**Prior checking opinion on the Early Warning Response System ("EWRS") notified by the European Commission on 18 February 2009**

Brussels, 26 April 2010 (case 2009-0137)

## 1. Proceedings

On 18 February 2009 the Commission notified the European Data Protection Supervisor ("**EDPS**") of its Early Warning Response System **("EWRS")** for the prevention and control of communicable diseases for "ex-post" prior checking. On 16 April 2009 the EDPS extended - by one month - the period available for him to issue his Opinion under Article 27(4) of Regulation 45/2001 ("**Regulation**"). On 11 May 2009 the EDPS requested a meeting to clarify some of the facts and view a demonstration of the EWRS. The meeting took place on 25 November 2009. At the meeting, the Commission undertook to provide further information. In the interim, the EDPS also conducted a survey among data protection authorities in Member States on their experience with the national use of the EWRS. In addition, on 17 December 2009, the EDPS sent the Commission a summary of his understanding of the facts, including his remaining requests for clarification. The Commission responded to the questions on 12 March 2010. On 18 March, the EDPS extended the deadline available for issuing the opinion by another month. Finally, on 16 April 2010, the EDPS sent the Commission the draft Opinion, for comments. The Commission commented on 22 April 2010.

## 2. The facts

**2.1. Introduction.** This prior checking covers the data protection aspects of the EWRS. ERWS is a communication tool used by the Commission, the European Centre for Disease Prevention and Control ("**ECDC**"), an independent European Union agency located in Sweden, and EU Member States (as well as Norway, Iceland and Lichtenstein[1]) for the exchange of information for the prevention of "communicable diseases" which are "relevant at Community level"[2]. These may include, for example, tuberculosis, measles, yellow fever, SARS, H1N1 and a large number of other communicable diseases.

While each Member State runs its own national system for infectious diseases prevention and control, this centralised network allows cross-border action, in particular, coordination of the Member States' measures to control communicable diseases. The EWRS is designed to ensure a rapid and effective response by the EU to events (including emergencies) related to communicable diseases. Therefore, the EWRS is frequently used for notification of outbreaks, exchange of information and discussion about the coordination of measures among the

[1] For the sake of simplicity, Norway, Iceland and Lichtenstein will not be specifically referred to each time in this Opinion. Instead, the term "EU Member States" will be used. Note also that the World Health Organisation ("**WHO**") also has read-only access to parts of the data in the EWRS, as will be described later in this Opinion.
[2] For definitions and further details, please see the documents referenced in Section 2.5 when discussing the legal basis of the EWRS.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

parties. The EWRS has been successfully used in a number of situations such as SARS, avian influenza in humans and other major communicable diseases. It constitutes an important tool to protect public health and thus, helps save lives.

In addition to users at the Commission, the ECDC, and the WHO, currently there are over a hundred competent authorities in Member States with access to the EWRS. The EWRS is operated by the ECDC. The EWRS has two communication channels: a general messaging channel making available all uploaded messages simultaneously to all users as well as a channel for "selective messaging" where the range of recipients can be more limited. The selective messaging channel can be used, among others, for "contact tracing", as described below. Due to the sensitivity of personal data processed, this Opinion focuses primarily on contact tracing.

**2.2. General messaging channel.** The so-called "general messaging channel" is used to share general information relevant to all Member States. This may include, typically, information about new threats and developments as well as preventive measures taken by the Member States in the fight against certain threats, such as, recently, H1N1. Member States, importantly, are obliged to notify cases of communicable diseases "of Community relevance" through the EWRS. The EWRS thus helps information exchange in order to achieve better coordination among Member States, the ECDC and the Commission. Important messages can trigger coordination meetings and become the starting point for a discussion for coordinated action. The decision on follow-up measures depends on the seriousness and the particularity of each case.

Messages posted via the general messaging channel are automatically available to all health authority contact points in all Member States as well as to the Commission (DG SANCO) and the ECDC.[3]

In addition to these recipients, the WHO also has access to the EWRS. The decision has been taken to give access to the WHO after the SARS crisis and after the entry into force of the new International Health Regulation (June 2007). Nevertheless the Member State contact point uploading a general message may also decide, by un-checking a checked box on the screen, not to make the information uploaded available to the WHO. In any event, the message is only sent to the WHO regional office for Europe, which treats it confidentially, under the International Health Regulations. Thus, the Commission explained to the EDPS, no message is sent on to individual WHO member states.

The Commission and contact points in Member States have each both read and write access, that is, they can both upload and review messages posted on the EWRS. On the other hand, the ECDC and the WHO have only read access. They cannot post messages on the EWRS.

The "general messaging channel" is not intended to be used to share personal data (except that the names and contact information of the EWRS contact points - that is, the health officials having access to the EWRS - are displayed with the messages circulated). No other personal data, in particular, no health-related personal data are systematically exchanged through the system.

[3] The notification lists other recipients of data within the Commission besides DG SANCO: DG TREN and "potentially other DGs and services". These DGs (Directorate Generals) do not have access to the EWRS. However, the Commission explained that the content of messages can be shared by DG SANCO *ad hoc* if considered relevant.

With that said, the Commission explained that it cannot be excluded that some data uploaded onto the system may be related to people who may be indirectly identifiable. This may be the case, for example, when a rare disease occurs in a small community, the name of the community is noted in the EWRS, and the identity of the patient is reported in the media or is otherwise known within that community.

The general messaging channel has the following pre-defined data fields:

- Name of the individual and organisation communicating the message
- Type of message (e.g. coordination of measures)
- Syndrome/disease (with a free text field for additional specification if needed)
- Pathogen (e.g. adenovirus)
- Reporting reason (e.g. A1)
- Country of occurrence
- Date of onset/detection
- Message body (free text)
- Attachments (maximum of three attachments, in common file formats such as word doc, pdf, etc; occasionally photographs are also attached)
- WHO visibility (i.e. whether the message should be visible to WHO)
- IHR WHO (additional information if the message needs to be communicated under the International Health Regulations to the WHO)

**2.3. Selective messaging and contact tracing.** Another part of the system, the so-called "selective messaging channel" can be used, as the name suggests, selectively, with the senders reaching with their messages only those recipients whom they previously selected from a list (32 checkboxes total including Member State contact points, the Commission and the ECDC). When messages are sent using this channel, those not designated as recipients cannot view the content of the messages, although they can see that a message was sent at a particular time, and can see who the sender and the recipients were.

As far as contact tracing is concerned, which is the main purpose for which the selective exchange messaging channel is used, the Commission and the ECDC are not recipients of the messages which the Member States interchange and therefore, they do not have access to the content of these messages. This is mirrored by the provision under the current legislation that excludes access by the Commission and the ECDC to the contact tracing messages circulated through the "selective messaging channel" (see Article 2.a2 of the EWRS Decision as modified by the Contact Tracing Amendment).

The WHO has no access to the "selective messaging channel" and no access to the data shared through the "selective exchange channel". However, in case of public health emergencies of international concern which imply the need for contact tracing outside the European Union, data can be transferred to the WHO outside of the EWRS under Article 23(1) of the new International Health Regulations.

Compared to the general messaging channel, the selective messaging channel has a simplified structure: there are no pre-defined data-fields; instead, there is only a free text subject line and a free text message body. In addition, there is also the list of recipients. The attachment facility is the same as in the general messaging channel.

Just like the general messaging channel, the selective messaging channel can also be used for messages containing - as a rule - no personal data: for example, when a message relates to

proposed measures to be adopted at the border of only two Member States, these countries may choose to use the selective messaging mechanism to communicate, rather than informing all other Member States.

In addition to these types of messages containing little or no health-related personal data, the selective messaging channel can also be used for "contact-tracing", as discussed below.

**2.4. Contact tracing.** Contact tracing is a procedure used to identify and reach persons ("**contacts**") who may have come into contact with an infected person. Once contacts are traced, they may be diagnosed and receive care. In addition, contact tracing also serves general public health interests by reducing or preventing the further spread of the disease (e.g. the infected or potentially infected people may be quarantined). Contact tracing involves sharing of often very sensitive medical information, with a potential impact not only on the privacy of the individuals concerned but also potentially leading to very important restrictions on the individual's freedom (e.g. quarantining or refusal of entry in a country).

Contact tracing is not used for every communicable disease. In some cases, such as in the case of tuberculoses, measles, haemorrhagic fever, contact tracing is widely accepted in the scientific world as a useful and necessary measure to help prevent or reduce the further spread of the disease. In some other cases, on the contrary, it is widely accepted that contact tracing is inefficient, and therefore, it should not be used as a public health policy measure. This is the case, for example, with H1N1. In a third category of diseases, for example, in those involving carrying a stigma such as sexually transmitted diseases, opinions vary with some experts advocating contact tracing while others suggesting that contact tracing may be counter-productive in that it would lead persons to avoid seeking medical treatment for fear that it would breach their right to privacy.

In the European Union, the ECDC issues non-binding opinions on whether contact tracing should be used for any specific disease and/or outbreak. To prepare its opinion, ECDC takes into consideration the nature of the disease, its infectivity (e.g. measles), its severity (e.g. haemorrhagic fever) and the context in which exposure has occurred (e.g. in an airplane or in another confined environment). These guidelines are generally respected in Member States. However, it is the Member States, rather than the ECDC, which ultimately decide, each according to its own policies and procedures, whether contact tracing should be used in its jurisdiction with respect to any particular disease and any particular event. With that said, cross-border contact tracing is sometimes initiated and coordinated by the ECDC, in cooperation with Member State authorities.

For sexually transmitted diseases, contact tracing is generally limited to sexual partners but for highly virulent diseases such as Ebola and tuberculosis, a thorough contact tracing would require information regarding casual contacts. These may include, for example, fellow travellers in an organized tour group; or those sitting next to the infected person, or in the rows immediately in front of, or behind him or her, on a commercial flight.

In 2008 and 2009, 44 events notified through the EWRS required contact tracing. They resulted in 66 selective exchange messages. Overall 419 contact persons were traced (of these 169 in 2009). One outbreak of hepatitis onboard a cruise ship generated 201 contacts to be traced. The average number of contacts traced per event is 9.5. However, most events (83%) are involving 3 contacts or less. The vast majority of the events related to tuberculosis. A typical case would involve a national of one Member State travelling to another Member State and being diagnosed there or shortly afterwards with a communicable disease.

Different contact tracing data are collected in different Member States. There is no one specific procedure to collect these data and the nature of the data will be variable in function of the different pathological situations and diseases involved in the specific event that is requiring contact tracing. For example, a person may need to be traced back because of being suspected to be infected with the rabies virus (a lethal infection in 100% of cases) as a consequence of a close contact with an infected dog. In this case the information to be acquired is related to his/her presence in a specific place and during a precise period of time. In other cases, individuals may need to be traced for a suspected tuberculosis or meningitis during a long haul flight: the data needed here are the seat numbers in the plane. The public health authorities in Member Sates are the only authorities responsible to collect such data on the basis of the specific situation. The Commission explained that airlines, tour operators and other authorities do not collect data for contact tracing purposes at national level.

EU legislation does not harmonize contact tracing activities. Instead, it requires Member States to share contact tracing data through the EWRS when the data are already "available" and when sharing them is "necessary". Applicable EU legislation establishes what categories of contact tracing data can be exchanged using the EWRS. The list includes the following:

- personal information: name; nationality; date of birth; sex; ID type, number and issuing authority; current home address; telephone numbers; e-mail
- travel specifications: flight number, date of flight; ship name, plate number, etc; seat number; cabin number
- contact information: names of visited persons/places of stay; dates and addresses of places of stay; telephone numbers; e-mail
- information on accompanying persons: names; nationality; ID type, number and issuing authority; current home address; telephone numbers; e-mail
- emergency contact details: name of the person to be contacted; address; telephone numbers; e-mail.

Once the data are notified via the EWRS, each Member State will implement, following their national legislation and in compliance with EU law, all the actions in order to contact the identified persons.

**2.5. Legal basis.** EWRS is established pursuant to Commission Decision 2000/57/EC of 22 December 1999 on the early warning and response system for the prevention and control of communicable diseases ("**EWRS Decision**"). The EWRS Decision, as an implementing measure by the Commission, follows on 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 ("**Community Network Decision**").

Subsequently, on 21 April 2004 Regulation (EC) No 851/2004 of the European Parliament and of the Council established a separate entity, ECDC, as an independent European centre for disease prevention and control ("**ECDC Regulation**"). The ECDC Regulation designated, in its Article 8, the ECDC to operate the EWRS.

Finally, contact tracing was introduced via an amendment to the EWRS Decision by Commission Decision 2009/547/EC of 10 July 2009 ("**Contact Tracing Amendment**").

**2.6. The roles of the Commission, the ECDC, Steria and contact points in Member States.** The notification indicates the Commission as the controller of the system. The notification also mentions that the system is "operated by" the ECDC. The notification also

mentions Steria, a service provider operating in Sweden and subject to Swedish law. Steria is referred to as "an external hosting provider" or "application service provider". No mention is made in the notification of the role of competent authorities in Member States. During the prior checking procedure, the following was additionally explained to the EDPS.

The EWRS Decision does not specifically assign the role of "controllers" or "co-controllers" to the Commission and to Member States. Neither does it explicitly define the precise roles of the controllers and the involvement or role of any eventual processors. With that said, it is the understanding of the Commission that each Member State authority has certain responsibility with respect to its own use of the EWRS, and for the data it uploads onto the system, and in that sense, acts as co-controller of the system. At the same time, the Commission, which operates the EWRS and ensures the security of the data exchanged in it, should also be considered as a controller, with respect to those activities for which it is responsible, including the functioning and security of the system.

The Commission also explained that the role of SANCO is generally management of coordination whereas the role of ECDC is risk assessment. ECDC is not part of the "EU network"; therefore, although ECDC operates the system, and has read access to any messages on EWRS, it has no write access and cannot post messages. The Commission and ECDC consider ECDC's role as that of a processor rather than a controller.

There is currently no contract in place between the Commission and ECDC regarding the roles and responsibilities of ECDC. Neither is there any other document - legally binding or otherwise - describing their respective roles. The Commission explained that at medium term a revision of the current EU legislation in the area of communicable diseases will be proposed. This may also be an opportunity to more fully address data protection issues, in particular, the roles and responsibilities of controllers, co-controllers and processors.

The Commission further explained that the ECDC signed a contract with Steria; and this contract includes provisions on data protection and security.

**2.7. Information to data subjects.** The notification suggests that information is provided to data subjects on an *ad hoc* basis by the national health authority involved. This may mean, in particular, that information could be given to a "contact" (verbally or in writing) when he or she is first contacted as part of the contact tracing procedure.

During the prior checking procedure, the Commission explained that a request to Member States on how they comply with the EU legislation on personal data protection (Directive 95/46/EC) has been circulated in the past and the Commission intends to table this issue again in the upcoming meeting of the EWRS Committee under the Community Network Decision.

Further, at the request of the EDPS, the Commission also confirmed that it plans to provide information about the data protection aspects of the EWRS on DG SANCO's website. The information will explain the workings of EWRS and data protection safeguards (e.g. how access rights can be exercised and whom data subjects can complain to). The site will also suggest best practices to the users of the system.

**2.8. Access rights (including rectification, erasure and blocking).** With regard to access rights, upon the request of the EDPS, the Commission explained that information on how to exercise these rights will be provided on DG SANCO's website as noted in Section 2.7 immediately above. No further details were given.

**2.9. Retention period.** With regard to messages in the selective messaging channel, the Commission plans to build in an automated feature into the EWRS which would allow the

automatic deletion of all personally identifiable contact tracing data within one year as of the upload of the information onto the EWRS. The Commission explained that the one-year period for retention of information regarding contact tracing is justified by the fact that incubation periods for some communicable diseases may be long, such as for tuberculosis, and therefore, it is possible that exposed people may need to be contacted up to such a period.

The Commission plans to retain certain data beyond these retention periods for statistical, scientific and research purposes in an anonymized format. The deletion of personal data after one year would be automatic, and would consist of removing the body of the contact tracing messages as well as their attachments (potentially containing the personal data) while keeping the header of the message, containing only structured fields such as name of the disease and country of origin.

General messages not containing personal data are kept indefinitely as they are used as baseline to detect unusual patterns of events in the analysis of trends. In these cases both the structured fields indicating disease, location and other pre-defined characteristics of the events, as well as the body of the message describing the event are kept.

**2.10. Security measures.** The Commission provided the following documents for EDPS review:

- Technical security measures for the EWRS IT infrastructure,
- EWRS application security, and
- extracts from the Service Contract between ECDC and Steria (on data protection and security).

**2.11. Accuracy and proportionality of data exchanged.** The Commission explained that accuracy and proportionality of the information uploaded in the EWRS could be considered as verified by the ECDC through its daily activities of monitoring events with potential impact on public health worldwide and more specifically in the EU.

Concerning training for users, the Commission pointed out that the system is user-friendly. The multiannual experience of the users in Member States ensures that new users based in Member States are trained by their national authorities on the spot. With that said, a training module is built in the system in order to allow the user to train alone or to address specific questions on selected functionalities in the application. In DG SANCO new users are regularly trained. For the training of new users a specific module called "TEST EWRS" has been developed and put in production in order to avoid the misuse of the "real" EWRS application for training new users. All the messages used to train users in this case are fictitious in order to avoid the use of real names and events which are by definition "confidential". A guide to use the EWRS is available in the training module.

## 3. Legal aspects and Recommendations

**3.1. Applicability of the Regulation.** The notified processing, insofar as it concerns the activities of the Commission and the ECDC, falls under the scope of Regulation (EC) 45/2001 ("**Regulation**") pursuant to its Articles 2 and 3. The processing of personal data by the Commission and ECDC is supervised by the EDPS (see Regulation, Article 1).[4]

[4] For a national contact point in a Member State the applicable law is its own national data protection law which must be in conformity with Directive 95/46/EC. The processing of personal data by these contact points is supervised by their national data protection authorities.

**3.2. Grounds for prior checking.** The processing is subject to Article 27(2)(a) of the Regulation which requires prior checking by the EDPS of, among others, "processing of data relating to health".

**3.3. Deadlines for notification and for issue of the EDPS opinion.** The EWRS was already in use before the EDPS was notified. The opinion of the EDPS should, as a rule, be requested and given prior to the start of any processing of personal data. Nevertheless, taking into account that a large number of processing operations were already in place before the EDPS started to operate in 2004 and some of the institutions and bodies have not yet fully cleared their backlog of notifications, these prior checking procedures are now carried out ex-post.

Pursuant to Article 27(4) of the Regulation, this Opinion must be delivered within two months, discounting any periods of suspension allowed for receipt of additional information requested by the EDPS. The procedure was suspended for 311 days. Further, the EDPS extended its deadline to issue an Opinion by two months. The Opinion must therefore be provided no later than 26 April 2010.

**3.4. Lawfulness of the processing (Article 5(a) of the Regulation).** The processing is based on the legal basis described in Section 2.5 above. Thus, specific legal instruments "adopted on the basis of the Treaties" allow and provide the basic conditions for the notified processing operations. The EDPS is also satisfied that the processing is necessary and proportionate for the public interests of protecting public health in the European Union. Therefore, the processing is lawful. With that said, in the short-to-medium term, it is necessary to strengthen and clarify the legal basis of the processing by establishing a more clear division of tasks and allocating more clearly the responsibilities, in particular, as between the Commission and the ECDC, but also among Member State contact points, as will be described in Section 3.5 below.

**3.5. Responsibility for the operation and use of the EWRS: controllers and processors**

**3.5.1. Need for clear designation of controllers and processors and clear allocation of responsibilities.** As a preliminary remark, the EDPS emphasises that in any situation where personal data are processed, it is crucial to correctly identify who the controller is. This has recently been emphasized by the Article 29 Data Protection Working Party in its Opinion 1/2010 on the concepts of "controller" and "processor", which was adopted on 16 February 2010. The primary reason why the clear and unambiguous identification of the controller is so crucial is that it determines who shall be responsible for compliance with data protection rules.

As noted in the Working Party Opinion[5], "[i]f it is not sufficiently clear what is required from whom - e.g. no one is responsible or a multitude of possible controllers - there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective." Clarity is especially needed in situations where multiple actors are involved in a cooperative relationship. This is often the case with EU information systems used for public purposes where the purpose of processing is defined in EU law.

For these reasons, the EDPS urges legislators, the Commission and the ECDC, to lay down, in a clear and unambiguous manner, the tasks and responsibilities of each party involved in the data processing, including the Commission, the ECDC and contact points in Member States. Ideally, and in the medium term, this should take a legally binding form, in EU legislation. As

[5] See page 7, Section II.3.

an interim solution (but also, to provide further detail in the long term even if further legislation will be adopted), clarifications may be provided in another, more practical form, for example, in a set of data protection guidelines for the EWRS. Technically, this may take, for example, the form of a Commission Recommendation.[6]

To put the importance of such clarifications and the adoption of the EWRS data protection guidelines into context, the EDPS emphasises the risks that any future contact tracing on a large-scale may potentially pose to fundamental rights. Although during the prior checking procedure (and the international survey) it was established that at present, the scope of the personal data exchanged in the system for contact tracing purposes is relatively limited, it is possible that in case of a major pandemic health threat in the future the EWRS contact tracing procedure may be put to use in a much larger scale. While this may be necessary and proportionate for legitimate public health purposes, it should not be forgotten that this may also affect the fundamental rights of a large number of people not only to data protection and privacy, but also to the freedom of movement and liberty (consider quarantines and travel restrictions). For these reasons, just as serious public health preparations are required to counter any potential health threats, timely preparations must also be made for such cases to ensure the protection of fundamental rights.

When allocating responsibilities in the EWRS data protection guidelines, in particular, the following issues need to be addressed:

- Who are responsible for ensuring the quality (proportionality, accuracy, etc) of the data?
- Who can determine retention periods?
- Who determines who can have access to the database?
- Who are authorized to make a transfer of the data to third parties?
- Who are providing notice to data subjects?
- Who are responsible for acting when access, rectification, blocking, or erasure is requested by data subjects?
- Who can decide on any exemptions and restrictions under Article 20 of the Regulation (and corresponding provisions of Directive 95/46)?
- Who bears ultimate responsibility for the security of the EWRS?
- Who makes decisions regarding the design of the EWRS (e.g. who may decide on the inclusion of an automatic feature to limit retention periods to one year?)

With respect to each item, it must be clarified who is authorized to make the ultimate decision, but also, who is making the decisions at the practical level and in what manner. If multiple parties are involved in any aspect, the rules for their cooperation should be clarified.

Finally, the EDPS emphasises that allocation of responsibility in a transparent and predictable manner is not only in the clear interest of data subjects but it is also in the interest of the controllers and processors. Indeed, in the absence of sufficient clarity, there is a risk that in case of a breach of data protection rules, the Commission and the ECDC may become jointly and severally liable for any breach, irrespective which party was at fault.

**3.5.2. Re-evaluation of the role of the ECDC.** During the prior checking procedure, the Commission and the ECDC suggested that their respective roles are best described as a controller-processor relationship, with the Commission determining for what purposes data

[6] See, for example, the Commission's Data Protection Guidelines for the Internal Market Information System at http://ec.europa.eu/internal_market/imi-net/docs/recommendation_2009_C2041_en.pdf

are collected and how they are processed, and the ECDC merely following instructions, as a processor.

The EDPS recommends that the Commission and ECDC should carefully re-evaluate

- whether their approach corresponds to the current factual situation, and
- for the future, whether a different allocation of roles may not be more practical and effective.

Indeed, during the prior checking procedure, the Commission and the ECDC did not provide sufficient evidence that the role of the ECDC is restricted to that of a processor merely following instructions from the Commission. At the same time, several historic, factual and legal aspects suggest that rather than a processor, the ECDC acts as a co-controller, sharing responsibility for decision-making with the Commission to a significant degree when determining the purposes and means of processing data. Without prejudice to any future position that the EDPS may take when presented with a more complete set of facts, or when the future legal framework or the circumstances might otherwise change, the EDPS considers that the role of the ECDC, as things stand currently, is better described as a co-controller jointly and severally responsible for the operation of the EWRS.

To explain, it is useful to make a distinction between the roles of the Commission and the EWRS in the operation of the system on one hand, and their roles as users of the system, on the other hand.

**3.5.2.1. ECDC and the Commission as operator/s of the EWRS.** It is clear from the historic background[7] that the operation of the EWRS, which was initially developed and operated by the Commission, has since then been transferred to the ECDC. The legal basis of this transfer is Article 8 of the ECDC Regulation, which provides that "[t]he Centre shall support and assist the Commission by operating the early warning and response system and ensuring with the Member States the capacity to respond in a coordinated manner." Thus, on a practical and day-to-day level, the operation of the EWRS informatics application is clearly the responsibility of the ECDC rather than that of the Commission.[8] It is also the ECDC, rather than the Commission which concluded and negotiated the agreement with Steria, which is used as a subcontractor to host the EWRS. From the facts presented to the EDPS, the Commission appears to no longer play any role in operating the EWRS.

Further, the emphasis, throughout the ECDC Regulation on the ECDC's independence also makes it questionable to what extent the Commission is able to instruct ECDC on data protection matters. It cannot be excluded that the ECDC, which has its own Management Board composed, primarily, of Member State representatives,[9] may have a different position on certain important data protection safeguards than the Commission. At the same time, the ECDC Regulation uses terms such as "support" and cooperation" when describing the relationship between the Commission and the ECDC. Indeed, it is possible that more strategic decisions regarding the EWRS are currently made jointly by the Commission and the ECDC

[7] See, for example, Section 8 (transfer of the EWRS to the ECDC) of the Commission's 15 May 2009 report to the Council and the European Parliament on the Operation of the Early Warning Response (EWRS) of the Community Network for epidemiological surveillance and control of communicable diseases during 2006 and 2007 (Decision 2000/57/EC).

[8] It is to be noted, however, that EWRS contact points are formally nominated by the Public Health Authorities in the Member States. These formal nominations are transmitted to the Commission and the Commission asks ECDC to activate their access to the informatics application. It is the ECDC then who provides the login and password to the EWRS contact points as well as to the EWRS users in the Commission and in the WHO.

[9] See Article 14 of the ECDC Regulation.

without a clear answer as to who decides in case of disagreement, and thus, who is ultimately responsible for decision-making. This supports the conclusion that ECDC and the Commission are currently acting as co-controllers, jointly and severally responsible for the operation of the system.

**3.5.2.2. ECDC and the Commission as users of the EWRS.** The Commission has both read and write access to the EWRS while the ECDC only has read access and is unable to post messages on the EWRS. It was also explained to the EDPS during the prior checking procedure that, in a broad and general perspective, the role of the ECDC is risk assessment, whereas the role of the Commission is cooperation.

From this it appears that the Commission, in addition to wearing a hat as a co-controller of the system when it comes to operation, is also wearing a separate hat as a separate and individual controller responsible for its own use of the system, much the same way as any national contact point is responsible for its own use of the EWRS as a separate controller. For example, the Commission is responsible for the accuracy and proportionality of any personal data it uploads on the system.

In a more limited way, ECDC also appears to act as a separate controller, for the use of the personal data to which it has only read-only access. For example, it is responsible as a controller to evaluate whether it is entitled to make any transfer to third parties of such data on a case by case basis.

**3.5.3. Member State contact points as separate controllers.** As for the role of Member State contact points, the EDPS is in agreement with the analysis of the Commission and the ECDC in that Member State contact points are each responsible as separate controllers for their own data processing operations when using the EWRS. Considering the number of different parties involved, and while fully acknowledging the role that national data protection authorities may play in ensuring compliance by the national contact points, the EDPS recommends the adoption of a set of data protection guidelines for the EWRS (see Section 3.5.1 above), as a means of promoting best practices and a consistent and transparent approach.

**3.5.4. Conclusion.** To summarise, with respect to responsibilities for the operation of the EWRS, the EDPS has not been provided convincing evidence to support that the current factual relationship between the Commission and the ECDC is other than joint controllership. Neither have their respective roles, tasks and obligations been clearly allocated as between them. Therefore, the EDPS is of the view that until further clarification of their roles, they are jointly and severally liable for the operation of the system.[10]

Controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the institutions and bodies involved. It must be specified who is responsible for what, and how data subjects can exercise their rights. In the short term, adoption of a set of data protection guidelines for the EWRS is recommended. The Commission is also encouraged to promote a revision of the legal framework to ensure a more secure legal basis and clear allocation of responsibilities.

**3.6. Data quality (adequacy, relevance, proportionality, fairness, lawfulness, purpose limitation, accuracy: Articles 4(1)(a),(b)(c) and (d)).**

[10] At the same time, each contact point in Member States, as well as every other user (the Commission, ECDC and the WHO) is each responsible only for its own use of the system, separately and individually.

In general terms, the EDPS is satisfied with the design of the EWRS for purposes of data quality, and has not detected any systemic failures leading to significant quality issues. In particular, the EDPS is satisfied with the use of the selective messaging channel to limit the recipients to those necessary for contact tracing purposes, and for the clear and simple structure for sending general messages.

With that said, maintaining compliance requires continuous efforts and attention. Each user of the system with write access (in particular, national contact points, but also the Commission) is individually responsible for the quality of data that they themselves upload. To facilitate compliance by the various users, the EDPS recommends that the operator of the system (Commission/ECDC) should make the following additional efforts:

**3.6.1. Integration of data protection into training.** The EDPS recommends that data protection elements should be integrated to any training given to the users of the system. In particular, the EWRS training module should include training materials on relevant data protection aspects of the use of the EWRS. This may include, among others, information on how to ensure that

- only relevant and not excessive data are included in the database (e.g. no contact tracing information is included for diseases where the benefits of contact tracing are not sufficiently proven; no personal data are to be included in general messages),
- any incorrect data are rectified and data included are kept up-to-date (e.g. names mistakenly noted are corrected),
- how to inform data subjects, and
- how to provide them access to their personal data, upon request.

The existence of the training module and the EWRS guide and the importance of integrating data protection into the training given to the users of the system should be brought to the attention of national contact points. The training module and the guide itself should also be prominently displayed in the EWRS user interface, and should, as a best practice, contain practical examples.

**3.6.2. On-line rectification/deletion of data.** If such a feature is not yet included, it should be ensured that the uploading authority should be able to directly delete, modify (rectify or up-date) on-line any data that are inaccurate, irrelevant, or no longer up-to-date. As a best practice, it would also be helpful if there would be a facility for any other recipients to send a message to the uploading authority if doubts arise regarding accuracy/up-to-datedness.

**3.6.3. Possible future structured format for contact tracing.** At the moment, and despite the specification of the Contact Tracing Amendment of what contact data can be exchanged, there are no structured data fields in the EWRS selective messaging channel to accommodate a more structured (and therefore, more limited and more consistent) information exchange. Contact tracing data are simply uploaded as attachments or in free text fields. Considering that at this time contact tracing procedures and the data collected significantly vary Member State by Member State, and further taking into account that the amount of contact tracing data exchanged is relatively limited, at present, the EDPS does not view this as a significant problem. However, this may need to be revisited in the future if and when contact tracing becomes more widespread.

**3.7. Retention of data (Article (4)(1)(e)).** With regard to retention, we welcome that the Commission proposed a mechanism and a reasonable deadline for “automatic” (i.e.

technically built-in) deletion for contact tracing messages. This is particularly important as it is a recurrent problem with large-scale IT databases that if deletion is conditioned upon "closure of cases" by case handlers and if a system does not provide for automatic deletion of inactive cases irrespective of closure, some cases may remain open unnecessarily and for an unduly long period of time. Therefore, we welcome the plans to build-in automatic deletion into the system to ensure that cases are closed in a timely manner.

At the moment, the EDPS has no objections against the proposal for keeping contact tracing data for a full year. However, the EDPS recommends that the necessity for the one-year period should be periodically re-assessed in the future, especially if contact tracing will be used in the future on a significantly larger scale and for diseases for which the incubation period is significantly shorter. For such a case, some differentiation might be advisable, for example, deletion of contact tracing data for tuberculosis only after one year but an earlier deletion in cases where the incubation period is significantly shorter.

Further, the EDPS recommends that at the same time when the automatic deletion will be built into the system, another feature would also be built in which would allow Member State contact points, if they wish, to delete any particular contact tracing data uploaded earlier than the default one year.

**3.8. Recipients and data transfers.** The EDPS welcomes the fact that the scope of the recipients is limited to those identified in Section 2.

In addition, the EDPS reminds the Commission and the ECDC that when data are transferred (outside the EWRS application) to the WHO, or if unforeseen data transfers are requested by any third party, the Commission and the ECDC should only allow such transfers subject to

- either the unambiguous or explicit (with respect to sensitive data) and informed consent of the data subject, or
- as otherwise specifically allowed by the Regulation.

In case of doubt, the EDPS recommends that the ECDC/Commission consults its Data Protection Officer ("**DPO**") before making the requested transfer. The EDPS also emphasises that pursuant to Article 7(3) of the Regulation the controller should inform the recipients that they may only process personal data transferred for the purposes for which they were transmitted.

**3.9. Right of access and rectification (Article 13).** The Commission and the ECDC should clarify and communicate in an effective way, both to the users of the system and to the data subjects concerned, how access rights can be effectively exercised by the data subjects, in particular, whom they can contact if they wish to have access to their data or rectify such data. This should be discussed in the data protection guidelines for the EWRS, on DG SANCO's (or ECDC's) website dedicated to the EWRS, and should also be made available for the users of the application, from within the EWRS application.

As the Working Party Opinion referred above[11] explains, "[p]arties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance." This entails - in the present case, and also considering the international character and the complexity of the system - that no matter how precisely the rules for rights of access will be established, it is crucial to ensure that data

[11] See the first sentence on top of page 24 in the Working Party Opinion.

subjects could contact any parties involved in an information exchange (EWRS contact points concerned, ECDC or the Commission) for access, and could receive a timely and clear reply from the very first one, rather than having to make repeated attempts to contact various parties until finally one accepts competence for dealing with the request. In general, all parties to a selective message containing contact tracing data should be ready to respond to access requests. This does not exclude the possibility of an "origin-based" approach whereby the parties cooperate with each other, or refer the issue for decision to the party who uploaded the message in the first place. These interim mechanisms, however, should not cause undue delays, confusion, or complexity for the data subject.

For this reason, we also encourage you to consider the possibility of "building in" into the system architecture ways to assist national contact points to cooperate in case an access request or request for rectification is made to one of them and they need to contact their counterparts elsewhere to be able to authorize the request or to ensure that the correction or update is made throughout the whole system. When such cooperation between competent authorities is necessary to ensure that access will be provided or corrections will be made, the EWRS system architecture should be taken advantage of: contact points should be able to communicate with each other about access or rectification requests in the same efficient way as when they are exchanging contact tracing information. This may be as simple as adding an additional feature for access requests under the selective messaging channel and explaining how to use it in the training module.

**3.10. Information to the data subject (Articles 11 and 12).** Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. Considering that the EWRS is used in 30 different countries as well as at the ECDC, the Commission and the WHO contact point for Europe, it is essential that consistent information is made available to data subjects regarding the workings of the EWRS, how their data are processed and how they can exercise their rights.

The ECDC/Commission, as the operator of the system is best positioned to play a coordinating role and provide centrally and easily available information on-line, on its website.[12] This should be complemented, whenever possible, by data protection notices provided by competent authorities in Member States according to their applicable laws. In all notices, special attention should be given to contact tracing.

**3.11. Security measures (Article 22)**

**3.11.1. General comments.** The documents provided to the EDPS suggest that the ECDC considered carefully the security dimension of the EWRS application. However, the documents mainly reflect security measures related to the infrastructure and the application. The security measures related to organisation and personnel involved in the management of the application seem to be not documented. The EDPS recommends the ECDC to document in detail also these dimensions and to regroup the infrastructure, technology, personnel and organisation security measures under a single umbrella defining the security policy for EWRS.

Further, the document entitled "Technical security measures for the IT infrastructure of the EWRS" does not always present clearly which measures are applied to EDCD servers, to Steria servers or to both. Part 3.3 related to server security and part 3.5 related to co-location

[12] See, for example, http://ec.europa.eu/internal_market/imi-net/data_protection_en.html, which provides information on the data protection aspects of the Internal Market Information System.

services illustrate well the lack of clarity on this. The EDPS recommends that a clear distinction is made between the security measures applied to Steria and EDCD, and that it is clearly underlined when such security measures apply to both.

**3.11.2. Mobile access to EWRS.** The EDPS agrees that in the light of the details provided, the security level from an application point of view should not decrease in the case of mobile access. However, the environment where this mobile connexion will take place will obviously be different from the traditional and relatively safe office connection. It is therefore necessary to raise awareness of the users regarding the conditions under which this connection will take place. Among others, some mobile operating systems offer also the possibility to keep the username and the password proposing them automatically for each connection. This option should be removed in order to avoid that access to EWRS is directly available in case the mobile device is stolen.

**3.11.3. Backup.** When backup tapes are stored in another location than where they were produced, it is standard security practice to encrypt the tapes before their transport to the end storage facility. This point is not detailed in the document related to technical security measures for the IT infrastructure of the EWRS. The EDPS recommends documenting this if this action is already undertaken. If this is not the case, the EDPS recommends the ECDC to identify the most suitable solution to implement this best practice.

**3.11.4. Security incidents.** A rigorous security incident management procedure (register, escalation plan, etc.) constitutes a powerful and efficient tool for continuous improvement of the security level of the application. Apart from the response time described in the document related to technical security measures and three countermeasures listed in the document entitled application security, a security incident management procedure is not presented in detail in the documents provided. The EDPS recommends the ECDC to develop and document a robust and coherent security incident management procedure.

**3.12. Contacts with data protection authorities in Member States.** It is possible that in some Member States the use of the EWRS by national contact points, in particular, for contact tracing purposes, may be subject to some form of notification or prior authorization requirement, on grounds that the contact points exchange medical data. Therefore, national contact points should consider whether to notify their national data protection authorities or otherwise seek advice regarding their use of the EWRS. To raise awareness on this issue among national contact points, the EDPS recommends that the Commission/ECDC informs national contact points about the potential need to consult national data protection authorities.

**3.13. Verifying and maintaining compliance**. Prior checking is a one-off exercise designed to assist the controller in designing (or re-designing, in case of ex-post prior checks) its system and establishing an appropriate set of data protection safeguards. It is crucial in all cases that once the prior checking and its follow-up has been concluded, controllers remain committed to good data protection practice and maintain compliance by periodically verifying and, when necessary, adjusting their practices.

The EDPS encourages the Commission and the ECDC to continue keeping data protection in mind when further developing the system. This should include further safeguards implemented at the practical level, using the principle of Privacy by design, and also cooperating, as necessary, with stakeholders, including data protection authorities in Member States, to make sure their concerns are addressed. As best practices, audits and periodic reporting would be particularly welcome and encouraged by us as tools to ensure verification of compliance and good administration. When appropriate, it may be useful to raise

significant data protection issues in the periodic reports on the EWRS required under Article 3 of the EWRS Decision.

Finally, we also point out that we view engagement of stakeholders including local data protection authorities, training, awareness raising and transparency as particularly important safeguards to ensure fair processing of data in the EWRS.

**Conclusion**

The EDPS finds no reason to believe that there is a breach of the provisions of the Regulation provided that the recommendations in Section 3 are implemented, namely:

- **Controllers and processors**

  Controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the institutions and bodies involved. It must be specified who is responsible for what, and how data subjects can exercise their rights. In the short term, adoption of a set of data protection guidelines for the EWRS is recommended. The Commission is also encouraged to promote a revision of the legal framework to ensure a more secure legal basis and clear allocation of responsibilities.

- **Data quality and training**

  Data quality should be individually assessed by the users uploading personal data on the EWRS. To facilitate this, data protection should be integrated into the training provided to users and there should also be online tools available for them to rectify any inaccurate data uploaded. In the future, it may also be advisable to provide a more structured format for the exchange of contact tracing information.

- **Retention of data**

  Automatic deletion of contact tracing data, as proposed by the Commission, is welcome. In addition, a facility should be provided to users to delete data earlier than the default one year. In the future there might also be a need for a more differentiated approach regarding different diseases with significantly shorter incubation periods.

- **Access rights of data subjects**

  A clear mechanism should be provided for data subjects to exercise their right of access. The fact that the data subject addressed his/her request to a party other than the one who uploaded the information should not cause undue delay in accommodating his/her request. The mechanism should be simple, user-friendly, and it should be communicated effectively to both the users of the system and to data subjects.

- **Information to data subjects**

  To ensure consistency and transparency, the operator of the EWRS should provide comprehensive and user-friendly information to data subjects on its website. This should

be complemented by notice provided by Member State contact points in accordance with national data protection laws.

- **Security**

Organisational measures related to management and staff should be documented. Clarifications and additional improvements are also necessary with a few specific issues as explained in this Opinion.

- **Cooperation with data protection authorities in Member States**

Data protection authorities in some Member States may need to be contacted by national contact points.

Done at Brussels, on 26 April 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor