proceedings.

³⁸ See, Article 8 of the Damages Directive. See also recital 33 of the Damages Directive. The recourse to sanctions is of the essence considering that in most cases national courts might be unable to exercise real time supervision of the parties' compliance with the rules of the disclosure order, notably in the case of a confidentiality ring.

³⁹ Article 8(2) of the Damages Directive.

⁴⁰ This disclosure measure is also referred to as confidentiality clubs, depending on the jurisdictions. This type of measure can also be used in administrative proceedings. For Commission procedures, see paragraphs 96 and 97 of Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU, OJ C 308, 20.10.2011, p. 6–32 and, paragraph 9 of Best Practices on the disclosure of information in data rooms in

B.1. Confidentiality rings as an effective means for protecting confidentiality

37. Confidentiality rings can be an effective measure for national courts to protect confidentiality in a variety of circumstances.
38. First, confidentiality rings can be effective to ensure disclosure of quantitative data or very sensitive commercial and/or strategic information that, while relevant for the claim of the party, are very difficult to summarise in a meaningful way⁴¹ or cannot be disclosed without risking being excessively redacted,⁴² and thus without losing evidentiary value. By disclosing documents in the confidentiality ring, relevant confidential information is effectively disclosed but the potential harm caused by the disclosure is controlled or minimised by restricting access to the information depending on the different circumstances of the case (e.g. type and nature of documents, relationship of the parties, composition of the ring, third party documents, etc.). In such situations, confidentiality rings help strike a balance between the need for disclosure and the obligation to protect confidential information.⁴³
39. Second, confidentiality rings may allow procedural economies and efficiencies in particular when the number of documents requested is voluminous and the parties are able to agree on a core list of documents considered relevant for the purposes of the claim. Disclosing parties will not need to engage in disputes over the confidentiality of specific items of information nor will the court need to examine these, thereby reducing the uncertainty and the potential delays caused by confidentiality negotiations. The disclosing party will not need to prepare non-confidential versions of the documents that will become accessible in the ring (except, in a more limited fashion, in cases where confidentiality rings are used as a filtering measure).⁴⁴
40. Third, for national courts, confidentiality rings may be an effective measure in terms of the financial costs of disclosure and in particular regarding the economic impact of imposing certain disclosure measures on the parties. This may be particularly the case where parties have different economic means and the difference in financial resources affect their ability to exercise fully their rights. For instance, if the parties engage in confidentiality disputes on whether further access is needed, the legal costs for both parties could increase substantially. In such a situation, opting for a confidentiality ring may contribute to lowering the costs of disclosure in particular in those cases

proceedings under Articles 101 and 102 TFEU and under the EU Merger Regulation, available at http://ec.europa.eu/competition/mergers/legislation/disclosure_information_data_rooms_en.pdf. For guidance on the use of confidentiality rings in Commission proceedings, see http://ec.europa.eu/competition/antitrust/conf_rings.pdf.

⁴¹ See, for example, OECD report of 5 October 2011 on Procedural fairness: transparency issues in civil and administrative enforcement proceedings, p. 12; see also, Scoping note on Transparency and Procedural Fairness as a long-term theme for 2019-2020, 6-8 June 2018, OECD Conference Centre, p.4.

⁴² For example, in relation to data collected by external contractors from the participants in a Commission's survey, in paragraph 21 of its Opinion in *Sainsbury's v Mastercard*, the Commission concluded that the information could not be anonymised in a way that fully respected the data providers' legitimate interest in the protection of their confidential information.

⁴³ See in this respect the disclosure into a confidentiality ring ordered by the General Court in case T-296/11, *Cementos Portland Valderrivas, SA v Commission*, paragraph 24: "[...] with a view to reconciling the adversarial principle and the characteristics of the preliminary investigation stage of the procedure, when the undertaking concerned has neither the right to be informed of the essential evidence on which the Commission relies nor a right of access to the file, the order of 14 May 2013 limited inspection of the information supplied by the Commission to the applicant's lawyers and made such inspection conditional upon them giving an undertaking of confidentiality."

⁴⁴ In this setting, the external counsel of the requesting party may be allowed to review all the information requested in a confidentiality ring with a view to identifying the selected items of information for which actual disclosure to the requesting party will be sought. For those documents, a non-confidential version will be prepared and shared with the requesting party. In such cases, the confidentiality ring will be used in combination with redactions.

where the parties are able to agree on a core list of documents considered relevant for the claim.

41. Fourth, confidentiality rings do not necessarily require the physical handing out of the information or the physical presence of the members of the ring in a particular location. It is often the case that the information is transferred and accessed by electronic means. Where possible, electronic disclosure has various benefits. For both national courts and parties, electronic disclosure does not impose burdens in terms of physical rooms that may have to be exclusively reserved for this use for several days, of the need to travel to the different locations, or of installing the required IT tools at those different locations, etc.
42. Finally, confidentiality rings may be an effective measure to avoid the risks of inadvertent errors (either human or technical) which may occur during the process of redacting confidential information from documents.

B.2. Organising a confidentiality ring

43. If a national court considers that a confidentiality ring is an effective measure of disclosure in a given case, it may need to decide on a number of elements that will be laid down in the court order, even if some aspects may be already established by general court guidance or other procedural rules.⁴⁵ The most significant elements are the following.

a. Identifying the information accessible in the ring

44. The national court will need to identify the specific items of evidence or categories of information (e.g. list of documents) that will be included in the confidentiality ring.
45. For example, in follow-on damages claims proceedings, the information to be disclosed in the confidentiality ring may include the confidential version of the decision of the Commission or the relevant national competition authority, information prepared and submitted by the disclosing party to them during the administrative proceedings and information obtained by the disclosing party during the access to the file procedure or other claim-specific information from parties and third parties that was not part of the administrative proceedings.
46. In this respect, as set out above, it may facilitate the decision of the court, if the parties agreed on a list of core documents considered relevant for the purposes of the proceedings. However, it is not always possible for the parties to agree to this type of disclosure since other interests, for instance those of third parties, may require the involvement of the national court. Therefore, the court may need to define the disclosure rules even if the parties agreed to the procedure.

b. Composition of the ring

47. After hearing the parties, the court may order who will be members of the confidentiality ring as well as the members' access levels.⁴⁶

⁴⁵ For an example of measures of organisation of procedure, see the practice rules for the implementation of the rules of procedure of the General Court, and in particular, pages 34-37 dealing with confidentiality, OJ 2015 L 152, p.1, corrigendum, OJ 2016 L 196, p.56, and the amendments adopted on 13 July 2016, OJ 2016 L 217, p.78.

⁴⁶ The decision of the composition of the ring may also define the maximum number of members per party.

48. The members of the confidentiality ring are likely to be those individuals who will have the right to review the documents in the confidentiality ring. The decision on the composition of the ring is a case-by-case exercise that will critically depend on the type and nature of the information concerned by the disclosure request.
49. The members of the confidentiality ring may range from external advisers of the parties (e.g. external legal counsel or other advisers) to in-house counsel and/or other company representatives.
50. Once the court has taken a decision on the composition of the confidentiality ring, it may need to identify each individual member by name, role or function and relation to the parties.⁴⁷ The court may also identify the personnel of the court that shall be present or can access the ring alongside the parties or at any other time in case of physical confidentiality rings.

External advisers

51. Depending on the relationship between the requesting and the disclosing parties, access to the ring may need to be limited to external advisers. External advisers may include not only legal counsel but also other advisers or experts such as, e.g. accountants, economists, financial advisors or auditors, depending on the needs of the case at hand.
52. The restriction of access to external legal counsel can be necessary because in-house counsel may serve their company in a variety of other functions as well. An in-house counsel may often be involved, directly or indirectly, in strategic decision-making of the company. The risk that information accessed in the confidentiality ring may later affect the in-house counsel's advice to the managers of the company for business decisions may be too high to allow them to access certain confidential data in certain circumstances (for example, where the parties to the civil proceedings are actual or potential competitors and access to commercially sensitive or strategic information may give them an unwarranted competitive advantage; where the parties are in a supply relationship; or where the information to be disclosed includes agreements that are still in force, and therefore contain current confidential information).
53. External counsel are generally not involved in the decision-making processes of the companies they represent and they are in a number of Member States' legal orders deemed able to view business secrets, strategic plans, or other sensitive data. However, since reserving access to external counsel may to some extent constrain the exercise of the parties' own right to access evidence, courts may need to carefully consider the type of documents concerned by the disclosure, and restrict access to external counsel only when considered necessary and possible under the EU (see in paragraph 55 below the rules of the Trade Secrets Directive) and national procedural rules.

In-house counsel and/or other company representatives

54. There may be circumstances where the national court may deem it appropriate for in-house counsel and/or company representatives (e.g. managers or other staff⁴⁸) to access confidentiality rings. This can be the case where (all or part of) the confidential information in question is regarded as less commercially sensitive or where disclosure to company employees may not be liable to cause harm due to, for example, the relationship between the parties.

⁴⁷ See Commission Opinion in *Servier*, cited above.

⁴⁸ E.g. individuals employed by the requesting party through labour contracts or other type of service or contractual agreements.

55. Access by in-house counsel and/or other company representatives may also be granted upon the motivated request of external legal representatives.⁴⁹ These requests are lodged where the external legal counsel considers that their client's case cannot be properly assured without information in certain of the documents (or parts thereof) being disclosed to the client. This is the case, for instance, where the external legal counsel is unable to judge the accuracy or the relevance of the information for the party's claim or where the information is very technical or product/service specific and requires sector or industry knowledge to make a relevance assessment. In particular, in litigations related to the unlawful acquisition, use or disclosure of trade secrets, Article 9(2) of the Trade Secrets Directive imposes that the restricted circle of persons entitled to access the evidence shall be composed of at least one natural person from each of the parties.⁵⁰
56. Furthermore, in some Member States' legal orders, it may be possible in specific situations to seek the court's consent to share specific items of information with in-house counsel or with company representatives without allowing the individuals to become members of the ring.
57. Access by in-house counsel and/or company representatives shall be assessed on a case-by-case basis and may depend on the closeness of the individuals suggested by the parties to the business or area of activity concerned by the request or other factual circumstances.
58. Therefore, depending of the specific national rules and the specific facts at hand, confidentiality rings may be composed of external legal counsel only or of a mix of external legal counsel, other external experts (e.g., economists, accountants, auditors, etc.), in-house counsel and/or company representatives.

Access rights

59. Where the confidentiality ring is composed of external legal counsel and in-house counsel and/or company representatives, it is possible that all parties have access to all the information disclosed in the ring or that different access rights are granted.
60. It may be the case that confidentiality rings consist of two access levels: an inner ring level composed by external legal counsel who have the right to access the most sensitive information, and an outer ring level composed of in-house counsel and/or company representatives who have the right to access the remaining confidential information.
61. Upon a justified request of the disclosing party, the court might - depending on national procedures - also impose special restrictions in relation to access of certain members of the ring to specific documents.
62. In some cases, the confidentiality rings could also be accessed by administrative and/or support personnel (including for example external eDisclosure or litigation support providers engaged to provide electronic technical services) under the supervision of the other persons identified in the ring and under the same confidentiality obligations.

⁴⁹ See, for inspiration, Access to File Notice, paragraph 47.

⁵⁰ This requirement is limited to trade secrets and cannot be extrapolated to other confidential information.

c. Written undertakings of the members of the ring

63. Members of the confidentiality ring may be asked to submit written undertakings to the court regarding the confidential treatment of any information included in the confidentiality ring.
64. Such undertakings may concern, *inter alia*, the duty not to disclose the confidential information to any person different from those listed by the court as ring members without the express consent of the court;⁵¹ the obligation to use the confidential information only for the purposes of the civil proceedings in which the disclosure order was issued; the obligation to ensure adequate custody of the information within the ring members; the obligation to adopt any measure necessary in the circumstances to prevent unauthorised access; the obligation to return or destroy any copies of documents containing confidential information; the obligation not to print the documents accessed in electronic form or to make them inaccessible to the identified persons from any computer or device after a specific date, etc.
65. These undertakings and, in particular, the obligation not to disclose the confidential information to the clients may be of significant relevance in those jurisdictions in which external legal counsels are bound, pursuant to deontological bar rules or other rules, to share the information with their clients.
66. In addition, where company representatives participate in a confidentiality ring, they may be subject to rather onerous requirements. For example, the national court may deem it appropriate to prescribe that the employee in question no longer works in the line of business concerned by the claim.

d. Logistics

67. Confidentiality rings require national courts to decide on various organisational, infrastructure and logistical measures.⁵² First, confidentiality rings may involve the physical or the electronic disclosure of confidential information. Physical disclosure may be organised and held at judicial premises with court personnel in control of the disclosure or by the parties at their premises with no involvement of the court. Physical disclosure may involve handing over paper copies of documents but also the disclosure of evidence by means of a CD, DVD or a USB key in a physical location in court premises or at parties' premises.
68. Disclosure in a confidentiality ring may occur also by electronic means. In such case, the data is uploaded and stored in an electronic location (e.g. cloud) for the duration of the disclosure exercise, and access to the information is protected by passwords.
69. If the disclosure of the information into the confidentiality ring is not done electronically but is held at the court's premises, the court may need to ensure that the facilities for accessing the information are adequate, unless the persons accessing the ring are allowed to bring their own equipment.
70. Second, the court may determine the duration of the disclosure exercise.

⁵¹ This is a departure from the usual practice in which a party's legal representative is permitted to disclose to his/her client information and pleadings received from other parties in the proceeding and discuss them freely.

⁵² The protection of confidential information in the context of disclosure requests may require changes to the usual functioning of the court's logistic or even telematics procedures, or putting in place ad hoc procedures on a case-by-case basis within the boundaries of the applicable national procedural laws.

71. Third, the court may also need to decide the hours of availability of the disclosure rooms (e.g. during business hours only), whether court personnel must be present in the disclosure rooms, whether notes or files can be brought into the rooms, etc.
72. Finally, to ensure that confidential information disclosed to the parties' external advisers in a confidentiality ring is protected throughout the proceedings, national courts may request that parties submit both a confidential and a non-confidential version of their pleadings (the latter, for instance, only including quantitative data in an aggregated or anonymised form),⁵³ that confidential information is only referred to in a confidential annex, or that other measures are taken to protect the confidential nature of the information.

C. Redactions

73. When deciding on the appropriate measure of disclosure, national courts may also consider ordering the disclosing party to edit the documents removing the confidential information. This procedure is known as redaction.
74. Redaction may involve the replacement of each piece of confidential information with anonymized data or aggregate figures, the substitution of deleted paragraphs by informative or meaningful non-confidential summaries or even the entire blacking-out of parts of the documents containing the confidential information.
75. Disclosing parties may be required to limit redactions to what is strictly necessary to protect the interests of the information owners. Limited redactions of certain confidential information may suffice to protect all confidential information in one or a number of documents. For example, redacting customers' names while leaving un-redacted the respective quantities of product supplied may be sufficient to protect confidentiality.⁵⁴
76. Redaction of relevant information without replacing the information by a non-confidential text may not strike the right balance between the right of the disclosing party to the protection of confidential information and the right of the party requesting access to the evidence to substantiate its claim or defence. Excessive redactions applied to entire pages or sections of documents or entire annexes may also not be acceptable for the purposes of the proceedings.

C.1. Redactions as an effective means for protecting confidentiality

77. Redactions may be an effective measure to protect confidential information for categories of documents when, despite the replacement of the confidential information with non-confidential text, the documents and information disclosed remain meaningful and suitable for the exercise of the rights of the party requesting disclosure.
78. Hence, the use of redactions may be especially effective where the confidential information concerns market data or figures (e.g. turnover, profits, market shares, etc.) which can be substituted with representative ranges or where qualitative data can be meaningfully summarised.

⁵³ The non-confidential versions of the pleadings must allow the other parties to understand the arguments and the evidence being referred to so that they can discuss the case with their legal representatives and instruct them accordingly.

⁵⁴ Accessibility to information on volumes supplied may be essential to quantify the harm suffered on the lower level of the supply chain (i.e. by indirect customers).

79. Redactions may also be an effective measure to protect confidential information when the volume of confidential information subject to disclosure is limited. A very large number of documents to be redacted may, depending on the circumstances of the case, suggest that other disclosure measures would be more appropriate, considering the time, cost and resources necessary to prepare non-confidential versions.
80. Finally, redaction of third party confidential information may also be effective in cases where the information holder may have in its possession information from third parties that may not be confidential to him but that may be confidential vis-à-vis the requesting party.⁵⁵ For example, this could be the case if the requesting party who will get access to the information and the third party are competitors. In such cases, the disclosing party may need to obtain the agreement of third parties to disclose the confidential information or otherwise obtain their agreement to a proposal for redactions.⁵⁶ However, national courts may find that redactions are less efficient in those cases where the request includes a large number of third party documents because the process of liaising with third parties in this respect might add complexity to the task.

C.2. Redacting confidential information

81. Depending on the different procedural rules, national courts may be more or less actively involved in the process of redactions. National courts may oversee and control the redaction process and be the interlocutor for the parties and third parties. Alternatively, parties may be primarily responsible for securing non-confidential versions and/or obtaining third parties' agreement to the proposals for redaction.
82. In any case, to steer the process of preparing non-confidential versions, national courts may find it useful to issue general guidance to parties and/or case-specific guidance for the proceedings pending before it, if possible under national procedural rules. Such guidance may be valuable to set out the procedure the courts may expect the parties to follow when dealing with redactions of confidential information and to clearly outline the respective responsibilities.
83. For efficient handling of the applications for redactions, national courts may request parties:
- (i) To mark all the confidential information in the original confidential documents in square brackets and highlighted in a way that remains legible before taking a decision on what should be redacted;
 - (ii) To draft a list of all the information proposed to be redacted (each word, data, paragraph and/or section to be redacted);
 - (iii) For each proposed redaction, to submit the reasons why the information should be treated confidentially;
 - (iv) To substitute the redacted information not with simple indications such as "business secret", "confidential" or "confidential information", but with an informative and meaningful non-confidential summary of the redacted

⁵⁵ This can occur because the third-party documents do not include confidential information vis-à-vis the information holder or because the information holder already had access to a non-confidential version of the documents, in which information regarded as confidential vis-à-vis the information holder had been previously redacted.

⁵⁶ This is because the fact that the information holder agrees for example to the conditions of a confidentiality ring does not mean that this would be acceptable for third parties. See, Commission Opinion in *Sainsbury's Supermarkets Ltd v MasterCard Incorporated and Others*, cited above, paragraph 23.

information.⁵⁷ When redacting quantitative data (e.g. sales, turnover, profits, market shares data, prices, etc.) meaningful ranges or aggregate figures may be used. For example, for sales and/or turnover data, ranges wider than 20% of the precise figure may not be meaningful; in the same vein, for market shares, ranges wider than 5% may also not be meaningful depending on the circumstances of the case pending before the court;

- (v) To submit non-confidential versions of the documents concerned which mirror the structure and format of the confidential versions. In particular, the information in the original document such as titles or headings, page numbers and paragraph listings would remain unmodified so that the person reading the document is able to understand the extent of the redactions and the impact of the redactions on the ability to understand the information once disclosed;
 - (vi) To ensure that the non-confidential versions submitted are technically reliable and that the information redacted cannot be retrieved by any means including the use of forensic tools.
84. Once the applications for redactions are submitted, it will be for the national court to decide whether the proposed redactions are acceptable. Where there is a dispute, the court should be able to hear the parties and third parties concerned before deciding.
85. Once redacted, the non-confidential versions of the original documents may be used throughout the civil proceedings and no further protection may be required.

D. Appointment of experts

86. In some jurisdictions, national courts may also decide to appoint a third party individual with expertise in a specific field (e.g. accounting, finance, competition law, audit, etc.) to access the confidential information concerned by a disclosure request. The role of such court appointed expert is different from party appointed experts, which are frequently used in some jurisdictions to support a party's claim or defence.
87. If national procedural rules allow, the expert's assignment may for example be to draft a meaningful non-confidential summary of the information to be made available to the requesting party. Alternatively, and depending on the national procedural rules applicable, the expert may be asked to draft a confidential report that may be made available only to the external counsel of the requesting party and a non-confidential version of the report for the requesting party.

D.1. Appointing experts as an effective means for protecting confidentiality

88. The appointment of experts may prove to be an effective measure first where the information to be disclosed is commercially very sensitive and quantitative or technical in nature (e.g. information included in commercial or accounting books, client data, manufacturing processes, etc.). In such cases, the experts may summarise and/or aggregate confidential information with a view to making it accessible to the party requesting disclosure.
89. Second, experts may also be effective where further access to confidential documents containing underlying data is sought by one of the parties. This may occur, for instance, in damages claims in which it is necessary to have access to underlying data

⁵⁷

See, for example, Article 103(3) Rules of Procedure of the General Court.

for estimating the share of the overcharge passed on (e.g. sales prices, volume of sales, rebates, internal documents showing pricing strategies, etc.).

90. Third, in cases where a very large number of the documents to be disclosed concerns third party confidential information, courts may consider it more effective to appoint an expert to access the information and give his opinion as to the confidential nature of the information, than to engage in discussions with parties about the scope of redactions or to set up a confidentiality ring.

D.2. Instructing experts

91. It will be for the national court to appoint and instruct the appointed experts. Depending on the different procedural rules, national courts may be able to appoint third party independent experts from a list of "court approved" experts, from a list of experts proposed by the parties, etc. Pursuant to national procedural rules, when appointing an expert, the national court may also need to consider or decide who will bear the expert costs.
92. Once the expert is chosen, national courts may request that the expert submits written undertakings regarding the confidential treatment of any information to which they will have access.
93. As in the case of the members of a confidentiality ring, experts may be required to agree not to disclose confidential information to any person other than those listed by the court or without the express consent of the court; to use the confidential information only for the purposes of the civil proceedings in which the disclosure order was issued; to ensure adequate custody of the information; to adopt any measure necessary in the circumstances to prevent unauthorised access and to return or destroy any copies of documents containing confidential information, etc.
94. Experts may be also required to declare any conflicts of interests that may prevent them from carrying out their task.
95. Furthermore, the court may instruct the expert as to the type of report to produce (e.g. summary, aggregate data report, etc.) and whether the expert is to produce both a confidential and a non-confidential version of the report.
96. Whenever a confidential version of the expert report is produced, it may generally only be shared with external legal representatives of the parties, while the parties may only receive access to a non-confidential version of the report. Where the national court restricts access to the confidential version of the report prepared by an expert only to a party's external legal representative, its external legal representative will be asked not to share the confidential information contained therein with his or her client. If under national procedural rules, parties are also allowed to appoint their own experts, the independent expert's assignment may take this into account and provide for access of parties' experts to the evidence as well.
97. Provided that, under national rules, parties were able to access a confidential version of the expert's report, all the caveats highlighted above regarding client's access to confidential information disclosed in a confidentiality ring (see paragraphs 54-57) would also apply in such situation.

IV. Protection of the confidential information throughout and following the proceedings

98. National courts may also need to consider how the confidential information will be used and cited, for instance, during pleadings and/or during the hearings.
99. For example, if the parties' representatives use information accessed in a confidentiality ring or included in a confidential expert report in their pleadings, national courts may ask them to refer only to such information in confidential annexes to be submitted alongside the main pleadings. If parties' representatives wish to refer to such information during the court's hearing or when an expert is heard on such evidence, national courts may organise *in camera* (i.e. closed) hearings, if possible under the applicable civil procedural rules.
100. The need to protect confidential information may also arise later, for example, at the time of the adoption, notification or publication of the judgments, in the case of requests for access to court's records or during appeals. Indeed, the confidential expert reports might be part of the court's file. In such cases, national courts may need to adopt measures to protect such information once the civil proceedings are closed or, if not procedurally possible, to request that the experts only prepare non-confidential versions of their reports.

A. *In camera* hearings

101. Pursuant to the principle of open justice, civil proceedings are generally public in nature⁵⁸ and national courts may weigh the interest to the protection of confidential information against the need to limit the interference with the principle of open justice.
102. National courts may decide to exclude references to confidential information at public hearings or to hold *in camera* only those parts of the hearings where confidential information might be discussed. In this case, national courts would have to decide who would be allowed to attend the closed session. This decision may depend on how and to whom the confidential information was disclosed (e.g. to the parties' external advisers, to an expert, to the parties' company representatives, etc.).
103. Hearings *in camera* may be an effective means to cross-examine confidential evidence disclosed through a confidentiality ring or to hear the experts on the confidential evidence included in their reports.
104. During *in camera* parts of hearings, only those external and/or internal company representatives who were granted access to the confidential documents in the confidentiality ring and (if applicable) as well as the expert who accessed the information would be permitted to participate.

B. Publication

105. National courts may have to ensure that any decisions or judgments that will be published exclude confidential information.
106. To protect confidential information of the parties or third parties, when rendering the judgment and ordering its publication, national courts may consider to anonymise any

⁵⁸ See, Article 6 of the European Convention of Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union, cited above. Exceptions to this principle may relate in some Member States to the maintenance of public order, the protection of fundamental rights or other overarching objectives.

information that could identify the source of the information/or to redact parts of the judgment referring to confidential information from the publicly available version of the ruling.⁵⁹

107. Beyond publication, the court may also have to consider how to protect the confidential information in the version of the judgment to be notified to the parties without prejudice to the right of appeal of the parties.

C. Access to court's records

108. National courts may also need to protect confidential information in relation to requests for access to court's records (either only the judgment or the entire file), if possible under national procedural rules.
109. National courts may decide to restrict access either with regard to part of the court's file (e.g. to refuse access to documents disclosed in a confidentiality ring, expert reports, minutes of hearings, confidential version of pleadings, etc.) or with regard to the entirety of the file. In particular, national courts may need to order a non-confidential version of the hearing minutes to incorporate into the court file records or decide that some information is referred to during the hearing without reading it on the record.
110. When deciding whether to restrict access partially or entirely, courts may need to evaluate who is requesting access to the court's file. For example, courts may need to take into account that persons requesting access may operate in the same market or activity as the parties involved in the civil proceedings (for instance, competitors of the parties, business partners, etc.) and may have a special interest in getting access to the court's file after the proceedings are closed.
111. Depending on the applicable national procedural rules, where the amount of confidential information is large, and measures such as confidentiality rings were ordered during the proceedings, the court may consider sealing the court's file from access entirely for a period of time to be more efficient than engaging in a review of the file with a view to carving out categories of documents or documents which would be accessible or not once the judgment is rendered.

⁵⁹

See also Article 9.2(c) of the Trade Secrets Directive.