Brussels, 17 January 2018

EDPS Decision concerning the transfers of personal data carried out by the European Centre for Disease Control to the World Health Organisation pursuant to Article 9(7) of Regulation (EC) No 45/2001

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[1] ('the Regulation'), and in particular Article 9(7) thereof,

Whereas:

(1) Under Decision No 1082/2013/EU[2], Member States have to report cases of certain diseases to the European Centre for Disease Control (ECDC)[3]. Data subjects are not directly identifiable from the content of the notifications, which contain information about cases of certain diseases, but no obvious identifiers allowing re-identification by parties other than the originating authority of the reporting Member State. ECDC instructs Member States to remove all personal identifiers prior to submission to ECDC; any unique record identifiers must not be traceable to individuals by ECDC. Member States also report aggregate data to ECDC, which do not qualify as personal data, and which this decision does not address.

(2) Under the International Health Regulations (IHR)[4], States Parties have to report cases of certain diseases to the World Health Organization (WHO). All EU Member States are States Parties to the IHR. The content of such notifications to be submitted to the WHO is identical to the content of the notification to be submitted to ECDC. Notifiable diseases under the IHR are a subset of notifiable diseases under Decision No 1082/2013/EU.

(3) ECDC notified its processing operations in this regard to the European Data Protection Supervisor (EDPS) for prior checking under Article 27 of the Regulation. The EDPS issued its Opinion on 3 September 2010, recommending among other points that ECDC ensure compliance with Article 9 of the Regulation when transferring personal data to recipients neither subject to the Regulation, nor to national legislation implementing Directive 95/46/EC[5]. All other recommendations made in the EDPS Opinion of 3 September 2010 have been implemented and are closed.

---

[1] OJ L 8, 12.1.2001, p. 1.
[2] OJ L 293, 5.11.2013, p.1.
[3] OJ L 142, 30.4.2004, p. 1.
[4] World Health Organization, International Health Regulations (2005), third edition, United Nations Treaty Series Volume 2509, I-44861.
[5] OJ L 281, 23.11.1995, p. 32, as amended.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

(4) In the follow-up to the EDPS Opinion of 3 September 2010, ECDC informed the EDPS about a planned structural transfer of personal data to the WHO. The WHO, as an international organisation, is neither subject to the Regulation, nor to national legislation implementing Directive 95/46/EC. It also has not been the subject of an adequacy decision of the European Commission under Article 25 of Directive 95/46/EC.

(5) Transfers of personal data from ECDC to international organisations not recognised as ensuring an adequate level of protection of personal data in the meaning of paragraphs 1 and 2 of Article 9 of the Regulation and which cannot be based on the derogations in paragraph 6, necessitate an authorisation from the EDPS under Article 9(7) of the Regulation.

(6) The reporting of cases of certain diseases to the WHO under the IHR aims to promote global public health by preventing, protecting against, controlling and responding to the international spread of disease. Under its founding Regulation, ECDC shall among other tasks 'provide timely information to [...] international organisations active within the field of public health'[6]. The announced transfers also aim at easing reporting burdens on Member States by forwarding to the WHO those notifications sent to ECDC that Member States are also obliged under the IHR to send to the WHO.

(7) With a view to guaranteeing protection of personal data transferred to the WHO, ECDC has negotiated a set of data protection clauses for the transfer of personal data to the WHO in this context. These clauses notably contain a strong commitment from the WHO not to try to re-identify data subjects. They also contain rules on purpose limitation, information security and onward transfers. The IHR also contain rules on data subjects' access rights vis-à-vis WHO.

(8) As the transfer of personal data from ECDC to the WHO qualifies as structural, using the public interest derogation in Article 9(6)(d) of the Regulation would not be appropriate.

(9) In line with the EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies[7], transfers for which the safeguards are adduced in non-binding instruments, such as the one negotiated between ECDC and the WHO, require authorisation by the EDPS under Article 9(7) of the Regulation.

(10) ECDC has provided the EDPS with a draft set of data protection clauses negotiated with the WHO.

HAS ADOPTED THIS DECISION:

Article 1

For the purposes of the present Decision:

(a) **EDPS** shall mean the European Data Protection Supervisor;

(b) **ECDC** shall mean the European Centre for Disease Control, established by Regulation (EC) No 851/2004[8];

(c) **WHO** shall mean the World Health Organization;

(d) **IHR** shall mean the International Health Regulations;

---

[6] Article 3(2)(c) of Regulation (EC) No 851/2004.

[7] EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies, 14.07.2014, available on the EDPS website at https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf.

[8] OJ L 142, 30.4.2004, p. 1-11.

(e) **Notifications** shall mean those reports sent to ECDC under Decision No 1083/2013/EU which Member States also have to notify to the WHO under the IHR;

(f) **Data protection clauses** shall mean the clauses negotiated between ECDC and the WHO and provided to the EDPS;

Article 2

1. Subject to the conditions laid down in Articles 3 and 4 below, the EDPS takes note that ECDC has provided sufficient safeguards in respect of transfers of personal data contained in the notifications from ECDC to the WHO.

2. Transfers of personal data from ECDC to the WHO within the meaning of paragraph 1 are therefore authorised.

Article 3

ECDC shall enter into an arrangement with the WHO based on the Data protection clauses notified to the EDPS and annexed to this Decision.

Article 4

ECDC shall issue detailed instructions setting out the specific implementing rules concerning the transfers addressed in this Decision, with particular regard to the safeguards aimed at ensuring respect for the principles of necessity, proportionality and data quality in the processing of personal data.

Article 5

The EDPS may exercise the existing powers conferred under Article 47 of the Regulation, and in particular the power to impose a temporary or definitive ban of the transfers addressed by this Decision. Such powers may be exercised in particular where:

(a) the EDPS or another competent data protection authority or court has determined that ECDC or the WHO 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 by the present Decision are not complied with.

Article 6

ECDC shall report on the implementation of this Decision on a regular basis, at least once a year.

Article 7

ECDC shall take all the measures to comply with this Decision and submit the first report to the EDPS in this regard within three months of the adoption of this Decision.

Article 8

This Decision is addressed to ECDC.

Done at Brussels, 17 January 2018

Wojciech Rafał WIEWIÓROWSKI
Assistant European Data Protection Supervisor

Annex: Data protection clauses for arrangement between ECDC and WHO

[DRAFT for signature by ECDC and WHO]

The data protection clauses

Definitions

For the purposes of the Clauses:

(a) *'personal data'* means any information relating to an identified or identifiable natural person hereinafter referred to as '*data subject*'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

(b) *'special categories of data'* means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life;

(c) *'process/processing'*, means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(d) *'controller'*, means the organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data;

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

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

(g) *"the ECDC"* shall mean the controller who transfers the personal data received from EU and WHO Member States in relation to HIV/AIDS, measles, rubella and influenza which are collected by the ECDC on behalf of ECDC and WHO in the European Surveillance System (TESSy) ;

(h) *"the WHO"* shall mean the controller who agrees to receive from the ECDC the personal data received from EU and WHO Member States in relation to HIV/AIDS, measles,

rubella and influenza which are collected by ECDC on behalf of ECDC and WHO in TESSy, for further processing in accordance with the terms of these clauses;

(i) *"the clauses"* shall mean these contractual clauses.

I. Obligations of the ECDC

The ECDC warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the ECDC.

b) It has instructed and throughout the duration of the personal data transfers under these clauses will instruct WHO to process the personal data transferred in accordance with these clauses.

c) It has informed the data subject through a privacy statement on its website that this data will be transmitted to the WHO, and may be further transferred to their member organizations. Data subjects have the right to contact the ECDC to oppose such further transfers by the WHO of their personal data. Upon receipt of such a request ECDC shall liaise with the WHO and request the WHO to take the action necessary to stop the further transfer.

d) It has used reasonable efforts to determine that WHO is able to satisfy its legal obligations under these clauses.

e) The ECDC shall inform the European Data Protection Supervisor, hereinafter referred to as the EDPS, and data subjects enquiring on the processing of personal data by WHO that the WHO information is privileged under the Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations and request the EDPS and data subjects to redirect any enquiries to WHO, which only WHO is entitled to respond based on the policies, rules and procedures of WHO. Responses shall be provided within three (3) months of receipt of the relevant query. For the avoidance of doubt, ECDC remains accountable to the EDPS for its own personal data processing operations, in accordance with applicable data protection law.

f) The ECDC will respond to queries from the EDPS and data subjects concerning the data processing operation by the WHO, only provided that parties have agreed that the ECDC will do so.

g) The ECDC shall demonstrate ECDC's compliance with data protection law to the EDPS, upon receipt of request.

II. Obligations of WHO

WHO warrants and undertakes that:

a) It will ensure an appropriate protection of personal data in accordance with its applicable policies, regulations and rules. Any operation performed upon personal data, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure, erasure or destruction_be based on the policies, rules and procedures of WHO and shall only be done as far as it is necessary for the performance of the mandate of WHO. Under no circumstances will WHO attempt to re-identify data subjects;

b) It will comply with the Data Protection Principles attached in the Annex attached;

c) It will have in place appropriate technical and organisational security measures concerning the risks inherent in any such operation and the nature of the information relating to the data subject concerned, in order to :

   i. protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;

   ii. prevent any unauthorized person from gaining access to computer systems performing such operations, and especially unauthorized reading, copying, alteration or removal of storage media; this includes unauthorized data input as well as any unauthorized disclosure, alteration or erasure of stored information;

   iii. ensure that authorized users of the WHO IT systems performing such operations can access only the information to which their access right refers.

   iv. provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

d) It will regularly refine and update the design of its organizational structure in such a way that it meets the requirements of these clauses.

e) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors and Member States , will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of WHO, including a data processor, and Member State to whom the personal data may be transferred, shall not attempt to re-identify data subjects and be obligated to process the personal data only on instructions from WHO and in compliance with the data protection principles in the annex.

f) Upon reasonable request of ECDC, the WHO will where possible, undertake an internal audit of its technical and security organizational measures to ascertain compliance with the warranties and undertakings in these clauses and provide ECDC with a report of this independent assessment. Such audit shall be conducted in accordance with WHO applicable policies, regulations and rules, in particular in accordance with the Single Audit Principle of the United Nations System which provides that WHO may only be audited by its internal and external auditors appointed by WHO Member States through the World Health Assembly.

g) WHO warrants that TESSy data will be solely used to allow tasks covered by the competence and mandate of WHO to be carried out. Upon reasonable request of ECDC, WHO will - where possible and no more than once a year - provide ECDC with a summary of the tasks carried out with the data.

h) WHO shall publish a Privacy Statement on its website for the purposes of informing data subjects about the processing of their personal data.

III. Liability and data subject rights

a) Each party shall be responsible to the other party, or a data subject, for any established liability caused by any breach of these clauses. Liability is limited to direct damage suffered and within the limits of any insurance in place. Damages of an indirect or punitive character (i.e. damages intended to punish a party for its conduct) are specifically excluded. This does not affect the liability of the ECDC under its data protection law.

b) In cases involving allegations of breach by WHO, any liability will be considered by WHO on a case-by-case basis and subject to its privileges and immunities. Any dispute in this regard between the parties, or between a data subject and WHO, will be solved through the resolution dispute mechanism set forth in clause IV.

IV. Resolution of disputes

a) Any matter relating to the interpretation of these clauses which is not covered by its terms shall be resolved by reference to applicable EU Data Protection law.

b) In the event of a dispute or claim brought by a data subject concerning the processing of his/her personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them through negotiation or any other peaceful and amicable means, including non-binding mediation or conciliation to the exclusion of any other judicial means. Both ECDC and WHO will endeavour to initiate promptly their respective review process and settle any such dispute or claim without undue delay. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means).

c) In the event that all efforts set out in IV. (b) fail, ECDC shall bear responsibility in accordance with Article 32 of Regulation (EC) No 45/2001 for any damage suffered by the data subject as a result of a violation of these clauses. Subject to clause III above, such responsibility covers damages resulting from violations committed by WHO in the unlikely event that the data subject was not able to obtain redress directly from WHO. ECDC shall always consult WHO before settling any disputes or claims with a data subject resulting from alleged violations of these clauses by WHO and shall not make any representation or commitment for or on behalf of WHO. WHO shall have the right to participate in the defense or settlement by ECDC of any such claim or dispute, subject always to its privileges and

immunities, or any matter relating thereto, and any settlement, including awarding damages to a data subject on account of alleged breach of these clauses by WHO, is subject to WHO's express written approval.

d) In addition, any dispute relating to the interpretation or application of these clauses between the ECDC and WHO, or concerning any alleged breach of any provision of these clauses, shall, unless amicably settled, be subject to conciliation. In the event of failure of the latter, the dispute shall be settled by arbitration. The arbitration shall be conducted in accordance with the modalities to be agreed upon by the parties or, in the absence of agreement, with the rules of arbitration of the International Chamber of Commerce. The parties shall accept the arbitral award as final.

V. Suspension and Termination

a) In the event that either party fails to respect its undertakings under these clauses, the other party may temporarily suspend the transfer of personal data following receipt of written notification from the other party until such breach is repaired, or as a result of agreement between parties to do so. Such suspension does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred. Any such suspension shall be reviewed within a reasonable period of time, in order to determine appropriate action to take next, including the possibility of termination of the clauses.

b) The parties agree that the clauses may be terminated following receipt of written notification from one party to another, or as a result of agreement between parties to do so. The parties agree that the termination of the clauses at any time, in any circumstances and for whatever reasons does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VI. Variation of these clauses

The parties may only modify these clauses upon mutual written agreement.

VII. Privileges and Immunities of WHO

Nothing in or relating to these clauses shall be deemed a waiver of any of the privileges and immunities of WHO in conformity with the Convention on the Privileges and Immunities of the Specialized Agencies approved by the General Assembly of the United Nations on November 21, 1947 or otherwise under any national or international law, convention or agreement

VIII. Contact persons for communications

For the purposes of the Clauses, the contact for communications shall be:

For ECDC:

For WHO: [redacted]

FOR WHO	FOR ECDC
Signed:	Signed:
Name:	Name:
Date:	Date:
Location:	Location:

APPENDIX

DATA PROCESSING PRINCIPLES

1. Purpose Limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in the preceding clauses or as subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant, and not excessive in relation to the purposes for which they were transferred and further processed. The data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or further processed.

3. Transparency: ECDC shall provide data subjects with specified information as required by the data protection laws applicable to ECDC, specifically Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

4. Security and confidentiality: Technical and organisational security measures shall be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, shall not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: ECDC shall ensure that data subjects shall have access to their personal data and shall be able to have the personal data about them rectified, blocked or erased in accordance with the data protection laws applicable to ECDC, specifically Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. A data subject may also raise an objection with ECDC to the processing of personal data relating to him/her if there are compelling legitimate grounds relating to the situation. The burden of proof for any refusal rests on ECDC, and the data subject may always challenge a refusal before the EDPS. In the event that ECDC is required by a data subject to have access to their personal data and have them rectified, blocked or erases in accordance with Regulation (EC) No 45/2001, ECDC shall immediately notify WHO thereof in writing. The WHO undertakes to assist ECDC with the resolution of any such data subject rights, should it be possible and reasonable to do so, and always in accordance with these clauses, Article 45 of the International Health Regulations 2005 and subject to its privileges and immunities. Furthermore, the WHO shall as far as practicable provide an individual with his or her personal data in an intelligible form, without undue delay or expense and, when necessary, allow for correction.