

PROPOSED GUIDELINES FOR IMPROVED ACCESS TO INVESTIGATION FILES IN EU TDI PROCEEDINGS

INTRODUCTION

Current EU TDI proceedings lack transparency, especially when compared with EU efforts to increase transparency in other areas, such as the disclosure of documents in the TTIP negotiations and the system of Best Practices on the Disclosure of Information in DG Competition proceedings. The new Rules of Procedure of the General Court also seek to address the lack of transparency and increase disclosure of confidential documents.¹

An increase of access to information in TDI proceedings is therefore necessary in order to improve transparency and ensure consistency with other EU areas. Increasing access will improve confidence in the process and in the findings of the Commission. It may also improve the quality of the Commission's findings.

The below proposed rules are based on the best practices found in administrative protective orders ("APO"s) created by various other WTO Members, including the US, Canada, and Mexico. It is also partially based on the best practices found in certain previous DSB proceedings. The guidelines aim to set out an improved framework and procedure for the access to confidential information during TDI proceedings within the EU, without impinging on the current EU and WTO system of confidentiality.

The question of increasing access to information during anti-dumping, anti-subsidy and safeguard proceedings has been raised before and has met various objections. Such objections have typically raised issues such as:

1. the risk of unauthorised disclosure;
2. the perception of such risk among third and analogue country producers;
3. the practical concerns relating to improved access, such as imposing effective sanctions for breach of confidentiality; and
4. the belief that improving transparency is not necessary.

However, these objections have been convincingly rebutted by a large number of experienced and qualified individuals in the field.² The risks of unauthorised disclosure associated with

¹ OJ L 152/1, 18.6.2015, Section VI.

² See, for example, the special edition of the Global Trade and Customs Journal devoted to this topic: (2014) 9 Global Trade and Customs Journal 7&8 and (2014) 9 Global Trade and Customs Journal 11&12, p. 502. See also the second special edition of the Global Trade and Customs Journal devoted to this topic: (2015) 10 Global Trade and Customs Journal 4.

increased access are not significant. A review of the various APO systems in the US, Canada and Mexico, as well as previous WTO practice, demonstrates that such systems can be secure and effective. Also, as regards concerns that there could be difficulty in imposing adequate sanctions to dissuade breaches of confidentiality due to the fact that EU lawyers may belong to several different National Bars, this is unlikely to be the case. In all jurisdictions such a breach of confidentiality is likely to already constitute a breach of professional duty, incurring serious professional consequences.

GUIDELINES

Pursuant to:

- Article 19 of Council Regulation (EC) No. 1225/2009 on protection against dumped imports from countries not members of the European Community ("Anti-Dumping Regulation");³
- Article 29 of Council Regulation (EC) No. 597/2009 on protection against subsidised imports from countries not members of the European Community ("Anti-Subsidy Regulation");⁴ and
- Article 9 of Council Regulation (EC) No. 260/2009 on the common rules for imports ("Safeguards Regulation"),⁵

certain information, *i.e.*,

- (1) information which is by nature confidential; and
- (2) information which is provided on a confidential basis;

must be treated upon good cause shown, as confidential by the European Commission and not be disclosed to other interested parties.

In TDI proceedings such confidential information is labelled "*limited*". Such information is also protected pursuant to Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council.⁶

However, access to such confidential information may be appropriate in many cases in order to fully safeguard procedural rights of interested parties and ensure that their rights of defence are not prejudiced. Therefore, in order to update and enhance Commission policy to these ends, these guidelines set out a restricted procedure for access to information to which confidential status applies under Article 19 of the Anti-Dumping Regulation, Article 29 of the

³ OJ L 343/51, 22.12.2009. *See also* Article 6 of the WTO Agreement on Implementation of Article VI of the GATT 1994 (Anti-Dumping Agreement).

⁴ OJ L 188/93, 18.07.2009. *See also* Article 12 of the WTO Agreement on Subsidies and Countervailing Measures.

⁵ OJ L 84/1, 31.3.2009. The equivalent Regulation for imports from non-WTO countries is published in OJ L 185/1, 17.7.2009.

⁶ OJ L 145/43, 31.5.2001.

of the Anti-Subsidy Regulation and Article 9 of the Safeguards Regulation⁷. Essentially, such confidential information (except for certain specifically exempted categories) shall be disclosed to a restricted number of "Authorised Persons", subject to compliance with a number of restrictive conditions, through a specific access mode. To facilitate the operation of these procedures, the interested parties shall submit certain information in the course of proceedings in a specified format. Any non-compliance of the submitting parties, as well as non-compliance of the Authorised Persons with the restrictive conditions, shall result in access to the confidential information being withdrawn and may be subject to more severe sanctions according to the circumstances.

These guidelines are without prejudice to access of interested parties to the "regular" non-limited file as this has existed until now.

1 SCOPE OF ACCESS GRANTED UNDER THESE GUIDELINES

Access for inspection shall be granted to the following information:

1. Confidential information submitted by interested parties and having the status of "limited information" as per Article 19 of the Anti-Dumping Regulation or Article 29 of the Anti-Subsidy Regulation or Article 9 of the Safeguards Regulation⁸; and
2. Documents prepared by the Commission in connection with the investigations relevant for the Commission's findings which are otherwise not disclosed to all interested parties on the grounds of confidentiality (*e.g.*, dumping margin calculations, injury margin calculations, verification (mission) reports). This includes all advice from the Commission Legal Service.

Within this confidential information access shall **not** be granted to "highly sensitive business information" (also called "HSBI" or "double-bracketed information"), which shall remain excluded from inspection and disclosure. Such ineligible information ("*excluded categories*") shall be only accessible by the Commission Services and shall not be disclosed to any interested party or its legal representative. This ineligible information includes the following categories of particularly sensitive information:

1. Names of the customers of the interested parties;
2. Information protected under legal profession privilege. Legal profession privilege shall cover both legal advice privilege (confidential communications between a client and his lawyer in which advice is sought or given within a relevant legal context) and litigation privilege (covers confidential documents prepared for the purpose of on-

⁷ These guidelines also apply to information to which confidential status applies under Article 7 of Regulation (EC) 625/2009.

⁸ These guidelines also apply to Confidential information submitted by interested parties and having the status of "limited information" as per Article 7 of Regulation (EC) 625/2009

going or contemplated litigation proceedings (the latter shall include proceedings before court, arbitrators and tribunals exercising judicial functions));

3. Classified (*e.g.* governmental secret) information; and
4. Specific secret commercial information in respect of which there is a clear and compelling need to withhold from disclosure *e.g.* corporate trade secrets, product formulas, *etc.*

Redaction of information under the excluded category of HSBI only concerns the HSBI-portion of a document, not automatically the whole document. Such HSBI shall be redacted when set out in the context of other confidential information that must be disclosed to Authorised Persons according to the conditions set out herein.

2 FILING OBLIGATIONS OF INTERESTED PARTIES UNDER THE GUIDELINES

In order to facilitate the disclosure of the confidential information pursuant to these guidelines, interested parties shall from now on submit their information in three versions:

- A. "**Open**" (also called "*public*" or "*non-confidential*" or "*non-limited*") version: this version will be available to all interested parties participating in the TDI proceeding;
- B. "**Limited**" (also called "*confidential*" or "*bracketed*") version: this version will be available to the Authorised Persons under the conditions set out below. Only information falling under one of the excluded categories enumerated in point 1 may be redacted; and
- C. "**Highly Sensitive Business Information**" (also called "*HSBI*" or "*double-bracketed*") – which will only be available to the Commission and the party that has submitted it.

Submissions which do not comply with these guidelines shall be rejected by the Commission, after the relevant party has been given a chance to comment and submit a revised version.

3 AUTHORISED PERSONS

3.1 Qualification criteria

Access to confidential information shall be provided to Authorised Persons representing interested parties in the relevant TDI proceeding under the following conditions:

1. The Authorised Person represents an interested party in the investigation;
2. The Authorised Person belongs to one of the following categories:

- The Authorised Person is an EU qualified lawyer or a foreign qualified lawyer properly registered with, and subject to the disciplinary jurisdiction and regulations and decisions of, a Bar or Law Society in an EU Member State (*e.g.* Brussels B-list, the Law Society of England and Wales); or
 - The Authorised Person is an external consultant or expert who appears regularly before the Commission in EU trade defence proceedings;
3. The Authorised Person is not involved in a competitive decision making position in respect of any interested party or competitors thereof;
 4. The Authorised Person has provided a bond/guarantee/security as described below. Firms or lawyers who regularly operate in trade proceedings may set one bond/guarantee/security that is valid for multiple investigations throughout; and
 5. The Authorised Person has provided a signed undertaking to comply with the rules set out in these guidelines.

3.2 Obligations

The Authorised Persons shall comply with the following obligations:

1. The Authorised Person shall use the confidential information in respect of which the access was granted under these guidelines only for the defence of the interests of the party to whom the access application relates, and not for itself or any other natural or legal person;
2. The Authorised Person shall safeguard the confidential information to which the access was provided, and shall apply the appropriate levels of security to ensure that the confidential information is available only to parties identified in the access application;
3. The Authorised Person shall not disclose such confidential information to any party (including its client) other than identified in the access application. To this effect the Authorised Person shall sign a Non-Disclosure Agreement, in the form set out at Annex B;⁹
4. Provided the Commission has reasonable suspicion that the Authorised Person has breached its obligations under these Guidelines, the Authorised Person shall submit to the Commission any information reasonably required by the Commission to demonstrate compliance with these conditions; and

⁹ The Non-Disclosure Agreement may be based on the Standard Non-Disclosure Agreement in Annex B to the 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. The DG Competition Standard Non-Disclosure Agreement may be amended in line with these guidelines.

5. The Authorised Person shall immediately inform the Commission of any changes in respect of the qualification criteria and any breaches of the restrictive covenants he/she is aware of in respect of himself/herself and/or any Authorised Person.

3.3 Bond/Guarantee/Security

In order to obtain access to the confidential information, the Authorised Person must provide a bond/guarantee/security of €500,000 [*suggested alternative: €1,000,000 for the first year, to be steadily reduced to €500,000 in the third year*] issued by a reputable financial institution¹⁰ [*Optional alternative: "issued by a reputable financial institution¹¹ or the Authorised Person or the firm of which such Authorised Person is a member, agent or an employee, provided the Authorised Person or such firm are established in a Member State, as applicable"*] as a security for the proper performance of the obligations of the Authorised Persons with regard to confidentiality and professional duty. The document evidencing the bond shall contain the following written guarantee:

"This bond is issued by [insert name of the Authorised Persons] to guarantee the terms of [the Regulations/Data Room Rules?] and as security for any damage that may be caused by the disclosure of confidential information or the use of it for personal benefit."

The bond/guarantee shall identify the Authorised Persons covered by it. One bond/guarantee may cover more than one Authorised Person provided all such covered Authorised Persons are members, agents or employees of one firm.

The guarantee shall remain in force for the duration of the proceedings until a final determination has been published in the Official Journal and for 3 years thereafter. Authorised Persons who regularly operate in TDI proceedings may set one bond that is valid for multiple investigations throughout.

The bond/guarantee/security is not required for law firms that demonstrate that they have sufficient professional liability insurance.

4 MODE OF ACCESS

4.1 Application for Access

The Commission shall provide access to the Authorised Person upon submission of the following information:

1. An application in writing containing the following information:

¹⁰ To be defined by reference to S&P/Moody's/Fitch Group ratings.

¹¹ To be defined by reference to S&P/Moody's/Fitch Group ratings.

- a. the case file number;
 - b. the name of the person requesting access as well as any other person that will have access to the confidential information (together "*Authorised Persons*"). Each of such Authorised Persons must comply with the qualification criteria set out in point 3.1 above;
2. Original or certified copy of a valid power of attorney executed by the party upon whose behalf access is requested;
 3. Copy of a valid identification document of the requesting person(s);
 4. In the case of an EU qualified lawyer or a foreign qualified lawyer properly registered with, and subject to the disciplinary jurisdiction and regulations and decisions of, a Bar or Law Society of an EU Member State, an original or certified copy of the relevant document evidencing the Authorised Person's membership of the relevant Bar Association or Law Society. In the case of external experts or consultants, evidence that the person appears regularly before the Commission in EU TDI proceedings;
 5. Signature of the standard non-disclosure agreement included as Annex B to these guidelines; and
 6. An original of the bond/guarantee/security for those firms/persons that are not exempt from this obligation.

4.2 Form of Access

Access to the confidential information shall be provided at a physical data room ("Data Room") at the Commission's premises. 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")). The following principles guide the Data Room:

1. The Data Room shall contain hard and soft copies (calculations in excel, etc.) of all submissions and other documents containing confidential information to be disclosed pursuant to these guidelines;
2. The Authorised Persons will have a predefined number of secure computer workstations at their disposal, managed by DG Trade 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. A computer workstation shall contain all submissions, including the necessary excel spreadsheet programs, relevant excel files, *etc.* The internet connection

and USB ports will be disabled to ensure that no limited information shall be electronically disseminated;

3. The Authorised Persons may not copy or scan any documents in the Data Room;
4. The Authorised Persons shall be permitted to make manuscript notes and make notes on their laptop computer. The use of modems, [portable] photocopiers, scanning devices, facsimile equipment, and any optical imaging devices (including phones with cameras) or electronic equipment other than a laptop computer is prohibited in the Data Room;
5. No document may be marked, altered, modified, varied (including varying the sequence thereof), damaged or destroyed in any way;
6. No documents in the Data Room may be removed from the Data Room, other than the manuscript notes and notes contained on a laptop computer of the Authorised Persons;
7. In order to ensure sufficient and timely access, three such Data Rooms shall be available at the same time. The Data Rooms will be opened from the date of the publication of the notice of initiation and will be available for use by prior appointment from 9.00AM until 6.00PM on each business day for the duration of the proceedings until one month after the final determination is published in the Official Journal;
8. No external communication in any form is allowed. The data room will be monitored at all times. Authorised Persons may not carry any electronic device, camera, mobile phone or other communication or recording device while they are in the Data Room;
9. Individual appointments to visit the Data Room must be fixed by contacting the relevant officials 24 hours in advance before access will be permitted. Access may not always be possible at an authorised person's desired time, in which case alternative times may be offered. Prior to getting access to the data room, the Authorised Person shall present an original valid identification document, *i.e.* a valid EU passport or EU ID card and must sign the Non-Disclosure Agreement. The Non-Disclosure Agreement sets out the obligations and liabilities of the persons accessing the Data Room.

5 NOTIFICATION OF MATERIALS

A service list will be drawn up for each case, naming the Authorised Persons to whom the access shall be granted pursuant to these guidelines. Upon new documents becoming available, an electronic notice shall be sent to each person on the service list.

6 CONSEQUENCES AND SUPERVISION OF BREACH

In order to ensure the non-disclosure of confidential information, it is necessary to provide for the possibility of imposing adequate sanctions for breach of the obligation not to disseminate confidential information or to use it for personal benefit. By signing the Non-Disclosure Agreement and agreeing to the Data Room Rules, the Authorised Persons 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 Authorised Persons, all of the relevant Authorised Persons will be immediately requested to leave the Data Room. This is notwithstanding the fact that such a breach is also likely to constitute a breach of professional duty under the relevant Bar or Law Society rules. Infringement of this requirement, other than honest mistakes, may result in sanctions, independent of such civil and criminal penalties as may also be applicable.

6.2 *Possible Sanctions:*

Sanctions may consist of one or any of the following:

1. refusal of the access to the confidential data;
2. forfeit of the above-mentioned bond/guarantee/security for those firms/persons that are not exempt from this obligation;
3. a substantial fine [*to be defined*];
4. referral to the relevant national Bar association; and/or
5. prohibition [*to be defined*] from appearing before the Commission in TDI investigations for a limited or unlimited time.

6.3 *Supervision of breach:*

Option A: For lawyers registered with the Brussels Bar: in case the allegation of an infringement or the proportionality of the sanction proposed are disputed by the Authorised Person concerned, the final decision as to the existence of an infringement shall be made by the Brussels Bar (by the French or Dutch sections at the discretion of the Authorised Person concerned). The Brussels Bar shall also make a recommendation as to the appropriate sanction. The Commission shall not impose a sanction more severe than the one proposed by the Brussels Bar. This provision is without prejudice to the Commission's right to refuse access to the confidential data on provisional basis subject to the final decision of the Brussels Bar;

Option B: For lawyers not registered in Brussels: if the Authorised Person is a lawyer, and the allegation of an infringement or the proportionality of the sanction proposed are disputed, the final decision as to the existence of an infringement shall be made after consultation of the Bar or Law Society authority of the place where the lawyer is practicing law and with whom the lawyer is (or

should be) registered. The Bar or Law Society authority shall make a recommendation as to the appropriate sanction. The Commission shall not impose a sanction more severe than the one proposed by the Bar or Law Society authority. This provision is without prejudice to the Commission's right to refuse access to the confidential data on provisional basis subject to recommendation of the relevant Bar or Law Society;

Option C: The same as Option A and B, but the decision is made by CCBE; and

Option D: For non-lawyers: In case the allegation of an infringement or the proportionality of the sanctions proposed are disputed by the Authorised Person concerned, the final decision as to the existence of an infringement shall be made by a panel composed of 3 arbitrators under the CEPANI Rules of Arbitration. The panel so composed shall also make a recommendation as to the appropriate sanction. The Commission shall not impose a sanction more severe than the one proposed by the panel. This provision is without prejudice to the Commission's right to refuse access to the confidential data on provisional basis subject to the final decision of the panel.

Such above proceedings under any of the options shall be kept confidential without prejudice to the right to disclose the final decision.

7 ROLE OF HEARING OFFICER

In case of a disagreement between DG Trade and the Authorised Person, in relation to the disclosure of confidential information, or the nature of the information submitted, including via the Data Room, the matter may also be brought before the Hearing Officer. Authorised Persons can, if they believe that further access is necessary for exercising their right to be heard, address the matter to the Hearing Officer. The Hearing Officer may take a decision on the basis of the Hearing Officers' Terms of Reference, including an order to make confidential information available in the Data Room.

Annex A: Standard Data Room Rules

Annex B: Standard Non-Disclosure Agreement

Annex A: Standard Data Room Rules**TERMS OF DISCLOSURE OF BUSINESS SECRETS AND OTHER CONFIDENTIAL
INFORMATION ON "AUTHORISED PERSONS ONLY" BASIS
("DATA ROOM RULES")****Case [M.XXXX/AT.XXXXX] - [CASE NAME]**

Within the framework of access to the Commission's file granted to [Names of Party/Parties to which data room access is granted through their Authorised Persons] in **Case [M.XXXX/AT.XXXXX] - [CASE NAME]** pursuant to the Commission Guidelines on Access to the File in TDI Proceedings, DG Trade makes available three rooms at its premises at Rue de la Loi 170, 1000 Brussels (the "Data Room") to the [external economic advisors and/or external legal counsel] (the "Authorised Persons") instructed by [Names of Party/Parties to which data room access is granted through their Authorised Persons] (the "[Party/Parties]") pursuant to the investigation in Case [M.XXXX/AT.XXXXX]. The [Party/Parties], [requested/accepted the] data room procedure by email dated [Date of email].

The Data Room contains information which DG Trade considers to constitute confidential information within the meaning at point 1 of the Commission Guidelines on Access to the File in TDI Proceedings, and therefore will be made available within the framework of the data room procedure and under the strict conditions set out in these Data Room Rules.

As set out in the Commission Guidelines on Access to the File in TDI Proceedings, DG Trade may, having balanced the effective exercise of the Parties' procedural rights and rights of defence with the legitimate confidentiality interests of data providers, disclose specific information for the sole purpose of allowing the Authorised Persons an opportunity to better understand the evidence available to DG Trade so that they can effectively exercise the [Party/Parties] procedural rights and rights of defence on its behalf. Further disclosure of the Data seen in the Data Room without the written prior agreement of DG Trade is strictly forbidden.

The Data Room Rules apply to the Authorised Persons and are set up in order to ensure the legitimate protection of the business secrets of data providers and other confidential information collected by the Commission within the framework of its on-going investigation in the above referenced case.

The Authorised Persons and any person who belongs to the team of such Authorised Persons are required to agree to these Data Room Rules and sign the standard non-disclosure agreement, appended at Annex B to the Commission Guidelines on Access to the File in TDI Proceedings ("Non-Disclosure Agreement") prior to obtaining access to the Data Room and

the Data therein. The Authorised Persons and any person who belongs to the team of such Authorised Persons commit to respect the letter and the spirit of the following conditions.

Prior to obtaining access to the Data, the Authorised Persons will make available to the case team (contact: contact person, tel: +xxxxx) the name, the number of a valid identity document (passport or identity card), the job title and employer of each member of the Authorised Persons team who will access the data room. The Authorised Persons shall not exceed [number of persons] persons. The identity of the Authorised Persons will be disclosed to Data Providers before access is given to the Data Room.

These persons only will be allowed access to the Data Room. The usual rules for access to Commission buildings apply. A visitor's badge will have to be worn visibly at all times. In order to speed up the access procedures, the Parties will have to inform the DG Trade case team 24 hours in advance and in writing (preferably by e-mail) of the composition of the Authorised Persons team that will be present on a specific date.

Entry to the Data Room, conduct within it and use of the Data are subject to these rules and to suitable undertakings in the form of the Non-Disclosure Agreement being given to DG Trade:

1 EQUIPMENT

- (1) In the Data Room, [number] secure PC workstation[s] managed by DG Trade and equipped with the necessary software and the relevant data sets, as the case may require, will be made available with the following technical specifications:
 - (a) [Word Processing Software (with an equation editor) / Spreadsheet Processing Software / PDF Reader Software].
 - (b) [Data Analysis and Statistical Software].
- (2) [This/These] PC workstation[s] [is/are] made available for the purpose of allowing the Authorised Persons an opportunity to verify the evidence in the Commission's file where the disclosure of such confidential information may be necessary for the effective exercise of the [Party/Parties'] procedural rights and rights of defence.
- (3) No external storage medium will be available to the Authorised Persons.

2 THE CONDITIONS OF ACCESS TO THE DATA

- (4) The Data will be made available to the Authorised Persons in electronic and hard copy form. The PC workstation[s] will have access to a specific folder in which there will be a number of read-only files for review by the Authorised Persons. The computer workstations will be backed-up daily to ensure business continuity.
- (5) During the course of the data room procedure, Authorised Persons may take manuscript notes in the data room and take notes on their laptop computers.

- (6) No external communication in any form is allowed. The data room will be monitored at all times. The use of modems, [portable] photocopiers, scanning devices, facsimile equipment, and any optical imaging devices (including phones with cameras) or electronic equipment other than laptop computers is prohibited in the Data Room.
- (7) 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, with the exception of the manuscript notes and notes on their laptop which they are permitted to make in the data room pursuant to paragraph (5).

3 DURATION OF THE DATA ROOM ACCESS

- (8) The Data Room will be open between the hours of 9h00 to 18h00 CET on business days from the date of publication of the notice of initiation until one month after the final determination is published in the Official Journal.

4 POSSIBLE PRESENCE OF INTERESTED PARTIES' LEGAL COUNSEL

- (9) At any point during the course of the Data Room procedure, interested parties' legal counsel, at their request, may be allowed access to the Data Room for the sole purpose of verifying that appropriate safeguards are in place.

5 SANCTIONS

- (10) By signing the Non-Disclosure Agreement and agreeing to the Data Room Rules, the Authorised Persons recognise their rights and accept the obligations stemming from the data room procedure. In case any of the rules or obligations is not respected by any of the Authorised Persons, all Data Room participants of the relevant party will be immediately requested to leave the data room.
- (11) In addition, in case of breach of these Data Room Rules and/or Non-Disclosure Agreement, the sanctions set out in section 6 of the Commission Guidelines on Access to the File in TDI Proceedings may be applied to the Authorised Persons in breach.

Annex B: Standard Non-Disclosure Agreement**NON-DISCLOSURE AGREEMENT**

Case [M.XXXX/AT.XXXXX] - [CASE NAME]

Whereas I, the undersigned,

Declare that I have been engaged as an Authorised Person by [Names of Party/Parties to which data room access is granted through their Authorised Person] (the "[Party/Parties]") in connection with the **Case [M.XXXX/AT.XXXXX] - [CASE NAME]** and I am duly authorised by the same to make the below undertakings;

Whereas the Commission has made available a data room containing data collected from interested parties during the course of its investigation in **Case [M.XXXX/AT.XXXXX] - [CASE NAME]** (the "Data");

Whereas, for the purpose of verifying the validity of the data submitted by interested parties, [name of Party/Parties] [has/have] released me from my professional duties and obligations I have towards [it/them], as [its/their] appointed external advisor in the above referenced proceeding, to disclose all relevant Data to my clients;

Whereas certain Data contained in limited (also called "Confidential" or "Bracketed") submissions made by interested parties or documents prepared by the Commission in connection with its investigation constitute business secrets and other confidential information and must not be disclosed under any circumstances to the [Party/Parties] or to any other third party;

Therefore, I solemnly undertake:

- (a) not to copy (in any format, physical, digital or otherwise) or remove any Data from the data room, save the manuscript notes and notes on my laptop computer I am permitted to remove from the data room pursuant to paragraph (7) of the Data Room Rules, and to fully abide by the procedures set forth in the attached Data Room Rules;
- (b) not to disclose, transmit, communicate or make the confidential Data (within the meaning at point 1 of the Commission Guidelines on Access to the File in TDI Proceedings) provided by the Interested Parties available in any manner, shape or form to any other person (including the [Party/Parties]);
- (c) to duly and promptly inform DG Trade of any breaches of these undertakings, whether as a result of my actions or failings or the actions of others, as soon as I become aware of them; and

- (d) to procure the full compliance with the terms of this agreement by any and all persons who work with me in any capacity in reviewing and analysing the Data in the data room, and to provide a list of all such persons to DG Trade and their signed acceptance of the terms of this agreement.

.....

Name:
Function:
Date:
Place: