

Stellungnahme zur Meldung des Datenschutzbeauftragten der Europäischen Zentralbank für eine Vorabkontrolle des „Verfahrens bei Unfällen und Berufskrankheiten“

Brüssel, den 20. Februar 2014 (Fall 2012–0792)

1. Verfahren

Am 14. September 2012 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) der Europäischen Zentralbank („EZB“) eine Meldung zur Vorabkontrolle im Sinne von Artikel 27 Absatz 3 der Verordnung (EG) Nr. 45/2001 („Verordnung“) betreffend das „Verfahren bei Unfällen und Berufskrankheiten“.

Nach Eingang der Meldung standen der EDSB und der DSB zur weiteren Information und Klärung hinsichtlich der vorliegenden Verarbeitung mehrmals miteinander in Kontakt.

Der Entwurf der Stellungnahme wurde dem DSB am 4. Februar 2014 zur Kommentierung vorgelegt. Die Antwort ging am 12. Februar 2014 beim EDSB ein.

2. Sachverhalt

Zweckbestimmung und betroffene Personen

Die GD Personal, Budget und Organisation („GD-H“) ist für die Verwaltung der Verfahren im Zusammenhang mit der Anerkennung von Arbeitsunfällen und Berufskrankheiten zuständig, um die Zahlung von Leistungen und die Erstattung medizinischer Ausgaben an die betreffenden Personen sicherzustellen.

Die betroffenen Personen sind die Bediensteten der EZB (und, insofern beteiligt, ihre Ehepartner, anerkannten Lebenspartner und/oder anspruchsberechtigten Kinder), die Mitarbeiter mit befristeten Arbeitsverträgen, die Teilnehmer am Graduiertenprogramm der EZB, mögliche Zeugen und (gegebenenfalls geschädigte) Dritte im Zusammenhang mit einem Unfall.

Rechtsgrundlage

Die Rechtsgrundlage für die Verarbeitung ist die Folgende:

- Artikel 7, 10, 16, 19, 28, 31, 32, 33 und 34 der Beschäftigungsbedingungen für das Personal der EZB;
- Anhang IV der Beschäftigungsbedingungen für das Personal der EZB und
- Artikel 12, 27, 28, 29 und 30 der Bedingungen für befristete Arbeitsverhältnisse für das Personal der EZB.

Verfahren und verarbeitete Daten

Die Informationen werden zunächst manuell und auf Papier erfasst (z. B. Arztberichte). Diese Informationen werden dann in eine Softwaredatenbank eingescannt.

Im Falle eines Arbeitsunfalls oder einer Berufskrankheit sollten betroffene Personen das Unfallmeldeformular oder den Antrag auf Anerkennung einer Berufskrankheit beim Bereich Gesundheit und Sicherheit der GD-H einreichen.

Sie sollten ferner ein ärztliches Attest und etwaige andere unterstützende Unterlagen in einem verschlossenen Umschlag beim medizinischen Berater der EZB einreichen. Auf der Grundlage des medizinischen Fachgutachtens eines oder mehrerer Ärzte (aus dem medizinischen Dienst der EZB oder externer Ärzte) fällt der Generaldirektor der GD-H oder sein Stellvertreter die endgültige Entscheidung über die Anerkennung eines Arbeitsunfalls, darüber, ob eine Krankheit berufliche Ursachen hat, und über die Festlegung des Grades permanenter Invalidität nach der Konsolidierung der Schäden.

Bei dem medizinischen Berater und den externen Ärzten der EZB handelt es sich um unabhängige medizinische Sachverständige, für die das Recht des EU-Mitgliedstaats gilt, in dem sie arbeiten. In Deutschland beispielsweise gilt für sie eine vertragliche und gesetzliche Ordnung, die sie nach § 203 Abs. 1 Nr. 1 des deutschen Strafgesetzbuchs (StGB) zu strenger Geheimhaltung und zur Wahrung von Dienstgeheimnissen verpflichtet. Ihre offizielle Ernennung erfolgt durch den Generaldirektor der GD-H oder seinem Stellvertreter (und/oder durch den Präsidenten der Hessischen Landesärztekammer im Falle von Einsprüchen), die „*Die Ernennungsurkunde zum medizinischen Sachverständigen*“ ausstellen. Durch „*Die Ernennungsurkunde zum medizinischen Sachverständigen*“ wird zwischen der EZB und den externen Ärzten (medizinische Sachverständige) ein stillschweigender Vertrag abgeschlossen, der die Datenschutzaspekte abdeckt (die sich auf Artikel 10 der Verordnung beziehen).

Zwischen den ernannten externen Ärzten und der GD-H erfolgt außer rein verwaltungstechnischen Elementen des Verfahrens, d. h. dem Einreichen von Unterlagen, der Zahlung von Auslagen usw., keine direkte Kommunikation. Die externen Ärzte/Sachverständigen übermitteln ihre medizinischen Befunde dem medizinischen Berater der EZB. Auf der Grundlage dieser medizinischen Befunde erstellt dieser nicht geheimhaltungspflichtige Informationen für die Verantwortlichen im Bereich Gesundheit und Sicherheit der GD-H.

Im Falle eines Einspruchsverfahrens gibt der Medizinische Ausschuss nach Abschluss seiner Beratungen (gemäß Artikel 6.6 der Beschäftigungsbedingungen für das Personal der EZB) seine Stellungnahme in Form eines ärztlichen Berichts ab. Durch den Medizinischen Ausschuss geht auch eine Zusammenfassung dieses Berichts mit nicht geheimhaltungspflichtigen Informationen an die Verantwortlichen des Bereichs Gesundheit und Sicherheit der GD-H.

Bei nicht berufsbedingten Unfällen sollte die geschädigte Person eine Schadensmeldung **über einen externen Administrator bei einem externen Versicherer** einreichen. Die Aufgaben des Versicherers beschränken sich auf Streitbeilegung und Risikoübernahme. Der externe Administrator stellt der GD-H nicht geheimhaltungspflichtige Informationen über Unfälle der betroffenen Personen für statistische Zwecke, Vertragsmanagement und Beschaffungsdienste bereit; diese sind 1.) Bedienstete, die den Unfall meldeten, 2.) Zeitpunkt des Unfalls, 3.) Art des Unfalls, 4.) ob der Unfall zu permanenter Invalidität führte und gegebenenfalls die Entschädigungshöhe und 5.) gegebenenfalls die begründete Verweigerung der Anerkennung eines Unfalls. Die EZB hat mit dem externen Versicherer und dem externen

Administrator, für die beide das Recht eines der EU-Mitgliedstaaten gilt, einen Vertrag geschlossen, und der Vertrag enthält Datenschutz-, Geheimhaltungs- und Sicherheitsbestimmungen.

Darüber hinaus hat die EZB mit **einem anderen externen Administrator** einen Vertrag für die Erstattung medizinischer Auslagen als Teil der Kranken- und Zahnversicherung der EZB geschlossen. Dem externen Administrator gehen Anspruchsformulare für die Erstattung von medizinischen Auslagen zusammen mit Rechnungen von den Bediensteten direkt zu und er leistet die entsprechenden Erstattungszahlungen. Für den Vertrag gelten nationale Rechtsvorschriften, und er enthält Bestimmungen zu Datenschutz, Geheimhaltung und Sicherheit.

Andere verarbeitete Daten

Abgesehen von Verwaltungs- und Unfalldaten der betroffenen Person müssen dem Unfallmeldeformular auch der Polizeibericht, falls verfügbar, Name und Adresse des/der Zeugen sowie Name, Adresse und Versicherer von am Unfall beteiligten (gegebenenfalls geschädigten) Dritten beigelegt werden.

Ferner muss der Antrag auf Erstattung von medizinischen Auslagen u. a. auch den Namen des Ehepartners, des anerkannten Lebenspartners bzw. oder anspruchsberechtigter Kinder enthalten, falls diese bei einem Unfall mit dem Bediensteten ebenfalls zu Schaden kamen.

Alle Verantwortlichen im Bereich Gesundheit und Sicherheit der GD-H und alle Mitarbeiter des medizinischen Dienstes der EZB haben Geheimhaltungserklärungen unterschrieben, nach denen sie der beruflichen Schweigepflicht unterliegen. Diese Geheimhaltungserklärungen enthalten auch Verweise auf Bestimmungen der Verordnung.

Empfänger

Nach dem obigen Verfahren sind die Folgenden Empfänger der verarbeiteten Daten:

Extern

- der medizinische Berater der EZB, der sowohl alle ärztlichen Atteste und eine Liste von vorausgegangenen medizinischen Untersuchungen der betroffenen Personen als auch das Antragsformular zur Anerkennung einer Berufskrankheit erhält;
- die externen Ärzte erhalten dieselben Informationen wie der medizinische Berater der EZB;
- der externe Unfallversicherer, der über den externen Administrator ein Unfall- oder Berufskrankheitsmeldeformular, unterstützende ärztliche Atteste nach dem Arztbesuch, ärztliche Atteste, die im Laufe des für die Stabilisierung des Gesundheitszustands relevanten Arbeitsunfall- und Berufskrankheitsverfahrens ergehen, sowie ärztliche Atteste über die Feststellung des Grades einer permanenten Invalidität erhält;
- der externe Administrator der Kranken- und Zahnversicherung der EZB, dem von den Bediensteten Antragsformulare zur Erstattung von medizinischen Auslagen zusammen mit Rechnungen zugehen.

Auskunftsrecht und Berichtigung

Betroffene Personen können ihre medizinischen Daten, die beim medizinischen Berater der EZB verwahrt werden, einsehen und Kopien davon machen. Sie dürfen auch ihre personenbezogenen Daten, die bei der GD-H verwahrt werden, einsehen.

Sie verfügen ferner über ein Berichtigungsrecht sowie über das Recht, ihrer medizinischen Akte Gegengutachten durch einen anderen Arzt oder einen diesbezüglich relevanten Gerichtsbeschluss beizufügen.

Informationspflicht

Die Datenschutzerklärung für Gesundheitsdaten enthält Verweise auf einige der Informationen, die in den Artikeln 11 und 12 der Verordnung aufgeführt sind.

Sie erscheint auf allen Formularen (Meldeformular für Arbeitsunfälle, Meldeformular für nicht arbeitsbedingte Unfälle, Antragsformular zur Anerkennung einer Berufskrankheit), die im Intranet öffentlich verfügbar sind.

Aufbewahrungspolitik

Alle Verwaltungs- und Finanzdaten eines Bediensteten werden ab dem Ende seines Beschäftigungsverhältnisses mit der EZB bzw. nach der letzten Rentenzahlung für eine Dauer von höchstens zehn Jahren in der Personalakte aufbewahrt.

Ärztliche Atteste und gesundheitsbezogene Unterlagen im Zusammenhang mit Unfällen oder Berufskrankheiten werden ab dem Datum ihres Einreichens für eine Dauer von fünf Jahren aufbewahrt.

Medizinische Akten in Papierform werden nach Schließung der Akte für eine Dauer von 30 Jahren aufbewahrt. In der **medizinischen Software** enthaltene Daten werden nach Schließung der Akte für eine Dauer von zehn Jahren gespeichert.

Gemäß den Erläuterungen des DSB der EZB gehen die EZB-Regeln über die Aufbewahrung zurzeit nicht spezifisch auf medizinische Akten in Papierform ein, sondern nur allgemein auf personenbezogene Daten. Hinsichtlich des Aufbewahrungszeitraums der medizinischen Akte hat die EZB das Verfahren zur Änderung der EZB-Dienstordnung über den Aufbewahrungszeitraum von medizinischen Akten eingeleitet. Der Aufbewahrungszeitraum der medizinischen Daten in Papierform wird an den für medizinische Daten in elektronischer Form geltenden Zeitraum angeglichen.

Gemäß der Meldung ist eine weitere Verarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken nicht beabsichtigt. Wie aus Vorstehendem (Seite 2) hervorgeht, sowie auf der Grundlage weiterer Informationen von dem für die Verarbeitung Verantwortlichen, erhält die GD-H jährlich von dem externen Administrator aggregierte anonyme Daten über Versicherungsfälle und Versicherungsleistungen für statistische, Vertragsverwaltungs- und Beschaffungszwecke.

Aufbewahrung und Sicherheitsmaßnahmen

Medizinische Akten werden im medizinischen Dienst der EZB in verschlossenen Schränken (feuerfesten Schränken) aufbewahrt. Medizinische Daten werden auch in elektronischer Form in der medizinischen Software gespeichert; sie enthalten alle zusätzlichen medizinischen Berichte, die Berichte des medizinischen Beraters der EZB sowie die endgültige Entscheidung des Generaldirektors der GD-H oder seines Stellvertreters. Nur der medizinische Berater und das Krankenpflegepersonal haben Zugriff auf die medizinische Akte der betroffenen Person und die medizinische Software. Die elektronischen Daten werden verschlüsselt in der Datenbank gespeichert; Benutzer und Änderungen müssen vom medizinischen Dienst der EZB ermächtigt und genehmigt werden.

Unfallmeldeformulare, vom medizinischen Berater der EZB oder einem anderen Arzt ausgestellte Krankmeldungen, Anträge zur Anerkennung einer Berufskrankheit und die vom Generaldirektor der GD-H gefassten endgültigen Entscheidungen werden getrennt in einem Sonderteil der Personalakte verwahrt. Zugriff auf diesen Teil wird nur Verantwortlichen des Bereichs Gesundheit und Sicherheit der GD-H gewährt. Personalakten werden in Sicherheitsschränken verwahrt.

3. Rechtliche Aspekte

3.1 Vorabkontrolle

Anwendbarkeit der Verordnung: Die analysierte Verarbeitung von Daten ist eine Verarbeitung personenbezogener Daten („*alle Informationen über eine bestimmte oder bestimmbare natürliche Person*“ – Artikel 2 Buchstabe a der Verordnung). Die Verarbeitung der Daten erfolgt durch die EZB, einer Einrichtung der Europäischen Union, im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts¹ fallen. Die Verarbeitung der Daten erfolgt sowohl manuell – und bildet bzw. würde damit Teil einer Datei (medizinische Berichte, medizinische Einzeldateien) bilden – als auch automatisch (Informationen werden in eine Softwaredatenbank eingegeben). Somit ist die Verordnung anzuwenden.

Gründe für die Vorabkontrolle: Gemäß Artikel 27 Absatz 1 der Verordnung unterliegen alle „*Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können,*“ der Vorabkontrolle durch den EDSB. Artikel 27 Absatz 2 der Verordnung enthält eine Liste von Verarbeitungen, die solche Risiken beinhalten können. Gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung unterliegen „*Verarbeitungen von Daten über Gesundheit*“ der Vorabkontrolle durch den EDSB, was hier zutrifft, da die Daten in die Kategorie von Daten über Gesundheit fallen.

Meldung und Frist für die EDSB-Stellungnahme: Die Meldung des DSB ging am 14. September 2012 ein. Nach dem Eingang standen der EDSB und der DSB zur weiteren Information und Klärung hinsichtlich der vorliegenden Verarbeitung mehrmals miteinander in Kontakt. Da es sich jedoch um einen Ex-post-Fall handelt, hat die Zweimonatsfrist, innerhalb derer der EDSB eine Stellungnahme abgeben muss, keine Geltung; der Fall wurde auf der Grundlage bestmöglichen Bemühens behandelt.

3.2 Rechtmäßigkeit der Verarbeitung

Gemäß Artikel 5 der Verordnung dürfen personenbezogene Daten nur aus einem der genannten Gründe verarbeitet werden.

Unter den fünf in Artikel 5 aufgeführten Gründen erfüllt die zu analysierende Verarbeitung die in Artikel 5 Buchstabe a der Verordnung genannten Bedingungen, nämlich, dass Daten verarbeitet werden können, wenn Folgendes gegeben ist: „*Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften (...) im öffentlichen Interesse (...) ausgeführt wird*“.

¹ Die Konzepte „Organe und Einrichtungen der Gemeinschaft“ und „Gemeinschaftsrecht“ können nach Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 nicht mehr eingesetzt werden. Artikel 3 der Verordnung Nr. 45/2001 ist daher im Lichte des Vertrags von Lissabon zu lesen.

Im vorliegenden Fall ergibt sich die **Rechtsgrundlage** für die Verarbeitung aus den rechtlichen Bestimmungen der im Sachverhalt erwähnten Beschäftigungsbedingungen für das Personal der EZB.

Die Notwendigkeit der Verarbeitung wird auch in Erwägungsgrund 27 der Verordnung erwähnt; dort heißt es: *„Die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zur Wahrnehmung einer Aufgabe im öffentlichen Interesse schließt die Verarbeitung personenbezogener Daten ein, die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist.“* Die Verarbeitung der betroffenen personenbezogenen Daten ist für die Verwaltung der Zahlung von Leistungen und die Erstattung medizinischer Auslagen an die betroffenen Personen im Zusammenhang mit Arbeitsunfällen und Berufskrankheiten notwendig. Diese Verarbeitung trägt somit zu der ordnungsgemäßen Verwaltung und der Funktionsfähigkeit der EZB bei.

3.3 Verarbeitung besonderer Datenkategorien

Gemäß Artikel 10 Absatz 1 der Verordnung ist die Verarbeitung von personenbezogenen Daten über Gesundheit untersagt, wenn sie nicht durch in Artikel 10 Absatz 2 und Artikel 10 Absatz 3 der Verordnung genannte Gründe gerechtfertigt ist.

In diesem Fall greift Artikel 10 Absatz 2 Buchstabe b: *„Absatz 1 (Untersagung der Verarbeitung von Daten über Gesundheit) findet nicht Anwendung, wenn (...) die Verarbeitung erforderlich ist, um den Pflichten und spezifischen Rechten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern sie aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer auf der Grundlage dieser Verträge erlassener Rechtsakte zulässig ist (...)“*. Die zu analysierende Verarbeitung ist notwendig, damit die EZB als Arbeitgeber ihren spezifischen arbeitsrechtlichen Pflichten und Rechten nachkommen kann. Die EZB führt diese Verarbeitung also in Übereinstimmung mit ihren Beschäftigungsbedingungen gemäß Artikel 10 Absatz 2 Buchstabe b der Verordnung durch.

Gemäß der Meldung gelten sowohl für alle Verantwortlichen in der GD-H als auch für die Mitarbeiter des medizinischen Dienstes der EZB darüber hinaus berufliche Geheimhaltungspflichten gemäß Geheimhaltungserklärungen. Damit wird Artikel 10 Absatz 3 der Verordnung Genüge getan.

3.4 Datenqualität

Zweckentsprechung, Erheblichkeit und Verhältnismäßigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung müssen personenbezogene Daten *„den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen“*. Es sollte daher überprüft werden, ob die erhobenen Daten für den Zweck erheblich sind, für den sie verarbeitet werden.

Die in dieser Stellungnahme beschriebenen Daten scheinen diesen Bedingungen bezüglich des Zwecks der vorstehend erläuterten Verarbeitung zu entsprechen.

Sachliche Richtigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung dürfen personenbezogene Daten nur dann verwendet werden, wenn sie *„sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind“*. Gemäß diesem Artikel sind *„alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder*

weiterverarbeitet werden, unrichtige oder unvollständige Daten gelöscht oder berichtigt werden“.

Im vorliegenden Fall lässt das bestehende Verfahren den Schluss zu, dass das System selbst die Qualität der Daten hinreichend gewährleistet. Der EDSB merkt jedoch an, dass medizinische Daten in der Papierakte einen anderen Aufbewahrungszeitraum haben als medizinische Daten in elektronischer Form. Es könnte die Gefahr bestehen, dass die sachliche Richtigkeit der medizinischen Daten der betroffenen Personen aufgrund unterschiedlicher Aufbewahrungszeiträume derselben Daten in unterschiedlichen Formen nicht vollständig gewährleistet ist. Der EDSB empfiehlt daher, dass die EZB alle angemessenen Maßnahmen ergreift, um sicherzustellen, dass der Grundsatz der sachlichen Richtigkeit gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung eingehalten wird (siehe Punkt 3.5 zum Aufbewahrungszeitraum).

Die Auskunfts- und Berichtigungsrechte scheinen der betroffenen Person offenzustehen, um seine personenbezogenen Daten über Unfälle und Berufskrankheiten so umfassend wie möglich zu machen. Diese Rechte stellen das zweite Mittel dar, anhand dessen sichergestellt wird, dass Daten über die betroffenen Personen sachlich richtig und auf dem neusten Stand sind (siehe Punkt 3.7 zum Auskunftsrecht).

Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise: Gemäß Artikel 4 Absatz 1 Buchstabe a der Verordnung dürfen personenbezogene Daten *„nur nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden“*. Die Rechtmäßigkeit der Verarbeitung wurde bereits in Punkt 3.2 dieser Stellungnahme erörtert. Der Aspekt der Verarbeitung nach Treu und Glauben ist mit den Informationen verknüpft, die der betroffenen Person zu geben sind (siehe Punkt 3.8 zur Informationspflicht).

3.5. Datenaufbewahrung

In Artikel 4 Absatz 1 Buchstabe e der Verordnung heißt es, dass personenbezogene Daten *„so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht“*.

Nach Ansicht des EDSB sind die Aufbewahrungszeiträume von Verwaltungs- und Finanzdaten und von ärztlichen Attesten im Zusammenhang mit der vorliegenden Verarbeitung angemessen und für die Zwecke, für die sie erfasst und weiterverarbeitet wurden, im Lichte von Artikel 4 Absatz 1 Buchstabe e der Verordnung notwendig.

Ferner begrüßt der EDSB die Initiative der EZB zur Änderung ihrer Dienstvorschriften in Bezug auf den Aufbewahrungszeitraum von medizinischen Akten und zur Abgleichung der Aufbewahrungszeiträume von medizinischen Daten in Papier- und in elektronischer Form. Der EDSB fordert die EZB auf, die EDSB-Leitlinien über die Verarbeitung von Gesundheitsdaten am Arbeitsplatz² zu berücksichtigen; dort wird empfohlen, dass medizinische Akten in Papier- und/oder elektronischer Form für höchstens 30 Jahre nach dem Einfügen des letzten medizinischen Dokuments in die Akte aufbewahrt werden sollten. Ferner hebt der EDSB hervor, dass die Art der medizinischen Dokumente aus der Perspektive ihrer Zwecke und den zur Bestimmung, welcher Aufbewahrungszeitraum für jede Art von Dokument geeignet und notwendig ist, geltenden Regeln geprüft werden sollte. Der EDSB

² <https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Guidelines>.

empfiehlt, dass die EZB einen Aufbewahrungszeitraum für medizinische Akten in Übereinstimmung mit den Leitlinien wählt.

Abschließend merkt der EDSB an, dass weder in der Meldung noch in der Datenschutzerklärung alle wie im Sachverhalt der vorliegenden Stellungnahme beschriebenen Aufbewahrungszeiträume klar angegeben werden. Der EDSB empfiehlt, dass die EZB beide Dokumente entsprechend aktualisiert.

In Bezug auf aggregierte anonyme Daten merkt der EDSB an, dass die Meldung unrichtige Informationen enthält, da es dort heißt, dass keine weitere Verarbeitung zu statistischen Zwecken beabsichtigt ist. Der EDSB empfiehlt daher, dass die EZB in der Meldung angibt, dass die GD-H jährlich von einem externen Administrator aggregierte anonyme Daten über Versicherungsfälle und Versicherungsleistungen für statistische, Vertragsverwaltungs- und Beschaffungszwecke erhält.

3.6 Datenübermittlung

In Artikeln 7, 8 und 9 der Verordnung sind bestimmte Pflichten geregelt, die Anwendung finden, wenn die für die Verarbeitung Verantwortlichen personenbezogene Daten an Dritte übermitteln. Für Übermittlungen an i) Organe oder Einrichtungen der EU (Artikel 7), ii) Empfänger, die der Richtlinie 95/46/EG unterworfen sind (Artikel 8) oder iii) sonstige Empfänger (Artikel 9) gelten unterschiedliche Vorschriften.

Externe Übermittlungen

Die EZB hat Verträge mit ihren medizinischen Beratern, anderen externen Ärzten, einem externen Versicherer und einem externen Administrator abgeschlossen, die alle in Übereinstimmung mit ihren Verträgen einzelstaatlichen Rechtsvorschriften unterliegen, die gemäß der Richtlinie 95/46/EG verabschiedet wurden. Damit findet Artikel 8 der Verordnung Anwendung. Nach dem Dafürhalten des EDSB ist die Übermittlung von Daten, wie im Sachverhalt angedeutet, für die obigen Empfänger zur Ausführung ihrer jeweiligen im öffentlichen Interesse gemäß Artikel 8 Buchstabe a der Verordnung durchgeführten Aufgaben notwendig.

3.7 Auskunftsrecht und Berichtigung

In Artikel 13 der Verordnung sind das grundsätzliche Recht auf Auskunft über die Daten auf Antrag der betroffenen Person und die entsprechenden Verfahren geregelt. Artikel 14 der Verordnung befasst sich mit dem Recht der betroffenen Person auf Berichtigung.

Sowohl in der Meldung als auch im Informationshinweis wird das Bestehen beider Rechte erwähnt, und es wird dort erläutert, wie betroffene Personen diese Rechte ausüben können. Die EZB verweist auch auf die Bedeutung des Rechts auf Berichtigung im Zusammenhang mit der Verarbeitung von Gesundheitsdaten.

Der EDSB weist allerdings die EZB auf Artikel 20 der Verordnung hin, in dem bestimmte Einschränkungen dieses Rechts geregelt sind, insbesondere, wenn eine solche Einschränkung für den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen notwendig ist. Beispielsweise können betroffene Personen ihr Recht auf direkten Zugriff auf ihre medizinischen Akten in den Räumlichkeiten des medizinischen Dienstes der EZB in der Gegenwart einer vom medizinischen Dienst bestimmten Person ausüben. Im Falle von

psychiatrischen/psychologischen Gutachten kann eine indirekte Einsichtnahme durch einen von der betroffenen Person benannten Arzt erfolgen. Die Einsichtnahme der persönlichen Aufzeichnungen von Ärzten durch betroffene Personen ist nicht gestattet, wenn diese Einschränkung gemäß den Bestimmungen von Artikel 20 Absatz 1 Buchstabe c der Verordnung und auf der Grundlage einer fallweisen Prüfung für den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen erforderlich ist.

Der EDSB empfiehlt daher, dass die EZB im Informationshinweis erläutert, dass Artikel 20 der Verordnung in Ausnahmefällen möglicherweise eingeschränkt Anwendung findet. Der EDSB fordert die EZB auf, eine mögliche Einschränkung des Zugriffs auf medizinische Akten von Fall zu Fall in Übereinstimmung mit dem Grundsatz der Verhältnismäßigkeit zu prüfen. Artikel 20 der Verordnung darf nicht zu einer allgemeinen Verweigerung des Zugriffs auf die persönlichen Aufzeichnungen von Ärzten in der medizinischen Akte führen.

3.8 Informationspflicht gegenüber der betroffenen Person

Nach Artikeln 11 und 12 der Verordnung sind der betroffenen Person Informationen zu geben, damit bei der Verarbeitung personenbezogener Daten Transparenz gewährleistet ist. Im vorliegenden Fall werden einige der Daten direkt von der betroffenen Person, andere von anderen Personen erhoben (d. h. Ärzten, GD-H-Beamten, Versicherer, Administrator, möglichen Zeugen oder geschädigten Dritten).

In dem hier zu prüfenden Fall enthält die Datenschutzerklärung die meisten der in Artikeln 11 und 12 der Verordnung aufgeführten Angaben. Der EDSB weist die EZB jedoch darauf hin, dass auch die folgenden Angaben in die Erklärung aufgenommen werden sollten:

- Aufbewahrungszeiträume aller Arten von verarbeiteten personenbezogenen Daten, wie in Punkt 3.5 dieser Stellungnahme dargestellt;
- das Auskunftsrecht sollte klarer dargestellt werden, wie in Punkt 3.7 dieser Stellungnahme dargestellt.

Der EDSB weist ferner darauf hin, dass die EZB bei einem Unfall u. U. personenbezogene Daten von möglichen Zeugen und Dritten (gegebenenfalls geschädigt) im Zusammenhang mit dem Unfall verarbeitet. Gemäß der Verordnung hat die EZB als für die relevante Verarbeitung Verantwortliche die Pflicht, diese betroffenen Personen zu informieren, wenn Daten über sie erfasst wurden. Der EDSB empfiehlt, dass die EZB eine kurze Datenschutzerklärung gemäß Artikel 11 der Verordnung verfasst und der Meldung diese Kategorien von betroffenen Personen als mögliche betroffene Personen, wenn ein Unfall passiert, hinzufügt.³

3.9 Vergabe von Unteraufträgen

Wird die Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen vorgenommen, so hat dieser einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung nach Artikel 23 zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen ausreichende Gewähr bietet.

³ Siehe EDSB-Stellungnahme vom 27. Juni 2012 zu der Meldung des Rates über „Gestion du Bureau Véhicules de Service“, Fall 2012-0157.

Im vorliegenden Fall ist das Vertragsverhältnis zwischen allen Auftragnehmern und der EZB durch einzelstaatliche Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG verbindlich geregelt; diese Verträge enthalten spezifisch Bestimmungen zu Datenschutz, Geheimhaltung und Sicherheit. Den Bestimmungen gemäß Artikel 23 der Verordnung ist somit Genüge getan.

3.10 Sicherheitsmaßnahmen

Gemäß Artikel 22 der Verordnung über die Sicherheit der Verarbeitung *„hat der für die Verarbeitung Verantwortliche technische und organisatorische Maßnahmen zu treffen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist“*. Durch diese Sicherheitsmaßnahmen sollten insbesondere unbefugte Offenlegung oder unbefugter Zugriff, versehentliche oder unrechtmäßige Vernichtung oder versehentlicher Verlust oder Modifizierung sowie alle anderen Formen unrechtmäßiger Verarbeitung verhindert werden.

Nach Prüfung der in der Meldung beschriebenen Sicherheitsmaßnahmen besteht kein Grund zu der Annahme, dass die von der EZB implementierten Maßnahmen nicht mit Artikel 22 der Verordnung übereinstimmen.

4. Schlussfolgerungen

Es besteht kein Grund zu der Annahme, dass ein Verstoß gegen die Bestimmungen der Verordnung vorliegt, sofern die folgenden Erwägungen in vollem Umfang berücksichtigt werden. Die EZB sollte insbesondere:

- alle angemessenen Maßnahmen ergreifen, um den Grundsatz der sachlichen Richtigkeit von medizinischen Akten sowohl in Papier- als auch in elektronischer Form sicherzustellen, und zwar den Aufbewahrungszeitraum von medizinischen Daten in Papierform mit den medizinischen Daten in elektronischer Form abzugleichen;
- den in den EDSB-Leitlinien empfohlenen Aufbewahrungszeitraum von medizinischen Akten übernehmen;
- in der Meldung angeben, dass die GD-H für statistische, Vertragsverwaltungs- und Beschaffungszwecke jährlich aggregierte anonyme Daten über Versicherungsfälle und Versicherungsleistungen von einem externen Administrator erhält;
- in der Meldung und der Datenschutzerklärung im Zusammenhang mit dem Recht auf Einsichtnahme in die medizinische Akte die Möglichkeit einer Anwendung von Artikel 20 der Verordnung erwähnen. Die EZB sollte sicherstellen, dass Einschränkungen der Einsichtnahme in medizinische Akten fallweise im Einklang mit dem Grundsatz der Verhältnismäßigkeit geprüft werden;
- in die Datenschutzerklärung die Angaben aufnehmen, die in Punkt 3.8 dieser Stellungnahme genannt sind;
- eine kurze Datenschutzerklärung für mögliche Zeugen und Dritte (gegebenenfalls geschädigt) im Zusammenhang mit einem Unfall verfassen und sollte diese der Meldung als eine zusätzliche Kategorie von betroffenen Personen hinzufügen.

Geschehen zu Brüssel, den 20. Februar 2014

(unterzeichnet)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter