JOINT CONTROLLERSHIP ARRANGEMENT

with regard to processing of personal data taking place in the context of the EU tobacco traceability system

The European Commission, represented by the Directorate-General for Health and Food Safety, represented for the purposes of signing this Joint Controllership Arrangement by Mr Andrzej RYS, Director of Directorate B: Health systems, medical products and innovation *(hereafter referred to as 'the Commission')*,

and

EU Member States' representatives or authorities participating in the EU tobacco traceability system under Commission Implementing Regulation (EU) 2018/574 *(hereafter referred to as 'the Member States'*),

The Commission and the Member States shall hereinafter be referred to jointly as "the Parties" or individually as "the Party".

Having regard to Directive 2014/40/EU of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC, and in particular Articles 15(1) and (5) thereof;

Having regard to Commission Implementing Regulation (EU) 2018/574 of 15 December 2017 on technical standards for the establishment and operation of a traceability system for tobacco products, and in particular Chapters III, V and VI thereof;

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), and in particular Article 5(1)(a) thereof;

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), and in particular Article 6(1)(e) thereof;

Whereas:

(1) 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 between them, 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;

(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 Article 15(8) of Directive 2014/40/EU provides that the Member States shall ensure that manufacturers and importers of tobacco products conclude data storage contracts with an independent third party, for the purpose of hosting the data storage facility for all relevant data;

(4) Whereas Article 23(1) of Directive 2014/40/EU establishes that the Member States shall ensure that manufacturers and importers of tobacco and related products provide the Commission and the competent authorities of the Member States with complete and correct information requested pursuant to that Directive and within the time limits set out therein;

(5) Whereas Article 23(2) of Directive 2014/40/EU establishes that the Member States shall ensure that tobacco and related products which do not comply with that Directive, including the implementing and delegated acts provided for therein, are not placed on the market;

(6) Whereas Article 23(3) of Directive 2014/40/EU provides that Member States shall lay down rules on penalties applicable to infringements of the national provisions adopted pursuant to that Directive and shall take all measures that are necessary to ensure that those penalties are enforced;

(7) Whereas Annex I Part A (3) of Commission Implementing Regulation (EU) 2018/574 provides that the Commission shall, within three months of the date of receiving the notification of a proposed third party provider and a draft data storage contract, and on the basis of an examination of the draft contract and the suitability of the proposed provider, in particular, as regards its independence and technical capacities as referred to in Article 15(8) of Directive 2014/40/EU, approve or reject the proposed provider and the draft contract;

(8) Whereas Annex I Part B (1) of Commission Implementing Regulation (EU) 2018/574 establishes that the Commission shall appoint, from amongst the providers of the primary repositories who have been approved in accordance with Part A within six months following the entry into force of Delegated Regulation (EU) 2018/573, a provider tasked with operating the secondary repository (‘the operator of the secondary repository’) for the purpose of carrying out the services specified in Chapter V of that Regulation;

HAVE AGREED AS FOLLOWS:

Article 1 – SCOPE OF THIS ARRANGEMENT

1.1 This Arrangement sets out the allocation of respective roles, responsibilities and practical arrangements between the Commission and the Member States for compliance with their data protection obligations under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, when carrying out the processing operation in the context of the EU tobacco traceability system.

1.2 For the purpose of this Arrangement, the definitions set out in Article 3 of Regulation (EU) 2018/1725 and Article 4 of Regulation (EU) 2016/679, respectively, shall apply.

1.3 Description of the purpose and the nature of the processing operations taking place in the context of the EU tobacco traceability system (hereafter, 'processing operation'):

The subject matter and purpose of the processing of personal data are the operation of an EU tracking and tracing system, which requires economic operators to register in the system and to record and transmit information on product movements and transactional data of tobacco products in the European Union. The collected data enables Member States and the Commission to carry out effective monitoring and enforcement activities in the context of Directive 2014/40/EU, in particular the fight against illicit trade in tobacco products.

1.4 The handling of data other than personal data is outside the scope of this Arrangement.

1.5 The processing operations consist of the following sets of processing operations:

- Set 1: Processing of personal data in the context of request for identifier codes for economic operators, facilities and machines used to manufacture tobacco products.
- Set 2: Processing of personal data in the context of recording and transmission of information on product movements.
- Set 3: Processing of personal data in the context of recording and transmission of information of transactional information.

The different processing activities that are part of the above three sets relate to different stages that the processing of personal data involves but serve the same purpose and involve the same type of personal data.

Article 2 – CONTROLLERS AND JOINT CONTROLLERS

2.1. For the purpose of this Arrangement, the Commission and the Member States are considered as controllers, as set out in Regulation (EU) 2018/1725 and Regulation (EU) 2016/679 respectively, in relation to the data processing activities taking place in the EU system for tobacco traceability (notably, its repositories system).

2.2. The Commission and the Member States act as **joint controllers**, pursuant to Article 28 of Regulation (EU) 2018/1725 and Article 26 of Regulation (EU) 2016/679, in relation to the sets of processing operations described under 1.5., for which they are hereafter collectively referred to as the 'Joint Controllers'.

Article 3 – 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.

3.1 Provision of information to data subjects

For set 1 of processing operations: the Member States are responsible for ensuring that a privacy statement providing the necessary information on the intended processing operations namely explaining how the data subjects' personal data are processed in connection with the issuing and registration of economic operators', facilities' and machines' identifier codes, recording and transmission of information on product movements and recording and transmission of transactional information in the tobacco products traceability system is published on the website of ID issuer.

For sets 2 and 3 of processing operations: the Commission is responsible for ensuring that the above mentioned privacy statement is published on the website of the primary repositories' providers.

The Commission is responsible for ensuring that the same privacy statement is published on the Commission's Tobacco Tracking and Tracing knowledge website[1].

3.2 Handling of data subject requests

3.2.1 The data subjects may exercise their rights under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, in respect of and against each of the Parties.

The Parties shall handle the requests of data subjects in accordance with the procedure described in section 3.2 of this Arrangement.

The Parties shall cooperate and, when so requested, provide each other with swift and efficient assistance in handling any data subject requests and in addressing any other issues, which may entail risks to the rights and freedoms of the data subjects.

Notwithstanding the possibility for data subjects to direct their requests to each joint controller, the Commission is the Joint Controller responsible for handling all data subjects' requests in relation to all processing activities. To comply with this role, the Commission shall designate a single contact point for handling all data subjects' requests.

The relevant email address is provided in Annex II to this Arrangement.

[1] https://ec.europa.eu/health/tobacco/tracking_tracing_system_en

Should a Member State receive a data subject request, that Member State shall forward the request promptly and at the latest within five working days of its receipt to the Commission.

The Commission shall send on behalf of the Parties an acknowledgment of receipt to the data subject within further five working days, while at the same time informing thereof the Member State, which received the request in the first place.

The Commission shall provide information on the action taken on a request to the data subject without undue delay and at the latest within one month of receipt of the request. That period may be extended pursuant to Article 14(3) of Regulation (EU) 2018/1725 and Article 12(3) of Regulation (EU) 2016/679, respectively.

The Member States shall assist the Commission in handling of the data subjects' requests regarding set 1 of the processing operations.

3.2.2 In a response to a data subject request, the Commission shall not disclose nor otherwise make available any personal data processed jointly, without first consulting other relevant Parties. Any person whose personal data is processed by the Parties in the context of the EU tobacco traceability system has specific rights as a data subject under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725 and Chapter III (Articles 12-23) of Regulation (EU) 2016/679, in particular the right to access, rectify or erase their personal data and the right to restrict or, where applicable, the right to object to processing or the right to data portability.

3.3 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:

1. any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing joint processing;
2. any security incidents that are linked to the joint processing operation;
3. 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;

4. any breach of the technical and/or organisational safeguards of the joint processing operation.

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 and 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 72 hours (where feasible) 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, as defined in Article 4(21) of Regulation (EU) 2016/679. 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.

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 that natural person. The Party responsible shall inform the other Parties of such communication.

3.4 Responsibility for the security of processing

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.

3.5 Processors

With regard to the processing operations taking place in the context of the EU tobacco traceability system, the provider of the secondary repository and the entities responsible for generating and issuing unique identifiers (the 'ID issuers') are considered processors in the sense of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

The provider of the secondary repository must have entered into an agreement on relevant parts of the processing of personal data with the providers of primary repositories who are considered sub-processors.

- The processing of personal data by the providers of the primary repositories should take place in accordance with the service agreement and *data processing agreement between the secondary repository provider and the primary repositories providers*.
- The processing of personal data by the provider of the secondary repository should take place in accordance with the contract *between the secondary repository provider and the Commission*.

The Commission, which concluded a processing agreement with the provider of the secondary repository, shall ensure on behalf of Joint Controllers that the latter acts only on instructions from and under the processing agreement with the Commission. The obligations referred to in the data processing agreement signed between the operator of the secondary repository and the Commission shall pass on in writing to the providers of primary repositories acting as data sub-processors.

The Member States, which concluded an agreement with the ID issuers or appointed them by means of a legal act, shall ensure on behalf of the Joint Controllers that the latter act only on instructions from and under the agreement with the Member States or the relevant legal act.

The processing of personal data by the provider of the secondary repository and the providers of primary repositories shall meet the requirements of Regulation (EU) 2016/679 and be processed solely for the purposes referred to in Directive 2014/40/EU and Commission Implementing Regulation (EU) 2018/574, as described in Article 25(2) of the Implementing Regulation.

Each Party shall ensure the compliance of such processing pursuant to Article 29 of Regulation (EU) 2018/1725 and Article 28 of Regulation (EU) 2016/679, respectively.

After the conclusion of this Arrangement, the joint controllers shall inform each other of any additional processor that they engage to process personal data on their behalf. The joint controllers should do so without undue delay and at the latest within five working days after the conclusion of the processing agreement with a processor. The joint controllers shall also adequately update Annex III to this Arrangement without undue delay and at the latest within 15 working days after the conclusion of the new processing agreement.

3.6 Localisation of personal data

The localisation of and access to the personal data collected for the purpose of the following processing activities:

- processing activities described in set 1 [‘Identifier Codes for Economic Operators, Facilities and Machines’], set 2 [‘Recording and transmission of information on product movements’] and set 3 [‘Recording and transmission of transactional information of the processing operations’] of processing operations shall comply with the following:

    i. the personal data shall only be processed by the processor and sub-processors as defined in this Arrangement;
    ii. the personal data shall only be processed within the territory of the European Union and shall not leave that territory.

The applicable legal framework[2] stipulates that access to data (including personal data) is limited to the competent authorities of the Member States, the Commission and external auditors approved by the Commission. However, under the same rules[3], in duly justified cases, the Commission or the Member States may grant manufacturers or importers of tobacco products access to stored data.

The Member States, the Commission and external auditors have full physical and virtual access to the data in the primary repositories and the secondary repository. Virtual access to the data is facilitated via graphical interfaces at the level of the secondary repository.

Access to personal data undergoing joint processing shall only be allowed to: a) authorised staff of the Commission and the Member States for the purposes of carrying out effective monitoring and enforcement activities in the context of Directive 2014/40/EU, b) authorised staff of the processors and sub-processors indicated under 3.5. for the purposes of operating the IT system, which facilitates the processing operation. This access shall be subject to ID and password requirements.

3.7 Other responsibilities of Joint Controllers:

3.7.1 The Commission shall ensure and is responsible for:

- Deciding on the means, requirements and purposes of processing;
- Maintaining a record of the processing operations regarding sets 2 and 3 of processing operations;
- Ensuring that the personal data undergoing processing are adequate, accurate, relevant and limited to what is necessary for the purpose;
- Ensuring a transparent information and communication to data subjects of their rights;
- Facilitating the exercise of the rights of data subjects;
- Handling of data subjects' requests;
- Ensuring that principles of privacy by design and privacy by default are respected;
- 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;
- 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[4] (in the Member States) regarding sets 2 and 3 of processing operations;
- Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality regarding sets 2 and 3 of processing operations;

[2] Art. 15(8) par. 3 of Directive 2014/40/EU and Art. 25(1)(k) of Commission Implementing Regulation 2018/574.
[3] Art. 15(8) par. 3 of Directive 2014/40/EU.
[4] The recipients of personal data are defined in Annex I, part 6 of the Arrangement.

- Cooperating with the European Data Protection Supervisor, on request, in the performance of its tasks.

3.7.2 The Member States shall ensure and are responsible for:

- Deciding on the means, requirements, purpose of processing;
- Maintaining a record of the processing operations regarding set 1 of processing operations;
- Ensuring that the personal data undergoing processing are adequate, accurate, relevant and limited to what is necessary for the purpose;
- Ensuring a transparent information and communication to data subjects of their rights;
- Facilitating the exercise of the rights of data subjects;
- Assist the Commission in handling the data subjects' requests regarding set 1 of processing operations;
- Ensuring privacy by design and privacy by default;
- Using only processors that meet the requirements of Regulation (EU) 2016/679 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) regarding set 1 of processing operations;
- Carrying out a prior consultation with their national supervisory authorities, where needed;
- Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality regarding set 1 of processing operations;
- Cooperating with their national supervisory authorities on request, in the performance of their tasks.

Article 4 – LIABILITY FOR NON-COMPLIANCE

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

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

Article 5 – COOPERATION BETWEEN THE PARTIES OF ARRANGEMENT

Each Party, when so requested, shall provide a swift and efficient assistance to the other Parties 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 6 –AMENDMENTS

6.1 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 by mutual agreement of the Parties at the operational level / level of a working group.

6.2 A Party that intends to withdraw from this Arrangement shall inform the other Parties accordingly in writing. The withdrawal shall come into effect within 30 days of the day when the withdrawing Party informed all other Parties of its intention to withdraw from this Arrangement.

Article 7 - ENTRY INTO FORCE

This Arrangement enters into force on the date on which the Commission and one EU Member State signs it and shall continue to be effective for as long as the tobacco traceability system is operational, or until the arrangement is replaced by a new arrangement determining the distribution of responsibilities in connection with the processing.