# EFTA SURVEILLANCE AUTHORITY

# Best Practices on the disclosure of information in data rooms in proceedings under Articles 53 and 54 EEA

## 1. SCOPE AND PURPOSE OF THE DATA ROOM BEST PRACTICES

(1) The purpose of this document (the "Data Room Best Practices") is to provide practical guidance on when and how to use data rooms to disclose in a restricted manner business secrets and other confidential information obtained during proceedings under Articles 53 and 54 EEA (the "EEA Antitrust Rules"). The document aims at increasing transparency and predictability of the process within the existing legal and procedural framework,[1] thereby enhancing the efficiency of antitrust investigations.

(2) The Data Room Best Practices make no claim to be comprehensive. The specific features of an individual case may require an adaptation of, or deviation from this guidance document. The Data Room Best Practices do not create or alter any rights or obligations as set out in the EEA Agreement or the Surveillance and Court Agreement as interpreted by the case law of the EFTA Court or the Court of Justice

[1] The Data Room Best Practices should be read in conjunction with Chapters II and III of Protocol 4 to the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice ("Surveillance and Court Agreement"), the EFTA Surveillance Authority Notice on best practices for the conduct of proceedings concerning Articles 53 and 54 of the EEA Agreement (the "Antitrust Best Practices"), Decision No 442/12/COL of 29 November 2012 on the function and terms of reference of the hearing officer in certain competition proceedings (OJ L 190, 11.7.2013, p. 93 and EEA Supplement to the OJ No 40, 11.7.2013, p. 3) ("Hearing Officers' Terms of Reference"), the EFTA Surveillance Authority Notice on the rules for access to the EFTA Surveillance Authority file in cases pursuant to Articles 53, 54 and 57 of the EEA Agreement (OJ C 250, 25.10.2007, p. 16 and EEA Supplement to the OJ No 50, 25.10.2007, p. 1) ("Access to File Notice").

of the European Union, nor does it alter the Authority's interpretative notices. The EFTA Surveillance Authority (the "Authority") may revise the Data Room Best Practices from time to time to reflect changes in legislation, jurisprudence and practice.

(3) The specific legal framework and constraints in proceedings under the EEA Antitrust Rules must be taken into account when deciding on when and how to use data rooms to disclose business secrets and other confidential information obtained during such proceedings. The Antitrust Best Practices provide some guidance on the circumstances where, and the conditions under which, a data room may be organised to disclose business secrets and other confidential information obtained in proceedings under the EEA Antitrust Rules.[2] The present Data Room Best Practices complement the Antitrust Best Practices and set out further details on the rules applicable to data room procedures.

## 2. GENERAL PRINCIPLES ON DATA ROOMS

(5) As part of their procedural guarantees intended to protect the rights of defence, addressees of a Statement of Objections[3] have the right to access the non-confidential version of the Authority's file.[4] The rationale behind access to the Authority's file is to allow the addressees of the Statement of Objections an opportunity, before a decision is taken, to examine the evidence in the Authority's file so that they are in a position to express their views on the conclusions reached in the Statement of Objections on the basis of that evidence and defend themselves against these objections.

(6) In principle, access to the Authority's file is granted by giving the addressees of a Statement of Objections access to an electronic version of all documents contained in the Authority's file, with the exception of internal documents and confidential information (i.e. business secrets and other confidential information).[5]

(7) The Authority obtains, in the course of its investigation, both quantitative and qualitative information, some of which may serve as evidence underpinning the reasoning in the Authority's Statement of Objections. Data collected from third parties (e.g. cost and price data, sales data, bidding data, margins, etc.) often constitute business secrets, which are by nature confidential. In particular, if the data are of a quantitative nature, it may not be possible to provide, in a timely manner, a meaningful non-confidential version. Exceptionally, this may also be true for qualitative information (e.g. internal strategy documents of competitors). However, granting access to such data may be necessary in certain circumstances for an effective exercise of the rights of defence.

---

[2] Point 93 of the Authority's Antitrust Best Practices.

[3] Issued pursuant to Article 10(1) of Chapter III of Protocol 4 to the Surveillance and Court Agreement.

[4] See Article 27(2) of Chapter II of Protocol 4 to the Surveillance and Court Agreement and Article 15(1) and (2) of Chapter III of Protocol 4 to the Surveillance and Court Agreement. Throughout the Data Room Best Practices, the term "EFTA Surveillance Authority file" is used as defined in point 8 of the Access to File Notice.

[5] See Article 15(2) of Chapter III of Protocol 4 to the Surveillance and Court Agreement.

(8) In accordance with Article 122 EEA, the Authority has a general duty to protect confidential information that could seriously harm the undertaking if disclosed.[6] Notwithstanding this, in antitrust proceedings confidential information may exceptionally be disclosed when such disclosure is necessary to prove an infringement of Articles 53 or 54 EEA,[7] or to safeguard the rights of defence of the parties.[8] In antitrust proceedings, confidential information will not be disclosed when the rights of defence of the parties may be effectively exercised on the basis of non-confidential versions of the documents in the Authority's file.

(9) Data rooms are 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 Authority has obtained the information (the "Data Providers"). By means of a data room, documents in the Authority's file are made accessible to an addressee of a Statement of Objections in a restricted manner, i.e. 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.

(10) It is in the Authority's discretion to decide whether a data room is appropriate in a particular case. The Authority decides to offer a data room, either on its own motion or upon a request from an addressee of a Statement of Objections, where it considers it to be necessary and proportionate in view of the principles set out above and provided that any legal and practical difficulties can be resolved swiftly in agreement with the addressees of the Statement of Objections and the Data Providers.

(11) In deciding whether a particular case is suitable for a data room procedure, the Authority will also take into account whether it is appropriate to provide access at that moment in time, having regard to the circumstances of the case at hand, the nature and degree of sensitivity of the information, the progress of the case, the resource implications of operating data rooms, risk of information leaks, and the need for speed.[9]

(12) Access to a data room is subject to compliance with the data room rules, confidentiality undertakings and sanctions in case of non-compliance (see **Annex A** for the standard data room rules (the "Data Room Rules"), and **Annex B** for the standard non-disclosure agreement (the "Non-Disclosure Agreement")).

## 3. SCOPE OF THE DATA INCLUDED IN THE DATA ROOM

(13) These Data Room Best Practices are based on those of the European Commission's DG Competition, whose best practices[10] served as a template. DG Competition has organised data rooms in a number of cases, mostly for the disclosure of quantitative data (e.g. individual sales data, price data, cost data, bidding data, margins, etc.) on

---

[6] This principle is also endorsed by case law, for instance, judgment in *General Electric Company* v *Commission*, T-210/01, EU:T:2005:456, paragraphs 631 and 650.

[7] See Article 15(3) Chapter III of Protocol 4 to the Surveillance and Court Agreement.

[8] See also in this context point 24 of the Access to File Notice.

[9] See footnote 6.

[10] 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.

which the Commission has relied directly or indirectly in its Statement of Objections. In a few exceptional cases, DG Competition has also organised data rooms for the disclosure of qualitative data (e.g. internal strategy documents). The same basic principles in terms of purpose and scope apply to both quantitative and qualitative data rooms.

(14) Quantitative data are frequently confidential, as they typically comprise sensitive internal strategic information. In addition to confidentiality concerns, an exchange of strategic data between competitors can lead to a reduction of competition, for example, by facilitating collusive practices, by harming consumers or by other means. Furthermore, it often proves impossible or very burdensome for the Data Provider to provide meaningful non-confidential versions in a timely manner,[11] due to the volume of the data and/or the difficulty of producing a non-confidential version with sufficient evidentiary value.

(15) Quantitative data included in a data room should enable the addressees of a Statement of Objections, through their external advisors (the "External Advisors"), to verify the methodology used by the Authority to collect, check the consistency of, manage and analyse, the data used in a Statement of Objections, as well as to replicate and check the robustness of the Authority's analysis. Therefore, software codes that may be necessary for the effective exercise of the rights of defence, in particular insofar as they have been used by the Authority for the purpose of the analysis set out in a Statement of Objections, may be included in a data room upon review by the Authority.[12]

(16) As set out in paragraph (13), exceptionally, qualitative confidential documents may also be disclosed to the External Advisors of the addressees of a Statement of Objections through a data room procedure. A qualitative data room may be organised where it is not possible or it is very burdensome for the Data Provider to provide meaningful non-confidential versions of such qualitative documents (for instance internal strategy documents) with sufficient evidentiary value and in a timely manner.[13] The organisation of a data room in these circumstances enables the addressees of the Statement of Objections, through their External Advisors, to verify the evidence in the Authority's file where the disclosure of such confidential information may be necessary for the effective exercise of the rights of defence, in particular insofar as such confidential information is relied upon in the Statement of Objections.

(17) Depending on the specific circumstances of the case, the Authority may anonymise certain data included in the data room by, for example, translating all documents into the same language,[14] removing their document IDs, changing the currency of economic values, redacting countries and territories, partially aggregating figures or taking any other measure deemed necessary in order to protect the identity and

[11] See footnote 6.

[12] Insofar as the software codes are not confidential, they would be disclosed in the ordinary course of access to the Authority's file. The full confidential version of the software codes would also be provided in the data room environment so as to enable replication and verification of the Authority's analysis.

[13] See footnote 6.

[14] The Authority is under no obligation to provide a translation of documents in the Authority's file (judgment in *Cimenteries*, T-25/95 et al., EU:T:2000:77, paragraph 635, and point 46 of the Access to File Notice.

confidentiality of Data Providers and minimise the risk of possible retaliatory measures.

## 4. ORGANISATION OF DATA ROOMS

### 4.1. Timing of a data room

(18) A data room can be organised at any point of time at which access to the Authority's file may be granted (i.e. after the notification of the Authority's Statement of Objections to the parties and before the Advisory Committee).[15] Normally, a data room is organised before the oral hearing.

### 4.2. Data room participants

(19) Because of the sensitive and confidential nature of the data contained in the data room, access to the data room is limited to a restricted group of persons on an "External Advisor only" basis.

(20) The External Advisors are in principle limited to the external economic advisors and/or the external legal counsel of the addressees of a Statement of Objections, depending on the quantitative or qualitative nature of the data room. A predefined number of External Advisors are granted access to the data room, in particular for the purpose of verifying the validity and soundness of the Authority's quantitative analyses adopted in a Statement of Objections, or whether the qualitative evidence on the Authority's file supports the conclusions drawn and the objections raised by it. The purpose of providing access to the data room is strictly limited to enabling the External Advisors to advise their clients, i.e. the addressees of a Statement of Objections, in exercising their rights of defence effectively without however disclosing to their client the confidential information they were able to see.

### 4.3. Data Room Rules

(21) Every data room organised by the Authority is subject to the Authority's Data Room Rules, which must be accepted by the addressees of a Statement of Objections and signed by the External Advisors prior to getting access to the data room.

(22) The Data Room Rules provide that access to the data room is granted under strict confidentiality obligations, increased security measures and appropriate supervision. The standard Data Room Rules are provided in **Annex A**.

(23) External Advisors shall neither remove data, information or documents from the data room, nor disclose confidential information obtained within the framework of a data room procedure to the addressees of the Statement of Objections or any third party. It is in the first place for the External Advisors to ensure that they comply with any relevant professional conduct rules and that they are able to operate on this basis, including obtaining waivers in relation to such rules from their clients where necessary.

[15] See points 26 to 28 of the Access to File Notice, Article 15(1) Chapter III of Protocol 4 to the Surveillance and Court Agreement.

(24) Similarly, an addressee of a Statement of Objections must never request nor receive any confidential information derived from the data room by its External Advisor(s). Only a non-confidential data room report may be provided by the External Advisors to the addressees of a Statement of Objections (see section 4.4 below).

(25) The Authority will make available to the External Advisors the technical equipment to enable the latter to prepare the data room report. The External Advisors will have a predefined number of secure computer workstations at their disposal, managed by the Authority and equipped with the necessary software and the relevant data sets, as the case may require. The computer workstations will be backed-up daily to ensure business continuity. To facilitate collaboration among External Advisors in the data room, a secured, shared collaborative space is set up in the PC workstations provided by the Authority. The data room is open for the number of days and during the working hours agreed with the Authority (taking into account the need for speed), and set out explicitly in the Data Room Rules.

(26) External Advisors may bring additional computer codes, paper material or text in electronic format in the data room (e.g. handwritten, printed notes or electronic text files, a copy of the Statement of Objections etc.), that may be necessary for the verification of the Authority's analysis and the preparation of the data room report. Paper material brought into the data room by the External Advisors may be reviewed by the Authority's officials at any time. Such documents may not, under any circumstances, be taken out of the data room and shall be destroyed at the end of the data room procedure.

(27) During the course of the data room procedure, External Advisors may (i) take notes on, copy or otherwise replicate the data, and (ii) print documents, on pre-numbered blank pages provided by the Authority. All printouts and notes may be reviewed by the Authority's officials at any time. Any such printouts and notes may not, under any circumstances, be taken out of the data room and shall be destroyed at the end of the data room procedure.

(28) No external communication in any form is allowed. The data room will be monitored at all times. External Advisors may not carry any electronic device, camera, mobile phone or other communication or recording device while they are in the data room.

(29) In addition, the Data Room Rules determine:

- the scope of the data included in the data room and any potential restrictions on its use,
- the equipment that will be made available,
- the duration and opening hours of the data room,
- the premises where the data room will be organised,
- the conditions under which access to the data room will be granted,
- the sanctions for non-respect of the Data Room Rules, and
- any other terms to which the data room will be subject in the individual case.

(30) Prior to getting access to the data room, the External Advisors must also sign the Non-Disclosure Agreement. The Non-Disclosure Agreement sets out the obligations and liabilities of the persons accessing the data room. In particular, by signing the Non-Disclosure Agreement, the External Advisors undertake, *inter alia,* to use the confidential data only for the purpose of verifying the Authority's analysis set out in a Statement of Objections, as described in paragraphs (15) and (16), and of drafting a non-confidential report in that respect.

### 4.4. Data room report

(31) After having obtained access to the data room, and only during access to the data room, External Advisors may prepare a data room report (the "Data Room Report"). The Data Room Report is the only means through which the External Advisors may communicate to and discuss the data in the data room with the addressees of the Statement of Objections (their clients), to which the latter would not have otherwise obtained access.[16]

(32) The Data Room Report contains the findings and conclusions of the External Advisors regarding their assessment of data relevant for the exercise of their client's rights of defence, as described in paragraphs (15) and (16). As a general rule, the analysis of quantitative data carried out by the External Advisors must be replicable by the Authority. In particular, any analysis underlying findings or conclusions in the Data Room Report shall be documented and identified by the External Advisors.

(33) The Data Room Report must only contain non-confidential information. At the end of the data room procedure, the Authority will review and approve the Data Room Report that has been prepared and finalised by the External Advisors to ensure that it does not contain any business secrets and other confidential information.[17] Only upon its approval, the Authority will send each addressee of the Statement of Objections the individual Data Room Report prepared by their respective External Advisors.

(34) The External Advisors shall not remove any data, information or documents from the data room, even if such data, information or documents do not contain business secrets and other confidential information.

(35) It is not possible to claim Legal Professional Privilege or other kind of privilege protection in respect of any part of the Data Room Report to be provided to the addressees of the Statement of Objections.

(36) During access to the data room, the External Advisors may decide to prepare and address to the Authority a non-redacted, confidential version of the Data Room Report for the sole purpose of explaining in more detail how the External Advisors

---

[16] For the avoidance of doubt, where External Advisors acting for multiple addressees of the Statement of Objections are granted access to a data room, only one Data Room Report may be prepared for each of the addressees of the Statement of Objections by their respective External Advisors during access to the Data Room.

[17] During the review of the Data Room Report, further redactions may be made by the Authority to protect third party business secrets and other confidential information, before the Data Room Report is approved by the Authority.

have conducted their calculations and have reached their findings and conclusions contained in the Data Room Report. In such case, the External Advisors shall explain the differences between both versions of the Data Room Report, highlighting in the non-redacted, confidential version of the Data Room Report any confidential information or results. The non-redacted, confidential version of the Data Room Report will be registered in the Authority's file, will remain in the sole possession of the Authority, and will not be made accessible to the addressees of the Statement of Objections.

### 4.5. Sanctions for non-respect of the Data Room Rules

(37) By signing the Non-Disclosure Agreement and agreeing to the Data Room Rules, the External Advisors recognise their rights and obligations stemming from the data room procedure. If any of the rules or obligations are not respected by any of the External Advisors, all of the relevant party's External Advisors will be immediately requested to leave the data room.

(38) In addition, the Authority and the Data Providers may take all appropriate legal action in case of breach of the Data Room Rules and/or the Non-Disclosure Agreement, including but not limited to damages actions. The Authority may also inform the relevant law bar associations or other professional associations, as appropriate, of a violation of the applicable deontological or professional conduct rules.[18]

## 5. INVOLVEMENT OF DATA PROVIDERS IN A DATA ROOM PROCEDURE

(39) Following a request to organise a data room by the addressees of a Statement of Objections, the Authority will inform the Data Providers in writing and seek to obtain their consent. The Authority will identify the information to be disclosed and provide the reasons for the proposed disclosure. The Authority will set a time period during which the Data Provider may submit any written comments.[19]

(40) Data Providers will be able to express any potential concerns in relation to the data room procedure, for example concerns about potential retaliatory measures from the addressees of a Statement of Objections, having the opportunity to consult the Data Room Rules and the Non-Disclosure Agreement and provide feedback, as well as to review the list of External Advisors for the purpose of identifying any potential conflicts of interest.

(41) The Authority may implement measures to address such concerns. For instance, if the Data Providers are concerned about potential retaliatory measures from the addressees of a Statement of Objections, the Authority may anonymise relevant variables,[20] or aggregate certain data to the extent that such altered data would still afford the addressees of a Statement of Objections an adequate opportunity to exercise their rights of defence.

---

[18] See point 48 of the Access to File Notice.

[19] See Article 8(1) of Hearing Officers' Terms of Reference.

[20] See paragraph (17).

(42) The Authority aims at reconciling the opposing interests of the addressees of a Statement of Objections and those of Data Providers in good faith, while expediting the proceedings to the extent possible.

(43) At any point during the course of the data room, the Data Providers' legal counsel, at their request, may be allowed access to the data room for the sole purpose of ensuring that appropriate safeguards are in place.

## 6. ROLE OF THE HEARING OFFICER

(44) In case of persisting disagreement between the Authority and the addressees of a Statement of Objections,[21] or the Data Provider,[22] in relation to the disclosure of confidential information, including via a data room, the matter may be brought before the Hearing Officer.[23] Addressees of a Statement of Objections can, if they believe that further access is necessary for exercising their right to be heard, address the matter to the Hearing Officer, after the Authority has first dealt with it.[24] This is also the case for Data Providers, should they object to the disclosure of information which they consider to be confidential.

(45) The Hearing Officer may take a decision on the basis of Articles 7 and 8 of the Hearing Officers' Terms of Reference, respectively, including the ordering of the disclosure of confidential information in a data room under the conditions laid down in Article 8(4) of the Hearing Officers' Terms of Reference.

[21] See Article 7(1) of the Hearing Officers' Terms of Reference.

[22] See Article 8(2) of the Hearing Officers' Terms of Reference.

[23] As set out in recitals 7 and 14 to the Hearing Officers' Terms of Reference, the Hearing Officer acts as an independent arbiter between the Authority and the respective parties to solve disputes about access to the Authority's file and the protection of business secrets and other confidential information.

[24] See Article 3(7) of the Hearing Officers' Terms of Reference.