Administrative Arrangement for the transfer of personal data between

the European Commission (the transferring Authority) and the Turkish Medicines and Medical Devices Agency (TITCK) (the receiving Authority)

The European Commission ("the transferring Authority") and the Turkish Medicines and Medical Devices Agency ("the receiving Authority") together the "Authorities", acting in good faith, will put into practice the safeguards specified in this Administrative Arrangement ("Arrangement") to the transfer of personal data between them.

The Authorities recognise the importance of the protection of personal data and of having robust data protection regimes in place.

The transfer of personal data from the European Union to third countries can be based on provisions to be inserted into administrative arrangements as specified in Article 48(3) (b) of the 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 ("Regulation 2018/1725")[1].

The Authorities take in into account the relevant legal framework for the protection of personal data in the jurisdiction of each Authority and acknowledge the importance of regular dialogue between the European Commission and the European Data Protection Supervisor ("EDPS"), and the Turkish Medicines and Medical Devices Agency ("TITCK") and the Turkish Personal Data Protection Board.

The Authorities intend to process personal data to carry out the public mandate and exercise of official authority vested in them and comply with relevant legal obligations as laid out in Regulation (EU) 2017/745 of the European Parliament and on the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC ("the MDR")[2], as amended, and in Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU ("the IVDR")[3], as amended.

The Authorities will ensure efficient cooperation between them while acting in accordance with their mandates as defined by the applicable sectoral laws. This is to enable the exchange of information between sectorial actors, national competent authorities and the Commission, in the medical devices and *in vitro* diagnostic medical devices sectors via the European database on medical devices ("Eudamed"), as defined in Article 33 and correlatives of the

---

1 OJ L 295, 21.11.2018, p. 39.
2 OJ L 117, 5.5.2017, p. 1.
3 OJ L 117, 5.5.2017, p. 176.

MDR or, where Eudamed is not fully functional on the date laid down in Article 123(3)(d) of the MDR or Article 113(3)(f) of the IVDR respectively, any alternative administrative and technical arrangements applied to facilitate the exchange of information related to Eudamed.

The Commission's role as controller of Eudamed and its electronic systems is defined in Article 33 of the MDR.

I. Purpose and Scope

The purpose of this Arrangement is to enable the Authorities to transfer personal data in accordance with the applicable legal requirements and applicable sectoral laws. Transfers of personal data under this Arrangement are limited to transfers between the European Commission and the Turkish Medicines and Medical Devices Agency, in their capacity as public Authorities and regulators of medical devices and *in vitro* diagnostic medical devices, via Eudamed or, where necessary, alternative administrative and technical arrangements.

The Authorities are committed to having in place appropriate safeguards for the processing of such personal data in the exercise of their respective regulatory mandates and responsibilities and to acting consistently with this Arrangement.

The data subjects affected by this Arrangement include natural persons representing economic operators (manufacturers, authorised representatives, importers, systems and procedure pack producers), person(s) responsible for regulatory compliance, notified bodies, sponsors, investigators, legal representatives, expert panels, ethics committee members, national competent authorities, and Commission staff. The categories of personal data processed relates to the identification and contact details of the data subjects and include the first name, last name, phone number, street, city, postcode, country and e-mail address, and in the case of clinical investigators, data on professional qualifications.

Types of processing of personal data under this Arrangement include mainly collection and storing in servers of the Data Centre of the European Commission's Directorate-General for Informatics ("DG DIGIT") but also other types of processing (e.g. organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, making available) may occur. Access to personal data is primarily granted through personalised user ID and password, or in limited cases, publically available[4]. Personal data will be processed by TİTCK to enable the Authority to act in accordance with its regulatory mandate and responsibilities under the applicable sectoral laws. Types of processing will mainly include consultation and use, but also other types of processing (e.g. organisation, structuring, making available or restriction) may occur.

Effective and enforceable rights and effective judicial redress are available to data subjects under applicable legal requirements in the jurisdiction of each Authority, however this Arrangement does not create any legally binding obligations, confer any legally binding rights, nor supersede the applicable legal requirements in each jurisdiction. The Authorities declare to have implemented, within their respective jurisdictions, the safeguards set out in Section III of this Arrangement in a manner consistent with applicable legal requirements.

[4] In accordance with Article 31(7) of the MDR, limited personal data specified in Section 1 of Part A of Annex VI of the MDR (the name, address and contact details of the person or persons responsible for regulatory compliance (PRRC) and economic operators (EO) registered in Eudamed) may be made directly available to the public without the need of user ID and password (anonymous user).

The Authorities provide safeguards to protect personal data through a combination of laws, regulations and their internal policies and procedures.

II. Definitions

For the purposes of this Arrangement:

(a) **"applicable legal requirements"** means the relevant legal framework for the protection of personal data applicable to each Authority;

(b) **"applicable sectoral laws"** means the relevant legal framework applicable laws concerning medical and *in vitro* diagnostic medical devices;

(c) **"controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(d) **"onward transfer"** means the transfer of personal data by a receiving Authority to a third party in another country who is not an Authority participating in this Arrangement;

(e) "**personal data"** means any information relating to an identified or identifiable natural person ("data subject") within the scope of this Arrangement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(f) "**personal data breach"** means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(g) **"processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(h) "**processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(i) **"data subject rights":**

i. **"right not to be subject to automated decisions, including profiling"** means a data subject's right not to be subject to legal decisions being made concerning him or her based solely on automated processing;

ii. **"right of access"** means a data subject's right to obtain from an Authority confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, to access the personal data;

iii. **"right of erasure"** means a data subject's right to have his or her personal data erased by an Authority where the personal data are no longer necessary for the purposes for which they were collected or processed, or where the data have been unlawfully collected or processed;

iv. "**right of information**" means a data subject's right to receive information on the processing of personal data relating to him or her in a concise, transparent, intelligible and easily accessible form;

v. "**right of objection**" means a data subject's right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her by an Authority, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the data subject or for the establishment, exercise or defence of legal claims;

vi. **"right of rectification"** means a data subject's right to have the data subject's inaccurate personal data corrected or completed by an Authority without undue delay;

vii. **"right of restriction of processing"** means a data subject's right to restrict the processing of the data subject's personal data where the personal data are inaccurate, where the processing is unlawful, where the Authority no longer needs the personal data for the purposes for which they were collected or where the personal data cannot be deleted;

(j) **"sharing of personal data"** means the sharing of personal data by a receiving Authority with a third party in its country, or in the case of the Commission the sharing of personal data with a third party in the EU/EEA;

(k) **"third party"** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

III. Personal data protection safeguards

1. **Purpose of processing**: Personal data in Eudamed are processed to enable all sectoral actors fulfil their obligations as defined by the applicable sectoral laws. Personal data in Eudamed are also processed to enable the Authorities to act in accordance with their regulatory mandates and responsibilities to ensure the application and enforcement of the provisions of the applicable sectoral laws. In particular, the Authorities process personal data to permit information exchange regarding devices on the market and the relevant economic operators, certain aspects of conformity assessment, notified bodies, certificates, clinical investigations, vigilance and market surveillance.

   Personal data are transferred between the Authorities only for the above purposes.

   The transferring Authority intends to transfer personal data only for the legitimate and specific purpose of assisting the receiving Authority to fulfil its regulatory mandate and responsibilities, which include regulating, supervising and enforcing compliance with the applicable sectoral laws in its jurisdiction. The receiving Authority will not further process the personal data in a manner that is incompatible with these purposes.

2. **Data quality and proportionality:** The transferring Authority intends only to transfer personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed.

   The transferring Authority will ensure that to the best of its knowledge the personal data that it transfers are accurate and, where necessary, up to date. Where an Authority becomes aware that personal data it has transferred to, or received from, another Authority is incorrect, it will advise the other Authority about the incorrect data without delay. Once it has been confirmed that the data is incorrect, the respective Authorities

will, having regard to the purposes for which the personal data have been transferred and further processed, take every reasonable step to supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.

3. **Transparency:**

Each Authority will provide general notice by publishing this Arrangement on the appropriate section of Eudamed or on their websites. The European Commission will in principle provide general notice to data subjects about: (a) how and why it may process and transfer personal data; (b) the type of entities to which such data may be transferred, (c) the rights available to data subjects.

Each Authority will provide contact details to data subjects for submitting a dispute or claim. A privacy statement will be available to data subjects by the transferring Authority in appropriate section of Eudamed.

4. **Security and confidentiality:**

The Authorities will have in place appropriate technical and organisational measures to ensure that the processing is in compliance with the provisions of this Arrangement and to protect personal data that are transferred to them against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. Such measures will include appropriate administrative, technical and physical security measures.

In the case of a personal data breach, each Authority will inform the other Authority without undue delay and not later than 24 hours after having become aware of the breach via appropriate email communication. Both Authorities will take all necessary measures to remedy and mitigate possible adverse effect of the personal data breach and will provide necessary and timely cooperation to each other, so that each of the Authorities can comply with its obligations arising from a personal data breach.

Where the personal data breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the breach shall be communicated to the data subject, without undue delay.

5. **Safeguards Relating to Data subject Rights**

The Authorities will apply the following safeguards to personal data transferred under this Arrangement:

The Authorities will have in place appropriate measures which they will follow, such that, upon request from a data subject, an Authority will (1) identify any personal data it has transferred to the other Authority pursuant to this Arrangement, (2) provide general information, including on the Authority's website, about safeguards applicable to transfers the other Authority, and (3) will ensure that the subject rights can be exercised.

Each Authority will allow a data subject who believes that his or her personal data are incomplete, inaccurate, outdated or processed in a manner that is not in accordance with applicable legal requirements or consistent with the safeguards set out in this Arrangement to make a request directly to such Authority for any rectification, erasure, restriction of processing, or where relevant, object to the processing of his or her personal data. Such a request can be made to any of the contacts published in the privacy statement.

Each Authority, in accordance with the applicable legal requirements, will address and respond to such requests of data subjects in a reasonable and timely manner, and in any case within one month. The period is extendable at a maximum by two further months,

however the data subject will be duly informed of any extension within one month. The Authorities will cooperate to accommodate the request of the data subject.

6. Onward transfers and sharing of personal data

6.1 Onward transfer of personal data

(1) Onward transfers of personal data by the receiving Authority to third parties are prohibited under this Arrangement.

(2) By way of exception and where deemed necessary, the receiving Authority will onward transfer personal data to a third party only with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement, including for data subjects.

(3) Prior to requesting the express authorisation of the transferring Authority, the receiving Authority will provide sufficient information on the type of personal data that it intends to transfer and the reasons and purposes for which it deems the transfer necessary.

6.2 Sharing of personal data

(1) Sharing of personal data by the receiving Authority with third parties is prohibited under this Arrangement.

(2) By way of exception and where it is deemed necessary, the receiving Authority will share the personal data only with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement, including for data subjects.

(3) Prior to requesting the express authorisation of the transferring Authority, the receiving Authority will provide sufficient information on the type of personal data that it intends to share and the reasons and purposes for which it deems the sharing necessary.

7. Limited data retention period: The Authorities will retain personal data for no longer than is necessary and appropriate for the purpose for which the data are processed. Such retention periods will comply with the applicable laws, rules and/or regulations governing the retention of such data in the jurisdiction of the Authorities. Retention of personal data in Eudamed shall not be longer than 15 years.

8. Redress: Each Authority provides assurance that in its legal order a data subject who believes that an Authority has failed to comply with the safeguards as set forth in this Arrangement, or who believes that his or her personal data have been subject to a personal data breach, may seek redress against that Authority to the extent permitted by applicable legal requirements.

In particular, any complaint against either Authority can be addressed to the EDPS, in the case of the European Commission, and the Turkish Personal Data Protection Board, in the case of the TITCK, as specified in the privacy statement. In addition, certain complaints against either Authority can be brought before the Court of Justice of the European Union, in the case of the European Commission, and the Turkish civil or administrative courts in the case of the TITCK. In the event of a dispute or claim brought by a data subject concerning the processing of the data subject's personal data against the transferring Authority, the receiving Authority or both Authorities, the Authorities will inform each other about any such disputes or claims, and will use best efforts to settle the dispute or claim amicably in a timely fashion.

In situations where a data subject raises a concern and a transferring Authority is of the view that the receiving Authority has not acted consistent with the safeguards set out in this Arrangement, a transferring Authority may suspend or terminate the transfer of personal data under this Arrangement to the receiving Authority until the transferring Authority is of the view that the issue is satisfactorily addressed by the receiving Authority, and will inform the data subject thereof. Prior to such time, access of the receiving Authority of the personal data will be blocked by the transferring authority.

IV. Oversight

1. Each Authority will conduct periodic reviews of its own policies and procedures that implement this Arrangement and of their effectiveness and upon reasonable request by an Authority, the other Authority will review its personal data processing policies and procedures to ascertain and confirm that the safeguards in this Arrangement are being implemented effectively. The results of the review will be communicated to the Authority that requested the review.
2. In the event that the receiving Authority is unable to effectively implement the safeguards in this Arrangement for any reason including in case of legislative change, it will promptly inform the transferring Authority, in which case the transferring Authority will temporarily suspend the transfer of personal data under this Arrangement to the receiving Authority, until such time as the receiving Authority informs the transferring Authority that it is again able to act consistent with the safeguards.
3. The implementation of this Arrangement is under independent supervision by the EDPS and the Turkish Data Protection Board. The receiving Authority will cooperate with the EDPS upon request.
4. In situations where the transferring Authority is of the view that the receiving Authority has not acted with the safeguards set out in this Arrangement, the transferring Authority will suspend the transfer of personal data to the receiving Authority under this Arrangement until the issue is satisfactorily addressed by the receiving Authority. In the event that the transferring Authority suspends the transfer of personal data to a receiving Authority under this paragraph IV (4) or under paragraph IV (2) above, or resumes transfers after any such suspension, it will promptly inform the EDPS.

V. Revision and discontinuation

1. The Authorities may consult and revise by mutual consent the terms of this Arrangement.
2. An Authority may discontinue its participation in this Arrangement, vis-à-vis the other Authority, at any time. It will endeavour to provide 30 days' written notice to the other Authority of its intent to do so. Any personal data already transferred pursuant to this Arrangement will continue to be treated consistently with the safeguards provided in this Arrangement.
3. The EDPS, in the case of the European Commission, and the Turkish Personal Data Protection Board, in the case of the TITCK, will be notified of any proposed material revisions to, or discontinuation of, this Arrangement.
4. The TITCK will complement this Arrangement with an annex enumerating the Turkish laws governing onward sharing with other public bodies, including for surveillance purposes, within three months following the signing of this Arrangement. The TITCK will immediately notify the European Commission of any changes to this annex.

Date: [...] 21/05/2021

The European Commission

Turkish Medicines and Medical Devices Agency