"Test run of the Geographic Information System tool at ECDC"

Prior Checking Opinion

Case 2016-0759

***

ECDC's mission is to strengthen Europe's defences against infectious diseases by identifying, assessing and communicating current and emerging threats to human health that they pose. For the purpose of combating the Legionnaires' disease, ECDC has developed a tool which will allow epidemiologists at national level to perform spatial analysis during outbreaks of this disease. Before making the tool available for epidemiologists of the Member States, ECDC will undertake a test run of the tool, using data from an outbreak of the Legionnaires' disease in Norway in 2005, in order to verify its accuracy. During the test run, the data processed will contain personal information related to health since they include geographical coordinates of patients during that outbreak. For this reason, it is important to ensure that there is a specific legal basis for the development of the tool including the test run and that individuals concerned are properly informed of the processing of their health data.

***

Brussels, 17 January 2017

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

1) The facts

The European Centre for Disease Prevention and Control (ECDC) has developed a *Geographic Information System* tool (the GIS tool), which allows epidemiologists to do basic spatial analysis during Legionnaires' disease outbreaks. The purpose of the processing operation submitted for prior checking is a test run of the GIS tool in order to validate its accuracy. For future use of the GIS tool, ECDC will merely act as a processor and host the tool which will be available for use by institutes, authorities and researchers of the Member States.

The test run consists of reproducing the analysis of a published outbreak report[1], using case and potential source locations, from a Legionnaires' disease outbreak in Sarpsborg, Norway, in 2005. The data which will be processed are geographical coordinates of 49 outbreak cases and eight potential sources (cooling towers), population density and data relating to wind velocity and direction at the time of the outbreak. Only data from the 2005 outbreak in Sarpsborg will be processed. According to information received, the data will be transferred from the Norwegian Institute for Public Health (NIPH), which is in possession of the data necessary for testing the GIS tool.

The purpose of the processing operation is to compare the results of the GIS tool developed by ECDC with the published outbreak report containing the investigation results of Norwegian investigators in order to ensure the accuracy of the GIS tool. The aim with the trial run is to test that the GIS tool gives the expected output (map and table similar to the ones in the published outbreak report). As soon as the testing of the tool and reporting of the test is finished, ECDC will delete the data. No personal data will be disclosed when the results of the test run are presented. Furthermore, the comparison will be used to support the formulation of additional requirements for the further development of the tool.

The data collected refer to health data as they include the location (geographical coordinates) of people that were diagnosed with Legionnaires' disease during the 2005 outbreak. Although no name or other personal information accompany the geographical coordinates, the patients concerned are identifiable via their residence location.

In the notification, ECDC states that the test run of the GIS tool is subject to prior checking on the grounds of Article 27(2)(a) since it includes processing of data relating to health. In this regard, ECDC puts forward that '*the combination of data collected could in theory be used to identify individuals providing historical information on their health*'.

2) Legal analysis

This prior checking Opinion[2] under Article 27 of Regulation (EC) 45/2001[3] (the Regulation) will focus on those aspects which raise issues of compliance with the Regulation or otherwise merit further analysis. For aspects not covered in this Opinion, the EDPS has, based on the documentation provided, no comments.

---

[1] http://cid.oxfordjournals.org/content/46/1/61.full

[2] According to Article 27(4) of the Regulation, the EDPS has to provide his Opinion within two months of receiving the notification, not counting suspensions. The notification was received on 1 September 2016. It was suspended from 2 September to 6 September 2016; from 13 September to 11 November 2016 and from 16 December 2016 to 13 January 2017. The EDPS shall thus render his Opinion by 31 January 2017.

[3] OJ L 8, 12.1.2001, p. 1.

a) **Legal basis, sensitive data, lawfulness**

According to the notification, the legal basis for the processing operation is laid down in Articles 3, 5, 9, 10 and 11 of Regulation (EC) 851/2004.[4]

The lawfulness of a processing must be justified on the basis of one of the five legal grounds under Article 5 of the Regulation. The notification does not include any information as to the lawfulness of the test run of the GIS tool. The EDPS considers, however, that the processing under analysis should be considered to be lawful under Article 5(a) of the Regulation.

Pursuant to Article 5(a) of the Regulation, the processing operation must be necessary for the performance of a task carried out in the public interest on the basis of the Treaties or another EU legal instrument.

Moreover, the processing under analysis concerns data related to health, which are considered to be sensitive under the Regulation and whose processing requires a specific legal basis. Article 10(1) of the Regulation prohibits the processing of personal data concerning health, unless grounds can be found under Article 10(2), (3) or (4) of the Regulation.

Article 10(4) of the Regulation provides that '*subject to the provision of appropriate safeguards, and for reasons of substantial public reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down in the Treaties*' or '***other legal instruments adopted on the basis thereof***' (our emphasis).

ECDC's mission is '*to identify, assess and communicate current and emerging threats to human health from communicable diseases*' in order to '*enhance the capacity of the Community and the Member States to protect human health through the prevention and control of human disease.*'[5] Developing the GIS tool seems to fall within the scope of this mission, since (once the test run has been successfully completed), the tool will be made available to epidemiologists in the Member States and allow them to perform spatial analysis during Legionnaires' disease outbreaks. However, this legal basis is not specific enough given that the processing operation concerns sensitive data. The provisions in Regulation 851/2004 do not explicitly cover the development of such a tool and, more particularly, the need to do a test run based on health data relating to actual individuals. There should be an internal ECDC decision or an agreement with the Member States on the development of this specific tool (including the test phase). This legal basis should provide in particular for the development of the tool, its links to ECDC's broader missions, the need to realise a testing phase based on real data, the further use of the tool by national entities and the role of ECDC in this context.[6]

The ECDC should provide the EDPS with a copy of the above internal decision or agreement with the Member States. If no such legal instrument is in place, the ECDC should adopt one.

[4] Regulation (EC) no 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European centre for disease prevention and control (OJ L 142, 30.04.2004, p. 1)
[5] Article 3 of Regulation (EC) 851/2004.
[6] I.e. as processor only, or somehow in charge of managing/improving the tool and therefore as a kind of co-controller.

The EDPS **strongly recommends** the ECDC to ensure that there is a specific legal basis, i.e. an internal ECDC decision or agreement with the Member States, on the development of the GIS tool. If no such legal instrument is in place, the ECDC should adopt one. The EDPS expects to receive a copy of the internal ECDC decision or agreement with the Member States.

b) **Information to data subjects**

Where the data have not been obtained from the data subject, the controller shall provide the data subject with certain information in accordance with Article 12(1) of the Regulation. Paragraph 2 of the same provision provides for an exemption where, in particular for processing for scientific research, the provision of such information proves impossible or would involve a disproportionate effort.

The EDPS welcomes the fact that ECDC intends to provide a data protection notice on the webpage hosting the GIS tool. However, the information required should be provided not only by publishing the data protection notice on the ECDC website as suggested, but also by requesting the data provider, NIHP, to contact directly each data subject, providing them with the data protection notice drafted by ECDC. According to the information provided, less than 50 data subjects are concerned (49 outbreak cases to be analysed). Consequently, it does not seem neither impossible, nor disproportionate, to contact them directly. Therefore, the exemption to the obligation to inform the data subject provided laid down in Article 12(2) does not seem to be applicable in this case, unless NIHP submits that informing the data subjects would indeed be impossible or involve a disproportionate effort.[7]

The EDPS draws ECDC' attention to the fact that in its quality of controller it is ultimately responsible for ensuring the information to data subjects under the Regulation and should therefore ensure that NIHP has properly done it on its behalf.

The EDPS **recommends** that ECDC publish a data protection notice on its website including all relevant information on the test run of the GIS tool. Furthermore, ECDC should request the data provider (NIHP) to contact each data subject directly and provide them with the data protection notice, and confirm to ECDC that it has done so (before the processing operation starts) unless doing so is impossible or would involve a disproportionate effort. The EDPS expects to receive a copy of the data protection notice and of the request to NIHP to provide the data subjects with the data protection notice.

c) **Data subjects' rights**

ECDC states in the notification that requests for exercising the right of access, rectification, blocking, erasing and objecting should be addressed through the provider of the data, i.e. NIHP, since ECDC is not aware of the identity of the data subjects. ECDC indicates that it will include a notice to this effect in the webpage where the GIS tool is hosted, informing the public that since there are no instances in which persons can be uniquely identified from the data held by the GIS tool, requests from these data subjects will be referred to the data provider, which may be able to retrieve the information.

[7] See Case 2015-0082.

The EDPS stresses the fact that, as controller of the test run, ECDC is responsible for ensuring compliance with the Regulation, including granting data subjects' rights. In practice, since it is NIHP which is in a position to identify the data subjects, ECDC should delegate the task of centralising any requests on the GIS tool to NIHP. The latter should, after having checked whether the concerned individual is in the database, submit relevant requests (for access, rectification, blocking and erasure) to ECDC which will grant the rights. This distribution of responsibilities should be laid down in an agreement between ECDC and NIHP and the data protection notice should be drafted so as to clearly reflect this division of tasks.

The EDPS **recommends** that the distribution of responsibilities regarding data subjects' rights should be laid down in an agreement between ECDC and NIHP. Furthermore, this division of tasks should be clearly reflected in the data protection notice.

d) **Security measures**

According to Article 22 of the Regulation, both technical and organisational measures need to be implemented in order to prevent, in particular, any unauthorised disclosure or access, accidental or unlawful destruction, accidental loss or alteration, as well as any other form of unlawful processing. These measures must ensure '*a level of security appropriate to the risks represented by the processing*'.

The EDPS has received ECDC's *Information Security Policy*[8], where the process *Information Security Risk Management* is mentioned and defined. The document also clearly states that this process must be applied to '*all information systems classified as SPECIFIC*'. An information system supporting a processing operation subject to prior-checking like the one at hand, most probably deserves to be considered as such.[9] However, the process previously mentioned has not been applied to this processing operation, neither has an *information security risk assessment* been performed.

ECDC should perform an information security risk assessment following any common information security risk assessment methodology that would cover all information security risks relating to the processing of personal data performed in light of the notification.

The EDPS therefore invites ECDC to take into consideration the following non-exhaustive list:

- Magerit[10],
- EBIOS11, or
- Octave12.

[8] This document is outdated since it states that it should have been reviewed by 29 May 2013.
[9] The classification guidelines on what is *STANDARD* and what is *SPECIFIC* do not allow to establish for sure if *prior-checked* 'systems' should be STANDARD or SPECIFIC.
[10] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VjHuoUbCfw0
[11] http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
[12] http://www.cert.org/resilience/products-services/octave/

These methodologies offer information related to threats, assets, vulnerabilities, etc., and the process in itself that ECDC might consider when performing an information security risk assessment.

The EDPS **recommends** that ECDC perform an information security risk assessment following any common information security risk assessment methodology that would cover all information security risks relating to the processing of personal data performed in light of the notification.

***

3) Recommendations and suggestions for improvement

In this Opinion, the EDPS has made recommendations to ensure compliance with the Regulation. Provided that the above recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

For the following **recommendation**, the EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion:

1. Ensure that there is a specific legal basis, i.e. an internal ECDC decision or agreement with the Member States, on the development of the GIS tool.
2. Publish a data protection notice on the ECDC website including all relevant information on the test run of the GIS tool and request the data provider to contact each data subject directly and provide them with the data protection notice.
3. Lay down the distribution of responsibilities regarding data subjects' rights in an agreement between ECDC and NIHP and ensure that this division of tasks is clearly reflected in the data protection notice.
4. Perform an information security risk assessment following any common information security risk assessment methodology.

Done at Brussels, 17 January 2017

(signed)

Wojciech Rafał WIEWIÓROWSKI