Stellungnahme zur Meldung des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten („ECDC“) vom 22. Juli 2009 für eine Vorabkontrolle des Europäischen Überwachungssystems „TESSy“ (The European Surveillance System)

Brüssel, 3. September 2010 (Fall 2009-0474)

1. Verfahren

Am 22. Juli 2009 übermittelte das ECDC dem Europäischen Datenschutzbeauftragten („**EDSB**“) eine Meldung für eine Ex-post-Vorabkontrolle des Europäischen Überwachungssystems für die epidemiologische Überwachung und Kontrolle übertragbarer Krankheiten. Der EDSB bat am 17. Juli 2009 (aufgrund einer Vorabmeldung per E-Mail am 16. Juli 2009) um eine Telefonkonferenz zur Klärung verschiedener Sachlagen. Die Telefonkonferenz fand am 10. September 2009 statt und das ECDC sagte während des Gesprächs zu, weitere Angaben zu liefern. Diese wurden am 14. Oktober 2009 und am 31. März 2010 vorgelegt. Der EDSB übersandte dem ECDC am 26. Mai 2010 eine Zusammenfassung seiner Auffassung zum Sachverhalt, einschließlich verschiedener weiterhin bestehender Fragen zur Klärung. Das ECDC bestätigte den Sachverhalt und beantwortete die Fragen am 17. Juni 2010. Der EDSB verlängerte am 18. Juni 2010 seinen Termin zur Abgabe seiner Stellungnahme um einen Monat. Der EDSB übersandte dem ECDC den Entwurf seiner Stellungnahme am 14. Juli 2010 zur Kommentierung. Das ECDC übermittelte seine Bemerkungen am 21. August 2010.

2. Sachverhalt

2.1. Einführung: Diese Vorabkontrolle umfasst die Datenschutzaspekte von TESSy. TESSy ist ein Kommunikationstool, das vom Europäischen Zentrum für die Prävention und die Kontrolle von Krankheiten („ECDC“) und den EU-Mitgliedstaaten zum Informationsaustausch im Zusammenhang mit der Prävention von „übertragbaren Krankheiten“ dient, die „auf Gemeinschaftsebene relevant“ sind, wie Tuberkulose, Masern, SARS, H1N1 und andere Krankheiten[1]. Insbesondere dient TESSy dazu, eine schnelle und effektive epidemiologische Überwachung zwischen den EU-Mitgliedstaaten sicherzustellen. Es stellt somit ein wichtiges Tool zum Schutz der öffentlichen Gesundheit dar.

2.2. Austausch personenbezogener Daten: Personenbezogene Daten werden in den Mitgliedstaaten über Kontaktstellen (zuständige Gesundheitsbehörden) in TESSy hochgeladen. Dazu verwenden die TESSy-Nutzer zumeist vorgegebene Datenfelder. Freie Textfelder werden seltener verwendet (nur *ad-hoc*, wenn eine wichtige Information nicht in den vorgegebenen Datenfeldern vorgesehen ist). Die vordefinierten Datenfelder enthalten in der Regel die Krankheitsart, das Alter der Patienten, ihr Geschlecht, das Melde- und das Geburtsland und die Nationalität. Je nach Art der Krankheit, oder aus anderen Umständen, wird häufig noch eine Reihe weiterer Datenfelder verwendet. Bei sexuell übertragbaren Krankheiten wird oft auch die

[1] Für Definitionen und weitere Einzelheiten siehe die Dokumente, auf die in Abschnitt 2.3 Bezug genommen wird, in dem die Rechtsgrundlage von TESSy behandelt wird.

sexuelle Orientierung gemeldet. Es gibt auch Datenfelder für Informationen wie „erster positiver HIV-Test“, „Diagnosedatum“, „Sterbedatum“ oder „vermuteter Hauptübertragungsweg“.

Über TESSy werden zwei Arten personenbezogener Daten ausgetauscht: Sammeldaten ohne „Record-ID“ und „fallbezogene Daten“ mit „Record-ID“.

Bei aggregierten Daten werden beispielsweise die Gesamtzahl der Fälle in einem bestimmten Land und der Anteil von Fällen mit bestimmten Merkmalen (Anzahl von Fällen im Alter von 0-5 Jahren, Anzahl von Fällen mit männlichem Geschlecht usw.) erfasst. Bei fallbezogenen Daten handelt es sich um einen Datensatz, der sich auf einzelne Patienten und das einmalige Auftreten einer Krankheit bezieht, zum Beispiel, wenn eine Person mit der Legionärskrankheit infiziert ist. Wenn die Infektion von Patienten während ihrer Lebenszeit mehrmals möglich ist, wird jede dieser Infektionen als Einzelfall behandelt. Beispiele fallbezogener Daten: Alter, Geschlecht, Diagnosedatum, Meldedatum, Ausgang (Todes- oder Überlebensfall).

Die „Record-ID“ ist eine Nummer, die von der hochladenden Partei zugewiesen wird und sich auf einen Datensatz zu einem Einzelfall bezieht (wie beispielsweise ein Patient mit Tuberkulose zu einem bestimmten Zeitpunkt und der Verlauf der Erkrankung). Die soll der hochladenden Partei bei Bedarf die einfache Aktualisierung ermöglichen (wenn beispielsweise die Einzelheiten der nachfolgenden Behandlung oder Genesung von Patienten aufgezeichnet werden sollen). Die „Record-ID“ ist nur den zuständigen Behörden in den Mitgliedstaaten und dem ECDC zugänglich. Sie sind deshalb nicht für andere Empfänger zugänglich, wie die Kommission oder das WHO-Regionalbüro in Europa.

In beiden Fällen werden „Anonymisierungstechniken“ verwendet, um den Datenschutz zu gewährleisten, direkte Identifikatoren zu entfernen und die indirekte Identifizierung der betroffenen Personen unter den gegebenen Umständen so schwierig wie möglich zu machen. Im Wesentlichen bestehen diese Techniken darin, personenbezogene Daten von persönlichen Identifizierungen zu entfernen (nicht nur direkte), um Datenschutzbedenken auszuräumen oder zu reduzieren, nützliche Informationen aber gleichzeitig beizuhalten.

Routinemäßig werden im ersten Schritt alle persönlichen Merkmale wie ID-Nummer, Name, Geburtsdatum usw. eliminiert. Die Techniken gehen jedoch oft viel weiter und machen es zunehmend schwieriger, bestimmte Personen auch nur indirekt zu identifizieren.

Gleichwohl hat das ECDC erklärt, dass es trotz der Anwendung von „Anonymisierungstechniken“ und trotz der Tatsache, dass TESSy nicht dazu dient, Informationen zur Identifizierung von Personen auszutauschen, mitunter erforderlich ist, die Daten relativ „granular“ zu halten anstatt auf einem „höheren“ Aggregationsniveau, um sicherzugehen, dass Daten zum Zweck der Überwachung, für die sie bestimmt sind, hilfreich sind. Aus diesem Grund werden beispielsweise fallbezogene Daten benötigt. Die Notwendigkeit der Granularität erklärt auch, warum beispielsweise bei Krankheiten, denen durch Impfung vorgebeugt werden kann, das Alter bei unter Zweijährigen in Monaten angegeben werden muss (anstatt in Jahren).

Die „Anonymisierungstechniken“ werden in den Mitgliedstaaten vor Übermittlung der Daten an TESSy angewendet (es sei denn, dass dies aufgrund des niedrigen Risikos einer indirekten Identifizierung der betroffenen Personen nicht erforderlich ist). Gleichwohl verbleiben auch nach der Anwendung der „Anonymisierungstechniken“ einige persönliche Identifikatoren in der Datenbank, die zu einer indirekten Identifizierung führen können. Hierzu gehören in der Regel folgende:

- Record-ID (siehe obige Beschreibung)
- Alter
- Geschlecht

Bei bestimmten Krankheiten können zusätzlich Kennungsinformationen gespeichert werden. Zu diesen gehören beispielsweise:

- Sterbedatum
- Alter in Monaten (nur bei unter Zweijährigen und bei Krankheiten, denen durch Impfung vorgebeugt werden kann)
- Geburtsland bzw. Nationalität des Patienten
- Geburtsland bzw. Nationalität der Mutter des Patienten (bei Krankheiten, die von der Mutter auf das Kind übertragen werden können)
- Wohnort (in NUTS-Code-Regionen).

2.3. Rechtsgrundlage: TESSy wurde gemäß der Entscheidung Nr. 2119/98/EG des Europäischen Parlaments und des Rates vom 24. September 1998 über die Schaffung eines Netzes für die epidemiologische Überwachung und die Kontrolle übertragbarer Krankheiten in der Gemeinschaft („**Entscheidung über ein Gemeinschaftsnetz**“) eingerichtet. Im Anschluss daran schufen das Europäische Parlament und der Rat am 21. April 2004 mit der Verordnung (EG) Nr. 851/2004 eine gesonderte Einrichtung, das ECDC, das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten („**ECDC-Verordnung**“). Unter Artikel 5 Absatz 2 der ECDC-Verordnung wird das ECDC als Betreiber des TESSy bestimmt.

2.4. Die Funktionen des ECDC und Kontaktstellen der Mitgliedstaaten: In der Meldung wird das ECDC als Verantwortlicher für die Verarbeitung von Daten im Rahmen des Systems benannt und zugleich wird mitgeteilt, dass das System vom ECDC „betrieben“ wird. Weder in der Entscheidung über ein Gemeinschaftsnetz noch in der ECDC-Verordnung sind Funktionen wie die des „für die Verarbeitung Verantwortlichen“ oder „für die Verarbeitung Mitverantwortlichen“ speziell dem ECDC oder den Behörden der Mitgliedstaaten zugeordnet oder ist die Rolle der Kommission in diesem Zusammenhang definiert. Auch die genauen Funktionen der für die Verarbeitung Verantwortlichen und die Einbeziehung oder die Rolle von eventuellen Auftragsverarbeitern sind darin nicht definiert.

Gleichwohl ist das ECDC der Auffassung, dass die Behörden jedes Mitgliedstaates eine bestimmt Verantwortlichkeit in Bezug auf die Nutzung des TESSy und in Bezug auf die Daten haben, die sie in das System hochladen. Sie sollten in diesem Sinne als separate Verantwortliche für die Verarbeitung von Daten im Rahmen des Systems fungieren. Gleichzeitig wird das ECDC, das TESSy betreibt und die Sicherheit des darin stattfindenden Datenaustauschs gewährleistet, als für die Verarbeitung Verantwortlicher in Bezug auf die Aktivitäten angesehen, für die es verantwortlich ist, wozu auch das Funktionieren und die Sicherheit des Systems gehören.

Des Weiteren erklärte das ECDC, dass es nicht Teil des „EU-Netzes“ sei und deshalb, auch wenn das ECDC das System betreibt und Lesezugriff zu allen Daten in TESSy hat, keinen Schreibzugriff hat und auch keine Daten in TESSy hochladen kann.[2] In Bezug auf die Kommission vertritt das ECDC die Ansicht, dass die Kommission (GD SANCO) genauso wie alle anderen, im nachfolgenden Abschnitt 2.5 (z. B. das WHO-Regionalbüro in Europa oder die

[2] Ausnahmen hierzu sind von den Betreibern der Datenbank vorgenommene Änderungen aufgrund direkter Anweisungen von Mitgliedstaaten (die aufgezeichnet sind). Diese bestehen hauptsächlich aus der Korrektur von Daten, die vom Mitgliedstaat nicht korrekt in TESSy gespeichert wurden und in den Mitgliedstaaten selbst nicht auf einfache Weise korrigiert werden können.

EFSA) aufgeführten, potenziellen „Nurlese-Empfänger“ keine „Funktion als ein für die Verarbeitung Verantwortlicher“ ausübt. Namentlich hat die Kommission keinen Schreibzugang und kann keine Daten in TESSy hochladen. Im Gegensatz zum ECDC ist die Kommission auch nicht für den „Betrieb“ des Systems verantwortlich.

2.5. Empfänger: Derzeit haben in den verschiedenen zuständigen Behörden der Mitgliedstaaten mehr als tausend Nutzer direkten Zugang zu TESSy.

Zusätzlich zu den zuständigen Behörden in den Mitgliedstaaten können das ECDC, die Kommission (GD SANCO) und die WHO ebenfalls direkten Zugang zu TESSy bekommen. Im Falle der WHO sind die Daten dem WHO-Regionalbüro für Europa im Rahmen der Internationalen Gesundheitsvorschriften zugänglich und werden von diesem vertraulich behandelt. Das ECDC erklärte dem EDSB, dass aus diesem Grund keine Daten an die einzelnen WHO-Mitgliedstaaten verschickt werden[3]. Unter der Voraussetzung, dass sie die erhaltenen Daten vertraulich behandeln, haben auch andere EU-Agenturen (wie die EFSA) und die GD GFS direkten Zugang zu den Daten. Der Zugang zu TESSy kann in diesen Fällen direkt sein und in ähnlicher Weise gewährt werden, wie für die zuständigen Behörden in den Mitgliedstaaten. Es sollte ein Vertrag abgeschlossen werden und die Personen, die Zugangsberechtigung erhalten, sollten eine Vertraulichkeitsvereinbarung unterschreiben. Die Veröffentlichung von Daten darf jeweils nur mit Genehmigung des Mitgliedstaates erfolgen, der die Daten zur Verfügung gestellt hat.

Die jeweiligen Kontaktstellen in den Mitgliedstaaten haben sowohl Lese- als auch Schreibzugang, das heißt, sie können Daten hochladen und in TESSy eingestellte Daten überprüfen. Hingegen haben das ECDC, die Kommission (einschl. GD GFS), EU-Agenturen und die WHO Nurlese-Zugang. Sie können Daten in TESSy weder einstellen noch modifizieren.

2.6. Datenübermittlung an Dritte: Datenanfragen von akademischen Institutionen, Universitäten, Nicht-EU-Gesundheitsbehörden, Nichtregierungsorganisationen und Handelsgesellschaften werden vom ECDC bewertet und unterliegen der „Peer-Review“ durch eine Gruppe von drei nationalen Überwachungskoordinatoren und zwei ECDC-Experten, wobei Kriterien angelegt werden, die das ECDC auf seiner Website zu veröffentlichen plant. Nach Unterzeichnung eines Vertrags, in dem die Rechte und Verpflichtungen der Nutzer von TESSy-Daten festgelegt sind, werden die Daten als TESSy-Auszug zur Verfügung gestellt.

2.7. Informationspflicht gegenüber betroffenen Personen: In der Meldung wird – in Anbetracht der Tatsache, dass personenbezogene Daten auf nationaler Ebene erfasst und ohne Kennung (außer der Record-ID) hochgeladen werden – darauf hingewiesen, dass es für das ECDC unmöglich ist, betroffenen Personen Informationen gemäß Artikel 12 der Datenschutzverordnung zu erteilen.

2.8. Auskunftsrechte (einschließlich Berichtigung, Löschung und Sperrung): Das ECDC erklärte, dass es dem ECDC aus demselben Grund nicht möglich ist, betroffenen Personen Auskunftsrechte einzuräumen, personenbezogene Daten zu berichtigen, zu sperren, zu löschen oder deren Nutzung zu widersprechen.

2.9. Aufbewahrungsfristen: In der Meldung wird erklärt, dass die Daten aufgrund ihrer „Anonymität“ unbefristet aufbewahrt werden. Des Weiteren erläuterte das ECDC, dass in den Fällen, in denen korrekte statistische Analysen (insbesondere in Bezug auf Korrelationen) nur

[3] Ausnahmen hierzu bilden HIV/AIDS-Daten, die zur „gemeinsamen Überwachung“ vom ECDC und von den WHO-Regionalbüros für Europa erfasst wurden und deren Daten allen Teilnehmern des HIV/AIDS-Netzes in der WHO-Euro-Region zur Verfügung stehen.

über sehr granulare Daten erfolgen können, die Analyse von Daten immer retrospektiv durchgeführt wird.

2.10. Sicherheitsmaßnahmen: Das ECDC erklärte, dass das Regelwerk zur Datenübermittlung, zum Zugang und zur Verwendung von Daten innerhalb von TESSy durch den Verwaltungsrat des ECDC genehmigt wurde. In dem Regelwerk sind die Zugangsrechte und Verantwortlichkeiten der verschiedenen Nutzer festgelegt. Nach den dem EDSB vorliegenden Unterlagen wird dieses Regelwerk von allen Mitgliedstaaten und der Kommission „nach Überprüfung im Jahr 2010" bestätigt und unterzeichnet werden.

In Bezug auf eine Kopie des für TESSy maßgeblichen Sicherheitsregelwerks erklärte das ECDC auf Anfrage, dass der kürzlich vom ECDC eingestellte IKT-Sicherheitsbeauftragte, ein systembezogenes Sicherheitsregelwerk im Rahmen eines allgemeinen Informations-Sicherheitsregelwerks entwickelt.

3. Rechtliche Aspekte und Empfehlungen

3.1. Anwendbarkeit der Verordnung: Die gemeldete Verarbeitung fällt in Bezug auf die Aktivitäten der Kommission und des ECDC unter die Verordnung (EG) Nr. 45/2001 („**Verordnung**") gemäß ihrer Artikel 2 und 3. Die Verarbeitung personenbezogener Daten durch die Kommission und das ECDC wird vom EDSB überwacht (siehe Verordnung, Artikel 1).[4]

Es ist wichtig anzumerken, dass aufgrund der bei Statistiken üblichen Standardverfahren statistische Daten trotz der verschiedenen, angewendeten „Anonymisierungstechniken" in bestimmten Situationen personenbezogene Daten enthalten können. Der EDSB hat bereits in früheren beratenden Stellungnahmen analysiert[5]: „*auch wenn aus Sicht des Datenschutzes der Begriff der Anonymität Daten einbezieht, die nicht mehr identifizierbar sind* […], *so sind anonyme Daten aus statistischer Sicht Daten, die keine direkte Identifizierung zulassen. Diese Definition impliziert, dass Daten bei einer indirekten Identifizierung aus statistischer Sicht durchaus zu den anonymen Daten zählen.*"

Der erste Schritt besteht normalerweise in der Entfernung direkter und offensichtlich persönlicher Identifikatoren, wie Kennziffern, Geburtsdaten und ähnlichem. Zudem werden oft verschiedene andere „Anonymisierungstechniken" eingesetzt, die eine Identifizierung bestimmter Personen zunehmend erschweren.

Es sei darauf hingewiesen werden, dass Daten trotz dieser Bemühungen als „personenbezogene Daten" angesehen werden, solange Einzelpersonen indirekt identifiziert werden können, dass diese Daten und deshalb der Verordnung unterliegen. Die bloße Tatsache, dass „Anonymisierungstechniken verwendet wurden", bedeutet nicht, dass die Daten im Sinne des Erwägungsgrunds 8 der Verordnung als anonymisiert gelten.[6]

---

[4] Das für die lokalen Kontaktstellen in einem Mitgliedstaat gültige Recht ist das nationale Datenschutzgesetz, das konform mit der Richtlinie 95/46/EG sein muss. Die Verarbeitung personenbezogener Daten durch diese Kontaktstellen wird durch die jeweiligen nationalen Datenschutzbehörden überwacht.

[5] Siehe Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz ABl. C 295 vom 7.12.2007, S. 1 und Stellungnahme vom 20. Mai 2008 zu dem Vorschlag für eine Verordnung über europäische Statistiken (KOM(2007) 625 endg.), ABl. C 308 vom 3.12.2008, S. 1.

[6] Erwägungsgrund 8, hierzu besonders: „*Um festzustellen, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder von jeder anderen Person nach vernünftiger Einschätzung zur Identifizierung der betreffenden Person genutzt werden können*."

Gleichfalls ist es wichtig, auf den Status „verschlüsselter Daten“ Daten hinzuweisen. In diesen Fällen sind Personen „*durch einen Code gekennzeichnet* […], *während der Schlüssel für die Zuordnung des Codes zu den Kennzeichen der Personen (z. B. Name, Geburtsdatum, Adresse) gesondert aufbewahrt wird*“.[7] Dies kann bedeuten, dass in bestimmten Situationen durch die Verwendung von „Codes“ die Beziehung zwischen statistischen Daten oder einem Satz statistischer Daten und personenbezogenen Daten zurückverfolgt werden kann. Gelegentlich ist dies beabsichtigt, wie beispielsweise bei klinischen Versuchen, um die Behandlung von Patienten im Falle schädlicher Gesundheitsauswirkungen zu ermöglichen, oder auch bei Langzeitstudien. Anderweitig ist es nicht erforderlich, dass die Möglichkeit zur Identifizierung von Personen über den Anfangszeitraum hinausgeht, was mitunter zur Überprüfung der Richtigkeit statistischer Daten erforderlich ist. In jedem Fall sollten adäquate technische, organisatorische und rechtliche Maßnahmen getroffen werden, um sicherzustellen, dass die Codes nur zu eindeutigen und hinreichend definierten Zwecken verwendet werden. Solang die Schlüssel nicht vernichtet worden sind und die Möglichkeit zur Wiedererstellung einer direkten Verbindung zu einer Person besteht, können verschlüsselte personenbezogene Daten nicht als vollständig „anonyme“ Daten angesehen werden.

Verschlüsselte Daten haben bei TESSy in zweierlei Hinsicht Relevanz. Erstens kann die zuständige Gesundheitsbehörde, die die Daten ursprünglich hochgeladen hat, betroffene Personen, die mit einer Record-ID versehen sind, bei auf Fällen basierenden Daten identifizieren. Zweitens ist es auch zumindest in einigen Fällen, in denen mehr aggregierte Daten als auf Fällen basierende Daten in TESSy hochgeladen wurden, nach wie vor möglich, dass die zuständigen Behörden der Mitgliedstaaten oder andere (beispielsweise die ursprünglich die Daten gesammelt haben) weiterhin die Schlüssel aufbewahren, die ihnen ermöglichen würden, die betreffenden Personen zu identifizieren.

3.2. Begründung der Vorabkontrolle: Die Verarbeitung erfolgt gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung, in dem unter anderem eine Vorabkontrolle der „Verarbeitung von Daten über Gesundheit“ durch den EDSB gefordert wird.

3.3. Fristen zur Meldung und für die Veröffentlichung der EDSB-Stellungnahme: TESSy wurde bereits vor der Meldung an den EDSB genutzt; diese Vorabkontrolle wird deshalb im Nachhinein durchgeführt und die EDSB-Empfehlungen sollten nachträglich umgesetzt werden. Der EDSB möchte das ECDC darauf aufmerksam machen, dass in Zukunft generell zuerst die Stellungnahme des EDSB eingeholt und abgegeben werden sollte, bevor eine Verarbeitung personenbezogener Daten beginnen kann.

Gemäß Artikel 27 Absatz 4 der Verordnung muss diese Stellungnahme innerhalb von zwei Monaten abgegeben werden, wobei Aussetzungszeiträume für die Wartezeit auf Zusatzinformationen, die der EDSB anfordert, in Abzug gebracht werden. Das Verfahren wurde für 261 Tage ausgesetzt (zusätzlich zu den Augustmonaten 2009 und 2010). Zudem verlängerte der EDSB seine Frist zur Veröffentlichung der Stellungnahme um einen Monat. Die Stellungnahme muss deshalb spätestens am 6. September 2010 vorgelegt werden.

3.4. Rechtmäßigkeit der Verarbeitung (Artikel 5 Buchstabe a der Verordnung): Die Rechtsgrundlage für die Verarbeitung ist im vorhergehenden Abschnitt 2.3 beschrieben. Somit bieten bestimmte Rechtsinstrumente, „die aufgrund der Verträge angewendet“ werden, die Grundbedingungen für die gemeldeten Verarbeitungen. Der EDSB zeigt sich auch damit zufrieden, dass die Verarbeitung von personenbezogenen Daten, nach Anwendung der adäquaten „Anonymisierungstechniken“ (gemäß den Datenschutzrisiken) und anderer in seiner

[7] Als Beispiel siehe Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe, ab Seite 18, über das Konzept personenbezogener Daten.

Stellungnahme dargelegter Sicherheitsmaßnahmen im öffentlichen Interesse zum Schutz der Gesundheit in der Europäischen Union erforderlich und angebracht ist. Die Verarbeitung ist somit rechtmäßig. Gleichwohl ist es empfehlenswert, die Rechtsgrundlage zur Verarbeitung durch Festlegung einer klareren Aufgabenteilung und eindeutigere Zuweisung von Verantwortlichkeiten zu stärken und zu klären, insbesondere zwischen dem ECDC, der Kommission und den Kontaktstellen der Mitgliedstaaten, wie dies im nachfolgenden Abschnitt 3.5 beschrieben wird.

3.5. Zuweisung von Verantwortlichkeiten für den Betrieb und die Nutzung von TESSy: Der EDSB betont in seiner Vorbemerkung, dass es, wann immer personenbezogene Daten bearbeitet werden, äußerst wichtig ist, den für die Verarbeitung Verantwortlichen ordnungsgemäß identifizieren zu können. Dies hat die Artikel-29-Datenschutzgruppe vor kurzem in ihrer Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" betont, die am 16. Februar 2010 angenommen wurde. Der primäre Grund, warum die klare, zweifelsfreie Identifizierung des Prüfers so wichtig ist, liegt darin, dass nur auf diese Weise festzustellen ist, wer für die Einhaltung von Datenschutzvorschriften verantwortlich ist.

In der Stellungnahme der Arbeitsgruppe[8] wird angemerkt: „Wenn nicht ausreichend klar ist, wer welcher Verpflichtung unterliegt – wenn beispielsweise niemand verantwortlich ist oder wenn es mehrere mögliche für die Verarbeitung Verantwortliche gitbt –, dann besteht das offensichtliche Risiko, dass nur unzureichende oder überhaupt keine Maßnahmen durchgeführt werden und die Rechtsvorschriften wirkungslos bleiben". Klarheit ist vor allem in Situationen nötig, wenn verschiedene Teilnehmer in ein kooperatives Verhältnis einbezogen sind. Dies ist oft der Fall, wenn EU-Informationssysteme zu öffentlichen Zwecken eingesetzt werden, deren Verarbeitungszweck in der EU-Gesetzgebung festgelegt ist.

Aus den vorgenannten Gründen empfiehlt der EDSB der Kommission und dem ECDC dringend, die Aufgaben und Verantwortlichkeiten aller Beteiligten an der Verarbeitung von Daten, einschließlich des ECDC, der Kommission und der Kontaktstellen in den Mitgliedstaaten, klar und eindeutig festzulegen. Idealerweise sollte dies mittelfristig in einer rechtsverbindlichen Form in der EU-Gesetzgebung festgelegt werden. Als Zwischenlösung (aber auch um langfristig weitere Einzelheiten zu erhalten, auch wenn weitere Rechtsvorschriften angenommen werden) können Erklärungen auf eine andere, praktischere Weise bereitgestellt werden. Dies kann in verschiedenen Formen geschehen. Eine Möglichkeit wäre, eine Reihe von Datenschutzleitlinien für TESSy zu erlassen. Fachlich gesehen kann dies zum Beispiel durch eine Empfehlung der Kommission erfolgen.[9]

Bei der Zuordnung von Verantwortlichkeiten in den TESSy-Datenschutzleitlinien sollten vor allem folgende Punkte berücksichtigt werden:

- Wer ist für die Sicherstellung der Datenqualität (Verhältnismäßigkeit, Richtigkeit usw.) zuständig?
- Wer kann Aufbewahrungsfristen bestimmen?
- Wer bestimmt, wer Zugang zu Datenbanken haben kann?
- Wer ist bevollmächtigt, Übermittlungen von Daten an Dritte vorzunehmen?
- Wer versendet Mitteilungen an betroffene Personen?

[8] Siehe Seite 7, Abschnitt II.3 der Stellungnahme

[9] Siehe beispielsweise die Datenschutzleitlinien der Kommission für das Binnenmarktinformationssystem unter http://ec.europa.eu/internal_market/imi-net/docs/recommendation_2009_C2041_de.pdf

- Wer ist auf Verlangen der betroffenen Personen für die Auskunft, Berichtigung, das Sperren oder Löschen verantwortlich?
- Wer ist letztendlich für die Sicherheit von TESSy verantwortlich?
- Wer fällt Entscheidungen über die Struktur von TESSy?

Bei all diesen Punkten sollte klargestellt werden, wer bevollmächtigt ist, endgültige Entscheidungen zu treffen und auch, durch wen und auf welche Weise Entscheidungen in der Praxis gefällt werden. Wenn in einem der Aspekte mehrere Parteien einbezogen sind, müssen die Regelungen für ihre Zusammenarbeit und die jeweiligen Verantwortlichkeiten klargestellt werden.

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter sollten auf eine Weise klar dargestellt werden, die ihrer effektiven Funktion wie auch dem rechtlichen Status der beteiligten Organe und Einrichtungen entspricht.

Letztendlich sollten die Leitlinien in Anbetracht der Anzahl der verschiedenen beteiligten Parteien, und unter vollständiger Anerkennung der Funktion, die die nationalen Datenschutzbehörden unter Umständen für die Sicherstellung der Einhaltung durch die nationalen Kontaktstellen innehaben, auch als Mittel dienen, bewährte Verfahrensweisen und ein konstante und transparente Vorgehensweise zu fördern.

3.6. Datenqualität (Zweckentsprechung, Erheblichkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Rechtmäßigkeit, Zweckbegrenzung, sachliche Richtigkeit: Artikel 4 Absatz 1 Buchstabe a, b, c und d):

Im Allgemeinen ist der EDSB mit der Struktur von TESSy im Zusammenhang mit der Datenqualität zufrieden und hat keine Fehler im System entdeckt, die zu wesentlichen Qualitätsproblemen führen können.

Gleichwohl erfordert die Einhaltung der Datenqualität kontinuierliche Bemühungen und Aufmerksamkeit. Jeder Nutzer des Systems mit Schreibzugang ist persönlich für die Qualität der von ihm hochgeladenen Daten verantwortlich. Zur Vereinfachung der Einhaltung durch die verschiedenen Nutzer empfiehlt der EDSB, dass die Datenschutzelemente Bestandteil aller Schulungen für die Nutzer des Systems sein sollten. Dazu gehören unter anderem Informationen darüber,

- wie sichergestellt wird, dass nur die erheblichen und keine zusätzlichen Daten in der Datenbank aufgezeichnet werden (z. B. dass geeignete Anonymisierungstechniken verwendet werden);
- wie sichergestellt wird, dass falsche Daten berichtigt und aufgezeichnete Daten aktuell gehalten werden;
- wie betroffene Personen informiert werden; und
- wie ihnen auf Anfrage Auskunft über ihre personenbezogenen Daten erteilt wird.

Die nationalen Kontaktstellen sollten auf das Bestehen von TESSy-Leitlinien und die Wichtigkeit der Einbeziehung des Datenschutzes in die Schulungen der Nutzer des Systems hingewiesen werden. Diese Leitlinien sollten in den TESSy-Schnittstellen gut sichtbar bereitgestellt werden und sollten optimaler Weise praktische Beispiele enthalten.

Der EDSB möchte die ECDC auch besonders darauf hinweisen, dass leere Textdatenfelder sorgfältig bearbeitet werden sollten, damit das Datenschutz-Risikoniveau ähnlich niedrig ist wie

in der restlichen Datenbank – z. B. sollten alle persönlichen Identifikatoren entfernt werden und in den Daten dürfen keine Sonderfälle enthalten sein.

3.7. Datenaufbewahrung (Artikel 4 Absatz 1 Buchstabe e): Der EDSB empfiehlt, dass Record-IDs sofort gelöscht werden, sobald sie nicht mehr zur Aktualisierung der Datenbank benötigt werden. Die Löschung sollte automatisch erfolgen, ihre Kriterien sollten klar festgelegt und es sollte sichergestellt werden, dass sie in die Systemarchitektur „eingebaut" ist.

Der EDSB hat, abgesehen von Record-IDs, zum gegenwärtigen Zeitpunkt, vorbehaltlich technischer und anderer Entwicklungen, keinen Einwand gegen die Aufbewahrung von Daten für einen unbestimmten Zeitraum, sofern Anonymisierungstechniken verwendet werden und der Zugang zu den Daten beschränkt und sicher ist, wie bereits in dieser Stellungnahme beschrieben.

3.8. Empfänger und Datenübermittlung: Der EDSB begrüßt die Tatsache, dass Beschränkungen hinsichtlich der Empfänger und der möglichen Empfänger von Daten, wie in Abschnitt 2 beschrieben, eingeführt und dass Sicherheitsmaßnahmen vorgeschlagen wurden, um sicherzustellen, dass übermittelte Daten vertraulich bleiben und nur zu den vorgesehenen Forschungszwecken verwendet werden. Insbesondere begrüßt der EDSB, dass ein bestimmtes Verfahren („**Peer Review**") eingesetzt wird, mit dem über Zugangsanfragen anhand von transparenten Kriterien (die noch nicht festgelegt und veröffentlicht sind) entschieden wird. Der EDSB begrüßt auch, dass die Daten nur nach Unterzeichnung eines Vertrags zugänglich sind, in dem die Rechte und Verpflichtungen der Nutzer von TESSy-Daten festgelegt sind.

In der Tat sind diese Sicherheitsmaßnahmen erforderlich, um den Datenschutz der betroffenen Personen zu gewährleisten, wenn Daten, die an Dritte weitergegeben werden, nicht vollständig „anonym" sind.

Der EDSB betont, dass die Notwendigkeit der Übermittlung gemäß Artikel 8 Buchstabe b der Verordnung angemessen begründet sein sollte. Letztendlich ist es von Bedeutung, dass i) Übermittlungen wirklich zu tatsächlichen Forschungszwecken erfolgen, dass die Forscher ii) die Vertraulichkeit der Daten sicherstellen und iii) sie nur zu den angegebenen Forschungszwecken verwenden. Das Verfahren der Peer-Review sollte unter anderem einschließen, dass der Antragsteller einen Forschungszweck angibt, die Peer-Reviewer die Identität und entsprechende Berechtigung des Forschers überprüfen (z. B. ob er oder sie einem Forschungsinstitut angeschlossen ist), diese eine Vertraulichkeitserklärung unterzeichnen usss und für die Sicherheit der Daten sorgt (z. B. durch eine sichere Internetverbindung oder Verschlüsselung von Daten, die in einem Medienbericht enthalten sind). Es sei darauf hingewiesen, dass Forscher bei jeglicher Verarbeitung nach der Übermittlung ihrer eigenen nationalen Gesetzgebung unterliegen, einschließlich Bedingungen für die Überwachung, Haftung und Durchsetzung. Gleichwohl empfiehlt der EDSB, dass der Vertrag auch angemessene Sanktionen enthält, wenn sich herausstellen sollte, dass Forscher oder Organisationen die gegebenen Zusicherungen nicht eingehalten haben.

Zusätzlich möchte der EDSB die Kommission und das ECDC daran erinnern, dass die internationale Übermittlung von Daten, insbesondere Datenübermittlungen an die WHO, nur gemäß Artikel 9 der Verordnung erfolgen dürfen. Der EDSB empfiehlt dem ECDC, die Möglichkeiten für die Einhaltung dieses Artikels im Rahmen des Follow-up zu dieser Stellungnahme zur Vorabkontrolle gemeinsam mit ihren Datenschutzbeauftragten (**DSB**) zu prüfen.

3.9. Auskunftsrecht und Berichtigung (Artikel 13): Obwohl die Daten statistischer Art sind (auch, wenn sie nur indirekt zu einer Identifizierung führen können) sollte das ECDC überdenken, ob nicht Situationen entstehen können, in denen betroffene Personen Auskunft über ihre Daten verlangen, diese Daten berichtigen möchten oder deren Nutzung widersprechen. Für diese Fälle sollten entsprechende Maßnahmen getroffen werden, auch wenn Anträge auf Auskunft eher selten sein werden. Dies sollte sowohl in den Datenschutzleitlinien für TESSy als auch auf der TESSy-Website der GD SANCO (bzw. des ECDC) enthalten sein und zudem den Nutzern der Anwendung ausgehend von der TESSy-Anwendung zur Verfügung stehen. Zumindest sollte für jede Organisation, die mit TESSy arbeitet, eine Kontaktperson angegeben sein, die für Anträge auf Auskunft zuständig ist. Bei der Zuweisung der Verantwortlichkeiten an verschiedene Parteien sollte, wie in Abschnitt 3.5 oben vorgeschlagen, überlegt werden, wer am besten geeignet ist, betroffenen Personen Auskunft zu geben (beispielsweise kann ausschließlich die Organisation, die die Daten ursprünglich hochgeladen hat, die statistischen Daten mithilfe ihres Schlüssels mit der betroffenen Person verknüpfen).

3.10. Informationspflicht gegenüber betroffenen Personen (Artikel 11 und 12): Gemäß Artikel 11 und 12 der Verordnung müssen betroffenen Personen bestimmte Informationen bereitgestellt werden, um die Transparenz der Verarbeitung personenbezogener Daten sicherzustellen. In Anbetracht der Tatsache, dass TESSy in 30 verschiedenen Ländern und vom ECDC, von der Kommission und der Kontaktstelle der WHO für Europa benutzt wird, ist es äußerst wichtig, dass Informationen, die betroffenen Personen über die Arbeit von TESSy bereitgestellt werden und die Art der Verarbeitung ihrer Daten einheitlich sind, wozu auch die Art und Weise gehört, wie sie ihre Rechte ausüben können.

Das ECDC ist als Betreiber des Systems besonders geeignet, die Koordinierung zu übernehmen und auf seiner Webseite zentral und online leicht zugängliche Informationen zu bieten[10]. Dies sollte, soweit möglich, von Datenschutzhinweisen begleitet werden, die von den zuständigen Behörden in den Mitgliedstaaten gemäß ihrer gültigen Rechtsprechung bereitgestellt werden.

3.11. Sicherheitsmaßnahmen (Artikel 22): Der EDSB empfiehlt dem ECDC die Entwicklung eines eigenständigen Sicherheitsregelwerks für TESSy. Grundlage dieses Regelwerks sollte eine genaue Risikobewertung sein, die potenzielle Bedrohungen für das System und seine Kommunikationsfuntion identifiziert. Hierbei sollten verbindliche Sicherheitsmaßnahmen für die Einführung festgelegt und bereits vorhandene Maßnahmen bewertet werden. Dieses Sicherheitsregelwerk sollte das bereits bestehende Regelwerk für das Auskunftsrecht ergänzen und – unter anderem – auch die Verwendung von Protokolldateien der Anwendung, die Sicherheit der Kommunikation zwischen Nutzern und dem System und die Verwaltung der Administratorrechte für das System klären.

Auch das Verfahren des ECDC zur Änderung bzw. Korrektur von Daten auf Verlangen eines Nutzers in einem Mitgliedstaat (als Ausnahme für Aktivitäten von Nutzern in den Mitgliedstaaten, die für diese mit den vorhandenen Tools schwierig oder unmöglich ist) sollte detailliert dokumentiert werden. Der EDSB begrüßt die Tatsache, dass dieses Verfahren protokolliert wird, wenngleich das ECDC die Möglichkeit prüfen sollte, diese Verfahrensweise für die Zukunft generell zu vermeiden und den Mitgliedstaaten alle erforderlichen Tools zur Verfügung zu stellen, damit diese die Daten in allen Fällen selbst korrigieren können.

In Anbetracht der großen Anzahl von Nutzern (etwa eintausend) und der Interaktion zwischen dem ECDC und den Mitgliedstaaten bei der Verwaltung dieser Nutzer empfiehlt der EDSB dem ECDC, die Möglichkeit zu prüfen, ob ein zeitlich begrenzter Nutzerzugang implementiert

[10] Als Beispiel, wie Informationen über Aspekte des Datenschutzes des Binnenmarktinformationssystems gehandhabt werden, siehe http://ec.europa.eu/internal_market/imi-net/data_protection_de.html

werden kann. Wer Nutzer benennt, sollte die Möglichkeit haben, die Erstellung eines Nutzerkontos anzufordern und eine Frist zu setzen, nach der das Konto automatisch geschlossen wird. Bei Konten, die zeitlich unbegrenzt gehalten werden, sollte das ECDC denjenigen, der die Nutzer benennt, regelmäßig auffordern, die Liste der Nutzer zu überprüfen und zu bestätigen. (In einem Kommentar zum Entwurf der Stellungnahme des EDSB bestätigte das ECDC, dass es gegenwärtig den zweiten Ansatz verfolgt, d. h., solange Konten zeitlich unbegrenzt geführt werden, sind regelmäßige Überprüfungen vorgesehen.)

Schlussfolgerungen

Der EDSB ist nicht der Ansicht, dass eine Verletzung von Bestimmungen der Verordnung vorliegt, vorausgesetzt, dass folgende, in Abschnitt 3 erläuterte Empfehlungen umgesetzt werden:

- **Zuweisung von Verantwortlichkeiten**

  Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter sollten auf eine Weise klar angegeben werden, die ihrer tatsächlichen Aufgabe und dem rechtlichen Status der beteiligten Organisationen entspricht. Es sollte spezifiziert werden, wer wofür zuständig ist und wie betroffene Personen ihre Rechte ausüben können. Die Annahme einer Reihe von Datenschutzleitlinien für TESSy wird empfohlen.

- **Datenqualität und Schulung**

  Die Datenqualität sollte von den Nutzern, die personenbezogene Daten in TESSy hochladen, bewertet werden. Um dies zu erleichtern, sollte der Datenschutz Bestandteil der Nutzerschulungen sein.

- **Datenaufbewahrung**

  Record-IDs sollten automatisch gelöscht werden, wenn ihre Verwendung nicht mehr erforderlich.

- **Datenübermittlung an Dritte**

  In Bezug auf die Datenübermittlung an Dritte und die WHO sollten zusätzliche Sicherheitsmaßnahmen, wie in Abschnitt 3.8 beschrieben, implementiert werden.

- **Auskunftsrechte betroffener Personen**

  Obwohl die Daten statistischer Art sind, sollte das ECDC überdenken, ob nicht Situationen entstehen können, in denen betroffene Personen Auskunft über ihre Daten verlangen, diese Daten berichtigen möchten oder deren Nutzung widersprechen. Für diese Fälle sollten entsprechende Maßnahmen getroffen werden, auch wenn Anträge auf Auskunft eher selten sein werden. Zumindest sollte für jede Organisation, die mit TESSy arbeitet, eine Kontaktperson angegeben sein, die für Anträge auf Auskunft zuständig ist.

- **Informationspflicht gegenüber betroffenen Personen**

  Um Kohärenz und Transparenz zu gewährleisten, sollte der Betreiber von TESSy umfangreiche und nutzerfreundliche Informationen für betroffene Personen auf seiner Webseite bereitstellen. Diese sollten von Hinweisen begleitet werden, die von den

Kontaktstellen der Mitgliedstaaten gemäß den nationalen Datenschutzgesetzen zur Verfügung gestellt werden.

- **Sicherheit**

Zur Gewährleistung der Sicherheit von TESSy und um eine gute Verwaltung zu belegen und zu dokumentieren, sollte so schnell wie möglich ein eigenständiges Sicherheitsregelwerk angenommen werden. Falls die festgesetzte Frist von drei Monaten für das Follow-up zu den Empfehlungen dieser Stellungnahme nicht zur Annahme und Umsetzung eines derartigen Regelwerks ausreicht, sollte das ECDC innerhalb von drei Monaten über die bis dahin getroffenen Maßnahmen berichten und dem EDSB einen klaren Plan (einschließlich offener Punkte und Fristen) zur endgültigen Annahme und Umsetzung vorlegen.

Brüssel den 3. September 2010

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter