EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Decision authorising, subject to conditions, the use of the administrative arrangement between the European Commission and the Turkish Medicines and Medical Devices Agency in the context of the Turkish participation in the EU regulatory system for medical devices Eudamed

(Case 2021-0347)

1. INTRODUCTION

1.1. This decision concerns the authorisation of the Administrative Arrangement (AA) to be concluded between the European Commission (the Commission) and the Turkish Medicines and Medical Devices Agency in the context of the Turkish participation in the EU regulatory system for medical devices, including the relevant database, Eudamed.

1.2. The EDPS issues this Opinion in accordance with Article 57(1)(n) and Article 58(3) (f) of the Regulation (EU) 2018/1725[1] ('the Regulation').

1.3. This Decision is addressed to the Commission.

2. BACKGROUND INFORMATION

2.1. On 6 November 2020, the Commission - DG SANTE submitted a request for informal consultation regarding the AA to be concluded between the Commission and the Turkish Medicines and Medical Devices Agency in the context of the Turkish participation in the EU regulatory system for medical devices, including the relevant database, Eudamed. On 25 January 2021 the EDPS shared with DG SANTE an informal advice on the matter.

2.2. On 24 March 2021, the Commission - DG SANTE submitted a request for an urgent formal authorisation of an 'Administrative Arrangement for the transfer of personal data between the European Commission and the Turkish Medicines and Medical Devices Agency' (the 'draft AA')[2]. The Commission justified the urgency of the case by a direct impact of the authorisation of AA, thus possible future data transfers, on the continuation of the EU-Turkey Customs Union for medical device from May

[1] Regulation (EU) 2018/1725 of the European Parliament and 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, OJ, L 295, 21.11.2018, pp. 39-98.

[2] The draft AA is annexed to this Decision.

2021. A Commission Decision must be adopted before concluding the Administrative Arrangement ahead of the 26 May 2021 deadline, when the Regulation (EU) 2017/745 ('MDR')[3] fully applies.

2.3. The 'MDR' and Regulation (EU) 2017/746 ('IVDR')[4] require an efficient cooperation between the authorities involved while acting in accordance with their mandates as defined by the applicable sectoral laws. To enable this cooperation, the exchange of information is required between sectorial actors, national competent authorities and the European Commission ('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 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.

2.4. On the basis of the draft AA the Commission and the Turkish Medicines and Medical Devices Agency plan to exchange personal data in their capacity as public authorities and regulators of medical devices and in vitro diagnostic medical devices. The personal data of 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 will be exchanged. The AA concerns following categories of personal data: 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.

3. LEGAL ANALYSIS

3.1. Transfers of personal data to recipients outside the European Union ('the Union') may generate additional risks for data subjects, as the applicable data protection rules in the recipient's jurisdiction may be less protective than inside the Union. For this reason, the Union legislator adopted specific rules for such transfers in Chapter V of the Regulation (Articles 46 to 51 of the Regulation).

3.2. The first mechanism is the adoption by the Commission of an adequacy decision recognizing that the third country or an international organisation provides a standard with regard to data protection that is essentially equivalent to that within

[3] Regulation (EU) 2017/745 of the European Parliament and of 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, OJ L 117, 5.5.2017, p. 1–175.

4 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, OJ L 117, 5.5.2017, p. 176–332.

the EU.[5] However, until now the Commission has not adopted any adequacy decision concerning Turkey.

3.3. In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on the condition that enforceable rights and effective legal remedies are available for individuals[6]. A legally binding and enforceable instrument between public authorities or bodies may provide for such appropriate safeguards.[7] Such safeguards may also be provided, subject to the authorisation from the EDPS, by inserting provisions into administrative arrangements between public authorities and bodies which include enforceable and effective data subject rights.[8]

3.4. The EDPB Guidelines on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679[9] for transfers of personal data between EEA and non-EEA public authorities and bodies (the 'EDPB guidelines')[10] set a list of minimum safeguards to be included in an administrative arrangement (AA). The criteria for appropriate safeguards under Article 48(3)(b) of the Regulation are the same as under Article 46(3)(b) of Regulation 2016/679. Therefore, the EDPB guidelines are relevant for AA concluded between European institutions, bodies, offices and agencies and public authorities in third countries, such as the draft AA.

3.5. Based on the above-mentioned EDPB guidelines, the draft AA should include a series of guarantees. The EDPS is of the opinion that the draft AA provides sufficient guarantees as regards the definition of key concepts and rights, the principle of purpose limitation, the principles of data accuracy and minimisation and the storage limitation principle. However, the draft AA does not meet all requirements of the following guarantees, as explained below.

Purpose and scope

3.6. The draft AA should define its purpose and scope in an explicit and specific way. In addition, it should clearly state the categories of personal data affected and the type of processing of the personal data, which is transferred and processed under the arrangement.

3.7. The EDPS notes that the current wording of the Section I on the purpose and scope provides only for the types of processing of personal data by the Commission, while the type of processing personal data transferred to Turkey is missing. The type of

5 Article 47 of the Regulation.
6 Article 48(1) of the Regulation.
7 Article 48 (2) (a) of the Regulation.
8 Article 48 (3) (b) of the Regulation.
9 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
10 EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (the 'EDPB guidelines').

processing operations on personal data transferred to Turkey should be described in the same degree of detail as they are described for the Commission.

3.8. The EDPS notes as well that under the last paragraph of Section I on the purpose and scope the parties agree that '*this Arrangement does not create any legally binding obligations, confer any legally binding rights, nor supersede the applicable legal requirements in each jurisdiction*', as well as through the whole AA parties decided to use the verb '*should*', instead of '*will*' or '*shall*'. The EDPS underlines that the main aim of the AA is to provide protection through the full commitments taken by both parties in order to bring their common arrangement into force and to ensure enforceable data subject rights and effective legal remedies, as required by Article 48(3)(b) of the Regulation. Especially the use of the verb '*should*' denotes a guideline or a recommendation and at the same time, it entails that a deviation or non-compliance with the AA may be possible in some circumstances. Therefore, the current wording of this Section is likely to undermine the commitments of the Commission and the Turkish Medicines and Medical Devices Agency.

Security and confidentiality of the data

3.9. To ensure security and confidentiality of the data, appropriate administrative, technical and physical security measures should be taken, including for example, marking information as personal data, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential. The arrangement may also provide for procedures for cases of personal data breaches and set out that if a receiving party becomes aware of a personal data breach, it informs the transferring party as soon as possible and uses reasonable and appropriate means to remedy the personal data breach and minimise the potential adverse effects.

3.10. In this respect the EDPS notes that the current wording of Section III (4) on informing data subjects of data breach incidents may prove in practice to be very burdensome on the data controllers as it requires to mandatorily report each breach which does not pose a high risk of adversely affecting data subjects.

Right to transparency

3.11. The parties to an AA must ensure that the latter contains clear wording describing the transparency obligations of the parties, which include both a general information and individual information to data subjects. First, a general notice to data subjects should be provided in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to data subjects under the applicable legal requirements, including how to exercise those rights and information about any applicable restrictions on the exercise of such rights, available redress mechanisms and the contact details for submitting a dispute or claim. The administrative arrangement should explain how this notice should be provided to data subjects and if individual notice needs to be provided.

However, for the transferring public body, a general information notice on the website of the public body concerned will not suffice. Individual information to data subjects should be made by the transferring body in accordance with the notification requirements of Articles 15 and 16 of the Regulation.

The administrative arrangement can provide for some exceptions to such individual information. These exceptions are limited and should be in line with the ones provided under Article 16(5) of the Regulation, for example, where the data subject already has the information or where the provision of such information proves impossible or would involve a disproportionate effort

3.12. The EDPS notes that the current wording of the Section III (3) of the draft AA on the transparency does not specify all elements that should be included in the general notice to the data subjects. At the same time, the obligation of publishing the text of AA on the websites of the Commission and the Turkish Medicines and Medical Devices Agency can cover these requirements, but the wording of the AA should be changed accordingly.

Rights of access, to rectification, erasure, restriction of processing and to object

3.13. Data subjects should be able to obtain confirmation of whether their data have been transferred. They should also be provided with access to their personal data upon request. In addition, data subjects may request that their data are rectified, erased, blocked or restricted and where relevant the right to oppose to the data processing on grounds relating to his or her particular situation. Any restriction to these rights has to be provided by law and is allowed only to the extent and for as long as this is necessary to protect confidentiality pursuant to professional secrecy or other legal obligations. The arrangement should furthermore specify when these rights can be invoked and include the modalities on how the data subjects can exercise these rights before both parties as well as on how the parties will respond to such requests.

3.14. The EDPS notes that the current wording of the Section III (5) of the draft AA on the safeguards relating to data subject rights does not provide for the modalities on how data subjects can exercise the rights of access, rectification, erasure, restriction of processing and to object as well as on how the parties will respond to such requests.

Restrictions on onward transfers

3.15. Onward transfers by the receiving public body to recipients not bound by the AA should, as a rule, be specifically excluded by the arrangement. Depending on the subject matter and the particular circumstances at hand, the parties may find it necessary to allow onward transfers. In this case, under the condition that the purpose limitation principle is respected, the AA should provide that such onward transfers can only take place if the transferring body has given its prior and express authorisation and the receiving third parties commit to respect the same data protection principles and safeguards as included in the AA.

As a rule, the same safeguards as for onward transfers should apply to sharing of personal data within the same country.

In this regard, an AA should only allow disclosures of personal data to other public authorities in the third country of the receiving public body that do not go beyond what is necessary and proportionate in a democratic society to safeguard important objectives of public interest and in accordance with the jurisprudence of the Court of Justice of the European Union[11]. In order to assess a possible access, the transferring public authority should take into account the elements recalled in the EDPB Recommendations 02/2020 on European Essential Guarantees for surveillance measures.[12] It may also be useful to include an annex to the arrangement enumerating the laws governing onward sharing with other public bodies including for surveillance purposes in the destination country.[13] Any changes to this annex should be notified to the transferring party within a set of time.[14]

3.16. In the present case, Section III (6) of the draft AA provides that the Turkish receiving authority should onward transfer personal data to a third party only with the prior written consent of the Commission. It is not clear whether the legal framework governing access to personal data by other public authorities, being national security agencies or law enforcement authorities, may still give access to the personal data at stake and if so, on which conditions.

The EDPS recalls that the Commission (data exporter), is responsible for making the necessary assessment of the assurances provided by the Turkish Medicines and Medical Devices Agency (data importer) by taking into account the above-mentioned European Essential Guarantees. The Commission should conduct this assessment with due diligence and request the necessary information from the Turkish Medicines and Medical Devices Agency.

In particular, the draft AA should be complemented by an annex enumerating the Turkish laws governing onward sharing with other public bodies including for surveillance purposes in the destination country. Any changes to this annex should be notified to the Commission within a set period of time.

---

11 See CJEU Judgement of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems, case C-311/18, ECLI:EU:C:2020/559, §§ 132-149, in particular §141.

12 EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

13 EDPB Guidelines, paragraph 47.

14 EDPB Guidelines, paragraph 47.

Redress

3.17. Data subjects should continue to benefit from redress mechanisms after their data has been transferred to a non-EEA country. These redress mechanisms must provide recourse for individuals who are affected by non-compliance with the provisions of the administrative arrangement and thus the possibility for data subjects whose personal data have been transferred from the EEA to lodge complaints regarding such non-compliance and to have these complaints resolved. In particular, the data subject must be ensured an effective route to complain to the public bodies that are parties to the administrative arrangement and to an independent oversight mechanism. Moreover, a judicial remedy including compensation for damages should be available. Alternative dispute settlement mechanisms (quasi-judicial, binding mechanisms such as arbitration or alternative dispute resolution mechanisms such as mediation, which would guarantee an independent review and bind the receiving public body) should be provided only if judicial remedies are not guaranteed in the third country. Furthermore, the administrative arrangement should contain an obligation for the parties to inform each other of the outcome of the proceedings, in particular if a complaint of an individual is dismissed or not resolved. The redress mechanism must also be combined with the possibility for the transferring party to suspend or terminate the transfer of personal data under the administrative arrangement where the parties do not succeed in resolving a dispute amicably until it considers that the issue has been satisfactorily addressed by the receiving party. Such a suspension or termination, if carried out, must be accompanied by a commitment from the receiving party to return or delete the personal data.

3.18. The EDPS notes that the current wording of the Section III (8) on the redress concerning the availability of the administrative and judicial redress is not precise enough. AA is a non-binding instrument and in order to ensure effective and enforceable rights, it should contain assurances from the public body receiving the EEA personal data that individual rights are fully provided by its domestic law and can be exercised by EEA individuals under the same conditions as is the case for citizens and residents of the concerned third country. Especially it should be clearly stated that under the Turkish legislation, there is (i) an effective route to complain to the public body that is party to the AA, (ii) to an independent oversight body (Data Protection Authority) and (iii) there exists judicial remedy including compensation for damages - both material and non-material. The same applies if administrative and judicial redress is available to EU individuals in the domestic legal framework of the receiving public body. In this context the EDPS acknowledges that on 2 May 2016 Turkey ratified the Council of Europe Convention 108[15] and its Additional Protocol[16].

---

15 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS no. 108).

16 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

Supervision oversight mechanism

3.19. The supervision oversight mechanism should consist of a combination of periodic reviews conducted externally and internally by each party. The combination of the external and internal oversight as well as the adopted possible consequences following a negative review – which may include a recommendation to suspend participation in the administrative arrangement – provides for a satisfactory level of protection. The arrangement must also provide for independent supervision in charge of ensuring that the parties comply with the provisions set out in the arrangement. For instance, the arrangement could invoke oversight by a competent supervisory authority in the country of the public body receiving the EEA personal data. The EDPS also recommends that the AA provides for the voluntary commitment of the receiving party to cooperate with the EDPS as supervisory authority of the Commission. Only in the absence of a supervisory authority specifically in charge with the supervision of data protection in the third country, there is a need to provide for alternative oversight.

3.20. The EDPS notes that the current wording of Section IV of the draft AA on the oversight the AA does not explicitly provide for the oversight by the EDPS and by the Turkish Personal Data Protection Board, although it is implied in particular under Section V (3) of the AA: *'The EDPS, in the case of the European Commission, and the Turkish Personal Data Protection Board, in the case of the TITCK, should be notified of any proposed material revisions to, or discontinuation of, this Arrangement'.*

4. AUTHORISATION SUBJECT TO CONDITIONS

4.1. Subject to the changes and conditions laid down in the following paragraphs of this Decision, the EDPS takes note that the AA provides appropriate safeguards in the sense of Article 48(1) of the Regulation. Pursuant to Article 58(3)(f) of the Regulation, the EDPS thus authorises the use of the AA as a means for adducing appropriate safeguards under Article 48(3)(b), under the conditions specified hereafter.

4.2. Following **changes** are required in the draft AA:

a) under each section to change the verb '*should*' to '*will*' or '*shall*';
b) under Section I on the purpose and scope the type of processing personal data transferred to Turkey should be explained in the same degree of detail as it is described for the Commission;
c) under Section III (3) on the transparency:
   - the wording should be further complemented and changed as following: '*Each Authority will provide general notice by publishing this Agreement on 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*

under the applicable legal requirements, including how to exercise those rights; (d) information about any applicable delay or restrictions on the exercise of such rights; and (e) contact details for submitting a dispute or claim. This notice will be effected by publication of this information by the European Commission in appropriate section of Eudamed along with this Agreement. The Turkish Medicines and Medical Devices Agency will also publish on its website appropriate information relating to its processing of personal data, including information noted above, as described in this Agreement';

- It is important to recall that, for the transferring public body, a general information notice on the website (i.e. Eudamed) of the public body concerned will not suffice and individual information to data subjects should be made by the transferring body in accordance with the notification requirements of Articles 15 and 16 of the Regulation. Therefore this section should be complemented by following information: '*Individual information will be provided to data subjects by the European Commission in accordance with the notification requirements and applicable exemptions and restrictions in Regulation (EU) 2018/1725 (as set forth in Articles 15, 16 and 25 of Regulation 2018/1725*';

d) under Section III (4) on the security and confidentiality:
   - the current wording on informing data subjects of data breach incidents may prove in practice to be very burdensome on the data controllers as it requires to mandatorily report each breach which does not pose a high risk of adversely affecting data subjects, therefore the wording should be changed as following '*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*';

e) under Section III (5) on the safeguards relating to data subject rights to complement the clause in order to include the modalities on how data subjects can exercise the rights of access, rectification, erasure, restriction of processing and to object as well as on how the parties will respond to such requests;

f) under Section III (8) on the redress the wording concerning the availability of the administrative and judicial redress is too vague and it should be further clarified. The available redress mechanisms in the Union and in Turkey should be specified;

g) under Section IV on the oversight the AA the wording should be modified to explicitly provide for the independent supervision by the EDPS and the Turkish Personal Data Protection Board.

4.3. The EDPS asks that the Commission:

a) complement the AA with an annex enumerating the Turkish laws governing onward sharing with other public bodies including for surveillance purposes in the destination country. This annex should be added to the AA within time agreed by the parties. Any changes to this annex should be notified to the Commission within a set period of time to be defined by the parties.

b) provide the EDPS with a list of the Turkish laws governing onward sharing within six months after the date of this Decision.

4.4. The EDPS urges the Commission to inform the EDPS without undue delay of any suspensions of transfers of personal data under Sections III (8) on the redress and IV on the oversight of the AA and any revision or discontinuation under Section V on the revision and discontinuation of the AA.

4.5. The EDPS asks the Commission to report on the implementation of this Decision on annual basis, with the first report due 6 months after the date of this Decision. These reports shall include the following information about the operation of the AA:

a) statistics on the amount of outgoing and incoming transfers;
b) the number of data subject requests and claims received from data subjects;
c) notifications received by Commission on the sharing of information to a third party following a legally enforceable demand or required by law.

4.6. The EDPS may exercise the existing powers conferred under Article 58 of the Regulation, and in particular, the power to order the suspension of data flows to recipients in Turkey under the AA. The EDPS may in particular do so when:

a) the EDPS or another competent supervisory authority or court has determined that Commission or a recipient party is in breach of the applicable standards of protection; or
b) there is a substantial likelihood that the standards of protection are being infringed; or
c) there are reasonable grounds to believe that any of the conditions set out in this Decision are not complied with.

5. JUDICIAL REMEDY

5.1. Pursuant to Article 64 of the Regulation, any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done at Brussels, 12 May 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

Annex: Draft Administrative Agreement for the transfer of personal data between the European Commission and the Turkish Medicines and Medical Devices Agency

ANNEX

Draft Administrative Arrangement for the transfer of personal data between the European Commission and the Turkish Medicines and Medical Devices Agency

The European Commission ("the transferring Authority") and the Turkish Medicines and Medical Devices Agency ("the receiving Authority") together the "Authorities", acting in good faith, should 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")[17].

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")[18], 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")[19], as amended.

The Authorities should 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 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

[17] *OJ L 295, 21.11.2018, p. 39.*
[18] *OJ L 117, 5.5.2017, p. 1.*
[19] *OJ L 117, 5.5.2017, p. 176.*

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[20].

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

---

[20] *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).*

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 should 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 should 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 should advise the other Authority about the incorrect data without delay. Once it has been confirmed that the data is incorrect, the respective Authorities should, 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 should provide contact details to data subjects for submitting a dispute or claim. This notice should be effected by the publishing of this information by each Authority on its website along with this Arrangement. A privacy statement should be available to data subjects by the transferring Authority in appropriate section of Eudamed.

   The Authorities commit to make this Arrangement available to data subjects on request, and publically available on the website of each Authority.

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

   In the case of a personal data breach, each Authority should 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 should take all necessary measures to remedy and mitigate possible adverse effect of the personal data breach and should 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 a personal data breach occurs, the breach should be communicated to the data subject, without undue delay.

5. Safeguards Relating to Data subject Rights

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

The Authorities should have in place appropriate measures which they should follow, such that, upon request from a data subject, an Authority should (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) should ensure that the subject rights can be exercised.

Each Authority should 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.

Each Authority, in accordance with the applicable legal requirements, should address in a reasonable and timely manner, and in any case within one month, extendable at maximum by two further months, a request from a data subject concerning the rectification, erasure, restriction of processing or objection to processing of his or her personal data.

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 should be prohibited under this Agreement.

2) By way of exception and where deemed necessary, the receiving Authority should 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 should 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 should be prohibited under this Arrangement.

2) By way of exception and where it is deemed necessary, the receiving Authority should 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 should 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 should retain personal data for no longer than is necessary and appropriate for the purpose for which the data are processed. Such retention periods should 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 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 should inform each other about any such disputes or claims, and should 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 should inform the data subject thereof. Prior to such time, access of the receiving Authority of the personal data should be blocked by the transferring authority.

IV. Oversight

1. Each Authority should 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 should 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 should 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 should promptly inform the transferring Authority, in which case the transferring Authority should 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 receiving Authority should 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 should 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 should 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 should 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 should continue to be treated consistent 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, should be notified of any proposed material revisions to, or discontinuation of, this Arrangement.

Date: 12 May 2021