

REGISTER NUMBER: 483

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 17/02/2009

Case number: 2009-137

Institution: European Commission

Legal basis: article 27-5 of the regulation CE 45/2001⁽¹⁾

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN⁽²⁾

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

2) Name and First Name of the Controller:RYAN John-F

3) Title:Head of Unit

4) Directorate, Unit or Service to which the Controller is attached:C.3

5) Directorate General to which the Controller is attached:SANCO

2/ Organisational parts of the institution or body entrusted with the processing of personal data

26) External Company or Directorate General to which the Processor is attached:

25) External Company or Directorate, Unit or Service to which the Processor is attached:

ECDC (European Centre for Disease Prevention and Control)

3/ Name of the processing

EWRS (Early Warning and Response System)

4/ Purpose or purposes of the processing

The purposes of processes are as follows:

- Process 1 aims at compile and updating the list of Members that are allowed to have access to the application (EWRS officially designated contact points in Member States), as a simple 'reader' of the circulated messages or as 'reader and writer'
- Process 2 aims at informing a Member State of the status of one of their citizen or about a foreign traveller within its territory who was found as being at imminent risk of transmitting or acquiring a specific transmissible disease with a view to provide adequate treatment and/or to protect other persons from the infection.
- Process 3 aims at informing other Member States of the occurrence of an event of interest for better understanding the pattern of transmission of such disease in general.
- Process 4 aims to inform a Member State of the possible place of stay of the infected person in order to contact him/her; the purpose of the process 2 may apply.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Process 1: EWRS contact points in Member States who have the right to access the EWRS application. The information is provided by the national public health authority in Member States to the Permanent Representation in Brussels.

Process 2: The personal data concerning a person (or a list of persons) in immediate danger is processed by the EWRS national contact point having collected the information as part of the assessment of a given event.

Process 3: The information that could be considered as indirectly personal results from the notification from an EWRS national contact point to other EWRS users of the occurrence of an event affecting a person in a given area and who is at potential risk of further spread to persons in other Member States.

Process 4: EWRS contact points may exchange between themselves, the Commission and ECDC information on eventual close relations or visited persons related to the infected person.

16) Category(ies) of Data Subjects:

Same answers as in 14)

6/ Description of the data or categories of data (including, if applicable, special categories of data (article 10) and/or origin of data)(including, if applicable, special categories of data (article 10) and/or origin of data)

17) Data field(s) of Data Subjects:

Attention: Please indicate and describe in the answer to this question also data fields which fall under article 10

Refer to fields mentioned in section 14).

Under process 1: name and surname, organisation, email, land telephone, mobile telephone and fax number as well as postal address and country.

Process 2 includes information falling under article 10. This information is provided by the notifying Member States as free text, not in structured fields. The nature of the information depends greatly on what identifier was available at the time of the detection of the risk for this person.

Process 3 also includes information falling under article 10 (health) - it is the notification of a public health event in a determined geographical area.

Process 2 and 4 include accordingly information as provided for in section 14).

18) Category(ies) of data fields of Data Subjects:

Attention: Please indicate and describe in the answer to this question also categories of data fields which fall under article 10

Free text reporting under process 2 and 3 are referring to the subject health condition as the main objective of the processing is to contact the subject and to protect him/her from the imminent health risk.

Free text reporting under process 4 may include also information on close relations or visited persons in relation to infected persons as the main objective of the processing is to contact the subject and to protect him/her from the imminent health risk."

7/ Information to be given to data subjects

15a) Which kind of communication(s) have you foreseen to inform the Data Subjects as described in articles 11 - 12 under 'Information to be given to the Data Subject'

Under process 1, a Privacy Statement is provided in order to inform the subject concerned (see attachment 1).

Under processes 2, 3 and 4, a specific template is provided to the subject to inform him/her on an 'ad hoc' basis (see attachment 2).

8/ Procedures to grant rights of data subjects (rights of access, to rectify, to block, to erase, to object)(*rights of access, to rectify, to block, to erase, to object*)

15b) Which procedure(s) did you put in place to enable Data Subjects to exert their rights: access, verify, correct, etc., their Personal Data as described in articles 13 - 19 under 'Rights of the Data Subject' :

Under process 1, a Privacy Statement is provided in order to inform the subject concerned (see attachment 1).

Under processes 2, 3 and 4, a specific template is provided to the subject to inform him/her on an 'ad hoc' basis (see attachment 2).

9/ Automated / Manual processing operation

7) Description of Processing:

Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

Collection, recording, storage of data concerning Institutions and persons formally appointed by national authorities to plan and respond to events of Community relevance caused by communicable diseases through an informatics application called 'Early Warning and Response System (EWRS)', under Decision 2119/98/EC of the Council and Parliament and under Commission Decision 2000/57/EC establishing the above mentioned Early Warning and Response System.

Collection, recording, storage of data concerning events to be notified under Decision 2119/98/EC of the Council and Parliament and under Commission Decision 2000/57/EC establishing the above mentioned Early Warning and Response System and which concern incidents and events of Community relevance caused by communicable diseases.

Data and information processed correspond to what is defined under Article 27, Paragraph 2 (a). In particular data relating to health are routinely processed.

This health data may include personal data related to persons who are or may have been infected in order to treat them and to prevent the transmission of serious communicable diseases to others. This process falls under Article 27.2. It may also concern information on their close relations or on visited persons in order to contact them.

8) Automated Processing operation(s):

There is no automated processing of the data.

9) Manual Processing operation(s):

All processes are manual.

Under process 1 in the description of processing, the Member State informs the Commission of the contact details of a Member. The Commission forwards this information to the European Centre for Disease Prevention and Control (ECDC) for updating the database of contacts.

Under processes 2, 3 and 4, the notifying Member State posts manually a message on the EWRS server.

10/ Storage media of data

The application is a standard 2-tier web application with front end / application server combination connected to a Storage Area Network for bulk data storage and connection to a database server. The database server is connected itself to the Storage area network.

The external secured access is limited to the web service. All other connections to the SAN and the SQL server are disconnected from the internet. The storage area network stores the data on high available disks with backup on tape. The application is mirrored to a geographical remote application service provider. The duplicated application architecture is equal to the ECDC site.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

1. Treaty establishing the European Community, in particular Articles 3(1), 95(3) and 152.
2. Decision No 2119/98/EC of the European Parliament and of the Council of 24 September 1998 setting up a network for the epidemiological surveillance and control of communicable diseases in the Community, in particular Articles 4 and 6 (OJ L 268, 3.10.1998, p.1), in attachment.
3. Commission Decision of 22 December 1999 on the early warning and response system for the prevention and control of the communicable diseases under Decision No 2119/98/EC of the European Parliament and of the Council (OJ L 21, 26.1.2000, p.32), in attachment.
4. Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control, in particular Articles 4b and 8 (OJ L 142, 30.04.2004, p.1).
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0851:EN:HTML>
5. Commission Decision amending Decision No 2000/57/EC on early warning and response system for the prevention and control of communicable diseases under Decision No 2119/98/EC of the European Parliament and of the Council (pending - for adoption I quarter 2009).

12) Lawfulness of Processing:

Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The lawfulness rests on Articles 5(a) of Regulation 45/2001 ? processing for the performance of a task carried out in the public interest?.or in the legitimate exercise of official authority vested in the Community institution or body ? 5(b) of Regulation 45/2001 - processing is necessary for compliance with a legal obligation to which the data controller is subject ? and 5(e) of Regulation 45/2001 - processing is necessary in order to protect the vital interests of the data subject.

The processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

12/ The recipients or categories of recipient to whom the data might be disclosed

20) Recipient(s) of the Processing:

Officials in the Member States, EEA countries and Candidate Countries, in DG SANCO, DG TREN and potentially other DGs and services, in EFSA, ECDC and WHO

The controller (DG SANCO) and processor (ECDC) can access all information in the system. The WHO can access information in relation to processes 2 and 3 if the sender of the message did not oppose to make readable the message to WHO.

21) Category(ies) of recipients:

Same as in paragraph 20)

13/ retention policy of (categories of) personal data

The storage of personal data in case of a person who has been infected either if sick or not (process 2-4) is limited to 1 year.

Concerning the personal data of the EWRS competent authorities in Member States, personal data are kept as long as follow-up actions to the relevant EWRS contact points network are necessary.

13 a/ time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject) (Please, specify the time limits for every category, if applicable)
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

22 b) Time limit to block/erase data on justified legitimate request from the data subjects

On justified legitimate request from the data subject, data will be erased within 5 days.

14/ Historical, statistical or scientific purposes

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

22 c) Historical, statistical or scientific purposes - If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification

For statistical purposes the data will be kept anonymously

Data regarding process 2 and 4 are important to be kept to document that all attempts have been made to contact a subject at imminent health risk, and that information remain available as the situation may unfold and new developments, new treatments, or new information in the future may be beneficial to the subject.

15/ Proposed transfers of data to third countries or international organisations

27) Legal foundation of transfer:

Only transfers to third party countries not subject to Directive 95/46/EC (Article 9) should be considered for this question. Please treat transfers to other community institutions and bodies and to member states under question 20.

Data are transferred to WHO (World Health Organization) in compliance with Article 45 of the International Health Regulations (IHR 2005).

<http://www.who.int/csr/ihr/en/>

International Health Regulations (IHR 2005)

Article 45 Treatment of personal data

1. Health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.

2. Notwithstanding paragraph 1, States Parties may disclose and process personal data where essential for the purposes of assessing and managing a public health risk, but State Parties, in accordance with national law, and WHO must ensure that the personal data are:

(a) processed fairly and lawfully, and not further processed in a way incompatible with that purpose;

(b) adequate, relevant and not excessive in relation to that purpose;

(c) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified; and

(d) not kept longer than necessary.

3. Upon request, WHO shall as far as practicable provide an individual with his or her personal data referred to in this Article in an intelligible form, without undue delay or expense and, when necessary, allow for correction.

28) Category(ies) of Personal Data or Personal Data to be transferred:

Data in Processes 2 and 4 may be transferred.

16/ The processing operation presents specific risk which justifies prior checking (please describe): (*please describe*):

7) Description of Processing:

Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

Collection, recording, storage of data concerning Institutions and persons formally appointed by national authorities to plan and respond to events of Community relevance caused by communicable diseases through an informatics application called 'Early Warning and Response System (EWRS)', under Decision 2119/98/EC of the Council and Parliament and under Commission Decision 2000/57/EC establishing the above mentioned Early Warning and Response System.

Collection, recording, storage of data concerning events to be notified under Decision 2119/98/EC of the Council and Parliament and under Commission Decision 2000/57/EC establishing the above mentioned Early Warning and Response System and which concern incidents and events of Community relevance caused by communicable diseases.

Data and information processed correspond to what is defined under Article 27, Paragraph 2 (a). In particular data relating to health are routinely processed.

This health data may include personal data related to persons who are or may have been infected in order to treat them and to prevent the transmission of serious communicable diseases to others. This process falls under Article 27.2. It may also concern information on their close relations or on visited persons in order to contact them.

12) Lawfulness of Processing:

Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The lawfulness rests on Articles 5(a) of Regulation 45/2001 ? processing for the performance of a task carried out in the public interest?.or in the legitimate exercise of official authority vested in the Community institution or body ? 5(b) of Regulation 45/2001 - processing is necessary for compliance with a legal obligation to which the data controller is subject ? and 5(e) of Regulation 45/2001 - processing is necessary in order to protect the vital interests of the data subject.

The processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

Article 27.2.(a) Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Article 27.2.(a) Processing of data relating to health

Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject,

n/a

Article 27.2.(c) Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

n/a

Article 27.2.(d) Processing operations for the purpose of excluding individuals from a right, benefit or contract,

n/a

Other (general concept in Article 27.1)

n/a

17/ Comments

1) Date of submission:

10) Comments if applicable:

36) Do you publish / distribute / give access to one or more printed and/or electronic directories?

Personal Data contained in printed and/or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

If Yes, please explain what is applicable.

no

37) Complementary information to the different questions if applicable, including attachments to this notification which should not be public :

Detailed information concerning 14) Data subjects is attached (EWRS - Persons concerned by the processing).

Detailed information concerning 32) Security measures is attached (EWRS - Security : organisational measures).

ECDC is the operator of the application.

Full geographical redundancy is ensured with an external hosting provider : Steria.

A contract has been signed including provisions related to security, confidentiality and data protection.

PLACE AND DATE:18/02/2009

DATA PROTECTION OFFICER: Administrator

INSTITUTION OR BODY:European Commission