Stellungnahme zu Meldungen der Datenschutzbeauftragten bestimmter EU-Agenturen über die *„Verarbeitung von Gesundheitsdaten am Arbeitsplatz“*

Brüssel, den 11. Februar 2011 (Fall 2010-0071)

1. Verfahren

Am 4. September 2008 versandte der Europäische Datenschutzbeauftragte (EDSB) an alle EU-Agenturen (Agenturen) ein Schreiben, welches das neue Verfahren zur Ex-post-Vorabkontrollanalyse im Hinblick auf gemeinsame Verfahren der Agenturen ankündigte.

Am 28. September 2009 übermittelte der EDSB allen EU-Agenturen die „*Leitlinien für die Verarbeitung von Gesundheitsdaten am Arbeitsplatz durch die Organe und Einrichtungen der Gemeinschaft*“ (EDSB-Leitlinien). Die Agenturen wurden ersucht, ihre Meldungen über Gesundheitsdaten zu übermitteln und ihnen ein Begleitschreiben des Datenschutzbeauftragten (DSB) beizufügen, in dem dieser auf besondere Aspekte in Bezug auf die hierzu erlassenen EDSB-Leitlinien hinweist. Für die Einreichung der Meldungen wurde eine Frist bis zum 16. November 2009 festgesetzt, doch sie wurde nur von sehr wenigen Agenturen eingehalten. Nach Ablauf der Frist gingen weitere Meldungen beim EDSB ein. Die letzte Meldung wurde am 20. September 2010 übermittelt.

Der EDSB hat von den DSB der folgenden 18 Agenturen Meldungen für eine Vorabkontrolle (im Sinne von Artikel 27 Absatz 3 der Verordnung (EG) Nr. 45/2001) und Begleitschreiben erhalten:

- Europäische Stiftung für Berufsbildung (**ETF**)
- Europäisches Zentrum für die Prävention und die Kontrolle von Krankheiten (**ECDC**)
- Agentur der Europäischen Union für Grundrechte (**FRA**)
- Exekutivagentur für die Forschung (**REA**)
- Europäisches Zentrum für die Förderung der Berufsbildung (**CEDEFOP**)
- Exekutivagentur für das transeuropäische Verkehrsnetz (**TEN-T EA**)
- Europäische Eisenbahnagentur (**ERA**)
- Exekutivagentur für Gesundheit und Verbraucher (**EAHC**)
- Europäische Fischereiaufsichtsagentur (**EUFA**)
- Exekutivagentur des Europäischen Forschungsrates (**ERCEA**)
- Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen (**FRONTEX**)
- Exekutivagentur für Wettbewerbsfähigkeit und Innovation (**EACI**)
- Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (**EU-OSHA**)
- Europäische Chemikalienagentur (**ECHA**)

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.eu.int - Website: www.edps.eu.int
Tel.: 02-283 19 00 - Fax: 02-283 19 50

- Europäische Stiftung zur Verbesserung der Lebens- und Arbeitsbedingungen (**EUROFOUND**)
- Europäische Umweltagentur (**EUA**)
- Europäische Agentur für Flugsicherheit (**EASA**)
- Europäische Agentur für die Sicherheit des Seeverkehrs (**EMSA**)

Am 10. Januar 2011 erhielten die DSB der betroffenen Agenturen den Entwurf der Stellungnahme, um ihrerseits Anmerkungen machen zu können. Nachdem der DSB einer Agentur um Fristverlängerung ersucht hatte, waren am 11. Februar 2011 die Anmerkungen einiger DSB eingegangen.

2. Rechtliche Aspekte

2.1. Vorabkontrolle

Die infrage stehenden Verarbeitungen erfassen verschiedene Verfahren − ärztliche Einstellungsuntersuchungen, ärztliche Jahresuntersuchungen und krankheitsbedingte Fehlzeiten – und verschiedene Gruppen von Betroffenen (ständige Bedienstete, Bedienstete auf Zeit, Vertragsbedienstete, nationale Sachverständige, Praktikanten, Bewerber für die vorgenannten Posten und Besucher der EU-Agenturen). Gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 („Verordnung“) unterliegen diese Verarbeitungen der Vorabkontrolle, da sie die Verarbeitung medizinischer Daten sowie gesundheitsbezogener oder im Zusammenhang mit Gesundheit stehender Verwaltungs- und Finanzdaten betreffen.

Der EDSB hat die Verfahrensweisen der einzelnen Agenturen in Bezug auf die datenschutzrechtlichen Grundsätze der Verordnung untersucht und geprüft, ob die einzelnen Agenturen die EDSB-Leitlinien einhalten. Da sich die Verfahren ähneln und die datenschutzrechtlichen Verfahrensweisen einiger Agenturen Gemeinsamkeiten aufweisen, hat der EDSB beschlossen, alle Meldungen im gleichen Zusammenhang zu prüfen und eine gemeinsame Stellungnahme zu veröffentlichen. In seiner gemeinsamen Stellungnahme identifiziert der EDSB Verfahrensweisen von Agenturen, die nicht im Einklang mit den Grundsätzen der Verordnung oder den EDSB-Leitlinien zu stehen scheinen, und er spricht maßgebliche Empfehlungen für die betroffene(n) Agentur(en) aus. Darüber hinaus wird auch auf einige bewährte Verfahrensweisen hingewiesen. Beispielsweise hebt der EDSB hervor, dass das **CEDEFOP** die Datenverarbeitungen und entsprechende Verfahrensweisen einer gründlichen Prüfung im Lichte der EDSB-Leitlinien unterzieht. Außerdem hat die **ETF** eine umfassende Publikation erstellt, die u. a. Verfahren zur Verwaltung von Personal- und medizinischen Akten behandelt.

Ein wichtiger Aspekt aller eingegangenen Meldungen ist der Umstand, dass mit Ausnahme der **FRA** alle Agenturen die medizinischen und Laboruntersuchungen von externen medizinischen Beratern oder Auftragnehmern durchführen lassen. Die meisten Agenturen nutzen den ärztlichen Dienst der Kommission in Brüssel und Luxemburg und haben entsprechende Dienstgütevereinbarungen (Service Level Agreements, SLA) abgeschlossen. Die Agenturen, die mit externen medizinischen Dienstleistern zusammenarbeiten, haben ebenfalls SLA abgeschlossen. Außerdem verwenden alle Agenturen (mit Ausnahme der **FRA**) den medizinischen Fragebogen, den der EDSB im Juli 2008 in Zusammenarbeit mit dem Inter-Institutional Medical College im Rahmen ärztlicher Einstellungsuntersuchungen gebilligt hat. Im Hinblick auf Sicherheitsmaßnahmen weist der EDSB darauf hin, dass anscheinend keine Agentur eine spezielle Sicherheitspolitik für die Verarbeitung gesundheitsbezogener Daten festgelegt hat (siehe unten Punkt 2.9 „Sicherheit“).

Der EDSB hält es für sinnvoll, die verschiedenen Beteiligten zu identifizieren, die bei den infrage stehenden Verarbeitungen involviert sind. Auf diese Weise können die entsprechenden Agenturen klar erkennen, wie die Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter gestaltet ist und wer für die Verwaltung der medizinischen Akten der Mitarbeiter verantwortlich ist.

i) Vom ärztlichen Dienst der Kommission geführte medizinische Akten

Die **REA, TEN-T EA, ERA, EUFA, ERCEA, FRONTEX** und **EACI** haben mit dem ärztlichen Dienst der Kommission in Brüssel eine SLA abgeschlossen, und die **EAHC** hat eine SLA mit dem ärztlichen Dienst der Kommission in Luxemburg vereinbart. Die medizinischen Akten werden vom ärztlichen Dienst der Kommission geführt.

ii) Von externen medizinischen Zentren geführte medizinische Akten

Die **ECHA, EASA,** das **CEDEFOP,** die **EUROFOUND, EUA**, **EU-OSHA** und **EMSA** haben ebenfalls eine SLA mit dem ärztlichen Dienst der Kommission abgeschlossen. Einige von ihnen – die **EUROFOUND, EUA, EU-OSHA** und das **ECDC** – haben auch mit den externen medizinischen Zentren, die die medizinischen Akten der Agenturmitarbeiter führen, Verträge abgeschlossen.

iii) Von externen medizinischen Beratern geführte medizinische Akten

Die **ECHA** und **EASA** haben ebenfalls Verträge mit externen medizinischen Zentren abgeschlossen, aber die medizinischen Akten ihrer Mitarbeiter werden von externen medizinischen Beratern geführt, die ihre Aufgaben auf dem Gelände der Agentur wahrnehmen. Das **CEDEFOP** und die **ETF** haben Verträge mit externen Beratern, die die Mitarbeiterakten führen.

Die **FRA** setzt keinen Vertrauensarzt und keinen ärztlichen Dienst ein. Die Mitarbeiter behalten ihre medizinischen Daten.

Das **ECDC**, die **EASA** und die **EAHC** haben in ihren Meldungen darauf hingewiesen, dass die Verarbeitungen im Zusammenhang mit ärztlichen Einstellungsuntersuchungen und ärztlichen Jahresuntersuchungen nicht nur gesundheitsbezogene Daten betreffen, sondern auch Daten erfassen, die dazu bestimmt sind, personenbezogene Aspekte der Betroffenen zu bewerten, um zu beurteilen, ob sich ein Mitarbeiter für die Dienststelle eignet (Artikel 27 Absatz 2 Buchstabe b). Der EDSB weist darauf hin, dass nach Artikel 28 Buchstabe e des Statuts der Beamten der Europäischen Gemeinschaften (Statut) bei der Entscheidung über die Eignung einer Person beurteilt werden muss, ob die Person die für die Ausübung ihres Amtes erforderliche körperliche Eignung besitzt, und keine Bewertung ihrer Kompetenz, ihrer Leistung oder ihres Verhaltens in Bezug auf die Arbeitsleistung durchzuführen ist. Somit ist Artikel 27 Absatz 2 Buchstabe b in diesem Zusammenhang nicht maßgeblich.

Das **ECDC**, die **EASA** und die **EUA** haben im Hinblick auf die ärztlichen Einstellungsuntersuchungen geltend gemacht, dass die Verarbeitung auch unter Artikel 27 Absatz 2 Buchstabe d der Verordnung falle, da sie darauf abziele, Personen von einem Vertrag auszuschließen. Der EDSB weist darauf hin, dass die Einstellung eines erfolgreichen Bewerbers von den Voraussetzungen abhängt, die in Artikel 28 des Statuts aufgeführt sind. Insbesondere Artikel 33 des Statuts sieht vor: „*Vor der Ernennung wird der ausgewählte Bewerber durch einen Vertrauensarzt des Organs untersucht, damit dieses die Gewissheit erhält, dass der Bewerber die Voraussetzungen des Artikels 28 Buchstabe e) erfüllt.*“ Somit soll die ärztliche Einstellungsuntersuchung gewährleisten, dass eine der sechs Einstellungsvoraussetzungen erfüllt ist − denn Artikel 28 Buchstabe e des Statuts sieht vor, dass zum Beamten nur ernannt werden darf, wer „*die für die Ausübung seines Amtes erforderliche körperliche Eignung besitzt*“ − und sie

ist nicht darauf gerichtet, Personen von einem Vertrag auszuschließen. Folglich unterliegt die Verarbeitung der ärztlichen Einstellungsuntersuchungen aufgrund der besonderen Risiken im Sinne von Artikel 27 Absatz 2 Buchstabe a der Verordnung und nicht aufgrund von Artikel 27 Absatz 2 Buchstabe d der Verordnung der Vorabkontrolle.

Nach Artikel 27 Absatz 4 der Verordnung gibt der EDSB seine Stellungnahme innerhalb von zwei Monaten nach Empfang der Meldung ab. Da die letzte Meldung am 20. September 2010 beim EDSB einging, ist dieses Datum nach Auffassung des EDSB das Eingangsdatum für alle Meldungen. Nach Ablauf der Frist hat sich der EDSB um die Beantwortung von Fragen bemüht und er hat die DSB um weitere Auskünfte ersucht. Am 6. Dezember 2010 übermittelte der EDSB allen betroffenen DSB eine E-Mail, die sie darüber in Kenntnis setzte, dass er aufgrund der Kompliziertheit des Falls gemäß Artikel 27 Absatz 4 der Verordnung entschieden hatte, die Aussetzung der Frist um einen Monat bis zum 9. Januar 2010 zu verlängern (da das Ende der Frist auf einen Sonntag fiel, wurde der Entwurf den DSB am 10. Januar 2011 zur Stellungnahme übersandt). Somit wurde die Frist für die Vorabkontrolle für 18 Tage ausgesetzt (wobei der Aussetzungszeitraum in Bezug auf die letzte eingegangene Meldung berechnet wird) und wegen der Kompliziertheit des Falls um einen Monat sowie um 15 Tage für die Einholung von Stellungnahmen der DSB verlängert. Die vorliegende Stellungnahme muss daher spätestens am 11. Februar 2011 abgegeben werden. Darüber hinaus wird der EDSB jeder Agentur ein individuelles Schreiben übermitteln, in dem darauf hingewiesen wird, dass er über die Maßnahmen in Kenntnis zu setzen ist, die zur Umsetzung der in dieser Stellungnahme veröffentlichten Empfehlungen innerhalb einer Frist von 3 Monaten getroffen werden.

2.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur verarbeitet werden, wenn dies nach Artikel 5 der Verordnung gerechtfertigt ist. Die infrage stehenden Verarbeitungen werden von Artikel 5 Buchstabe a erfasst, denn nach dieser Vorschrift dürfen Daten verarbeitet werden, wenn die Verarbeitung „*für die Wahrnehmung einer Aufgabe erforderlich [ist], die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer aufgrund dieser Verträge erlassener Rechtsakte im öffentlichen Interesse oder in legitimer Ausübung öffentlicher Gewalt ausgeführt wird, die dem Organ oder der Einrichtung der Gemeinschaft oder einem Dritten, dem die Daten übermittelt werden, übertragen wurde*“.

Folglich ist nach Artikel 5 Buchstabe a zunächst festzustellen, ob eine besondere Rechtsgrundlage für die Verarbeitung gegeben ist, und anschließend ist zu prüfen, ob die Verarbeitung für die Wahrnehmung einer im öffentlichen Interesse auszuführenden Aufgabe erforderlich ist.

Maßgebliche Rechtsgrundlagen im Vertrag oder in anderen Rechtsakten
Rechtsgrundlagen für die Durchführung einer Einstellungsuntersuchung finden sich in den Artikeln 28 und 33 des Statuts und in den Artikeln 12 Buchstabe d, 13 Absatz 2 und 83 Absatz 2 der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Gemeinschaften (BBSB).

Für die ärztlichen Jahresuntersuchungen ist die Rechtsgrundlage Artikel 59 Absatz 6 des Statuts und Artikel 16 Absatz 1, Artikel 59 und Artikel 91 BBSB.

Artikel 59 Absatz 1 des Statuts ist die Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten im Rahmen einer ärztlichen Kontrolluntersuchung während krankheits- oder unfallbedingter Fehlzeiten.

Die **TEN-T EA** und die **EUA** scheinen in der Meldung und der Datenschutzerklärung keine spezifische Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Verbindung mit ärztlichen Einstellungsuntersuchungen, Jahresuntersuchungen und krankheitsbedingten Fehlzeiten angegeben zu haben. Der EDSB empfiehlt, gemäß den eindeutigen Bestimmungen der EDSB-Leitlinien alle betroffenen Mitarbeiter in den Datenschutzerklärungen über die speziellen Vorschriften in Kenntnis zu setzen (siehe unten Punkt 2.8 „Informationspflicht gegenüber der betroffenen Person").

Die **EUROFOUND** hat Artikel 59 Absatz 6 des Statuts als Rechtsgrundlage für die medizinischen Jahresuntersuchungen angegeben. Die **EUROFOUND** sollte darüber hinaus die Rechtsgrundlage für die Jahresuntersuchungen von Bediensteten auf Zeit und Vertragsbediensteten gemäß den Bestimmungen der BBSB anführen. Außerdem empfiehlt der EDSB, in der Meldung und der Datenschutzerklärung die genaue Rechtsgrundlage einer für potenzielle Mitarbeiter geltenden Einstellungsuntersuchung anzugeben (siehe zur Datenschutzerklärung Punkt 2.8).

Wie in den Leitlinien hervorgehoben wird, kann die Weiterverarbeitung medizinischer Daten, die auf der Grundlage von Bestimmungen des Statuts erhoben wurden, nur dann als rechtmäßig angesehen werden, wenn sie aufgrund einer in Kenntnis der Sachlage und ohne Zwang erteilten Einwilligung des Betroffenen erfolgt oder wenn die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen notwendig ist. Der Betroffene sollte die Möglichkeit haben, im Hinblick auf die Weiterverarbeitung seiner medizinischen Daten für die Zwecke der medizinischen Nachkontrolle die Einwilligung zu verweigern und/oder zu widerrufen. Im vorliegenden Fall ist die Einwilligung nur dann wirksam, wenn sie aufgrund der Informationen erteilt wird, die jede Agentur ihren Mitarbeitern gemäß den Artikeln 11 und 12 der Verordnung übermitteln sollte (siehe Punkt 2.8 „Informationspflicht gegenüber der betroffenen Person").

Erforderlichkeit für die Wahrnehmung einer Aufgabe im öffentlichen Interesse
Bei der Beurteilung, ob die infrage stehenden Verarbeitungen die zweite Voraussetzung des Artikels 5 der Verordnung (EG) Nr. 45/2001 erfüllen, stellt der EDSB fest, dass die ärztlichen Einstellungsuntersuchungen und die besonderen ärztlichen Kontrolluntersuchungen erforderlich sind, um die Eignung und die krankheitsbedingten Fehlzeiten der Agenturmitarbeiter zu verwalten und zu überwachen. Darüber hinaus können die ärztlichen Jahresuntersuchungen aus anderen Gründen für erforderlich und daher rechtmäßig angesehen werden, insbesondere für die Zwecke der Einrichtung eines Gemeinsamen Krankenfürsorgesystems (Artikel 72 und 73 des Statuts). Solche Verarbeitungen sind daher im Zusammenhang mit der im öffentlichen Interesse erfolgenden Wahrnehmung der Aufgabe der Agenturen von Artikel 5 Buchstabe a der Verordnung erfasst.

In jedem Fall sollten alle Agenturen sicherstellen, dass der betroffene Mitarbeiter

- vom untersuchenden Arzt über das Ergebnis der Jahresuntersuchung in Kenntnis gesetzt wird,
- darüber aufgeklärt wird, dass er auf Wunsch zusätzliche Informationen/Erläuterungen vom Arzt erhalten kann,
- berechtigt ist, die Jahresuntersuchung von einem Arzt seiner Wahl durchführen zu lassen und mittels Kostenerstattung so gestellt zu werden, als wenn die Untersuchung im medizinischen Zentrum der Agentur durchgeführt worden wäre.

2.3. Verarbeitung besonderer Datenkategorien

Im Rahmen der Auswahl- und Einstellungsverfahren ist die Verarbeitung bestimmter Daten der „*besonderen Datenkategorien*" im Sinne von Artikel 10 der Verordnung (EG) Nr. 45/2001 untersagt, sofern keine Ausnahme gemäß Artikel 10 Absätze 2 bis 5 vorliegt.

Einige Agenturen machen geltend, dass sie keine medizinischen Daten im engeren Sinne erhielten und die Verarbeitungen daher keiner Vorabkontrolle unterlägen. Insbesondere die **EU-OSHA, REA, TEN-T EA** und **EAHC** haben angegeben, dass sie nur Gesundheitszeugnisse, Verwaltungsdaten zu krankheitsbedingten Fehlzeiten, ärztlichen Bescheinigungen, Jahresuntersuchungen und zum Erwerb medizinischer Geräte für die täglichen Aufgaben einiger Mitarbeiter verarbeiten.

Wie der EDSB in seinen Leitlinien hervorgehoben hat, bezieht sich der Begriff „Gesundheitsdaten" vor allem auf zwei verschiedene Datenkategorien: medizinische Daten und Verwaltungsdokumente, die personenbezogene Daten über den Gesundheitszustand einer Person beinhalten. Viele Agenturen erheben und verarbeiten z. B. Verwaltungsvermerke, die die gesundheitliche Eignung für einen Dienstposten bescheinigen, Rechnungen über ärztliche Jahresuntersuchungen oder Impfungen von Betroffenen, Vermerke über etwaige Anträge auf medizinische Nachkontrolle oder Informationen über krankheitsbedingte Fehlzeiten, die der Personalabteilung zu administrativen Zwecken übermittelt werden. Diese Daten beziehen sich auf den Gesundheitszustand einer Person und können dazu führen, dass die Krankheit oder Arbeitsunfähigkeit eines bestimmten Betroffenen identifiziert werden kann. Auch wenn eine ärztliche Bescheinigung keine genauen Angaben zur spezifischen Erkrankung enthält, kann der Betroffene als Person identifiziert werden, die aufgrund einer kurz- oder langzeitigen Erkrankung mit ärztlicher Behandlung oder aufgrund einer besonderen krankheitsbedingten Beurlaubung dem Dienst ferngeblieben ist.

Selbst wenn also keine medizinischen Daten im engeren Sinne verarbeitet werden, sind die infrage stehenden Verarbeitungen somit gesundheitsbezogen und daher fallen sie unter Artikel 27 Absatz 2 Buchstabe a der Verordnung und erfordern eine Vorabkontrolle.

Aus diesem Grund empfiehlt der EDSB, alle Mitarbeiter der Personalabteilungen der **ETF,** des **ECDC,** der **FRA, REA,** des **CEDEFOP,** der **TEN-T EA, EAHC, ECHA, EU-OSHA, EACI, EUROFOUND, EUA, EASA** und **EMSA**, die für die Verwaltung von Gesundheitszeugnissen und sonstigen Informationen über den Gesundheitszustand ihrer Mitarbeiter zuständig sind, daran zu erinnern, dass diese Daten nach den Grundsätzen der ärztlichen Schweigepflicht zu verarbeiten sind. Der EDSB fordert diese Agenturen auf, die zuständigen Mitarbeiter Vertraulichkeitserklärungen unterzeichnen zu lassen, in denen sich diese in Entsprechung zur Geheimhaltungspflicht von ärztlichem Personal gemäß Artikel 10 Absatz 3 der Verordnung (EG) Nr. 45/2001 verpflichten, das Berufsgeheimnis zu wahren. (Diese Überlegung ist im Zusammenhang mit Artikel 7 Absatz 3 der Verordnung zu sehen, siehe Punkt 2.6 der vorliegenden Stellungnahme.)

Der EDSB nimmt die Vertraulichkeitserklärung des **CEDEFOP** zur Kenntnis und empfiehlt die ergänzende Aufnahme des folgenden Satzes: „*Ich verpflichte mich zur Einhaltung des Berufsgeheimnisses entsprechend der Geheimhaltungspflicht von ärztlichem Personal gemäß Artikel 10 Absatz 3 der Verordnung (EG) Nr. 45/2001.*" Diese Ergänzung nimmt besonderen Bezug auf die verarbeiteten Gesundheitsdaten und unterstreicht ihre Vertraulichkeit.

2.4. Datenqualität

Zweckentsprechung, Erheblichkeit und Verhältnismäßigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung (EG) Nr. 45/2001 müssen personenbezogene Daten „*den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen*".

Die infrage stehenden gesundheitsbezogenen Daten, die von den Agenturen erhoben werden, und die medizinischen Daten, die von den externen Dienstleistern einiger der Agenturen erhoben und verarbeitet werden, scheinen grundsätzlich gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung den Zwecken, für die sie erhoben werden, zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen.

Dennoch weist der EDSB auf den Grundsatz der Verhältnismäßigkeit hin, insbesondere in Bezug auf die **ECHA**, **EASA**, das **CEDEFOP**, die **EUROFOUND**, **EUA**, **EU-OSHA**, **EMSA**, das **ECDC** und die **ETF**. Diese Agenturen haben sich nicht ausschließlich an den medizinischen Dienst der Kommission gebunden und lassen medizinische Daten im Rahmen der ärztlichen Einstellungsuntersuchung und der Jahresuntersuchung durch ihre externen Dienstleister verarbeiten. Sie sollten daher sicherstellen, dass die Datenerhebung zu anderen Zwecken als zur Feststellung der körperlichen Arbeitsfähigkeit, zur Feststellung des Anspruchs auf garantierte Leistungen in Bezug auf Invalidität oder Tod und zum Schutz der Gesundheit ihrer Mitarbeiter untersagt ist. Daher empfiehlt der EDSB, dass die Agenturen „*allgemein eine gründliche Überprüfung der Fragen, die im Fragebogen für die ärztliche Einstellungsuntersuchung und die ärztliche Jahresuntersuchung aufgeführt sind, im Lichte der Grundsätze der Zweckentsprechung, Erheblichkeit und Verhältnismäßigkeit für die Zwecke der Beurteilung der Diensttauglichkeit vornehmen*“[1].

1) Ärztliche Einstellungsuntersuchung

Der EDSB stellt fest, dass die **ECHA** in ihrem medizinischen Fragebogen ein Foto der zur ärztlichen Einstellungsuntersuchung geladenen Betroffenen verlangt. Nach Auffassung des EDSB ist diese Information für den Verarbeitungszweck, nämlich die Beurteilung der Eignung des Bewerbers für die ausgeschriebene Stelle, nicht erheblich.

2) Ärztliche Kontrolluntersuchung durch einen Arzt für Allgemeinmedizin

Für den Fall, dass ihre Mitarbeiter eine Jahresuntersuchung bei einem Arzt ihrer Wahl durchführen möchten, sollten die **ETF**, **FRONTEX**, **EACI**, **EU-OSHA, ECHA, EUROFOUND, EUA, EASA** und **EMSA** grundsätzlich festlegen, dass der Hausarzt des Betroffenen die Untersuchungsergebnisse nicht an den Arzt der Agentur oder den medizinischen Dienst der Kommission übermitteln darf, wenn der Betroffene nicht in Kenntnis der Sachlage und ohne Zwang seine Einwilligung erteilt hat. Der Arzt sollte lediglich eine Erklärung an die Personalabteilung der Agentur senden und bestätigen, dass die Untersuchung durchgeführt wurde, und gegebenenfalls, soweit dies erforderlich ist, darauf hinweisen, dass für den Betroffenen besondere Vorkehrungen am Arbeitsplatz getroffen werden müssen.

Das **CEDEFOP** hat geltend gemacht, dass die medizinischen Jahresuntersuchungen nicht vorrangig der Prävention dienen, sondern der Überprüfung, ob der betreffende Mitarbeiter für seine Aufgaben geeignet ist oder sein Arbeitsplatz angepasst werden muss. Nach Auffassung des **CEDEFOP** sollten daher alle medizinischen Ergebnisse dem externen Vertrauensarzt des **CEDEFOP** übermittelt werden, da allein dieser beurteilen könne, ob der Betroffene nach arbeitsmedizinischen Gesichtspunkten geeignet sei, in der jeweiligen Arbeitsumgebung zu arbeiten. Der EDSB weist darauf hin, dass nach datenschutzrechtlichen Gesichtspunkten die Betroffenen frei darüber entscheiden sollten, ob ihr Hausarzt dem Arzt der Agentur ihre medizinischen Ergebnisse übermittelt. Für die Agentur sollte eine Erklärung ausreichen, die die

[1] Siehe Stellungnahme des EDSB vom 14. Juni 2007 [Anm. d. Übers.: EN „14 *July* 2007“ korrigiert] zur Verarbeitung medizinischer Daten durch den medizinischen Dienst des EP in Brüssel und Straßburg (Fall 2004-205).

Eignung des Mitarbeiters bestätigt. Allerdings könnten nach Auffassung des EDSB in bestimmten problematischen Fällen, in denen der Gesundheitszustand eines Mitarbeiters eine Gefahr für seine Kollegen oder seine eigene Arbeitsleistung darstellen kann, diese speziellen Ergebnisse dem Arzt der Agentur unter der Bedingung übermittelt werden, dass der Betroffene vor der Übermittlung der medizinischen Daten in Kenntnis gesetzt wird.

Sachliche Richtigkeit: Nach Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten „*sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht*" sein. Darüber hinaus 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*".

Dieser Grundsatz sollte sowohl auf medizinische Akten als auch auf Personalakten angewandt werden.

Die **ETF,** das **ECDC,** die **REA,** das **CEDEFOP,** die **ERA, EAHC, EUFA, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EUA, EASA** und **EMSA** sollten sicherstellen, dass für die Einstellung angefertigte Gesundheitszeugnisse und Bescheinigungen über die Jahresuntersuchungen in den Personalakten geführt werden. Gegebenenfalls sollten auch aktualisierte Unterlagen über den Gesundheitszustand in die Akten aufgenommen werden, insbesondere im Falle einer Jahresuntersuchung. Interne Vermerke sollten entsprechend an die zuständigen Mitarbeiter der Personalabteilung gerichtet werden.

Die **ETF**, **ECHA** und **EASA** sollten die Einhaltung des Qualitätsgrundsatzes sicherstellen, indem z. B. eine entsprechende Bestimmung in die Verträge mit den externen medizinischen Beratern und medizinischen Zentren aufgenommen wird. Ebenso sollten das **ECDC**[2], die **EU-OSHA**, **EUROFOUND**, **EUA** und **EMSA** mit ihren jeweiligen externen medizinischen Diensten verfahren. Die Bestimmung sollte spezielle Methoden anführen, mit denen sich gewährleisten lässt, dass die medizinischen Daten der Betroffenen **sachlich richtig**, **vollständig** und **auf dem neuesten Stand** sind. Insbesondere sollte die Bestimmung vorsehen, dass

- die Einwilligung und die Unterschrift der Betroffenen im Hinblick auf Informationen über Kontakte zu ihrem behandelnden Arzt oder Facharzt dazu beitragen können, die Vollständigkeit der medizinischen Daten im ärztlichen Bericht zu gewährleisten;
- die Betroffenen den ärztlichen Untersuchungsbericht unterzeichnen können, damit die sachliche Richtigkeit ihrer Verwaltungsdaten überprüft werden kann;
- die Betroffenen den medizinischen Beratern und medizinischen Diensten der vorgenannten Agenturen weitere ärztliche Gutachten vorlegen können, um die Vollständigkeit ihrer medizinischen Akte zu gewährleisten;
- der medizinische Berater sicherstellt, dass medizinischen Formularen keine Kommentare oder Anmerkungen von Dritten hinzugefügt werden.

Soweit der medizinische Dienst der Kommission[3] bei einigen Agenturmitarbeitern einige oder alle ärztlichen Untersuchungen durchführt und ihre medizinischen Akten vom medizinischen Dienst der Kommission geführt werden, sollten diese Agenturen − insbesondere die **REA, TEN-T EA, ERA, EAHC, EUFA, ERCEA, FRONTEX, EACI** und **EMSA** − dafür sorgen, dass den

---

[2] Der EDSB hat das Schreiben der **ECDC**-DSB vom 29. Januar 2010 zur Kenntnis genommen, in dem diese darauf hinwies, dass die Agentur den Auftragsverarbeiter angewiesen habe, die Empfehlung des EDSB hinsichtlich der Unterzeichnung von Laborberichten durch die Betroffenen umzusetzen.

[3] Es ist daran zu erinnern, dass die Tätigkeiten des medizinischen Dienstes der Kommission in Brüssel und Luxemburg der Vorabkontrolle durch den EDSB unterlagen. Die Stellungnahme wurde am 10. September 2007 abgegeben (Fall 2004-232).

Betroffenen die vorgenannten Verfahrensweisen im Hinblick auf die sachliche Richtigkeit ihrer medizinischen Akte bekannt sind.

Falls die **FRA** einen Auftragsverarbeiter unter Vertrag nimmt, der alle medizinischen Untersuchungen durchführt, sollte sie die vorstehenden Empfehlungen berücksichtigen.

Werden im Falle krankheitsbedingter Fehlzeiten die gesundheitsbezogenen Verwaltungsdaten elektronisch erhoben, sollten die **ETF**, das **ECDC**, die **FRA**, **REA**, **ERA**, **EAHC**, **EUFA**, **FRONTEX**, **EU-OSHA**, **EACI**, **EUA**, **EUROFOUND** und **EMSA** sicherstellen, dass ein Prüfpfad vorhanden ist, mit dem sich die Aktivitäten der Nutzer nachvollziehen lassen (siehe Ausführungen zur Sicherheit unter Punkt 2.10).

2.5. Datenaufbewahrung

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001 müssen personenbezogene Daten „*so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht*".

Der EDSB weist gemäß den Leitlinien darauf hin, dass grundsätzlich ein Zeitraum von 30 Jahren, nachdem das letzte medizinische Dokument in die Akte aufgenommen wurde, als maximale Aufbewahrungsfrist für medizinische Daten in diesem Zusammenhang anzusehen ist. Jede Aufbewahrungsfrist sollte im Lichte von Artikel 4 Absatz 1 Buchstabe e der Verordnung beurteilt und festgelegt werden. Wie der EDSB in seinem Brief vom 26. Februar 2007 an das Kollegium der Verwaltungschefs[4] empfohlen hat, sollte die Art der medizinischen Dokumente im Lichte der geltenden Vorschriften untersucht werden, um festzustellen, welche Aufbewahrungsfrist für die jeweilige Dokumentenkategorie geeignet ist. Daher ist zu prüfen, inwieweit und zu welchem Zweck es erforderlich ist, bestimmte medizinische Dokumente während und nach der Beschäftigungszeit eines Mitarbeiters aufzubewahren. Es ist daran zu erinnern, dass das Kollegium der Verwaltungschefs den EDSB am 11. Oktober 2010 gemäß Artikel 28 Absatz 1 der Verordnung zu besonderen Aufbewahrungsfristen für bestimmte medizinische Dokumente konsultiert hat. Nachdem sich der EDSB mit dem CPAS, dem maßgeblichen Unterausschuss des Kollegiums, ausgetauscht hat, wird er bald über die Konsultation entscheiden und dabei seinen Brief vom 26. Februar 2007 und seine Stellungnahmen im Rahmen der Vorabkontrolle zugrunde legen.

In diesem Zusammenhang und zur Vermeidung von Missverständnissen sollte die **EACI** ihre Datenschutzerklärung um den folgenden Zusatz ergänzen: Die Aufbewahrungsfrist für medizinische Daten beträgt maximal 30 Jahre „*nach Aufnahme des letzten medizinischen Dokuments in die Akte im Lichte von Artikel 4 Absatz 1 Buchstabe e der Verordnung*". Darüber hinaus sollte die **EACI** gemäß den EDSB-Leitlinien besondere Aufbewahrungsfristen für krankheitsbedingte Fehlzeiten und im Hinblick auf nicht eingestellte Bewerber festlegen.

Der EDSB stellt fest, dass das **ECDC** Gesundheitszeugnisse von eingestellten und nicht eingestellten Bewerbern für einen maximalen Zeitraum von 30 Jahren aufbewahrt.
Außerdem hat die **EUROFOUND** angegeben, dass „*eine Kopie der Bescheinigung über die Einstellungsuntersuchung dauerhaft in der Personalakte geführt wird. Das Original wird in der medizinischen Akte aufbewahrt. Die medizinische Akte wird als Teil der Personalakte eines Mitarbeiters dauerhaft aufbewahrt.*"
Die **ECHA** hat in ihrer Meldung darauf hingewiesen, dass „*die medizinischen Akten der*

[4] Siehe http://www.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Adminmeasures.

Mitarbeiter nach Beschäftigungsende für weitere 10 Jahre aufbewahrt werden".
Auch die **EASA** hat in ihrer Meldung angegeben, dass „*die Ergebnisse in die medizinische Akte aufgenommen werden, die nach dem Ende des Beschäftigungsvertrags für weitere 10 Jahre aufbewahrt wird*".
Der EDSB weist darauf hin, dass es sich bei den Daten, die von den Auftragsverarbeitern der Agenturen in den medizinischen Akten zu führen sind, um die Laborergebnisse der Einstellungsuntersuchungen und der etwaigen sonstigen, vom Betroffenen erwünschten ärztlichen Untersuchungen handelt. Gemäß den vorstehenden Erwägungen sollten die medizinischen Akten nach dem Ende der Beschäftigungsdauer des jeweiligen Mitarbeiters für maximal weitere 30 Jahre aufbewahrt werden. Gesundheitszeugnisse über die Eignung des Mitarbeiters sollten in der Personalakte geführt werden. Gemäß den EDSB-Leitlinien zur Einstellung von Personal[5] empfiehlt der EDSB, dass Personalakten für die Dauer von 10 Jahren nach dem Ende des Zeitraums der aktiven Beschäftigung eines Mitarbeiters oder der letzten Ruhegehaltszahlung aufbewahrt werden.
Somit gehen die Datenaufbewahrungsfristen des **ECDC** und der **EUROFOUND** über den Zweck der Datenerhebung hinaus, und die Datenaufbewahrungsfrist der **ECHA** und **EASA** entspricht nicht den vorgenannten Grundsätzen. Der EDSB ersucht alle vier Agenturen, die in den medizinischen Akten und den Personalakten geführten Daten erneut zu prüfen und gemäß den vorstehenden Erwägungen angemessene Datenaufbewahrungsfristen festzulegen.
Darüber hinaus sollten das **ECDC** und die **ECHA** im Lichte der EDSB-Leitlinien eine Aufbewahrungsfrist für die Daten nicht eingestellter Bewerber festlegen und den Betroffenen ermöglichen, die Daten oder die Ablehnungsentscheidung innerhalb dieser Frist anzufechten. Außerdem empfiehlt der EDSB, dass das **ECDC** und die **ECHA** besondere Aufbewahrungsfristen für Daten zu krankheitsbedingten Fehlzeiten festlegen.

Die **FRA** hat in ihrer Meldung angegeben, dass sie die Gesundheitszeugnisse eingestellter Bewerber für einen unbegrenzten Zeitraum, d. h. solange die Personalakte existiert, in den Personalakten aufbewahrt. Nach Auffassung des EDSB ist diese Frist unverhältnismäßig und nicht erforderlich im Sinne von Artikel 4 Absatz 1 Buchstabe e der Verordnung. Wie bereits festgestellt wurde, empfiehlt der EDSB, dass die **FRA** Personalakten für die Dauer von maximal 10 Jahren nach dem Ende des Zeitraums der aktiven Beschäftigung eines Mitarbeiters oder der letzten Ruhegehaltszahlung aufbewahrt.

Die **EAHC** sollte im Hinblick auf die Aufbewahrungsfrist für Gesundheitszeugnisse, die im Rahmen von Einstellungsuntersuchungen angefertigt und in der Personalakte geführt werden, den gleichen Empfehlungen folgen und eine Datenaufbewahrungsfrist für nicht eingestellte Bewerber gemäß den EDSB-Leitlinien festlegen.

Der **ETF** empfiehlt der EDSB, besondere Aufbewahrungsfristen für Daten über krankheitsbedingte Fehlzeiten, besondere ärztliche Kontrolluntersuchungen und nicht eingestellte Bewerber gemäß den EDSB-Leitlinien festzulegen.

Der EDSB ersucht die **REA**, bei der Festlegung ihres eigenen speziellen Aufbewahrungsverzeichnisses nicht nur die gemeinsame Aufbewahrungsliste der Kommission „Common Commission-level retention list", sondern auch die Empfehlungen der EDSB-Leitlinien zu berücksichtigen, insbesondere sollte die **REA** Aufbewahrungsfristen für gesundheitsbezogene Daten (Gesundheitszeugnisse und ärztliche Bescheinigungen) sowohl eingestellter als auch nicht

[5] Leitlinien für die Verarbeitung personenbezogener Daten [Anm. d. Übers.: „personenbezogener Daten" ergänzt in Übereinstimmung mit der dt. Übersetzung auf der EDSB-Website http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines] im Zusammenhang mit der Einstellung von Personal, 10. Oktober 2008.

eingestellter Bewerber und für Daten zu krankheitsbedingten Fehlzeiten und gegebenenfalls besonderen ärztlichen Kontrolluntersuchungen festlegen. Sobald das Verzeichnis festgelegt ist, sollte der EDSB davon in Kenntnis gesetzt werden.

Die **TEN-T EA** hat dem EDSB die Aufbewahrungsfristen für Daten zu krankheitsbedingten Fehlzeiten und nicht eingestellten Bewerbern mitgeteilt und diese erscheinen angemessen. Der EDSB empfiehlt, diese Aufbewahrungsfristen sowohl in der Meldung als auch in der Datenschutzerklärung anzugeben.

Die **FRONTEX** sollte im Lichte der EDSB-Leitlinien eine Aufbewahrungsfrist für gesundheitsbezogene Daten nicht eingestellter Bewerber festlegen.

Die **ERA** und **EU-OSHA** sollten eine besondere Aufbewahrungsfrist für Daten zu krankheitsbedingten Fehlzeiten gemäß Artikel 59 Absatz 4 des Statuts und im Lichte der EDSB-Leitlinien festlegen.

Die **EUA** hat in ihrer Meldung für die folgenden Daten keine Aufbewahrungsfristen angegeben:

- Gesundheitszeugnisse in den Personalakten
- Daten zu krankheitsbedingten Fehlzeiten
- besondere ärztliche Kontrolluntersuchungen und
- Daten zu nicht eingestellten Bewerbern

Der EDSB empfiehlt der **EUA,** für diese Daten besondere Aufbewahrungsfristen festzulegen und im Lichte von Artikel 4 Absatz 1 Buchstabe e der Verordnung sicherzustellen, dass ihr externer medizinischer Dienstleister die medizinischen Daten ihrer Mitarbeiter für einen Zeitraum von maximal 30 Jahren nach Aufnahme des letzten medizinischen Dokuments in der Akte des Mitarbeiters aufbewahrt.

Die **ERA** hat in ihrer Meldung angegeben, dass „*Daten über krankheitsbedingte Fehlzeiten zu statistischen Zwecken anonym verarbeitet werden; daher ist die Verordnung (EG) Nr. 45/2001 nicht anwendbar*". Zur Klarstellung verweist der EDSB auf Artikel 4 Absatz 1 Buchstabe e der Verordnung, der ausdrücklich bestimmt, dass „ … *personenbezogene Daten, die für historische, statistische oder wissenschaftliche Zwecke über den vorstehend genannten Zeitraum hinaus aufbewahrt werden sollen, … nur in anonymisierter Form … gespeichert werden. Die Daten dürfen jedenfalls nicht für andere als historische, statistische oder wissenschaftliche Verwendungszwecke verwendet werden*". Die **ERA** ist nach dieser Bestimmung eindeutig verpflichtet, die Daten in anonymisierter Form zu speichern, wenn sie für statistische Zwecke verwendet werden. Die Verordnung ist nur dann nicht anwendbar, wenn eine anonymisierte Speicherung erfolgt. Der EDSB ersucht die **ERA**, Nachweise für die Methode zu erbringen, mit der die Anonymisierung der Daten für statistische Zwecke erreicht wurde.

2.6. Datenübermittlung

Artikel 7 Absatz 1 erfasst Verarbeitungen, bei denen personenbezogene Daten innerhalb der Organe oder Einrichtungen der Gemeinschaft oder an andere Organe oder Einrichtungen der Gemeinschaft übermittelt werden, „*wenn die Daten für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen*".

Interne Datenübermittlung innerhalb der Agentur:

i) Arztrechnungen

Der EDSB begrüßt die besonderen Vorschriften des **ECDC**, denen zufolge der für die Verarbeitung Verantwortliche der **ECDC**-Finanzabteilung/Buchhaltung nur die Gesamtkosten übermittelt, die dem externen medizinischen Auftragnehmer zu zahlen sind. Darüber hinaus ist von dem zuständigen Mitarbeiter der Buchhaltungsabteilung eine Vertraulichkeitserklärung zu unterzeichnen.

Die **FRA** sollte sicherstellen, dass das Erstattungsdokument (Anhang 2 der Meldung) vom Arzt des Betroffenen ausgefüllt wird und dieser dann lediglich den zu erstattenden Gesamtbetrag an die gemeinsame Stelle für Versicherungsleistungen der Agentur weiterleitet.

Die **ETF, FRONTEX, EU-OSHA, EUA** und **EASA** haben keine Angaben dazu gemacht, ob sie im Zusammenhang mit der Kostenerstattung ein besonderes Verfahren für die etwaige Übermittlung von Gesundheitsdaten an die für den Verwaltungshaushalt zuständige Abteilung der Agentur eingeführt haben. Der EDSB fordert die vorgenannten Agenturen eindringlich auf, ein Verfahren einzuführen, bei dem der medizinische Dienst der Agentur zunächst alle Arztrechnungen zur Abzeichnung erhält und anschließend der Haushaltsabteilung nur den zu erstattenden Gesamtbetrag übermittelt.

Die **REA**, **ERA** und **FRONTEX** sollten ein Verfahren einführen, bei dem der medizinische Dienst der Kommission alle Arztrechnungen abzeichnet und anschließend ein Formular ausfüllt, das den zu erstattenden Gesamtbetrag anführt. Dieses Dokument sollte ausschließlich durch den medizinischen Dienst der Kommission unmittelbar an die zuständige Finanzabteilung der jeweiligen Agentur übermittelt werden.

Was die Auffassung des **CEDEFOP** betrifft, erinnert der EDSB daran, dass die Leitlinien darauf abzielen, bewährte Verfahrensweisen zu harmonisieren und ein einheitliches Vorgehen aller Agenturen zu gewährleisten. Daher fordert der EDSB das **CEDEFOP** auf, seine Politik im Hinblick auf Arztrechnungen zu ändern und den Empfehlungen der Leitlinien zu folgen.

ii) Übermittlungen an andere Einrichtungen

Darüber hinaus sollten die Agenturen im Zusammenhang mit Übermittlungen an andere Einrichtungen sicherstellen, dass nur solche Personen medizinische Akten erhalten, die zum Zugriff auf gesundheitsbezogene Daten ermächtigt sind und dem Berufsgeheimnis unterliegen.

Dies sollte bei der **FRA**, **REA**, **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **ERCEA**, **FRONTEX**, **EACI**, **EU-OSHA**, **ECHA**, **EUA** und **EASA** der Fall sein, wenn die Agenturen Gesundheitszeugnisse von Mitarbeitern oder sonstige Dokumente, die sich auf ihre Gesundheit beziehen, an eine andere Einrichtung übermitteln müssen.

iii) Einhaltung von Artikel 7 Absatz 3 der Verordnung

Artikel 7 Absatz 3 der Verordnung bestimmt: „*Der Empfänger verarbeitet die personenbezogenen Daten nur für die Zwecke, für die sie übermittelt wurden.*“ Den Meldungen zufolge haben die **ETF**, das **ECDC**[6], die **FRA**, **REA**, **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **ERCEA**, **FRONTEX**, **ECHA**, **EU-OSHA**, **EACI**, **EUROFOUND**, **EUA**, **EASA** und **EMSA** keine Dokumente oder sonstigen Angaben übermittelt, die die Wahrung des Grundsatzes von Artikel 7 Absatz 3 belegen. Der EDSB empfiehlt, dass z. B. jede Agentur einen internen Vermerk abfasst oder die potenziellen

[6] Der EDSB stellt fest, dass die **ECDC**-Mitarbeiter der Meldung zufolge über die Vertraulichkeit der Datenverarbeitung in Kenntnis gesetzt wurden. Sie haben vom DSB Anweisungen erhalten und die Agentur führt derzeit Schulungen und Informationsveranstaltungen durch. Dieses Verfahren ist zu begrüßen und sollte von allen anderen Agenturen übernommen werden.

Empfänger eine Erklärung unterzeichnen, die sie ausdrücklich daran erinnert, dass sie die empfangenen Daten nur für den Zweck, für den sie übermittelt wurden, verarbeiten dürfen.

Der EDSB empfiehlt, die vorgenannten Punkte ii) und iii) zusammen mit der unter Punkt 2.3 genannten Empfehlung umzusetzen. Folglich sollten die betreffenden Agenturen im Hinblick auf sowohl Artikel 10 Absatz 3 als auch Artikel 7 Absatz 3 der Verordnung (EG) Nr. 45/2001 interne Vermerke oder Erklärungen abfassen, die von den Mitarbeitern zu unterzeichnen sind.

Externe Übermittlung

i) Übermittlung im Lichte von Artikel 8 der Verordnung
Artikel 8 der Verordnung legt die Bedingungen fest, unter denen personenbezogene Daten an Empfänger übermittelt werden dürfen, die den aufgrund der Richtlinie 95/46/EG erlassenen nationalen Rechtsvorschriften unterliegen könnten.

Die **ETF**, das **ECDC**, die **FRA**, **REA**, **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **ERCEA**, **FRONTEX**, **EACI**, **EU-OSHA**, **ECHA**, **EUROFOUND**, **EASA** und **EMSA** liefern in ihren Meldungen keine Informationen zu einer etwaigen Übermittlung an Empfänger, die in den Geltungsbereich der Richtlinie fallen. Zwar sind solche Übermittlungen selten, doch sie können nicht ausgeschlossen werden. Falls die Agenturen z. B. nationalen Behörden Gesundheitsdaten übermitteln müssen, weil diese eine Untersuchung durchführen, sollte nachgewiesen werden, dass die Übermittlung im Sinne von Artikel 8 Buchstabe a der Verordnung notwendig ist. Darüber hinaus weist der EDSB darauf hin, dass bei der Zusammenarbeit mit nationalen Behörden die Anforderungen und Verfahren einzuhalten sind, die die nationalen Regelungen zur ärztlichen Schweigepflicht vorschreiben. In jedem Fall ist es äußerst wichtig, dass nur zweckentsprechende, erhebliche und nicht unverhältnismäßige Daten übermittelt werden dürfen.

ii) Übermittlung im Lichte von Artikel 9 der Verordnung
Artikel 9 der Verordnung bestimmt, dass personenbezogene Daten an Empfänger, die nicht den aufgrund der Richtlinie 95/46/EG erlassenen nationalen Rechtsvorschriften unterliegen, übermittelt werden dürfen, wenn das Drittland oder die internationale Organisation ein angemessenes Schutzniveau gewährleisten Die Angemessenheit des Schutzes sollte im Hinblick auf die in Artikel 9 Absatz 2 genannten Kriterien beurteilt werden. Artikel 9 Absatz 6 enthält Ausnahmebestimmungen. In allen Fällen, in denen Daten außerhalb des Geltungsbereichs der Richtlinie übermittelt werden, sollten die Agenturen die Einhaltung von Artikel 9 gewährleisten.

Bei einer solchen Übermittlung sollten die Agenturen die Einhaltung von Artikel 9 gewährleisten.

2.7. Recht auf Auskunft und Berichtigung

Artikel 13 der Verordnung sieht ein Auskunftsrecht vor und bestimmt die Modalitäten seiner Anwendung nach einem entsprechenden Antrag der betroffenen Person. Artikel 14 der Verordnung bestimmt: „*Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass unrichtige oder unvollständige personenbezogene Daten unverzüglich berichtigt werden.*“

Auskunftsrecht

Eingestellte Mitarbeiter

i) Recht auf freie und ungehinderte Auskunft innerhalb angemessener Fristen
Die meisten Agenturen lassen die medizinischen Daten ihrer Mitarbeiter extern verarbeiten und

daher führen sie keine medizinischen Akten. Daher muss zwischen dem Auskunftsrecht im Hinblick auf einerseits die medizinische Akte und andererseits die Personalakte eines Mitarbeiters klar unterschieden werden.

- **Medizinische Akte des Mitarbeiters**

Der EDSB hält es für zweckdienlich, dass die **ECHA**, **EU-OSHA**, **EUA**, **EASA** und **EMSA** durch den Vertrag mit ihrem externen medizinischen Dienstleister/Berater sicherstellen, dass er eine angemessene Frist festlegt, in der ein Antrag auf freie und ungehinderte Auskunft gemäß der Richtlinie 95/46/EG zu bearbeiten ist. Dies sollte in den Datenschutzerklärungen, die die Betroffenen über ihre Rechte informieren, ausdrücklich erwähnt werden (siehe Punkt 2.8).

- **Personalakte des Mitarbeiters**

Die **ETF**, das **ECDC**, **CEDEFOP**, die **TEN-T EA**, **ERA**, **EAHC**, **ECHA**, **EUA** und **EMSA** sollten in ihrer Datenschutzerklärung oder in einem anderen Vermerk darauf hinweisen, dass nach Eingang eines entsprechenden Antrags gemäß Artikel 13 der Verordnung (EG) Nr. 45/2001 innerhalb einer angemessenen Frist freie und ungehinderte Auskunft über alle in der (von der Personalabteilung der Agentur geführten) Personalakte befindlichen Gesundheitszeugnisse, die im Rahmen von Einstellungs- und Jahresuntersuchungen ausgefertigt werden, erteilt wird.

ii) Auskunft in verständlicher Form

Diejenigen Agenturen, die auf externe medizinische Dienstleister zurückgreifen, d. h. die **ECHA**, **EASA**, das **CEDEFOP**, die **EUROFOUND**, **EUA**, **EU-OSHA**, **EMSA**, das **ECDC** und die **ETF**, sollten sicherstellen, dass die Ärzte, die für die Durchführung der ärztlichen Untersuchungen zuständig sind, den Betroffenen die medizinischen Ergebnisse in verständlicher Form mitteilen. Dies bedeutet, dass sie die Daten (z. B. medizinische Codes oder die Ergebnisse von Blutuntersuchungen) interpretieren und/oder die Entschlüsselung der Daten ermöglichen sollten.

iii) Kopien der medizinischen Akten

Falls Betroffene Kopien ihrer medizinischen Akten anfordern, sollten die **ECHA**, **EU-OSHA**, **EASA** und **EMSA** sicherstellen, dass die Ärzte, die für ihre medizinische Akten zuständig sind, diesem Wunsch nachkommen.

iv) Auskunft über psychologische oder psychiatrische Daten

Soweit es sich bei den verarbeiteten Daten um psychologische oder psychiatrische Daten handelt, sollten die **ETF**, das **ECDC**, die **REA**, **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **ERCEA**, **FRONTEX**, **ECHA**, **EU-OSHA**, **EACI**, **EUROFOUND**, **EASA** und **EMSA** sicherstellen, dass die Betroffenen mittelbar Auskunft erhalten, wenn auf Einzelfallbasis festgestellt wird, dass gemäß Artikel 20 Absatz 1 Buchstabe c der Verordnung zum Schutz des Betroffenen eine mittelbare Auskunft notwendig ist. Die Möglichkeiten für eine mittelbare Auskunftserteilung sollten im Lichte der Schlussfolgerungen 221/04 vom 19. Februar 2004 ausgestaltet werden und die vorgenannten Agenturen sollten die Betroffenen über diese Möglichkeiten informieren (siehe Punkt 2.8).

<u>Nicht eingestellte Mitarbeiter, Besucher, Praktikanten</u>

Den Meldungen zufolge werden einige Gruppen von Betroffenen nicht berücksichtigt, z. B. nicht eingestellte Personen, Besucher, Praktikanten und sonstige Personen, die während ihres Aufenthalts in den Agenturen ärztlich behandelt werden könnten. Daher sollten das **ECDC**, die **REA**, **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **FRONTEX**, **ECHA**, **EU-OSHA**, **EACI**, **EASA** und **EMSA** diesen Betroffenen das Recht einräumen, auf Antrag Auskunft über die verarbeiteten Daten zu erhalten, die sich auf ihren Gesundheitszustand beziehen. Diese Information sollte in die Datenschutzerklärung aufgenommen werden.

Berichtigungsrecht

Die **ETF**, **FRA**, **REA**, das **CEDEFOP**, die **TEN-T EA**, **ERA**, **EAHC**, **EUFA**, **ERCEA**, **FRONTEX**, **ECHA**, **EU-OSHA**, **EUROFOUND**, **EUA**, **EASA** und **EMSA** sollten sicherstellen, dass dieses Recht von den Betroffenen verstanden wird (z. B. durch entsprechende Informationen in der Datenschutzerklärung) und ihnen gewährt wird, und zwar nicht nur das Recht auf Berichtigung etwaiger administrativer Fehler in ihrer medizinischen Akte, sondern auch das Recht auf Ergänzung der Akte durch Zweitgutachten weiterer Ärzte.

2.8. Informationspflicht gegenüber der betroffenen Person

Die Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 bestimmen, dass die Betroffenen über die Verarbeitung von Daten, die sich auf sie beziehen, informiert werden müssen, und sie führen eine Reihe allgemeiner und ergänzender Punkte auf. Die ergänzenden Informationen sind anwendbar, sofern sie unter Berücksichtigung der spezifischen Umstände der Verarbeitung notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten. Im vorliegenden Fall werden die medizinischen Daten teilweise vom Betroffenen und teilweise vom medizinischen Dienst der Kommission oder externen Ärzten und medizinischen Dienstleistern geliefert.

Datenschutzerklärung

Die Informationen, die die **ETF** unter Punkt 1.7 des Schreibens an den EDSB geliefert hat, sind für das Recht auf Information nicht erheblich. Außerdem hat die **ETF**, obwohl sie in der Meldung alle Informationen im Sinne der Artikel 11 und 12 aufgeführt hat, keine Datenschutzerklärung verfasst, in der den Betroffenen die nach diesen Bestimmungen erheblichen Informationen erläutert werden. Daher ersucht der EDSB die **ETF** im Lichte der EDSB-Leitlinien, den Betroffenen eine Datenschutzerklärung zu unterbreiten, die einfach zugänglich ist und in der alle in den Artikeln 11 und 12 angeführten Informationen erläutert werden.

Das **ECDC** sollte die Datenaufbewahrungsfristen in den Datenschutzerklärungen zur Einstellungsuntersuchung und zur ärztlichen Jahresuntersuchung ergänzen (siehe Punkt 2.5) und die Betroffenen darauf hinweisen, dass ein externer medizinischer Dienst ihre medizinischen Akten aufbewahrt, wohingegen Personalakten von der Personalabteilung der Agentur geführt werden.

Der EDSB empfiehlt, dass die **FRA**, **REA**, **TEN-T EA**, **FRONTEX, EU-OSHA**, **EUROFOUND**, **EUA** und **EASA** so bald wie möglich eine Datenschutzerklärung abfassen, die alle Rechte der Betroffenen gemäß den Artikeln 11 und 12 der Verordnung aufführt.

Das **CEDEFOP** hat Angaben dazu gemacht, welche Informationen es gemäß den Artikeln 11 und 12 der Verordnung in der Datenschutzerklärung übermitteln möchte. Sobald eine Datenschutzerklärung mit Hinweisen auf alle zweckdienlichen Informationen abgefasst ist, sollte dem EDSB eine Kopie zugesandt werden.

Der EDSB ist der Auffassung, dass die „*besondere Datenschutzerklärung e-HR*“ der **ERA** für die Verarbeitung gesundheitsbezogener Daten durch die Agentur nicht erheblich ist. Daher wird empfohlen, dass eine geeignete Datenschutzerklärung zu den besonderen Verarbeitungen der Agentur ausgearbeitet wird. Sie sollte den Betroffenen alle maßgeblichen Informationen im Sinne der Artikel 11 und 12 erläutern.

Die **EAHC** hat in ihrer Meldung angegeben, dass die maßgeblichen Informationen im Intranet zu

finden seien. Die **EMSA** hat dem EDSB einige Links zu Dokumenten im Intranet übermittelt, die für die Artikel 11 und 12 der Verordnung nicht maßgeblich zu sein scheinen. Daher fordert der EDSB die **EAHC** und die **EMSA** auf, eine Datenschutzerklärung zu Verarbeitungen im Zusammenhang mit Einstellungsuntersuchungen, Jahresuntersuchungen und krankheitsbedingten Fehlzeiten auszuarbeiten. Die Datenschutzerklärung sollte eindeutige und detaillierte Informationen zum Recht des Betroffenen auf Information im Sinne der Aufzählung in den Artikeln 11 und 12 der Verordnung enthalten.

Der Zweck der Verarbeitung, der nach der Datenschutzerklärung der **EUFA** darin besteht, „*die Rechte und Pflichten der EUFA-Mitarbeiter und ANS zu verwalten*", ist vage und missverständlich formuliert. Der EDSB empfiehlt, dass die Agentur einen Satz hinzufügt, aus dem hervorgeht, dass der Zweck der Verarbeitung die Rechte und Pflichten der Agenturmitarbeiter *im Zusammenhang mit der Verarbeitung ihrer gesundheitsbezogenen Daten betrifft*.

Nach Auffassung des EDSB betrifft die Datenschutzerklärung der **ERCEA** das Einstellungsverfahren und das Anlegen von Personalakten. Dies ist nicht ausreichend, da die von der Agentur verarbeiteten gesundheitsbezogenen Daten von der Erklärung nicht erfasst sind. Aus diesem Grund empfiehlt der EDSB, dass eine angemessene Datenschutzerklärung abgefasst wird, die alle Rechte im Sinne der Artikel 11 und 12 im Zusammenhang mit den infrage stehenden besonderen Verarbeitungen aufführt.

Die Schreiben, mit denen die **ECHA** die Betroffenen auffordert, sich einer Einstellungsuntersuchung beim medizinischen Dienst der Kommission und im medizinischen Zentrum in Helsinki zu unterziehen, enthalten einen Datenschutzhinweis. Der gleiche Datenschutzhinweis findet sich auch in den Schreiben, die sich auf die Jahresuntersuchung, Sonderurlaub zur ärztlichen Behandlung und krankheitsbedingtes Fernbleiben vom Arbeitsplatz beziehen.
Die **ECHA** sollte darüber hinaus einen Datenschutzhinweis ausarbeiten, der sich auf ärztliche Untersuchungen durch externe medizinische Berater bezieht.
Sie sollte die Empfehlungen, die der EDSB zum Auskunfts- und Berichtigungsrecht (siehe Punkt 2.7) abgegeben hat, in all ihren Datenschutzhinweisen berücksichtigen. Darüber hinaus sollte sie im Lichte der EDSB-Leitlinien für Gesundheitsdaten die folgenden Informationen hinzufügen:

- die Rechtsgrundlage für die einzelnen Verarbeitungen von Gesundheitsdaten;
- die Aufbewahrungsfrist für medizinische Daten, die der externe medizinische Berater für eingestellte und nicht eingestellte Personen aufbewahrt;
- die Aufbewahrungsfrist für Daten in Verbindung mit krankheitsbedingten Fehlzeiten und
- das Recht der Betroffenen, sich jederzeit an den EDSB zu wenden.

Der EDSB weist alle Agenturen darauf hin, dass die Datenschutzerklärung nicht nur an alle neu eingestellten Mitarbeiter (wie die **REA** in ihrer Meldung angegeben hat), sondern an das gesamte Personal der Agenturen zu richten ist. Sie sollte z. B. auf der Website der jeweiligen Agentur leicht zu finden sein.

Zusätzliche Informationen

Neben den Rechten, die in den Artikeln 11 und 12 aufgeführt sind, sollte die Datenschutzerklärung weitere Informationen zu den infrage stehenden Verarbeitungen enthalten. Der EDSB weist erneut auf die Empfehlungen hin, die er in seinen Leitlinien für Gesundheitsdaten abgegeben hat.

Die **REA**, **TEN-T EA**, **ERA**, **ERCEA**, **FRONTEX, EAHC, EU-OSHA, EUROFOUND, EUA,** das **CEDEFOP,** die **EASA** und **EMSA** sollten in der Datenschutzerklärung angeben, welcher

Akteur (medizinischer Dienst der Kommission, externer Dienstleister, Arzt der Agentur) für die Durchführung der Einstellungs-, Jahres- und sonstigen Untersuchungen zuständig ist und wo die medizinischen Akten der Mitarbeiter aufbewahrt werden.

Die **REA**, das **CEDEFOP**, die **TEN-T EA**, **ERA**, **EAHC**, **ERCEA**, **FRONTEX, EU-OSHA, EUROFOUND** und **EUA** sollten darüber hinaus angeben, welche gesundheitsbezogenen Daten von den Personalabteilungen der Agenturen erhoben und gespeichert werden und zu welchen Zwecken dies geschieht.

Medizinische Fragebögen

Die **ETF** sollte auf den beiden Fragebögen „sorveglianza sanitaria" und „visite periodiche" (die Fragebögen werden bei der Jahresuntersuchung vom medizinischen Berater der Agentur verwendet) angeben, ob die Beantwortung der Fragen freiwillig oder verpflichtend ist und welche Konsequenzen sich gegebenenfalls aus der Nichtbeantwortung ergeben.

Ärztliche Kontrolluntersuchungen

i) Wahl eines Hausarztes

Im Hinblick auf ärztliche Kontrolluntersuchungen sollten die **ETF, REA, TEN-T EA, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EUA**, **EASA** und **EMSA** die Betroffenen darüber informieren, dass sie selbst ihren Hausarzt auswählen dürfen und wie sie praktisch vorgehen müssen, wenn sie die Untersuchung von einem Arzt ihrer Wahl durchführen lassen wollen.

ii) Übermittlung der ärztlichen Untersuchungsergebnisse

Darüber hinaus sollten die **ETF, REA,** das **CEDEFOP,** die **TEN-T EA, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EUA**, **EASA** und **EMSA** in der Datenschutzerklärung darlegen, ob der Hausarzt des Betroffenen die Ergebnisse der ärztlichen Untersuchung an den Arzt der Agentur oder den medizinischen Dienst der Kommission oder einen externen medizinischen Dienstleister weiterleiten muss und zu welchem Zweck eine solche Weiterleitung erfolgt. Der EDSB weist nachdrücklich darauf hin, dass − wie in den Leitlinien erläutert − die medizinischen Ergebnisse einer Jahresuntersuchung ohne die in Kenntnis der Sachlage und ohne Zwang erteilte Einwilligung des Betroffenen in keinem Fall an den Arzt der Agentur oder den medizinischen Dienst der Kommission weitergeleitet werden dürfen.

iii) Mittelbare Auskunft über psychologische oder psychiatrische Daten

Schließlich empfiehlt der EDSB, dass die **ETF,** das **ECDC,** die **FRA, REA,** das **CEDEFOP,** die **TEN-T EA, ERA, EAHC, EUFA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EUA**, **EASA** und **EMSA** die Betroffenen in der Datenschutzerklärung oder einem internen Vermerk über die Möglichkeit informieren, im Lichte der Schlussfolgerungen 221/04 vom 19. Februar 2004 mittelbar Auskunft über psychologische oder psychiatrische Daten zu erhalten.

2.9. Sicherheit

Gemäß Artikel 22 der Verordnung (EG) Nr. 45/2001 „*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*".

Der EDSB stellt fest, dass die Kommission mit zahlreichen Agenturen, z. B. der **EACI, EAHC, ERCEA, REA** und **ERA**, Vereinbarungen (Memoranda of Understanding, MoU) über die Geltung des Sicherheitskonzepts für die Informationssysteme der Europäischen Kommission

getroffen hat. Außerdem hat die **ERCEA** einen kurzen Sachstandsbericht über die Ausarbeitung des IT-Sicherheitskonzepts durch ihren Beauftragten für die lokale IT-Sicherheit verfasst[7]. Die MoU soll jedoch weder das IT-Sicherheitskonzept der Agentur noch etwaige zu treffende Sicherheitsmaßnahmen im Sinne von Artikel 22 der Verordnung ersetzen.

Wie unter Punkt 2.4 dargelegt, scheinen die **ETF**, das **ECDC**, die **FRA**, **REA**, **ERA**, **EAHC**, **EUFA**, **FRONTEX**, **EU-OSHA**, **EACI**, **EUROFOUND**, **EUA** und **EMSA** keinen Prüfpfad angelegt zu haben, mit dem sich die Aktivitäten der Nutzer nachvollziehen lassen, insbesondere im Falle krankheitsbedingter Fehlzeiten, bei denen gesundheitsbezogene Verwaltungsdaten elektronisch erhoben werden. Diese Sicherheitsmaßnahme sollte gemäß den technischen und organisatorischen Maßnahmen, die in Artikel 22 der Verordnung vorgesehen sind, getroffen werden.

Darüber hinaus stellt der EDSB fest, dass einige Agenturen Dokumente zu ihrer Informations- und Kommunikationspolitik im IT-Bereich übermittelt haben. Diese Dokumente sind für die speziellen Anforderungen von Artikel 22 der Verordnung nicht erheblich. Daher empfiehlt der EDSB, dass alle Agenturen ein eigenes spezifisches Sicherheitskonzept erarbeiten, das die Elemente berücksichtigt, die in Artikel 22 Absatz 2 Buchstaben a bis j der Verordnung aufgeführt sind. Dieses spezifische Sicherheitskonzept sollte auf einer von jeder Agentur durchzuführenden Risikobewertung basieren und im Rahmen der tatsächlichen Verarbeitung von medizinischen und/oder gesundheitsbezogenen Daten am jeweiligen Standort der Agentur umgesetzt werden. Jede Agentur sollte dem EDSB eine Abschrift über ihre spezifischen Sicherheitsmaßnahmen zukommen lassen.

2.10. Vergabe von Unteraufträgen

Im Lichte von Artikel 23 der Verordnung sollten die Agenturen einen Auftragsverarbeiter auswählen, der gewährleisten kann, dass im Rahmen der Verarbeitung medizinischer Daten angemessene technische und organisatorische Sicherheitsvorkehrungen getroffen werden können.

Der EDSB hat drei Gruppen identifiziert, an die Aufträge vergeben werden können:
i) der medizinische Dienst der Kommission handelt als Auftragsverarbeiter der Agentur und die Verarbeitung ist durch eine SLA geregelt;
ii) ein externes medizinisches Zentrum führt einige bzw. die Mehrzahl der ärztlichen Untersuchungen im Namen der Agentur durch; und
iii) der medizinische Berater verarbeitet medizinische Daten im Namen der Agentur an ihrem Standort.

Der EDSB weist darauf hin, dass bei der Umsetzung von Sicherheitsmaßnahmen unterschiedlich vorzugehen ist, je nachdem, welche der vorgenannten Gruppen betroffen ist:

- Im Falle von SLAs wurden die Sicherheitsvorkehrungen bereits von der Kommission getroffen. Selbstverständlich bedeutet dies jedoch nicht, dass die Agenturen an ihren Standorten kein eigenes Sicherheitssystem einrichten sollen (siehe Punkt 2.9).
- Soweit Agenturen Verträge mit externen medizinischen Zentren geschlossen haben, sollten sie sicherstellen, dass ein angemessenes Sicherheitsniveau festgelegt und vom externen Auftragnehmer gemäß Artikel 23 Absatz 2 Buchstabe b und Absatz 3 der Verordnung umgesetzt wird.
- Soweit die medizinischen Berater ihre Aufgaben am Standort der Agenturen wahrnehmen,

[7] Der Beauftragte für die lokale IT-Sicherheit der **ERCEA** hat den EDSB mit Schreiben vom 23. September 2010 über die laufenden Arbeiten zur Ausarbeitung des IT-Sicherheitskonzepts im Bereich gesundheitsbezogener Daten informiert.

sollten die Agenturen in ihrem Vertrag mit dem medizinischen Berater sicherstellen, dass der Berater die internen Sicherheitsmaßnahmen der Agentur beachtet, die gemäß Artikel 23 Absatz 1 der Verordnung mit Artikel 22 übereinstimmen müssen.

Insbesondere die **EU-OSHA** sollte dafür sorgen, dass gemäß Artikel 23 der Verordnung ein Vertrag oder ein sonstiger verbindlicher Rechtsakt zwischen dem externen medizinischen Dienst und der Agentur geschlossen wird. Dieser Rechtsakt sollte festlegen, dass der Auftragsverarbeiter nur auf Weisung der Agentur handeln darf. Außerdem sollte der Dienstleister den nationalen Rechtsvorschriften unterliegen, die Artikel 16 oder Artikel 17 Absatz 3 zweiter Spiegelstrich der Richtlinie 95/46/EG durchführen, und er muss die Einhaltung der nationalen Rechtsvorschriften im Hinblick auf Sicherheit und Vertraulichkeit gewährleisten. Sobald die **EU-OSHA** einen Vertrag abgeschlossen hat, der diese Aspekte berücksichtigt, sollte sie dem EDSB eine Abschrift zukommen lassen.

Die **EAHC** und die **EASA** haben 2006 eine SLA mit dem medizinischen Dienst der Kommission in Luxemburg abgeschlossen. Die SLA enthält jedoch keine Bestimmungen zur Anwendbarkeit der Verordnung. Der EDSB hebt hervor, dass die SLAs, die 2008 von den betreffenden Agenturen mit dem medizinischen Dienst der Kommission in Brüssel abgeschlossen wurden, eine Regelung zur Verordnung (EG) Nr. 45/2001 enthalten. Daher empfiehlt der EDSB, dass die **EAHC** und die **EASA** ihre SLA mit dem ärztlichen Dienst der Kommission in Luxemburg aktualisieren und eine Bestimmung aufnehmen, die den medizinischen Dienst zur Anwendung der Verordnung verpflichtet.

Die **ETF**, die **ECHA**, das **CEDEFOP**, die **EUROFOUND** und die **EASA** haben dem EDSB ähnliche Abschriften ihrer Verträge mit den als Auftragsverarbeiter handelnden externen medizinischen Dienstleistern und medizinischen Beratern übermittelt. Der EDSB empfiehlt ihnen, die folgenden Punkte in die Verträge aufzunehmen:

- Die **ECHA**, **EASA** und **EMSA** sollten ihre Verträge mit externen medizinischen Zentren um einen Zusatz ergänzen, der die Sicherheitsmaßnahmen, die von der Agentur verlangt werden und die der Auftragsverarbeiter gemäß Artikel 23 Absatz 2 Buchstabe b und Absatz 3 der Verordnung umzusetzen hat, eindeutig bestimmt.
- Die **ETF**, **ECHA** und **EASA** sollten in ihren Verträgen mit medizinischen Beratern die Sicherheitsmaßnahmen darlegen, die sie an ihrem Standort getroffen haben, und sie sollten im Lichte von Artikel 23 Absatz 1 der Verordnung sicherstellen, dass das Schutzniveau vom medizinischen Berater gewahrt wird.
- Was die Artikel I.9 der Verträge im Hinblick auf den Datenschutz betrifft, weist der EDSB darauf hin, dass der bloße Verweis auf die personenbezogenen Daten des Auftragnehmers und das Recht auf Auskunft über diese Daten nicht ausreicht. Auch die Betroffenen sollten einbezogen werden, da sie Gegenstand der Vertragsdurchführung sind. Daher empfiehlt der EDSB, dass die **ETF**, **ECHA**, **EASA** und **EMSA** in allen Verträgen jeden Verweis auf den „Auftragnehmer" in Artikel I.9 durch den Zusatz „*und die Betroffenen, deren Daten vom Auftragnehmer verarbeitet werden*" ergänzen.

Die **EUROFOUND** verweist in Artikel I.8 ihres Vertrags auf den „Auftragnehmer" und sollte ebenfalls den Zusatz „*und die Betroffenen, deren Daten vom Auftragnehmer verarbeitet werden*" aufnehmen.

Das **ECDC** und das **CEDEFOP** sollten eine datenschutzrechtliche Bestimmung sowie einen Zusatz über die Sicherheitsmaßnahmen, die sie vom Auftragsverarbeiter gemäß Artikel 23 Absatz 2 Buchstabe b und Absatz 3 der Verordnung verlangen, in ihre Verträge mit externen medizinischen Dienstleistern aufnehmen.

Die **EUA** hat dem EDSB keine Abschrift ihres Vertrags mit dem externen medizinischen Dienstleister übermittelt. Der EDSB empfiehlt der **EUA**, dafür Sorge zu tragen, dass der Vertrag mit den Anforderungen von Artikel 23 der Verordnung übereinstimmt, und er fordert sie auf, ihm eine entsprechende Abschrift des Vertrags zu übermitteln.

Schlussfolgerungen

Für die Agenturen haben sich die EDSB-Leitlinien als hilfreiches Instrument erwiesen, um die Auswirkungen der datenschutzrechtlichen Grundsätze der Verordnung (EG) Nr. 45/2001 auf die Verarbeitung von Daten im Zusammenhang mit Einstellungsuntersuchungen, Jahresuntersuchungen und krankheitsbedingten Fehlzeiten zu analysieren. Wie unter Punkt 2.1 dargelegt wurde, haben einige Agenturen trotz der eindeutigen Erläuterung, die die EDSB-Leitlinien zum weit gefassten Begriff „Gesundheitsdaten" enthalten, die Auffassung vertreten, dass die von ihnen verarbeiteten Daten keine besonderen Risiken im Sinne von Artikel 27 Absatz 2 Buchstabe a der Verordnung enthielten.

Darüber hinaus weist der EDSB im Zusammenhang mit der vorliegenden Analyse nachdrücklich auf zwei weitere Aspekte hin: die Rechtsgrundlage für die Vergabe von Unteraufträgen und die Datenschutzerklärung. Der EDSB stellt fest, dass einige Agenturen gemeinsame Elemente aus ihren Verträgen mit externen medizinischen Dienstleistern entfernt haben, insbesondere Sicherheitsmaßnahmen und datenschutzrechtliche Bestimmungen. Es handelt sich dabei um wesentliche Elemente, die in den Verträgen mit Auftragsverarbeitern enthalten sein sollten.

Des Weiteren ist den Agenturen die Bedeutung der Datenschutzerklärung nicht bewusst. Lediglich die **EACI** hat eine fast vollständige Datenschutzerklärung gemäß den Artikeln 11 und 12 der Verordnung verfasst. Der EDSB erinnert an den Grundsatz, dass die Verarbeitung nur dann rechtmäßig ist, wenn der Betroffene umfassend informiert wird, und daher sollten Informationen gemäß den Artikeln 11 und 12 der Verordnung übermittelt werden. Folglich sollte der für die Verarbeitung Verantwortliche den Betroffenen alle notwendigen Informationen über die Verarbeitung und diesbezügliche Rechte der Betroffenen verfügbar machen, bevor mit der Verarbeitung begonnen wird. Dies gilt insbesondere für Fälle, in denen die Verarbeitung auf der Einwilligung des Betroffenen beruht.

Im Rahmen seiner Durchsicht der DSB-Begleitschreiben, der Angaben in den Meldungen und einiger Anmerkungen zum Entwurf der Stellungnahme, der den DSB zur Kommentierung übermittelt wurde, erscheint dem EDSB der Hinweis geboten, dass die bloße Absicht oder Bestätigung, dass eine bestimmte datenschutzrechtliche Verfahrensweise gemäß den Leitlinien und Empfehlungen des EDSB angewandt werden wird, für die Umsetzung der EDSB-Empfehlungen nicht ausreicht. Vielmehr müssen konkrete Maßnahmen ergriffen werden. Nachdem der EDSB seine Stellungnahme abgegeben hat und diese dem für die Verarbeitung Verantwortlichen übermittelt worden ist, muss dieser die Empfehlungen des EDSB umfassend berücksichtigen, konkrete Maßnahmen zur schnellstmöglichen Umsetzung treffen und den EDSB über diese Maßnahmen in Kenntnis setzen. Dies erfolgt im Rahmen der Nachverfolgung der EDSB-Empfehlungen für Verarbeitungen, die der Vorabkontrolle unterliegen. Die Nachverfolgung sollte innerhalb von 3 Monaten nach Abgabe der Stellungnahme erfolgen.

Daher wird in jeder Agentur der für die Verarbeitung Verantwortliche im Lichte des kürzlich verabschiedeten EDSB-Strategiepapiers zur Überwachung und Gewährleistung der Einhaltung der

Verordnung (EG) Nr. 45/2001[8] hiermit aufgefordert, spezifische und konkrete Maßnahmen zu erlassen, um die Empfehlungen umzusetzen, die der EDSB für die Verarbeitung gesundheitsbezogener Daten abgegeben hat. Im Zusammenhang mit der Nachverfolgung sind die Agenturen somit verpflichtet, dem EDSB Dokumente zu übermitteln, die nachweisen, dass seine Empfehlungen tatsächlich umgesetzt wurden.

Geschehen zu Brüssel

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter

[8] Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001, Strategiepapier, 13. Dezember 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_DE.pdf.