JOINT CONTROLLERSHIP ARRANGEMENT

with regard to processing of personal data in the context of the cooperation mechanism under Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

The European Commission, Directorate-General for Trade *(hereafter referred to as 'the Commission')*

and

EU Member States' representatives or authorities participating in the cooperation mechanism under Regulation (EU) 2019/452 *(hereafter referred to as 'the Member States'),*

Having regard to Article 14 of Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (hereafter, Regulation (EU) 2019/452)[1];

Having regard to 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereafter, Regulation (EU) 2018/1725)[2];

Having regard to 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 (hereafter, Regulation (EU) 2016/679)[3];

(1) *Whereas* Article 28 of Regulation (EU) 2018/1725 establishes that where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers who, by means of an arrangement, shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16 of Regulation (EU) 2018/1725;

[1] OJ L 791, 21.03.2019, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 1.

(2) Whereas Article 26 of Regulation (EU) 2016/679 establishes that where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers, who by means of an arrangement, shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679;

(3) Whereas Regulation (EU) 2019/452 establishes a cooperation mechanism under which the Member States and the Commission exchange information about and the assessment of foreign direct investments likely to affect security or public order. This exchange of information may involve processing of personal data;

(4) Whereas Article 14 of Regulation (EU) 2019/452 establishes that processing data under that Regulation is in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 and only in so far as it is necessary for the screening of foreign direct investments by the Member States and for ensuring the effectiveness of the cooperation provided for in Regulation (EU) 2019/452.

HAVE AGREED AS FOLLOWS:

Article 1. SCOPE OF THIS ARRANGEMENT

1.1 The Commission and Member States act as joint controllers in relation to the processing of personal data in the context of the cooperation mechanism under Articles 6 to 11 of Regulation (EU) 2019/452 (hereafter, the 'cooperation mechanism'), and are hereafter collectively referred to as the 'Joint Controllers'/'Parties'.

1.2 This Joint Controllership Arrangement (hereafter, 'Arrangement') sets out the allocation of respective roles, responsibilities and practical arrangements between the Commission and the Member States as Joint Controllers pursuant to Article 28 of Regulation (EU) 2018/1725 and Article 26 of Regulation (EU) 2016/679. For the purpose of the document, the definitions set out in Article 3 of Regulation (EU) 2018/1725 shall apply.

Article 2. SUBJECT MATTER AND DESCRIPTION OF THE PROCESSING

2.1. The purpose of the processing is exchange of information in order to facilitate as far as necessary the screening of foreign direct investments ('FDI') by the Member States and ensuring the effectiveness of the cooperation mechanism provided for in Regulation (EU) 2019/452.

2.2. Whereas for a large majority of processing of personal data one or several of the Joint Controllers is/are solely responsible and in such cases act(s) as sole data controllers (see Article 4), some activities are common to the Joint Controllers.

2.3. The data subjects whose data could be processed:

- Natural persons involved in management, ownership structure or representation of the entities involved in FDI transaction (investor or target companies),
- Natural persons operating contact points referred to in Article 11 of Regulation (EU) 2019/452 and other natural persons assessing FDIs in the Member States and in the Commission.

2.4. The categories of personal data processed are:

- Names of the natural persons who are investors or target companies and their addresses,
- Names and contact data of natural persons involved in management of investors or target companies,
- Names and positions of person involved in operating contact points,
- Contact data of natural persons operating contact points.

2.5. Description of the origin of the personal data processed and the nature of the processing

The processing of personal data will be a part of the information exchanged on FDI taking place in a Member State between the Commission and Member States. Under this cooperation mechanism, Member States and the Commission share information and can raise concerns through their comments or, where relevant, Commission opinion. Each Member State may submit comments if an FDI is likely to affect its security of public order or in case it has relevant information on an FDI. The Commission may issue an opinion if an FDI is likely to affect the security or public order of more than one Member State or of the Union as a whole, notably in the context of projects and programmes of Union interest.

Personal data of natural persons holding a position in the management or ownership structure or represent entities involved in FDI transaction (investors or target companies) will typically originate from the Member State in the territory of which the FDI takes place. In less frequent instance, personal data may originate from other Member State that submits comments or additional information on an FDI or from the Commission.

Personal data of natural persons operating contact points in the Member States and in the Commission will originate from the Member States or the Commission respectively.

The Commission and the Member States will normally perform most of their processing of personal data separately in the contexts of their internal assessment of FDI. Respectively, the Commission's processing of personal data in the context of its internal assessment of FDI notified under the cooperation mechanism is subject to Regulation (EU) 2018/1725, whereas Regulation (EU) 2016/679 applies the data processing by the Member States.

Once the data originating from one of the Member States is shared with the Commission and other Member States through the cooperation mechanism, the Commission and all Member States become Joint Controllers for the processing of personal data exchanged.

2.6. Duration of the processing

Personal data related to the implementation of Regulation (EU) 2019/452 are kept only for the time strictly necessary to achieve the purposes of screening of foreign direct investments ('FDI') by the Member States and ensuring the effectiveness of the cooperation mechanism provided for in Regulation (EU) 2019/452.

Article 3. SCOPE OF THE JOINT CONTROLLERSHIP

Joint Controllership under this Arrangement comprises all processing carried out jointly by the Commission and Member States for which they are Joint Controllers, that is:

- the exchange of information, including personal data, concerning FDI subject to the cooperation mechanism,
- the provision of comments, the issuance of opinions, in relation to the assessment whether the FDI is likely to affect security or public order.

Article 4. RESPONSIBILITIES, ROLES AND RELATIONSHIP TOWARDS DATA SUBJECTS

In order to guarantee compliance with applicable data protection rules, each of the Parties shall comply with the general principles of data protection, as laid down in Article 4 of Regulation (EU) 2018/1725 and Article 5 of Regulation (EU) 2016/679, respectively.

Information of data subjects:

The data subjects shall be informed of the processing by the Party that collected personal data from those data subjects. As generally personal data will be collected by the Member States, it is the role of a Member State to inform data subjects concerned of the processing.

In view of the objectives of Regulation (EU) 2019/452, the Member States (or, where applicable, the Commission) may restrict the right to information of data subjects in accordance with Article 23 of Regulation (EU) 2016/679 (or with Article 25 of Regulation (EU) 2018/1725, respectively).

Handling of data subject requests:

The requests of data subjects shall be handled by the Party who collected personal data from the data subjects. As generally personal data will be collected by the Member States, it is the responsibility of a Member State to handle requests from data subjects concerned.

Without prejudice to the handling of data subject requests by the Member States, the Parties shall cooperate and, when so requested, provide each other with swift and efficient assistance in handling any data subject requests.

The Parties shall not disclose or release any personal data processed jointly in response to a data subject access request without first consulting the other relevant Party or Parties wherever possible/ if required.

In view of the objectives of Regulation (EU) 2019/452, the Member States (or, where applicable, the Commission) may restrict the right to file a request in accordance with Article 23 of Regulation (EU) 2016/679 or with its national law (or with Article 25 of Regulation (EU) 2018/1725, respectively).

Management of security incidents, including personal data breaches:

The Parties shall handle security incidents, including personal data breaches, in accordance with their internal procedures and applicable legislation.

The Parties shall in particular provide each other with swift and efficient assistance as required to facilitate the identification and handling of any security incidents, including personal data breaches, linked to the joint processing.

The Parties shall notify each other of the following:

a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing joint processing;

b) any security incidents that are linked to the joint processing;

c) any personal data breach (i.e. any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data undergoing joint processing), the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d) any breach of the technical and/or organisational safeguards of the joint processing.

Each Party is responsible for all security incidents, including personal data breaches, that occur as a result of an infringement of that Party's obligations under this Arrangement and Regulation (EU) 2018/1725 or Regulation (EU) 2016/679, respectively.

The Parties shall document the security incidents (including personal data breaches) and notify each other without undue delay and at the latest within 48 hours after becoming aware of a security incident (including a personal data breach).

The Party, responsible for a personal data breach, shall document that personal data breach and notify it to the European Data Protection Supervisor or the competent national supervisory authority. It shall do so without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The Party responsible shall inform the other Parties of such notification.

Unless the right of the data subject to be informed of the personal data breach had been restricted, the Party, responsible for the personal data breach, shall communicate that personal data breach to the data subjects concerned if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The Party responsible shall and inform the other Parties of such communication.

Responsibility for the security of processing

In accordance with Article 11 of Regulation (EU) 2019/452, the Commission will provide a secure and encrypted system to support direct cooperation and exchange of information between the contact points in the Member States and the Commission itself. While the Parties are Joint Controllers for personal data exchanged within that secure and encrypted system, each of the Parties may further process this data within other systems used by it for its internal processes only for the purposes of screening of FDI and effectiveness of the cooperation mechanism. To this end, each Party shall implement appropriate technical and organisational measures, designed to:

i. ensure and protect the security, integrity and confidentiality of the personal data jointly processed, in line with IT Security Decision of the Commission[4];
ii. protect against any unauthorised or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to any personal data in its possession;
iii. not disclose or allow access to the personal data to anyone other than the beforehand agreed recipients or processors.

[4] Commission Decision (EU, EURATOM) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

Each Party shall implement appropriate technical and organisational measures to ensure the security of processing pursuant to Article 33 of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/679, respectively.

The Parties shall provide swift and efficient assistance to each other in case of security incidents or personal data breach.

Localisation of personal data

Personal data, collected for the purpose of the processing, shall only be processed within the territory of the European Union and shall not leave that territory.

Personal data collected for the purpose of processing by the Commission and by the Member States shall be stored on secured systems.

Access to personal data undergoing joint processing shall only be allowed to authorised and security-cleared staff of the Commission and the Member States for the purposes of administering and operating the IT system, which facilitates the processing. This access shall be subject to specific security procedures including 2 factor authentication and smartcards for all users.

Article 5. OTHER RESPONSIBILITIES OF JOINT CONTROLLERS:

The Commission shall ensure and is responsible for:

- Deciding on the means, requirements, purpose of processing;
- Recording of the processing;
- Ensuring that the personal data undergoing processing are adequate, relevant, accurate and limited to what is necessary for the purpose;
- Deciding to restrict the application of or derogate from data subject rights, where necessary and proportionate;
- Identifying and assessing the lawfulness, necessity and proportionality of transmissions and transfers of personal data;
- Notifying any personal data breaches within IT systems used for the cooperation mechanism to the European Data Protection Supervisor (EDPS);
- Transferring data subjects' requests to the relevant Member States designated authorities if a subject asks questions about its personal data subject to the cooperation mechanism;
- Erasing, when necessary upon a request from a Member States designated authority, personal data to which the Commission has access within IT systems;
- Defining, implementing and providing the technical means to ensure availability and smooth functioning of IT systems that will be used for the cooperation mechanism and exchanges between the contact points;

- Performing, when necessary, analysis that may relate to the personal data stored in IT systems;
- Using only processors that meet the requirements of Regulation (EU) 2018/1725 and to govern the latter's processing by a contract or legal act;
- Defining and implementing, where necessary, with the approval of the Member States designated authorities, any system developments that may have an effect on the type of or the way personal data is processed;
- Carrying out a prior consultation with the European Data Protection Supervisor, where needed;
- Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Cooperating with the European Data Protection Supervisor, on request, in the performance of his or her tasks.

The Member State(s) shall ensure and are responsible for:

- Deciding on the means, requirements, purpose of processing;
- Recording of the processing;
- Ensuring that the personal data undergoing processing are adequate, accurate, relevant and limited to what is necessary for the purpose;
- Validating personal data submitted under the cooperation mechanism;
- Communicating with data subjects to clarify any technical errors or lack of clarity in the initial registration;
- Communicating any personal data breaches within their processing of personal data under the cooperation mechanism to the competent supervisory authorities of the Member State, in accordance with Articles 33 and 34 of the Regulation (EU) No 2016/679;
- Ensuring that their staff, who have access to personal data within the cooperation mechanism, are adequately trained to ensure that they perform their tasks in compliance with the rules applicable to the protection of personal data;
- Providing opinions to the Commission on any developments that may have an effect on the type of or the way personal data is processed;
- Handling of data subjects' requests;
- Deciding to restrict the application of or derogate from data subject rights, where necessary and proportionate;
- Using only processors that meet the requirements of Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively and to govern the latter's processing by a contract or legal act;
- Identifying and assessing the lawfulness, necessity and proportionality of transmissions and transfers of personal data;

- Establishing and keeping up to date the list of all recipients of personal data (in the Member States);
- Carrying out a prior consultation with national data protection supervisory authority, where needed;
- Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Cooperating with national data protection supervisory authority, on request, in the performance of his or her tasks.

Article 6. LIABILITY FOR NON-COMPLIANCE

The Commission shall be liable for non-compliance in line with Chapter VIII of Regulation (EU) 2018/1725.

The Member State(s) shall be liable for non-compliance in line with Chapter VIII of Regulation (EU) 2016/679.

Article 7. COOPERATION BETWEEN THE PARTIES OF ARRANGEMENT

Each Party, when so requested, shall provide a swift and efficient assistance to the other Party(ies) in execution of this Arrangement, while complying with all applicable requirements of Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, and other applicable data protection rules.

Article 8. SETTLEMENT OF DISPUTES

This arrangement is governed by European Union law.

The Parties shall endeavour to settle amicably any dispute arising out or relating to the interpretation or application of this Arrangement.

If at any time a question, a dispute or difference shall arise between the Parties, in relation to or in connection with this Arrangement, the Parties will use every endeavour to resolve it by a process of consultation, consensus and application of common sense.

The preference is that all disputes are settled at the operational level as they arise, and that they are settled by the contact entities listed in Annex for specific processing.

The purpose of the consultation shall be to review and agree so far as is practicable the action taken to solve the problem arisen and the Parties shall negotiate with each other in good faith to that end. Each Party shall respond to a request for amicable settlement within 7 working days of such request. The Period to reach an amicable settlement shall be 30 days from the date of the request.

If the dispute cannot be settled amicably, each Party may submit for mediation or/and judicial proceedings in the following manner:

(a) in case of mediation, the Parties shall jointly appoint a mediator acceptable by each of them, who will be responsible for facilitating the resolution of the dispute within two months from the referral of the dispute to him/her,

(b) in case of judicial proceedings, the matter shall be referred to the Court of Justice of the European Union in accordance with the Treaty on the Functioning of the European Union.

Article 9. AMENDMENTS

At any time, the Parties may, by mutual consent, amend or supplement this Arrangement. Any such amendment or supplement shall be made in writing.

The annexes to this Arrangement may be amended at the operational level / level of a working group, and the other Party(ies) must be notified on amendment.

Article 10. ENTRY INTO FORCE

This Arrangement enters into force on the date on which the last Party signs it and it is valid for the duration of the processing and shall continue to be effective for a period of the application of Regulation (EU) 2019/452.

Done in Brussels, on