RECOMMENDATIONS

COMMISSION RECOMMENDATION

of 6 February 2012

on data protection guidelines for the Early Warning and Response System (EWRS)

(notified under document C(2012) 568)

(Text with EEA relevance)

(2012/73/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) 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 [1] established a network for the epidemiological surveillance and control of communicable diseases in the Community and an early warning and response system (hereinafter, the 'EWRS') for the prevention and control of these diseases.

(2) In its Decision 2000/57/EC of 22 December 1999 on the 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 [2] the Commission adopted implementing provisions on the EWRS, whose aim is to bring into structured and permanent communication with one another, through appropriate means, the Commission and the competent public health authorities responsible in Member States of the European Economic Area for determining the measures which may be required to protect public health and to prevent and halt the spread of communicable diseases [3].

(3) The right to personal data protection is recognised by the Charter of Fundamental Rights of the European Union, in particular in Article 8 thereof.

(4) Moreover, the exchange of information by electronic means between the Member States, and between the Member States and the Commission, must comply with the rules on the protection of personal data laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [4], and in Regulation (EC) No 45/2001 of the European Parliament and of 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 [5].

(5) Commission Decision 2009/547/EC of 10 July 2009 amending Decision 2000/57/EC on the 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 [6] introduced specific safeguards for the exchange of personal data between Member States in the course of contact tracing procedures for the identification of infected persons and of persons potentially in danger, in the occurrence of an event related to communicable diseases having a potential EU dimension.

(6) On 26 April 2010, the European Data Protection Supervisor (hereinafter referred to as the 'EDPS') issued a Prior Checking Opinion [7] where it called for a clarification of the responsibilities of the various actors

[1] OJ L 268, 3.10.1998, p. 1.
[2] OJ L 21, 26.1.2000, p. 32.
[3] The EWRS is reserved to the reporting, by the competent public health authorities of the Member States, of specified threats to public health ('events') as defined in Annex I to Decision 2000/57/EC cited.
[4] OJ L 281, 23.11.1995, p. 31.
[5] OJ L 8, 12.1.2001, p. 1.
[6] OJ L 181, 14.7.2009, p. 57.
[7] Prior Checking Opinion of 26 April 2010 of the European Data Protection Supervisor on the Early Warning and Response System notified by the European Commission on 18 February 2009 (case C 2009-0137). The Opinion is published on the EDPS website at the following address: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_EN.pdf

involved in the EWRS, and for properly addressing the potential risks posed to fundamental rights by the processing of contact tracing data on a larger scale, in the event of major pandemic health threats occurring in the future.

(7) Taking into account the recommendations made by the EDPS in its Opinion, the Commission has developed a set of data protection guidelines for the EWRS, which should help to clarify the respective roles, tasks and obligations of the various actors of the system and in that way guarantee effective compliance with the abovementioned data protection rules and ensure the provision of clear information and easily available mechanisms for data subjects to assert their rights,

HAS ADOPTED THIS RECOMMENDATION:

1. Member States should draw the attention of users of the EWRS on the guidelines in the Annex to this Recommendation.

2. EWRS national competent authorities should be encouraged to make contacts with their national Data Protection Authorities for guidance and assistance on the best way to implement these guidelines under national law.

3. Member States are recommended to provide feedback to the European Commission on the implementation of the guidelines in the Annex, not later than 2 years after the adoption of this Recommendation. This feedback will be shared with the EDPS and will be taken into account by the Commission to assess the level of data protection in the EWRS as well as the content and timeliness of any future measures, including the possible adoption of a legal instrument.

4. This Recommendation is addressed to the Member States.

Done at Brussels, 6 February 2012.

For the Commission

John DALLI

Member of the Commission

ANNEX

DATA PROTECTION GUIDELINES FOR THE EARLY WARNING AND RESPONSE SYSTEM (EWRS)

1. INTRODUCTION

The EWRS is a web-based application designed by the European Commission, in cooperation with the Member States, with the aim to bring into structured and permanent communication with one another the Commission and the competent public health authorities responsible in EEA Member States for determining the measures required to protect public health. The European Centre for Disease Prevention and Control (hereinafter, the 'ECDC'), an EU agency, is also connected to the EWRS since 2005 ([1]).

Cooperation between national health authorities is vital for enhancing Member States's capacity to prevent the potential spread of communicable diseases within the EU, as well as their readiness to respond in a coordinated and timely manner to events caused by communicable diseases which are, or have the potential to become, public health threats.

Previous outbreaks of SARS, Pandemic Influenza A(H1N1) and other communicable diseases have clearly demonstrated how previously unknown diseases may spread rapidly, causing high mortality and morbidity. Fast travel and global trade facilitate the transmission of communicable diseases, which do not recognise borders. Early detection and efficient communication and coordination at the European and international level are essential to control such contingencies and to prevent seriously prejudicial developments.

The EWRS has been designed as a centralised mechanism to enable Member States to send alerts, share information and coordinate their response, in a timely and secure manner, in relation to events posing a potential health threat on the EU.

2. SCOPE AND OBJECTIVES OF THE GUIDELINES

The management and use of the EWRS may involve the exchange of personal data in specific cases where the relevant legal instruments so provide (see Section 4 on the legal grounds for the exchange of personal information in the EWRS).

Personal information exchanges between the competent health authorities in the Member States must comply with the rules on personal data protection laid down in the national laws transposing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

However, since EWRS users are not data protection experts and may not always be sufficiently aware of data protection requirements imposed by law, it is advisable to provide EWRS users with guidelines in which the functioning of the EWRS from a data protection perspective is explained in a user-friendly and easily understandable manner. The guidelines also aim to raise awareness and promote best practices and a consistent and uniform approach to data protection compliance among EWRS users in the Member States.

However, it should be noted that these guidelines are not intended to provide a comprehensive review of all data protection issues in connection with the EWRS. Further guidance and assistance may be obtained from the data protection authorities (hereinafter 'DPAs') in the Member States. In particular, EWRS users are strongly encouraged to seek advice from their respective DPAs on the best way to implement these guidelines at the national level, so as to ensure that the country-specific data protection requirements are fully complied with. A list of DPAs and their contact details can be found at the following address:

http://ec.europa.eu/justice/policies/privacy/nationalcomm/index_en.htm

Finally it has to be stressed that these guidelines are not an authentic interpretation of EU Law on data protection as in the institutional system of the Union the task to interpret EU law is exclusively conferred to the Court of justice.

3. APPLICABLE LAW AND SUPERVISION

Determination of the applicable law depends on who the EWRS user is. In particular, the processing of personal data by the Commission and the ECDC within the framework of the system management and operation (to the extent illustrated in the following sections) is governed by Regulation (EC) No 45/2001.

([1]) The ECDC also supports and assists the Commission in the operation of the EWRS application. This task was assigned to the ECDC by 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 and in particular Article 8 thereof (OJ L 142, 30.4.2004, p. 1).

As regards the processing of personal data by EWRS national competent authorities, the applicable law is the relevant national data protection legislation transposing Directive 95/46/EC. It should be noted that this Directive leaves a certain margin of manoeuvre to the Member States to transpose its provisions into national law. In particular, the Directive allows Member States to introduce exemptions or derogations to a number of its provisions in specific cases. At the same time, the national data protection law to which the EWRS user is subject may set out more stringent or country-specific data protection requirements not foreseen by the laws of other Member States.

In consideration of these peculiarities, EWRS users are advised to discuss these guidelines with their respective DPAs to ensure that all requirements posed by the applicable national laws are met. For instance, the detail of information to be provided to data subjects at the time of data collection may differ significantly from one Member State to another, as well as the rules for the processing of special categories of personal data (e.g. health data) of individuals.

One of the main features of the EU data protection legal framework consisting of Regulation (EC) No 45/2001 and Directive 95/46/EC is its supervision by public, independent data protection authorities. The processing of personal data by EU institutions and bodies is supervised by the European Data Protection Supervisor (hereinafter referred to as the 'EDPS') ([1]), whereas the processing by natural or legal persons, national public authorities, agencies or other bodies in the Member States is supervised by their respective DPAs. Supervisory authorities have been empowered in all Member States to hear claims lodged by citizens concerning the protection of their rights and freedoms in regard to the processing of personal data. For more detailed information on how to deal with data subjects' requests or complaints, EWRS users are invited to refer to Section 9 on access to personal data and other rights of data subjects.

4. LEGAL GROUNDS FOR THE EXCHANGE OF PERSONAL INFORMATION IN THE EWRS

Decision No 2119/98/EC established the setting up of a network at EU level (hereinafter, the 'Network') to promote cooperation and coordination between the Member States, with the assistance of the Commission, with a view to improving the prevention and control of communicable diseases in the EU ([2]). Within this framework, the EWRS was set up as one of the pillars of the Network, allowing for the exchange of information, consultation and coordination at the European level in the occurrence of events caused by communicable diseases having the potential to endanger public health in the EU.

It should be noted that not all information exchanged within the EWRS is of a personal nature. Actually, in general, no health-related or other personal data of identified or identifiable natural persons is exchanged in this framework.

What is 'personal data'?

For the purposes of Directive 95/46/EC and Regulation (EC) No 45/2001, personal data shall mean any information relating to an identified or identifiable natural person ('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 physical, physiological, mental, economic, cultural or social identity ([3]).

The competent health authorities in EEA Member States mostly communicate to the Network, through the EWRS, information regarding — inter alia — the appearance or resurgence of cases of communicable diseases, together with information on control measures applied, or information on unusual epidemic phenomena or new communicable diseases of unknown origin ([4]), which may require timely and coordinated action by the Member States to contain the risk of propagation within the EU ([5]). On the basis of the information available through the Network, Member States will consult each other in liaison with the Commission with a view to coordinating their efforts for the prevention and control of those diseases, including with regard to the measures they have adopted or intend to adopt at national level ([6]).

However, in some cases, the information exchanged through the system does actually concern individuals and can be considered personal data.

First of all, the processing of a limited amount of personal data of EWRS authorised users is inherent in the system management and operation. Indeed, processing of the users' contact details (name, organisation, e-mail address, telephone number, etc.) is essential in order to set up and run the system. These personal data are collected by the Member States, and further processed under the Commission's responsibility, solely for the purposes of cooperating effectively on the management of the EWRS and the underlying Network.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS
([2]) The categories of communicable diseases covered by the Network are limited to those listed in the Annex to Decision No 2119/98/EC.
([3]) Article 2(a) of Directive 95/46/EC and Article 2(a) of Regulation (EC) No 45/2001.
([4]) Article 4 of Decision No 2119/98/EC.
([5]) Annex I to Decision 2000/57/EC on the definition of 'events' to be reported within the EWRS.
([6]) Article 6 of Decision No 2119/98/EC.

More importantly, the occurrence of an event related to communicable diseases with a potential EU dimension may require the implementation of particular control measures, the so called 'contact tracing' measures, by the affected Member States in collaboration with each other, in order to identify infected persons and persons potentially in danger and to prevent the transmission of serious communicable diseases. Such collaboration may involve the exchange through the EWRS of personal data, including sensitive health data, of confirmed or suspected human cases between the Member States directly concerned by the contact tracing measures ([1]).

What is 'processing of personal data'?

For the purposes of Directive 95/46/EC and Regulation (EC) No 45/2001, processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ([2]).

In the abovementioned cases, the processing of personal data within the EWRS must be justified on the basis of specific legal grounds. In this regard, Article 7 of Directive 95/46/EC, and the corresponding provisions of Article 5 of Regulation (EC) No 45/2001, set out the criteria for making data processing legitimate.

With regard to the contact details of EWRS users, processing of these data is based on:

— Article 5(b) of Regulation (EC) No 45/2001: 'processing is necessary for compliance with a legal obligation to which the controller ([3]) is subject'. The processing is necessary for the management and operation of the EWRS by the Commission, with support from the ECDC, and

— Article 5(d) of Regulation (EC) No 45/2001: 'the data subject has unambiguously given his or her consent'. Contact details of users are obtained from the data subjects themselves, after having put them in the conditions to signify an informed agreement to their personal data being processed within the EWRS (see Section 8 on the provision of information to data subjects).

The criteria laid down in Article 7(c), (d), and (e) of Directive 95/46/EC are the most relevant for the exchange of contact tracing data (e.g. contact details of the infected person, conveyance and other data related to the person's travel itinerary and places of stay, information on visited persons and persons potentially exposed to contamination) of individuals within the EWRS ([4]):

— Article 7(c) of Directive 95/46/EC: 'processing is necessary for compliance with a legal obligation to which the controller is subject'. The establishment of an early warning and response system for the prevention and control of communicable diseases in the EU is required by Decision No 2119/98/EC. This Decision poses an obligation on the Member States to report through the EWRS certain events caused by communicable diseases which are, or have the potential to become, public health threats ([5]). The reporting obligation covers also the measures taken by the competent authorities in the concerned Member States to prevent and halt the spread of those diseases, including the contact tracing measures implemented to trace infected persons or those who are potentially in danger of being infected ([6]),

— Article 7(d) of Directive 95/46/EC: 'processing is necessary in order to protect the vital interests of the data subject'. In principle, the exchange between the concerned Member States of personal data of infected individuals, and of individuals who are in imminent danger of being infected, is necessary to provide them with the appropriate care or treatment, as well as to permit tracing and identification for isolation and quarantine purposes, with the aim of protecting the health of the concerned individuals and, ultimately, that of EU citizens at large,

— and Article 7(e) of Directive 95/46/EC: 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'. The EWRS is a tool designed to help Member States to coordinate their efforts for the prevention and control of serious communicable diseases within the EU. Therefore, the system is conceived to serve the performance of a public interest task vested in the Member States to protect public health.

([1]) Clarification on the legitimate purposes for processing personal data within the EWRS to include 'contact tracing' data was the result of the amendments introduced to Commission Decision 2000/57/EC by Decision 2009/547/EC.
([2]) Article 2(b) of Directive 95/46/EC and Article 2(b) of Regulation (EC) No 45/2001.
([3]) As regards the definition of 'controller' see Section 5 below.
([4]) An indicative list of personal data which may be exchanged for the purposes of contact tracing is annexed to Decision 2009/547/EC.
([5]) Article 1 and Annex I to Decision 2000/57/EC on the definition of 'events' to be reported within the EWRS.
([6]) Article 2a of Decision 2000/57/EC introduced by Decision 2009/547/EC.

The same reasons of public interest may justify the processing by Member States of sensitive health data (e.g. information on the event posing a health threat, data related to the health conditions of the infected persons and of persons potentially exposed to contamination) within the EWRS. Although the processing of data concerning health is prohibited in principle by Article 8(1) of Directive 95/46/EC, the processing of this special category of data within the EWRS is covered by the exemption granted under Article 8(3) of the same Directive in so far as the processing is 'required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy'.

Additional exemptions to the prohibition to process personal health data may be provided, for reasons of substantial public interest and subject to the provision of suitable safeguards, by the national laws of the Member States, or by decision of the national DPAs in the Member States ([1]).

5. WHO IS WHO IN THE EWRS? THE ISSUE OF JOINT CONTROLLERSHIP

The EWRS has been conceived as a multiple user system connecting, through appropriate technical means including different structured communication channels, the designated contact persons from the competent public health authorities in EEA Member States (hereinafter, the 'national EWRS focal points'), the Commission, the ECDC and, to a limited extent, also the WHO.

Each of these EWRS actors is a separate user of the system, although access to the information exchanged within the system has been modulated through the creation of different user profiles and of 'selective' communication channels, which provide for appropriate safeguards to ensure compliance with applicable data protection rules.

In particular, the system consists of two main communication channels. A first channel, the so called 'general messaging' channel, allows the competent health authority in a given Member State to notify all national EWRS focal points, the Commission, the ECDC and the WHO of information concerning events caused by communicable diseases having a potential EU dimension which are covered by the reporting obligations laid down in Decision No 2119/98/EC ([2]).

In general, no health-related or other personal data of identified or identifiable natural persons is communicated through the general messaging channel. Specific safeguards have been introduced into the system to prevent unlawful data processing within this channel (see Section 7).

However, in the occurrence of events caused by communicable diseases with a potential EU dimension, it may be necessary for the affected Member States, in collaboration with each other, to implement particular contact tracing measures with a view to tracing infected persons, and other individuals exposed to contamination, so as to prevent the spread of those serious diseases.

In order to ensure compliance with data protection rules, appropriate safeguards have been introduced to limit the exchange of contact tracing and health data of individuals only to the Member States directly concerned by a given contact tracing procedure, and to exclude the other Member States of the Network, the Commission and the ECDC from accessing these data ([3]).

To this end, the so called 'selective messaging' channel has been built into the EWRS to guarantee an exclusive communication channel between the Member States concerned by a given contact tracing measure.

By exchanging personal information through the selective messaging channel, competent authorities take the role of 'controller' with respect to the processing of these personal data and therefore assume responsibility for the lawfulness of their processing activities and for ensuring compliance with data protection obligations set out in the applicable national laws transposing Directive 95/46/EC.

([1]) As foreseen by Article 8(4) of Directive 95/46/EC.
([2]) Cf., in particular, Articles 4, 5 and 6 thereof.
([3]) Article 2a of Decision 2000/57/EC introduced by Decision 2009/547/EC.

Who is the 'controller'?

For the purposes of Directive 95/46/EC, ' "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data' ([1]).

In principle, users at the Commission and the ECDC do not have access to personal data exchanged through the selective messaging channel ([2]). However, for technical reasons, the central storage of data in the EWRS is the ultimate responsibility of the Commission as the system administrator and coordinator. In this capacity, the Commission is also responsible for the registration, storage and further processing of personal data of the EWRS authorised users necessary to run the system.

The EWRS is therefore a clear example of joint controllership, where the responsibility for ensuring data protection is allocated, at different levels, between the Commission and the Member States. Moreover, since 2005 the Commission and the Member States in their capacity as co-controllers have decided to delegate the daily operation of the EWRS informatics application to the ECDC, which performs this task on behalf of the Commission. Further to this delegation, the agency has assumed the responsibility to ensure, as 'processor', the confidentiality and security of the processing operations carried out within the system, in accordance with the obligations laid down in Articles 21 and 22 of Regulation (EC) No 45/2001.

Who is the 'processor' and what are its obligations?

For the purposes of Regulation (EC) No 45/2001, ' "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller' ([3]).

The Regulation foresees that, where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational measures required for data security purposes. The controller shall be ultimately responsible for ensuring compliance with those measures. Nevertheless, the obligations set out in Articles 21 and 22 of the Regulation with regard to the confidentiality and security of processing are also incumbent on the processor ([4]).

6. APPLICABLE DATA PROTECTION PRINCIPLES

The processing of personal data within the EWRS must comply with a set of data protection principles set out in Regulation (EC) No 45/2001 and Directive 95/46/EC.

In their capacity as controllers, the Commission and the competent authorities in the Member States are responsible for ensuring compliance with these principles each time they process personal data through the EWRS. A selection of core data protection principles is provided hereafter. This is without prejudice to other applicable data protection requirements set out in the relevant legal instruments, for which guidance is given under different sections of the present guidelines. In particular, EWRS users are invited to read carefully Section 8 on the provision of information to data subjects and Section 9 on access and other rights of data subjects.

6.1. *Principles relating to the lawfulness of processing and to purpose limitation*

Controllers should ensure that personal data are processed fairly and lawfully. This principle implies, first of all, that the collection and any further processing of personal data should be based on legitimate grounds provided by law ([5]). Secondly, personal data may be collected only for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with those purposes ([6]).

([1]) Definition laid down in Article 2(d) of Directive 95/46/EC.

([2]) In exceptional circumstances, the Commission may be involved in the exchange of personal data through the EWRS selective channel where this is absolutely necessary to coordinate, or to allow for, the timely and effective implementation of public health measures required under Decision No 2119/98/EC and its implementing rules. In these cases, the Commission will ensure that processing is lawful and that it is carried out in compliance with the provisions of Regulation (EC) No 45/2001.

([3]) Definition laid down in Article 2(e) of Regulation (EC) No 45/2001.

([4]) These principles are embedded in Article 23(1) of Regulation (EC) No 45/2001 on the processing of personal data on behalf of controllers.

([5]) The principle of lawfulness of processing results from the joint provisions of Article 6(1)(a), Article 7 and Article 8 of Directive 95/46/EC. Cf. also the corresponding provisions of Regulation (EC) No 45/2001.

([6]) The principle of purpose limitation is enunciated in Article 6(1)(b) of Directive 95/46/EC and in the corresponding provision of Article 4(1)(b) of Regulation (EC) No 45/2001.

6.2. *Principles on data quality*

Controllers should ensure that personal data are adequate, relevant and not excessive in relation to the purposes for which they are collected. Furthermore, data should be accurate and kept up to date [1].

6.3. *Principles on data retention*

Controllers should ensure that personal data are kept in a form which permits identification of data subjects for no longer than it is necessary in view of the purposes for which the data were collected, or for which they are further processed [2].

6.4. *Principles on confidentiality and data security*

Controllers should ensure that any person having access to personal data and acting under their authority or under the authority of the processor, including the processor himself, do not process these data except on instructions from the controller [3]. Furthermore, controllers are required to implement appropriate technical and organisational measures to protect personal data against accidental, unauthorised or unlawful destruction or loss, alteration, disclosure or access, and against all other unlawful forms of processing [4].

In view of a correct and effective application of the abovementioned principles in the context of their use of the system, EWRS users are recommended in particular that:

In order to make sure that the processing operation has a legal basis, that data are collected for legitimate and explicit purposes and that they are not further processed in a way incompatible with those purposes, each time they collect or otherwise process personal data through the EWRS, EWRS users should:

— assess on a case-by-case basis whether the implementation of coordinated contact tracing measures, and the consequent activation of the EWRS selective channel to exchange related contact tracing and other personal data, is justified in consideration of the nature of the disease and the scientifically proven benefits of contact tracing for preventing or reducing the further spread of the disease, taking into account the risk assessment provided by the health authorities in Member States and by the existing scientific agencies, namely ECDC and WHO,

— not use the general messaging channel to exchange contact tracing and other personal data. They should ensure, in particular, that no such data are included in the body of the general messages they post, in their attachments or in any other form. The use of the general messaging channel for contact tracing purposes would be illegitimate and disproportionate, since it would result in personal data being disclosed to recipients (including the Commission and the ECDC) not concerned by a given contact tracing procedure and which do not need to have access to those data,

— when using the selective functionality, adopt a 'need-to-know' approach and select as recipients of selective messages containing personal data only the competent authorities in the Member States which need to cooperate on a given contact tracing procedure.

EWRS users should be particularly vigilant when exchanging, through the selective messaging channel, sensitive data concerning the health conditions of an identified or identifiable person, e.g. infected or potentially exposed persons whose contact details or other personal information are concomitantly disclosed through the EWRS, so that the person in question may be directly or indirectly identified. In this case, all the abovementioned recommendations continue to apply; additionally, EWRS users should remember that the exchange of sensitive data is permitted under Directive 95/46/EC only in very limited circumstances. In particular [5]:

— the person whose data are being collected has given his or her explicit consent to their processing (Article 8(2)(a) of Directive 95/46/EC). However, the need to timely intervene in situations of sanitary emergency may render it impossible to provide data subjects with all the information required for them to be able to signify an informed consent (see Section 8 on the provision of information to data subjects). Furthermore, the possibility that data may be eventually disclosed through the EWRS is not necessarily known at the time when they are collected,

[1] Article 6(1)(c) and (d) of Directive 95/46/EC and Article 4(1)(c) and (d) of Regulation (EC) No 45/2001.
[2] Article 6(1)(e) of Directive 95/46/EC and Article 4(1)(e) of Regulation (EC) No 45/2001.
[3] The principle of confidentiality is laid down in Article 16 of Directive 95/46/EC and the corresponding provision of Article 21 of Regulation (EC) No 45/2001.
[4] The principle of data security is enunciated in Article 17 of Directive 95/46/EC and the corresponding provision of Article 22 of Regulation (EC) No 45/2001.
[5] For the full list of exemptions to the prohibition to process certain special categories of data, including health data, see Article 8(2), (3), (4), (5) of Directive 95/46/EC.

— failing data subjects' consent, processing of health data may be considered legitimate if it is necessary for the 'purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services', provided that health data are processed by a health professional subject to the obligation of professional secrecy, or by another person also subject to an equivalent obligation (Article 8(3) of Directive 95/46/EC). In other terms, each time they send a selective message containing sensitive health data to recipients in other Member States, EWRS users should assess whether disclosing such data is strictly necessary to allow competent authorities in the concerned Member States to implement specific measures required for one of the abovementioned purposes. EWRS users are also reminded that additional grounds for processing health data may be provided by their respective national laws transposing Directive 95/46/EC, or by decision of their national DPA ([1]).

In order to ensure the quality of personal data they exchange through the system, and in particular, before posting a selective message, EWRS users need to consider whether:

— the personal data they want to exchange are strictly needed to allow an efficient contact tracing procedure. In other terms, the competent authority posting the message should provide the authority(s) in the other concerned Member State(s) only with those personal data which are needed to unambiguously identify the infected or exposed persons. The indicative list of personal data which may be exchanged for contact tracing purposes, annexed to Decision 2009/547/EC, should not be seen as granting a blanket and unconditional authorisation to process these categories of data. At the same time, precaution must be extreme as regards processing of personal data other than those listed in that Annex, as disclosure is likely to be excessive and unreasonable. Instead, a case-by-case assessment should be made of whether inclusion of a certain personal data is strictly necessary for the purposes of a given contact tracing procedure.

Further processing and storage of personal data outside the EWRS:

It is of the utmost importance to note that national data protection laws transposing Directive 95/46/EC also apply to the storage and further processing, outside the EWRS, of personal data obtained through the system. This may occur, for instance, when personal data stored centrally by the system are then stored in the local PCs of users or in databases established at national level; or whether these data are transmitted by the competent authority responsible for their processing within the EWRS to other authorities or to any third parties. In these cases, EWRS users are reminded that:

— the storage and further processing outside the EWRS must not be incompatible with the original purposes for which data were collected and exchanged within the EWRS,

— this further processing must have a legal basis in the relevant national data protection laws; be necessary, adequate, relevant and not excessive in relation to the original purposes of collection in the EWRS,

— data must be kept up to date and deleted once no longer needed for the purposes for which they were further processed,

— when data are extracted from the EWRS and disclosed to third parties, the controller must inform data subjects of this circumstance so as to guarantee fair processing, unless this would be impossible or involve disproportionate effort, or if disclosure is expressly laid down by law (see Article 11(2) of Directive 95/46/EC). Considering that disclosure may be required by the laws of only one of the Member States involved, and therefore may not be widely known elsewhere, efforts should be made to provide information even when the disclosure is expressly laid down by law.

7. A DATA PROTECTION FRIENDLY ENVIRONMENT

Several features have been already built into the EWRS to enhance compliance with data protection principles outlined in Section 6 and to prompt EWRS users to assess data protection aspects each time they use the system. For example:

— a warning is visibly displayed in the EWRS messages overview page, informing users that the general messaging channel is not designed for accommodating contact tracing and other personal data, since use of this channel may result in these data being unnecessarily disclosed to recipients other than those who need to access them,

— access to the information exchanged within the system has been modulated through the creation of different user profiles and of selective communication channels, which provide for appropriate safeguards to ensure compliance with data protection rules,

([1]) Article 8(4) of Directive 95/46/EC.

— in particular, the selective messaging channel of the EWRS provides an exclusive communication channel for the exchange of personal information between the concerned Member States only. A default option has been built into the system which automatically excludes the Commission and the ECDC from the list of possible recipients of selective messages containing personal data [1],

— the system automatically erases all selective messages containing personal information 12 months after the date of posting of the messages (for more details, see Section 11 on data retention),

— a feature has been built into the system to allow users to directly rectify or delete, at any time, those selective messages containing personal information which is inaccurate, not up to date, no longer needed or otherwise not compliant with data protection requirements. The system will automatically notify the other EWRS user(s) involved in that specific selective information exchange that the message has been deleted, or its content rectified, to ensure compliance with data protection rules,

— a specific mechanism has been made available in the selective messaging channel to allow the national authorities concerned by a given information exchange to communicate and cooperate on access, rectification, blocking or deletion requests of data subjects.

Furthermore, in the medium term it is envisaged that the training module available from within the EWRS application will be integrated in order to provide EWRS users with extensive explanations on the functioning of the system from the data protection perspective. The use of the various features and functionalities aimed at enhancing compliance with data protection rules will be illustrated by means of practical examples.

It is the Commission intention to work with the Member States to ensure that the concept of privacy by design will inform these and any other future developments of the EWRS right from the outset [2], and that the principles of necessity, proportionality, purpose limitation and data minimisation will be taken into due account when decisions are made on what information can be exchanged through the EWRS, with whom, and under which conditions.

8. THE PROVISION OF INFORMATION TO DATA SUBJECTS

One of the main requirements under the EU data protection legal framework is the obligation for a data controller to provide clear information to data subjects about the processing operations it intends to carry out on their personal data.

In line with its coordinating role within the EWRS and in order to fulfil the abovementioned obligation [3], the Commission has made available a clear and comprehensive privacy statement on its webpage dedicated to the EWRS, with regard to the processing operations carried out under the Commission's own responsibility and to those carried out by competent authorities in particular in the context of contact tracing activities.

However, responsibility with respect to the provision of information to data subjects is also incumbent on the national competent authorities in the Member States in their capacity as controllers, for their respective processing operations within the EWRS.

What 'information' must national EWRS competent authorities provide to data subjects?

In cases of collection of data directly from the data subject, Article 10 of Directive 95/46/EC states that the controller or his representative must provide, at the time of the collection, a data subject from whom data are collected with at least the following information, except where the data subject already has it:

(a) the identity of the controller and of his representative, if any;

---

[1] Nevertheless, the alternative option is given to EWRS users to also use this channel for the selective sharing of information related to technical issues which do not involve transmission of personal data. When the alternative option is chosen instead of the default one, the Commission and the ECDC may be selected as recipients by the authority posting the message. This feature has been enabled in the system to take into account the institutional role of the Commission in the coordination of risk and event management issues and of the ECDC in performing risk assessment tasks.

[2] According to the principle of 'Privacy by Design', Information and Communication Technologies (ICTs) are to be designed and developed taking into account privacy and data protection requirements from the very inception of the technology and at all stages of its development.

[3] The information obligation incumbent on the Commission is based on Articles 11 and 12 of Regulation (EC) No 45/2001.

(b) the purposes of the processing for which the data are intended;

(c) any further information such as:

— the recipients or categories of recipients of the data,

— whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

— the existence of the right of access to and the right to rectify the data concerning him or her,

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 of Directive 95/46/EC lists the minimum information to be provided by the data controller where data have not been obtained from the data subject. This information must be given at the time of undertaking the recording of personal data or, if a disclosure to third parties is envisaged, no later than the time when the data are first disclosed [1].

It results from the abovementioned provisions that, at the time of collecting personal data from individuals (or, at the latest, at the time when data are first disclosed through the EWRS), for the purposes of adopting the measures required to protect public health in relation to events to be notified under Decision No 2119/98/EC and its implementing rules, a legal notice containing the information listed in Articles 10 and 11 of Directive 95/46/EC must be given by the national competent authorities directly to data subjects. The notice should include also a brief reference to the EWRS and a link to the relevant documents and privacy statements in the competent authorities' national websites, as well as to the Commission's EWRS-dedicated webpage.

The exact detail of information to be provided in the legal notice may differ significantly from one Member State to another. Certain national laws foresee more extensive obligations for data controllers covering the provision of further information, such as information on data subjects' right to obtain redress, on data storage and retention periods, on data security measures, etc.

It is true that the need to timely intervene in situations of sanitary emergency may render it impossible, when the data have not been obtained from the data subject, to provide notice to data subjects to inform them about the purposes of the processing of their personal data. In this regard, Article 11(2) of Directive 95/46/EC states that the right of information of data subjects may be restricted where 'the provision of such information proves impossible or would involve a disproportionate effort, or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards'.

More generally, it should be noted that specific restrictions or limitations to data subjects' right to information may be applicable under national data protection laws transposing Directive 95/46/EC [2]. Any such country-specific limitations or restrictions should be unambiguously mentioned in the privacy notices provided to data subjects or in the privacy statements published on the competent authorities' national websites.

It is for the national competent authorities in the Member States to decide in which form and how exactly to convey this information to data subjects. As most competent authorities will carry out processing operations other than exchanges of information within the EWRS, the way they inform individuals may, if appropriate, be the same way chosen for conveying similar information for other processing operations under national law. Furthermore, it is recommended that competent authorities update or complement the privacy policies or statements — if they already have any on their national websites — with a specific reference to the exchange of personal data within the EWRS.

---

[1] The information to be provided is that listed in Article 10 cited with the addition of the categories of data concerned. This information is obviously not required in case of collection directly from the data subject, who is informed of the categories of data concerned as these are collected.

[2] Article 13(1) of Directive 95/46/EC on exemptions and restrictions states as follows: 'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others'.

For all the abovementioned reasons, it is of the utmost importance that competent authorities in the Member States consult their respective national DPAs when developing standard legal notices and privacy statements in accordance with Articles 10 and 11 of Directive 95/46/EC.

9. ACCESS TO PERSONAL DATA AND OTHER RIGHTS OF DATA SUBJECTS

Data protection requirements on the provision of information to data subjects examined in the previous Section 8 are ultimately aimed at ensuring the transparency of personal data processing operations. Transparency is also the underlying objective of the provisions on access rights of data subjects laid down in the EU data protection legal instruments ([1]).

What is the data subject's 'right of access to data'?

Data controllers are required to guarantee every data subject the right to obtain, without excessive delay or expense, confirmation as to whether or not personal data relating to him or her are being processed, as well as information on the purposes of this processing and on the recipients to whom data may be disclosed.

Data controllers must also guarantee data subjects' right to obtain the rectification, erasure or blocking of data the processing of which does not comply with the applicable data protection laws, for example because of the incomplete or inaccurate nature of the data.

Finally, data controllers must notify third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out upon legitimate request from the data subject, unless this proves impossible or involves a disproportionate effort.

In their capacity as controllers, the Commission and the Member States share responsibility with respect to the provision of rights of access, rectification, blocking and deletion of personal data processed within the EWRS in the terms outlined hereafter.

The Commission bears responsibility for giving access to personal data of the national EWRS focal points, and for dealing with the related rectification, blocking and deletion requests. National focal points are invited to refer to the specific clause in the comprehensive privacy statement on the Commission's EWRS-dedicated webpage ([2]) for more detailed information on how to exercise their rights as data subjects.

EWRS users are also informed that a feature has already been built into the system allowing them to directly modify their personal data. However, data fields on which a given EWRS account is identified (user's accredited e-mail address, account type, etc.) cannot be changed by users themselves, in order to prevent the risk of unauthorised users gaining access to the system. Therefore, any request to modify these data fields should be addressed to the data controller at the Commission, as indicated in the comprehensive privacy statement on the Commission's EWRS-dedicated webpage.

The responsibility for dealing with data subjects' requests concerning contact tracing, health and other personal data exchanged between Member States through the EWRS rests with the respective competent authorities involved in a given selective information exchange. This responsibility is governed by the relevant provisions of the national data protection laws transposing Directive 95/46/EC.

However, it should be noted that specific restrictions or limitations to data subjects' rights of access, rectification, erasure or blocking of data may be applicable under national data protection laws transposing Directive 95/46/EC ([3]). Any such limitations or restrictions should be unambiguously mentioned in the privacy notices provided to data subjects or in the privacy statements published on the competent authorities' national websites. EWRS contact points are therefore advised to contact their national DPAs to get more information on this issue.

The complexity of the EWRS, with multiple users involved in joint processing operations, requires a clear and simple approach towards data subjects' right of access, since data subjects are not familiar with the functioning of the system and should be put in the conditions to effectively exercise their rights.

([1]) Article 12 of Directive 95/46/EC and Articles 13 to 18 of Regulation (EC) No 45/2001.
([2]) The privacy statement is also available to all EWRS users from within the secure section of the EWRS application.
([3]) Article 13(1) of Directive 95/46/EC cited.

A recommended approach would be that, if a data subject believes that his or her personal data are being processed within the EWRS, and he or she would like to have access to it or have it deleted or rectified, the data subject should be able to address any of the national competent authorities with which he or she had contacts and/or who collected his or her data in relation to a specific event posing a public health risk (e.g. both the authority of the country of which the data subject is a citizen and the authority of the country of stay of the person at the time of the event), as well as any other authority involved in that given information exchange in relation to the implementation of contact tracing measures.

No competent authority involved in the concerned information exchange should refuse access, rectification or deletion on the ground that it did not introduce the data in the EWRS, or that the data subject should contact another competent authority. In particular, if the request of the data subject is received by a competent authority other than that who posted the original information through the selective exchange channel, the receiving authority should forward the request, through the specific mechanism referred to in Section 7, to the competent authority having posted the original message, who will decide on the request.

If appropriate, before taking a decision the competent authority who posted the information in the system may contact other competent authorities involved in the information exchange or otherwise concerned by the request of the data subject through the specific mechanism referred to in Section 7.

Data subjects should be also informed that, if they are not satisfied with the answer received, they may contact another competent authority involved in the information exchange. In any case, data subjects have the right to lodge a complaint with the national data protection authority of one of these competent authorities that suits him or her best. If necessary and appropriate, national DPAs should cooperate with each other to deal with the complaint (Article 28 of Directive 95/46/EC).

Finally, further to a specific recommendation made by the EDPS in its Opinion, the Commission has implemented a new feature within the EWRS to allow online rectification and deletion, for data protection compliance purposes, of selective messages containing personal information which is inaccurate, not up to date, no longer needed or otherwise not compliant with data protection requirements.

10. DATA SECURITY

Access to the system is limited to authorised users from the Commission and the ECDC and to formally appointed EWRS national focal points. Access is protected through secured and personalised user account and password.

The procedures for the handling of personal information in the EWRS are set with reference to the requirements indicated in Articles 21 and 22 of Regulation (EC) No 45/2001.

11. DATA RETENTION

In accordance with data protection requirements under Article 4(1)(e) of Regulation (EC) No 45/2001 and Article 6(1)(e) of Directive 95/46/EC, the system will automatically erase all selective messages containing personal information 12 months after the date of posting of the messages.

This safeguard, which is intrinsic to the system design, does not however dispense EWRS users — since solely and individually responsible for their own processing operations within the selective messaging channel — from taking action to remove from the system those personal data which become no longer needed before the expiration of the default 1-year period.

To this end, the Commission has implemented a new feature within the EWRS to allow users to directly delete, at any time, those selective messages containing personal information which is no longer needed.

Finally, it should be recalled that national competent authorities are responsible for complying with their own data protection rules on the retention of personal data set out in the relevant legislation transposing Directive 95/46/EC. Automatic erasure of personal information stored in the system after 1 year does not prevent EWRS users from storing the same information outside the EWRS for different (e.g. longer) periods, provided this is done in conformity with the obligations stemming from their respective national data protection laws and that the periods provided for in the national legislation are compatible with the requirements set in Article 6(1)(e) of Directive 95/46/EC.

12. COOPERATION WITH NATIONAL DATA PROTECTION AUTHORITIES

Competent authorities are encouraged to seek the advice of their respective national DPAs, particularly when confronted with issues related to data protection which are not covered by these guidelines.

Competent authorities must also be aware that, under the terms of national laws transposing Directive 95/46/EC, it might be necessary for them to notify their respective DPAs of their own data processing activities within the EWRS. In certain Member States, a prior authorisation from the national DPA might be even required.