„Testlauf des geografischen Informationssystems beim ECDC“

Stellungnahme zur Vorabkontrolle

Fall 2016-0759

***

Die Mission des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten (ECDC) besteht darin, Europa im Kampf gegen Infektionskrankheiten stark zu machen, indem durch diese hervorgerufene derzeitige und neu auftretende Risiken für die menschliche Gesundheit ermittelt, bewertet und Informationen darüber weitergegeben werden. Zur Bekämpfung der Legionärskrankheit hat das ECDC ein Instrument entwickelt, mit dem Epidemiologen auf einzelstaatlicher Ebene bei Ausbrüchen dieser Krankheit eine räumliche Analyse durchführen können. Bevor das Instrument Epidemiologen der Mitgliedstaaten zur Verfügung gestellt wird, wird das ECDC unter Verwendung von Daten zu einem Ausbruch der Legionärskrankheit in Norwegen im Jahr 2005 einen Testlauf mit dem Instrument durchführen, um dessen Präzision zu prüfen. Die Daten, die bei dem Testlauf verarbeitet werden, werden personenbezogene Informationen zur Gesundheit enthalten, da sie die geografischen Koordinaten der Patienten während dieses Ausbruchs enthalten. Vor diesem Hintergrund muss sichergestellt werden, dass eine spezifische Rechtsgrundlage für die Entwicklung des Instruments sowie für die Durchführung des Testlaufs vorhanden ist und dass die betroffenen Personen ordnungsgemäß über die Verarbeitung ihrer Gesundheitsdaten informiert werden.

***

Brüssel, den 17. Januar 2017

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30 – 1000 Brüssel, Belgien
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

1) Sachverhalt

Das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) hat ein geografisches Informationssystem („GIS-Instrument“) entwickelt, das es Epidemiologen bei Ausbrüchen der Legionärskrankheit ermöglicht, grundlegende räumliche Analysen durchzuführen. Grund der Meldung der Verarbeitung zu einer Vorabkontrolle ist ein Testlauf des GIS-Instruments, um seine Präzision zu prüfen. Bei zukünftigen Verwendungen des GIS-Instruments wird das ECDC lediglich als Auftragsverarbeiter fungieren und das Instrument anbieten, das von Instituten, Behörden und Forschern der Mitgliedstaaten genutzt werden kann.

Bei dem Testlauf wird die Analyse eines veröffentlichten Berichts über einen Ausbruch nachgebildet[1], wobei Positionsdaten der Fälle und der potenziellen Ursprungsorte eines Ausbruchs der Legionärskrankheit im Jahr 2005 in Sarpsborg, Norwegen, verwendet werden. Bei den Daten, die verarbeitet werden sollen, handelt es sich um die geografischen Koordinaten von 49 Ausbruchsfällen und acht potenziellen Ursprungsorten (Kühltürme), Daten zur Bevölkerungsdichte und Daten zur Windgeschwindigkeit und Windrichtung zum Zeitpunkt des Ausbruchs. Es werden ausschließlich Daten von dem Ausbruch in Sarpsborg im Jahr 2005 verarbeitet. Gemäß den vorliegenden Informationen werden die Daten vom norwegischen Institut für öffentliche Gesundheit (Norwegian Institute for Public Health, NIPH) erteilt werden, das über die Daten verfügt, die zur Prüfung des GIS-Instruments benötigt werden.

Der Zweck der Verarbeitung besteht darin, die Ergebnisse des vom ECDC entwickelten GIS-Instruments mit dem veröffentlichten Bericht über den Ausbruch zu vergleichen, der die Forschungsergebnisse norwegischer Wissenschaftler enthält, um so die Präzision des GIS-Instruments zu gewährleisten. Anhand des Testlaufs soll geprüft werden, ob das GIS-Instrument das erwartete Ergebnis liefert (Karte und Tabelle, die denen des veröffentlichten Berichts über den Ausbruch ähneln). Sobald die Prüfung des Instruments und die Berichterstattung zum Test abgeschlossen sind, wird das ECDC die Daten löschen. Bei der Vorstellung der Ergebnisse des Testlaufs werden keine personenbezogenen Daten offengelegt. Daneben wird der Vergleich zur Formulierung zusätzlicher Anforderungen verwendet werden, um die Weiterentwicklung des Instruments zu unterstützen.

Bei den erhobenen Daten handelt es sich um Gesundheitsdaten, denn sie beinhalten die Positionsdaten (geografische Koordinaten) von Personen, bei denen während des Ausbruchs im Jahr 2005 die Legionärskrankheit diagnostiziert wurde. Obgleich zusammen mit den geografischen Daten keine Namen oder sonstigen personenbezogenen Daten genannt werden, können die betroffenen Patienten anhand ihres Wohnorts identifiziert werden.

In der Meldung gibt das ECDC an, der Testlauf des GIS-Instruments unterliege gemäß Artikel 27 Absatz 2 Buchstabe a der Vorabkontrolle, da er die Verarbeitung von Gesundheitsdaten beinhalte. In diesem Zusammenhang führt das ECDC aus, dass *„die Kombination der erhobenen Daten theoretisch dazu verwendet werden könnte, einzelne Personen zu identifizieren und historische Daten zu deren Gesundheit bereitzustellen.“*

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

2) Rechtliche Prüfung

Diese Vorabkontrollstellungnahme[2] gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001[3] („Verordnung") befasst sich vorrangig mit Aspekten, die im Hinblick auf die Einhaltung der Verordnung problematisch sind oder ansonsten einer genaueren Betrachtung bedürfen. Bezüglich der in dieser Stellungnahme nicht behandelten Aspekte sieht der EDSB aufgrund der ihm vorliegenden Unterlagen keinen Äußerungsbedarf.

a) Rechtsgrundlage, sensible Daten, Rechtmäßigkeit

Gemäß der Meldung sind die Artikel 3, 5, 9, 10 und 11 der Verordnung (EG) 851/2004 Rechtsgrundlage für die Verarbeitung.[4]

Die Rechtmäßigkeit einer Verarbeitung muss mit einer der fünf in Artikel 5 der Verordnung genannten rechtlichen Voraussetzungen begründet werden. Die Meldung enthält keine Informationen zur Rechtmäßigkeit des Testlaufs des GIS-Instruments. Allerdings ist der EDSB der Ansicht, dass die analysierte Verarbeitung gemäß Artikel 5 Buchstabe a der Verordnung als rechtmäßig zu betrachten ist.

Gemäß Artikel 5 Buchstabe a der Verordnung muss die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich sein, die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer Rechtsakte der EU im öffentlichen Interesse ausgeführt wird.

Daneben betrifft die analysierte Verarbeitung Daten über Gesundheit, die gemäß der Verordnung als sensibel zu betrachten sind und für deren Verarbeitung eine spezifische Rechtsgrundlage erforderlich ist. Die Verarbeitung personenbezogener Daten über Gesundheit ist gemäß Artikel 10 Absatz 1 der Verordnung untersagt, es sei denn, dass in Artikel 10 Absätze 2, 3 oder 4 der Verordnung Gründe für die Verarbeitung gefunden werden können.

Artikel 10 Absatz 4 der Verordnung sieht Folgendes vor: *„Vorbehaltlich angemessener Garantien können aus Gründen eines wichtigen öffentlichen Interesses andere als die in Absatz 2 genannten Ausnahmen durch die Verträge zur Gründung der Europäischen Gemeinschaften* oder ***andere auf der Grundlage dieser Verträge erlassene Rechtsakte (...) vorgesehen werden"*** (Hervorhebung d. A.).

Der Auftrag des ECDC besteht darin, *„durch übertragbare Krankheiten bedingte derzeitige und neu auftretende Risiken für die menschliche Gesundheit zu ermitteln, zu bewerten und Informationen darüber weiterzugeben"*, um *„die Fähigkeit der Gemeinschaft und der Mitgliedstaaten zu verbessern, die menschliche Gesundheit durch Prävention und Kontrolle menschlicher Erkrankungen zu schützen."*[5] Die Entwicklung des GIS-Instruments scheint in diesen Aufgabenbereich zu fallen, denn das Instrument wird (nach erfolgreicher Durchführung des Testlaufs) Epidemiologen in den Mitgliedstaaten zur Verfügung gestellt werden und es

[2] Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten nach Eingang der Meldung abzugeben (Aussetzungen fallen nicht unter diese Frist). Die Meldung wurde am 1. September 2016 eingereicht. Die Frist wurde vom 2. bis 6. September 2016, vom 13. September bis 11. November 2016 und vom 16. Dezember 2016 bis 13. Januar 2017 ausgesetzt. Der EDSB muss seine Stellungnahme also bis spätestens 31. Januar 2017 abgeben.

[3] ABl. L 8 vom 12.1.2001, S. 1.

[4] Verordnung (EG) Nr. 851/2004 des Europäischen Parlaments und des Rates vom 21. April 2004 zur Errichtung eines Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten (ABl. L 142, 30.04.2004, S. 1).

[5] Artikel 3 der Verordnung (EG) Nr. 851/2004.

diesen ermöglichen, bei Ausbrüchen der Legionärskrankheit räumliche Analysen durchzuführen. Allerdings ist die Rechtsgrundlage nicht spezifisch genug, da sich die Verarbeitung auf sensible Daten bezieht. Die Bestimmungen der Verordnung 851/2004 decken nicht ausdrücklich die Entwicklung eines solchen Instruments ab, insbesondere nicht die Notwendigkeit der Durchführung eines Testlaufs mit Gesundheitsdaten realer Personen. Es sollte ein interner Beschluss des ECDC gefasst oder eine Vereinbarung mit den Mitgliedstaaten zur Entwicklung dieses spezifischen Instruments (einschließlich der Testphase) abgeschlossen werden. Die Rechtsgrundlage sollte insbesondere die Entwicklung des Instruments vorsehen sowie auf seine Verbindungen zu den umfassenderen Aufgaben des ECDC, die Notwendigkeit, eine Testphase mit realen Daten durchzuführen, die weitere Verwendung des Instruments durch nationale Einrichtungen und die Rolle des ECDC in diesem Kontext[6] Bezug nehmen.

Das ECDC sollte dem EDSB eine Abschrift des vorstehend genannten internen Beschlusses oder der Vereinbarung mit den Mitgliedstaaten zur Verfügung stellen. Ist ein derartiges Rechtsinstrument nicht vorhanden, dann sollte das ECDC ein solches verabschieden.

Der EDSB **empfiehlt** dem ECDC **dringend**, das Vorhandensein einer besonderen Rechtsgrundlage sicherzustellen, z. B. in Form eines internen Beschlusses des ECDC oder einer Vereinbarung mit den Mitgliedstaaten zur Entwicklung des GIS-Instruments. Ist ein derartiges Rechtsinstrument nicht vorhanden, dann sollte das ECDC ein solches verabschieden. Der EDSB erwartet, eine Abschrift des internen Beschlusses des ECDC oder der Vereinbarung mit den Mitgliedstaaten zu erhalten.

b) Information der betroffenen Person

Für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, muss der für die Verarbeitung Verantwortliche der betroffenen Person bestimmte Informationen gemäß Artikel 12 Absatz 1 der Verordnung erteilen. Absatz 2 derselben Bestimmung sieht eine Ausnahme vor für den Fall, dass – insbesondere bei Verarbeitungen für Zwecke der wissenschaftlichen Forschung – die Information der betroffenen Person unmöglich ist oder unverhältnismäßigen Aufwand erfordern würde.

Der EDSB begrüßt den Umstand, dass das ECDC beabsichtigt, in die Website, auf der das GIS-Instrument angeboten wird, einen Datenschutzhinweis aufzunehmen. Jedoch sollten die erforderlichen Informationen nicht nur wie vorgeschlagen durch Veröffentlichung des Datenschutzhinweises auf der Website des ECDC zur Verfügung gestellt werden, sondern der Datenlieferant (NIHP) sollte auch aufgefordert werden, sich mit allen betroffenen Personen direkt in Verbindung zu setzen und diesen den vom ECDC verfassten Datenschutzhinweis mitzuteilen. Gemäß den vorliegenden Angaben sind weniger als 50 Personen betroffen (es sind 49 Fälle des Krankheitsausbruchs zu analysieren). Daher scheint eine direkte Kontaktaufnahme mit den betroffenen Personen weder unmöglich zu sein noch unverhältnismäßigen Aufwand zu erfordern. Somit scheint die in Artikel 12 Absatz 2 festgelegte Ausnahme von der Pflicht zur Information der betroffenen Person im vorliegenden Fall nicht anwendbar zu sein, es sei denn, das NIHP argumentiert, die Information der betroffenen Personen sei tatsächlich unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden.[7]

[6] Das heißt lediglich als Auftragsverarbeiter oder als auf irgendeine Weise mit der Verwaltung/Verbesserung des Instruments Betrauter und somit als eine Art Mitverantwortlicher.
[7] Siehe Fall 2015-0082.

Der EDSB macht das ECDC auf die Tatsache aufmerksam, dass es in seiner Eigenschaft als für die Verarbeitung Verantwortlicher letztendlich dafür zuständig ist, sicherzustellen, dass die betroffenen Personen gemäß dieser Verordnung informiert werden, und es sich daher zu vergewissern hat, dass das NIHP diese Informationspflicht in seinem Auftrag erfüllt hat.

Der EDSB **empfiehlt** dem ECDC, auf seiner Website einen Datenschutzhinweis zu veröffentlichen, der alle maßgeblichen Informationen zu dem Testlauf des GIS-Instruments enthält. Daneben sollte das ECDC den Datenlieferanten (NIHP) auffordern, sich mit allen betroffenen Personen direkt in Verbindung zu setzen und diesen den Datenschutzhinweis zu übermitteln und gegenüber dem ECDC die Erfüllung dieser Pflicht zu bestätigen (ehe die Verarbeitung beginnt). Eine Ausnahme besteht dann, wenn dies unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Der EDSB erwartet, eine Abschrift des Datenschutzhinweises und der Aufforderung an das NIHP, den betroffenen Personen den Datenschutzhinweis zu übermitteln, zu erhalten.

c) Rechte der betroffenen Personen

In der Meldung erklärt das ECDC, dass Anträge für die Wahrnehmung des Rechts auf Auskunft, Berichtigung, Sperrung, Löschung und Widerspruch an den Datenlieferanten zu richten sind, d. h. an das NIHP, da das ECDC die Identität der betroffenen Personen nicht kennt. Das ECDC gibt an, dass es diesbezüglich in die Website, auf der das GIS-Instrument angeboten wird, einen Hinweis aufnehmen werde, um die Öffentlichkeit darüber zu informieren, dass Personen in keinem Fall aufgrund der im GIS-Instrument vorhandenen Daten eindeutig identifiziert werden können und daher Anträge der betroffenen Personen an den Datenlieferanten weitergeleitet werden, der unter Umständen die Informationen abrufen kann.

Der EDSB unterstreicht, dass das ECDC als für den Testlauf Verantwortlicher sicherzustellen hat, dass die Bestimmungen der Verordnung eingehalten werden; dazu gehört auch die Wahrung der Rechte der betroffenen Personen. Da das NIHP in der Lage ist, die betroffenen Personen zu identifizieren, sollte das ECDC die Aufgabe der Zentralisierung aller Anträge zum GIS-Instrument an das NIHP übertragen. Letzteres sollte zunächst prüfen, ob die betroffene Person in der Datenbank vorhanden ist, und dann relevante Anträge (auf Auskunft, Berichtigung, Sperren und Löschen) an das ECDC weiterleiten, das diese Rechte dann gewährt. Die Verteilung der Zuständigkeiten sollte in einer Vereinbarung zwischen dem ECDC und dem NIHP festgelegt werden und der Datenschutzhinweis sollte so formuliert werden, dass daraus diese Aufgabenteilung klar hervorgeht.

Der EDSB **empfiehlt**, die Verteilung der Zuständigkeiten bezüglich der Rechte der betroffenen Personen in einer Vereinbarung zwischen dem ECDC und dem NIHP festzulegen. Weiterhin sollte diese Aufgabenverteilung aus dem Datenschutzhinweis klar hervorgehen.

d) Sicherheitsmaßnahmen

Gemäß Artikel 22 der Verordnung sind technische und organisatorische Maßnahmen zu treffen, um insbesondere einer unbefugten Weitergabe, einem unbefugten Zugriff sowie einer zufälligen oder unrechtmäßigen Vernichtung, einem zufälligen Verlust oder einer Veränderung sowie jeder anderen Form der unrechtmäßigen Verarbeitung personenbezogener Daten vorzubeugen. Diese Maßnahmen müssen *„ein Schutzniveau (...) gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.“*

Der EDSB hat die *Informationssicherheitspolitik* des ECDC erhalten[8], in der der Prozess des *Informationssicherheits-Risikomanagements* erwähnt und definiert wird. In dem Dokument heißt es auch ausdrücklich, dass dieser Prozess auf *„alle Informationssysteme, die als SPEZIFISCH eingestuft werden“*, anzuwenden ist. Ein Informationssystem wie das vorliegende, das eine der Vorabkontrolle unterliegende Verarbeitung unterstützt, ist höchstwahrscheinlich als „spezifisch“ einzustufen.[9] Allerdings wurde der vorstehend genannte Prozess nicht auf diese Verarbeitung angewandt und es wurde auch keine *Informationssicherheits-Risikobewertung* durchgeführt.

Das ECDC sollte unter Anwendung einer allgemeinen Methode zur Informationssicherheits-Risikobewertung eine Informationssicherheits-Risikobewertung durchführen, die alle Informationssicherheitsrisiken abdeckt, die mit der gemäß der Meldung vorgenommenen Verarbeitung personenbezogener Daten in Zusammenhang stehen.

In diesem Sinne ersucht der EDSB das ECDC, die folgende, nicht abschließende Liste zu berücksichtigen:

- Magerit[10],
- EBIOS[11] oder
- Octave[12].

Diese Methoden bieten Informationen zu den Bedrohungen, Werten und Schwachstellen usw. und zum Prozess selbst, die das ECDC bei der Durchführung einer Informationssicherheits-Risikobewertung berücksichtigen könnte.

Der EDSB **empfiehlt**, dass das ECDC unter Anwendung einer allgemeinen Methode zur Informationssicherheits-Risikobewertung eine Informationssicherheits-Risikobewertung durchführt, die alle Informationssicherheitsrisiken abdeckt, die mit der gemäß der Meldung vorgenommenen Verarbeitung personenbezogener Daten in Zusammenhang stehen.

***

3) Empfehlungen und Verbesserungsvorschläge

In dieser Stellungnahme hat der EDSB Empfehlungen ausgesprochen, um die Einhaltung der Bestimmungen der Verordnung sicherzustellen. Sofern die oben genannten Empfehlungen umgesetzt werden, besteht nach Auffassung des EDSB kein Anlass zu der Annahme, dass ein Verstoß gegen die Verordnung vorliegt.

---

[8] Dieses Dokument ist nicht mehr aktuell, da es darin heißt, dass es bis zum 29. Mai 2013 überarbeitet werden sollte.
[9] Die Richtlinien zur Einstufung, wann es sich um STANDARD-Systeme und wann es sich um SPEZIFISCHE Systeme handelt, erlauben keine sichere Festlegung, ob vorab geprüfte „Systeme“ STANDARD-Systeme oder SPEZIFISCHE Systeme sind.
[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/

Im Hinblick auf nachstehende **Empfehlungen** erwartet der EDSB deren **Umsetzung sowie dokumentierte Nachweise** dieser Umsetzung innerhalb von **drei Monaten** nach Ergehen dieser Stellungnahme:

1. Sicherstellen des Vorhandenseins einer spezifischen Rechtsgrundlage zur Entwicklung des GIS-Instruments, d. h. in Form eines internen Beschlusses des ECDC oder einer Vereinbarung mit den Mitgliedstaaten.
2. Veröffentlichung eines Datenschutzhinweises auf der Website des ECDC, der alle maßgeblichen Informationen zu dem Testlauf des GIS-Instruments enthält; Aufforderung an den Datenlieferanten, sich mit allen betroffenen Personen direkt in Verbindung zu setzen und diesen den Datenschutzhinweis zu übermitteln.
3. Festlegung der Verteilung der Zuständigkeiten im Hinblick auf die Rechte der betroffenen Personen in einer Vereinbarung zwischen dem ECDC und dem NIHP und Sicherstellung, dass diese Aufgabenteilung klar aus dem Datenschutzhinweis hervorgeht.
4. Durchführung einer Informationssicherheits-Risikobewertung unter Anwendung einer allgemeinen Methode zur Informationssicherheits-Risikobewertung.

Brüssel, den 17. Januar 2017

Wojciech Rafał WIEWIÓROWSKI