Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Kommission für eine Vorabkontrolle über die Zutrittsgenehmigung und Zugangskontrolle für physischen Schutz (Entrance Permission and Access Control for Physical Protection) im JRC-ITU

Brüssel, 24. Juli 2012 (Fall 2008-0726)

I. Verfahren

Am 28. November 2008 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) der Kommission eine Meldung für eine Vorabkontrolle („die Meldung“) der Verarbeitungsvorgänge im Zusammenhang mit Zutrittsgenehmigungen und Zugangskontrolle zum physischen Schutz im **Institut für Transurane** der Gemeinsamen Forschungsstelle in Karlsruhe („JRC-ITU“).

Am 26. Januar 2009 forderte der EDSB zusätzliche Auskünfte an, die der DSB der Kommission am 20. Februar 2009 übersandte. Aufgrund der Zusatzinformationen verkomplizierte sich der Fall und eine genauere Prüfung wurde erforderlich. Daher beschloss der EDSB am 23. Februar 2009 eine Verlängerung der Prüfungsfrist um drei Wochen. Am 4. März 2009 wurde ein zweites Informationsersuchen zusammen mit dem Entwurf der Darstellung des Sachverhalts an den DSB der Kommission übermittelt. Am 9. April 2009 forderte der EDSB eine Rückmeldung zu zwei weiteren Fragen an.
Die Antworten gingen beim EDSB am 4. Mai 2009 ein.

Am 11. Mai 2009 übersandte der EDSB dem DSB der Europäischen Kommission den Entwurf seiner Stellungnahme zur Kommentierung. Am 5. Dezember 2011 und am 26. Juni 2012 wurden Erinnerungsschreiben an den DSB der Kommission gesandt. Kommentare zum Entwurf der Stellungnahme gingen beim EDSB jedoch nicht ein.

II. Sachverhalt

Das Zutrittsgenehmigungs- und Zugangskontrollsystem für physischen Schutz (Entrance Permission and Access Control for Physical Protection System) („EPACPP-System“) gehört zur Sicherheitsinfrastruktur des JRC-ITU und dient der Kontrolle und Verwaltung von Zugangsrechten zu den Räumlichkeiten des JRC-ITU. Darüber hinaus unterstützt das EPACPP den Strahlenschutzdienst des JRC-ITU bei der Kontrolle des Strahlenschutzstatus von Besuchern. Gegenstand der Vorabkontrolle ist die Verarbeitung der Daten für den erstgenannten Zweck. Datenschutzfragen im Zusammenhang mit dem zweiten Zweck werden

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

an dieser Stelle nicht behandelt, da der EDSB bereits eine Vorabkontrolle der Verarbeitungen im Zusammenhang mit Strahlenexposition durch Dosimetrie-Messungen vorgenommen hat[1].

In diesem Zusammenhang ist das erhebliche Interesse der Öffentlichkeit an der Sicherheit der Aktivitäten zu berücksichtigen, die Anlass für die Datenverarbeitung sind. Gleichzeitig kommt es darauf an, dass solche Sicherheitsmaßnahmen so durchgeführt werden, dass das Recht auf Datenschutz und auf Schutz der Privatsphäre nicht gefährdet wird.

Das EPACPP-System verfolgt einen doppelten ***Zweck***: *(i)* Kontrolle und Verwaltung der Zugangsrechte zum JRC-ITU. Dies gilt insofern für den gesamten Standort JRC-ITU, als das ganze JRC-ITU als Nuklearanlage gilt. *ii)* Kontrolle des Strahlenschutzstatus.

Hauptverantwortlich für die Datenverarbeitung ist das JRC-ITU, insbesondere dessen für die nukleare Sicherheit zuständige Referat (Referat E07), das für die hier zu prüfende Verarbeitung den für die Verarbeitung Verantwortlichen („JRC-ITU“) vertritt. Es kommen zwei Auftragsverarbeiter zum Einsatz, einer, der Aufgaben im Bereich des physischen Schutzes wahrnimmt (bezeichnet als „Gruppe Physischer Schutz“), und ein anderer, der die für die Datenverarbeitung verwendete Software und Hardware entwickelt.

Der ***Ablauf der Verarbeitung*** lässt sich folgendermaßen beschreiben:

Zur Verarbeitung der Daten von Besuchern und Kurzzeitauftragnehmern:

i) *Erfassungsphase*: In dieser Phase füllen Besucher und Kurzzeitauftragnehmer ein Formular („Antragsformular“) mit Angaben zu ihrer Identität, ihrem Geburtsort, ihrer Staatsangehörigkeit, ihrer Passnummer, ihrer Privatanschrift und ihrem Arbeitgeber aus. Darüber hinaus macht die besuchte Person in dem Antragsformular Angaben zur Dauer des Aufenthalts, zur Notwendigkeit des Zutritts zu kontrollierten Bereichen und zum Grund des Aufenthalts und der/den besuchten Person(en). Diese Informationen werden an die DS der GD ADMIN weitergeleitet, damit diese eine Unbedenklichkeitsbescheinigung ausstellen kann (siehe weiter unten).

ii) *Ausstellen einer Ausweiskarte:* Nach Prüfung des Antragsformulars und nach Eingang der Unbedenklichkeitsbescheinigung wird von Mitarbeitern der Gruppe Physischer Schutz ein Ausweis mit den genehmigten Zugangsrechten ausgestellt. Der Ausweis enthält den Vor- und Nachnamen, die Ausweisnummer sowie ein Foto, mit dessen Hilfe die Person und ihre Zugangsrechte zu den verschiedenen Sicherheitsbereichen jederzeit identifiziert werden können.

iii) *Verwendung der Ausweiskarte:* Sobald der Ausweiskarteninhaber einen Sicherheitsbereich betreten möchte, erfolgt durch die Gruppe Physischer Schutz bzw. durch Wachpersonal, das Aufgaben im Bereich des physischen Schutzes wahrnimmt, eine Überprüfung der Identität der Person und ihrer Zugangsrechte.

iv) *Datenspeicherung:* Alle Daten werden in die zentrale Datenbank ZES der Gruppe Physischer Schutz eingegeben.

[1] Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission zur Vorabkontrolle von „AGS-EDV-Datenbank beim JRC-ITU in Karlsruhe“, Brüssel, 10. Januar 2008 (Fall 2007-0378).

Verarbeitung von Daten von Kommissionsbediensteten des ITU und von Langzeitauftragnehmern (zusammen als „ITU-Mitarbeiter“ bezeichnet), die täglich Zutritt zu Nuklearbereichen oder anderen Sicherheitsbereichen benötigen:

Bei ITU-Mitarbeitern erfolgt die vorstehend beschriebene Verarbeitung bei Aufnahme ihrer Tätigkeit für das ITU. Darüber hinaus findet eine weitere Verarbeitung statt, die das Scannen [biometrischer Daten] umfasst:

i) *Erfassungsphase*: In dieser Phase nimmt [eine Kamera] Schwarzweißaufnahmen der [biometrischen Daten] von ITU-Mitarbeitern auf (bezeichnet als „[...]-Codes“). Dies geschieht durch Bedienungspersonal, das in Verfahren zur Erfassung biometrischer Daten besonders geschult wurde. Durchgeführt wird dies von der Gruppe Physischer Schutz im Antragsbüro („Application Office“) in den Räumlichkeiten des ITU, einem der Sicherheitsbereiche mit eingeschränktem Zugang. Bei „Falschrückweisungen“ ist vorgesehen, dass nach der Identifizierung durch das Wachpersonal eine manuelle Kontrolle vorgenommen wird.

Erfasst werden alle ITU-Mitarbeiter (also Kommissionsbedienstete und Langzeitauftragnehmer), da der gesamte Standort des JRC-ITU als Nuklearanlage gilt. Betroffen sind rund 400 Mitarbeiter des ITU.

ii) *Speicherung [biometrischer Daten]:* Die Bilder [biometrischer Daten] werden in einer [...]-Code-Datenbank gespeichert. Wie bereits beschrieben, werden die Identifizierungsdaten in der zentralen Datenbank ZES gespeichert. Damit soll sichergestellt werden, dass der „[...]-Code“ nur verwendet werden kann, wenn jemand gleichzeitigen Zugriff auf beide Datenbanken hat. Der Zugriff auf beide Datenbanken ist auf die Gruppe Physischer Schutz beschränkt.

iii) *Scannen [biometrischer Daten]:* [...]Im vorliegenden Fall wendet das JRC-ITU EPACPP den Suchmodus „Vergleich Eins-zu-viele“ an. Es werden jedoch nicht nur die [biometrischen Daten] überprüft; darüber hinaus werden die Personen gewogen, um messen zu können, dass jeweils nur eine autorisierte Person die Schleuse passiert. Bei Falschrückweisungen ist vorgesehen, dass durch das Wachpersonal eine manuelle Kontrolle und Identifizierung vorgenommen wird.

Der Server der zentralen Datenbank dient als administrative Schnittstelle zum System. Dort sind Informationen über die Nutzer und ihre Zugangsrechte gespeichert. Ferner werden dort alle erfolgreichen oder erfolglosen Zugangsversuche gespeichert.

Betroffene Personen sind Bedienstete des ITU und Langzeitauftragnehmer. Außerdem werden auch Daten von Besuchern und Kurzzeitauftragnehmern im Zusammenhang mit der Ausstellung befristeter Ausweiskarten verarbeitet.

Es werden folgende ***Kategorien personenbezogener Daten*** verarbeitet: i) Identifizierungsdaten (Name, Personalnummer, Bild, Geburtsdatum und Geburtsort, Staatsangehörigkeit, Privatadresse); ii) Angaben zur Berufstätigkeit (Name des Unternehmens, Beginn und Ende der Arbeit im JRC-ITU); iii) Informationen zur Unbedenklichkeitsbescheinigung; iv) Zugangsrechte und Login-Daten (Datum, Uhrzeit, Zugang gewährt oder verweigert), und v) Strahlenschutzinformationen (Ausbildung, beruflich bedingte Exposition).

Einige Informationen werden an die DS der GD ADMIN ***übermittelt***. Jeder aus einem nicht der EU angehörenden Land stammende Besucher, der Zugang zu den Räumlichkeiten des

ITU möchte, muss von der DS der GD ADMIN sicherheitsüberprüft werden. Zu diesem Zweck werden Daten wie Geburtsdatum und Geburtsort, Staatsangehörigkeit, Personalidentifizierungsnummer und Privatadresse, Unternehmen und Zweck des Besuchs an die DS der GD ADMIN weitergegeben. Bei einem Sicherheitszwischenfall können Informationen auch an die zuständigen nationalen Behörden in Deutschland übermittelt werden.

Zum Einsatz von ***Auftragsverarbeitern***, in diesem Fall der Gruppe Physischer Schutz und eines Privatunternehmens, das für die Pflege und Entwicklung der für die Datenverarbeitung verwendeten Software und Hardware zuständig ist. Nach den dem EDSB vorliegenden Informationen wurden mit den Auftragsverarbeitern Vereinbarungen getroffen, die gewährleisten, dass die Auftragsverarbeiter angemessene Sicherheitsmaßnahmen zum Schutz der Daten ergreifen.

Zum Thema ***Informationspflicht gegenüber der betroffenen Person*** besagt die Meldung, dass im Intranet des JRC-ITU sowie bei den Wachposten am Eingang zu den Räumlichkeiten des ITU eine Datenschutzerklärung zur Verfügung gestellt wird. Die Datenschutzerklärung enthält Folgendes: i) Erläuterung des Zutrittsgenehmigungs- und Zugangskontrollsystems des ITU; ii) Angaben dazu, welche personenbezogenen Daten für welchen Zweck und mit welchen technischen Mitteln erfasst wurden; iii) Angaben zum Schutz der Daten und zu Garantien; iv) Aufbewahrungsfrist; v) Hinweise auf die Rechte der betroffenen Person (auf Auskunft, Berichtigung und Löschung) und das Recht, sich an den EDSB zu wenden. Der DSB hatte die Datenschutzerklärung der Meldung beigefügt. In der Datenschutzerklärung werden die Rechte der betroffenen Person erläutert und werden Kontaktinformationen gegeben, damit betroffene Personen diese Rechte auch tatsächlich ausüben können.

Zur ***Datenaufbewahrung*** besagen Meldung und Datenschutzerklärung, dass Daten von Besuchern, die keinen Zugang zu eigentlichen Nuklearbereichen haben, fünf Jahre nach dem letzten Besuch gespeichert werden. Bei Mitarbeitern des JRC-ITU werden die Daten fünf Jahre nach Ablauf der Unbedenklichkeitsbescheinigung gelöscht. Diese Informationen werden aus folgendem Grund für diesen Zeitraum aufbewahrt: Bei den meisten Besuchern handelt es sich um Fachkräfte oder hochrangige Wissenschaftler, die regelmäßig, normalerweise über mehrere Jahre hinweg, das JRC-ITU besuchen. Deshalb hat das JRC-ITU beschlossen, die Daten für fünf Jahre aufzubewahren, um die Verlängerung der Unbedenklichkeitsbescheinigungen beantragen zu können, ohne von der betreffenden Person bei jedem Besuch im JRC-ITU die Daten erheben zu müssen.

Bei Besuchern und ITU-Mitarbeitern, die Zutritt zu den eigentlichen Nuklearbereichen haben und mit dosimetrischen Daten registriert sind, werden die Daten 95 Jahre nach dem Geburtsdatum der betroffenen Person aufbewahrt. Mit Ausnahme der [...]-Codes gilt dies für alle Daten. Sie werden aufbewahrt, um alle Zwischenfälle oder Fragen im Zusammenhang mit den Dosimetrie-Werten zurückverfolgen und die betreffende Person identifizieren und kontaktieren zu können.

Es werden ***Sicherheitsmaßnahmen*** durchgeführt. Die Informationen werden in gesicherten IT-Systemen gespeichert, die von der Gruppe Physischer Schutz betreut und verwaltet werden. Für den Zugriff auf das Datenbanksystem sind eine Nutzeridentifizierung und ein Passwort erforderlich. Die Sicherung der Daten erfolgt automatisch auf einem Bandlaufwerk. Alle Daten in Papierform werden in gesicherten Bereichen aufbewahrt.

III. Rechtliche Aspekte

III.1. Vorabkontrolle

Gegenstand dieser Vorabkontrollstellungnahme ist die Verarbeitung personenbezogener Daten durch das JRC-ITU, mit der die Identität von Personen kontrolliert wird, die das JRC-ITU betreten oder verlassen, und ihnen der Zugang genehmigt oder verweigert wird.

Die Verordnung (EG) Nr. 45/2001[2], gilt für die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind"* und für die Verarbeitung *„durch alle Organe und Einrichtungen der Gemeinschaft, soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen"*[3]. Aus den nachstehend dargelegten Gründen sind alle Elemente vorhanden, die die Anwendung der Verordnung auslösen.

Erstens werden personenbezogene Daten gemäß der Begriffsbestimmung in Artikel 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 erhoben und weiter verarbeitet. Zweitens werden die erhobenen personenbezogenen Daten einer in Artikel 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 definierten *„automatisierten Verarbeitung"* sowie manuellen Verarbeitungsvorgängen unterzogen. Die personenbezogenen Daten wie [biometrische] Daten werden nämlich tatsächlich erhoben und automatisiert verarbeitet, beispielsweise bei der Entnahme [biometrischer] Vorlagen. Schließlich erfolgt die Verarbeitung durch eine Einrichtung der EU, in diesem Fall durch das JRC-ITU in Karlsruhe, im Rahmen des EU-Rechts (Artikel 3 Absatz 1 der Verordnung (EG) Nr. 45/2001). Somit liegen bei dieser Verarbeitung alle Elemente vor, die die Anwendung der Verordnung auslösen.

In Artikel 27 Absatz 1 der Verordnung (EG) Nr. 45/2001 ist festgelegt, dass *„Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können"*, vom EDSB vorab kontrolliert werden. Der EDSB ist der Ansicht, dass das Vorhandensein einiger biometrischer Daten wie im vorliegenden Fall, in dem biometrische [...] genommen werden, besondere Risiken für die Rechte und Freiheiten betroffener Personen darstellen. Seine Ansicht stützt sich im Wesentlichen auf die aufgrund einiger diesen Daten innewohnenden Merkmale höchst heikle Natur biometrischer Daten. So verändern beispielsweise biometrische Daten die Beziehung zwischen Körper und Identität unwiderruflich, da sie die Merkmale des menschlichen Körpers maschinenlesbar und einer weiteren Nutzung zugänglich machen. Darüber hinaus hält der EDSB fest, dass bei solchen Daten Verknüpfungsmöglichkeiten und der neueste Stand technischer Instrumente zu Ergebnissen führen können, die von den betroffenen Personen nicht erwartet und/oder nicht erwünscht werden. Diese Risiken rechtfertigen eine Vorabkontrolle der Datenverarbeitung durch den EDSB, der die Einhaltung strenger Datenschutzvorkehrungen zu überprüfen hat.

Ex post-Vorabkontrolle. Da die Vorabkontrolle dazu dient, sich mit Situationen zu befassen, die gewisse Risiken beinhalten können, gibt der EDSB seine Stellungnahme idealerweise vor Aufnahme der Verarbeitungen ab. Im vorliegenden Fall wurden die Verarbeitungen jedoch bereits eingeleitet. Dies stellt kein unüberwindliches Hindernis dar, sofern alle Empfehlungen des EDSB umgesetzt und die Verarbeitungsvorgänge entsprechend angepasst werden.

[2] Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft (nunmehr der EU) und zum freien Datenverkehr („Verordnung (EG) Nr. 45/2001").

[3] Siehe Artikel 3 der Verordnung (EG) Nr. 45/2001.

Meldung und Frist für die Stellungnahme des EDSB. Die Meldung ging am 28. November 2008 ein. Die Frist für die Abgabe der Stellungnahme durch den EDSB wurde um drei Wochen verlängert. Die Frist für die Abgabe der Stellungnahme durch den EDSB wurde für insgesamt 1 256 Tage ausgesetzt, um weitere Auskünfte vom JRC-ITU anzufordern und Gelegenheit zur Äußerung zum Entwurf der Stellungnahme des EDSB zu geben.

III.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe nach Artikel 5 der Verordnung (EG) Nr. 45/2001 vorliegen.

Artikel 5 der Verordnung (EG) Nr. 54/2001 führt mehrere Gründe an, und die zur Vorabkontrolle gemeldete Verarbeitung fällt unter Artikel 5 Buchstabe a, dem zufolge Daten verarbeitet werden dürfen, 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“*.

Bei der Prüfung der Frage, ob die Verarbeitungen im Einklang mit Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001 stehen, sind drei Elemente zu berücksichtigen.

Erstens, ob entweder der Vertrag oder ein anderer Rechtsakt die geplanten Datenverarbeitungsvorgänge vorsieht („Rechtsgrundlage“). Nach Auffassung des EDSB gelten als ***Rechtsgrundlage*** für die Verarbeitung:

- Beschluss der Kommission 2001/844/EG, EGKS, Euratom (Sicherheitsbestimmungen);
- Beschluss der Kommission 2006/3602/EG betreffend die Sicherheit von Informationssystemen;
- IT-Sicherheitsstrategie der Kommission (PolSec);
- deutsche Rechtsvorschriften einschließlich i) Atomgesetz (AtG) §9+§12b+§12c in der Fassung vom 15.07.1985. (ii) Atomrechtliche Zuverlässigkeitsüberprüfungsverordnung (AtZüV) in der Fassung vom 1.7.1999 http://www.gesetze-im-internet.de/atz_v/index.html (iii) Strahlenschutzverordnung (StrlSchV) §42 in der Fassung vom 20.7.2001

Zweitens hält der EDSB im Hinblick auf die Frage, ob die Verarbeitungen im öffentlichen Interesse vorgenommen werden, fest, dass die Aufgabe des JRC-ITU darin besteht, die wissenschaftlichen Grundlagen für den Schutz der europäischen Bürger vor Risiken im Zusammenhang mit dem Umgang mit hochradioaktivem Material und dessen Lagerung bereitzustellen. Die Kommission nimmt die Verarbeitung in legitimer Ausübung ihrer öffentlichen Gewalt und unter Berücksichtigung des Interesses der Öffentlichkeit an einer ordnungsgemäßen und sicheren Durchführung dieser Forschungstätigkeit vor.

Schließlich stellt sich die Frage, ob die Verarbeitungen für die Wahrnehmung dieser Aufgabe tatsächlich erforderlich sind („Erforderlichkeitsprüfung“). Gemäß Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001 muss die Verarbeitung, wie bereits ausgeführt, „für die Wahrnehmung einer Aufgabe erforderlich“ sein. Hierzu besagt Erwägungsgrund 27 der Verordnung Folgendes: „*Die Verarbeitung personenbezogener Daten für die 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". Um dem hochsensiblen Charakter der Zielsetzung und der beim JRC-ITU verarbeiteten Informationen gerecht zu werden und den unerlaubten Zugriff auf diese sensiblen Informationen und deren Offenlegung zu verhindern, muss das JRC-ITU Hochsicherheitsmaßnahmen bei der Kontrolle des Zugangs zu den Räumlichkeiten des JRC-ITU durchführen können. Zu diesen Maßnahmen gehören auch strenge Zugangskontrollsysteme, bei denen biometrische Daten kontrolliert werden. Daher kann nach Auffassung des EDSB die Umsetzung strenger Zugangskontrollsysteme, die die Verarbeitung personenbezogener Daten einschließlich biometrischer Daten nach sich zieht, im vorliegenden Fall vernünftigerweise als notwendige interne Kontrollmaßnahme zum Schutz hochsensibler Daten und anderer Interessen der EU gelten.

III.3. Verarbeitung besonderer Datenkategorien

Die gemeldete Datenverarbeitung berührt keine Daten, die in die in Artikel 10 Absatz 1 der Verordnung (EG) Nr. 45/2001 genannten Datenkategorien fallen.

III.4. Datenqualität

Zweckentsprechung, Erheblichkeit und Verhältnismäßigkeit. Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung (EG) Nr. 45/2001 dürfen personenbezogene Daten nur den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, müssen dafür erheblich sein und dürfen nicht darüber hinausgehen. Dies wird als Grundsatz der Datenqualität bezeichnet. Im Zusammenhang mit der Prüfung der Frage, ob die hier zu behandelnde Verarbeitung, bei der im Wesentlichen biometrische Daten verarbeitet werden, diesem Grundsatz entspricht, merkt der EDSB Folgendes an:

i) Verantwortung für die Gesamtbeurteilung der Auswirkungen der Datenerhebung: Nach dem Verständnis des EDSB ist das JRC-ITU zu dem Schluss gelangt, dass die Datenverarbeitung einschließlich der Erhebung [biometrischer] Daten bezüglich anderer personenbezogener Daten für den Schutz der Gebäude des JRC-ITU erforderlich ist. Das JRC-ITU konnte jedoch nicht hinreichend belegen, dass es eine gründliche Beurteilung der Auswirkungen der Verwendung der Daten vorgenommen und die Gründe bewertet hat, aus denen diese Technik angewandt wurde, und auch nicht nachgewiesen hat, dass andere, weniger in die Privatsphäre eindringende Methoden in Erwägung gezogen wurden. Mit Blick auf die Zukunft und insbesondere auf mögliche Aktualisierungen des Systems sollte das JRC-ITU eine ordnungsgemäße Folgenabschätzung vornehmen, bei der nicht nur auf technische Aspekte und Sicherheitsaspekte eingegangen wird, sondern auch Fragen des Datenschutzes berücksichtigt werden.

ii) Beurteilung der Frage, ob die betroffenen Personen, deren Daten verarbeitet werden, angemessen sind: Die Meldung besagt, dass alle Mitarbeiter des JRC-ITU als betroffene Personen gelten. Weiter heißt es dort, das System sei für die Kontrolle der Identität und für die Gewährung oder Verweigerung des Zutritts an allen Ein- und Ausgängen des JRC-ITU konzipiert. Folglich muss sich jeder Mitarbeiter des JRC-ITU den Erfassungsverfahren unterziehen. Falls der gesamte Standort (Gebäude) des JRC-ITU als Nuklearanlage gilt, sollte das JRC-ITU die Zahl der erfassten Personen nicht auf eine ausgewählte Gruppe mit Zutritt zu bestimmten Einrichtungen beschränken. Aus den dem EDSB vorgelegten Informationen geht allerdings nicht klar hervor, ob Mitarbeiter, die Aufgaben außerhalb der Nuklear- und Sicherheitsbereiche (beispielsweise in der Verwaltung) wahrnehmen, den gleichen Sicherheitsgarantien unterliegen sollten. Hierzu und mit Blick auf mögliche Aktualisierungen

des Systems empfiehlt der EDSB dem JRC-ITU, die Möglichkeit zu prüfen, ob nicht die Erfassung von [...]-Codes auf die Mitarbeiter des JRC-ITU beschränkt werden kann, die in Nuklearbereichen und besonders gesicherten Bereichen tätig sind.

iii) Beurteilung der Frage, ob die Art der erhobenen Daten angemessen ist: Die Art der erhobenen Daten, bei denen es sich im Wesentlichen um die [biometrischen] Vorlagen und die dazu gehörenden Identifizierungsdaten handelt, entspricht den Daten, die für ein auf der Verarbeitung biometrischer Daten beruhendes Zugangskontrollsystem erforderlich sind. Damit entsprechen die erhobenen Daten nach Auffassung des EDSB den Zwecken der Verarbeitung und sind dafür erheblich.

Verarbeitung nach Treu und Glauben und Rechtmäßigkeit. Gemäß Artikel 4 Absatz 1 Buchstabe a der Verordnung dürfen personenbezogene Daten nur nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden. Die Frage der Rechtmäßigkeit wurde bereits erörtert (siehe Abschnitt III.2). Der Aspekt der Verarbeitung nach Treu und Glauben hängt eng damit zusammen, welche Informationen den betroffenen Personen zur Verfügung gestellt werden (siehe Näheres hierzu in Abschnitt III.8).

Sachliche Richtigkeit. Nach Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten *„sachlich richtig sein und, wenn nötig, auf den neuesten Stand gebracht"* werden, und es *„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 bestehen die personenbezogenen Daten hauptsächlich aus biometrischen Daten, die zu Zugangskontrollzwecken verwendet werden. Einige Schlüsselmerkmale biometrischer Systeme wirken sich unmittelbar auf das Ausmaß der sachlichen Richtigkeit der entweder in der Erfassungs- oder der Identifizierungsphase eines solchen Systems generierten Daten aus. Je nach der Ausformung des biometrischen Systems (mit diesen Schlüsselelementen oder ohne sie) ist die sachliche Richtigkeit der Daten betroffen oder nicht betroffen. Im Folgenden sollen diese Schlüsselelemente kurz beschrieben und soll der Frage nachgegangen werden, inwieweit sie in dem zu prüfenden biometrischen System berücksichtigt worden sind.

Erstens muss in der Erfassungsphase nach alternativen Möglichkeiten für die Identifizierung von Personen gesucht werden, die selbst vorübergehend für eine Erfassung nicht in Frage kommen. Dies wird üblicherweise als „Ausweichverfahren" bezeichnet[4]. Im vorliegenden Fall ist vorgesehen, dass Angehörige des zur Gruppe Physische Sicherheit gehörenden Wachpersonals, die an den Eingängen zu Sicherheitsbereichen postiert sind, manuell die Identität kontrollieren. In Anbetracht der Tatsache, dass der Anteil der Ausweichverfahren bei dieser Art von System sehr niedrig ist (0 % nach 12 Erfassungsrunden), dürften die vom JRC-ITU vorgesehenen Verfahren angemessen sein.

Zweitens sind ähnliche Maßnahmen auch für Personen vorzusehen, die zwar ordnungsgemäß erfasst wurden, aber falsch identifiziert werden (üblicherweise als „Falschrückweisung" bezeichnet). Sind diese Maßnahmen nicht in die Systemarchitektur eingebettet, könnte die Richtigkeit der vom System generierten Information gefährdet sein. Vor allem bei Falschrückweisungen erstellt das System einen Eintrag, dem zufolge eine bestimmte Person ohne die entsprechenden Zugangsrechte versucht hat, sich Zugang zu einem

[4] Eine Darstellung der Datenschutzgrundsätze, die für Ausweichverfahren gelten, findet sich in der Stellungnahme vom 13. Oktober 2006 zu dem Entwurf einer Verordnung (EG) des Rates zur Festlegung der Form der Ausweise für die Mitglieder und Bediensteten der Organe, ABl. C 313 vom 20.12.2006, S. 36.

Sicherheitsbereich zu verschaffen, obwohl die Person sehr wohl diese Zugangsrechte hatte. Gleichzeitig wird der betreffenden Person aufgrund der Fehlidentifizierung auch ein Recht verwehrt (das Recht auf Zugang zu bestimmten Bereichen), das ihr eigentlich gewährt werden müsste.

Bei einer Falschrückweisung oder anderen Problemen hat die betreffende Person beim „Application Office" der Gruppe Physischer Schutz Meldung zu erstatten. Nach Ansicht des EDSB sollte diese Lösung den Aufwand bei Falschrückweisungen verringern.

Drittens stützt sich das EPACPP des JRC-ITU auf [biometrische] Vorlagen, die in einer zentralen Datenbank gespeichert sind und mit dem Einsatz von Kameralesegeräten kombiniert sind. Der EDSB hält fest, dass dies die Verwendung biometrischer Daten für Zwecke der Identifizierung und Zugangskontrolle als „Vergleich Eins-zu-viele" zur Folge hat. Diese Art von Suchmodus führt nicht immer zu richtigen Ergebnissen. Das heißt, es können dabei Personen fehlidentifiziert werden und so falsche Aufzeichnungen entstehen. Ein alternativer Suchmodus wie „Eins-zu-eins" wirft diese Probleme nicht auf, da die biometrischen Daten nur mit einer Vorlage und nicht mit sehr vielen Vorlagen verglichen werden. Beim „Eins-zu-eins"-Suchmodus wird die Vorlage üblicherweise auf einem Chip gespeichert, der sich im Besitz der zu identifizierenden Person befindet. Die Vorlage kann aber auch in einer zentralen Datenbank gespeichert werden; in diesem Fall müsste sie jedoch an ein weiteres Identifizierungsinstrument gekoppelt sein, das folgendermaßen funktionieren könnte: So könnte beispielsweise eine mit einem Chip versehene Identifizierungskarte die Identität der Person an die Identifizierungseinheit senden, die wiederum die der Identität zugeordnete Vorlage mit den zu dem betreffenden Zeitpunkt der Einheit vorgelegten biometrischen Daten vergleicht. Wie darüber hinaus weiter unten beschrieben, bedeutet der Suchmodus „Eins-zu-eins" weniger Verarbeitung von Daten und trägt damit zur Wahrung des Grundsatzes der Verhältnismäßigkeit bei.

Im vorliegenden Fall wendet das JRC-ITU EPACPP den Suchmodus „Eins-zu-viele" an. [...]. Grundsätzlich befürwortet der EDSB den Einsatz des Suchmodus „Eins-zu-viele", bei dem die Identifizierungseinheit die [biometrischen Daten] der Person mit einer einzigen Vorlage vergleicht (die der Identität zugeordnet ist). Wie bereits ausgeführt, liefert ein solcher Suchmodus genauere Ergebnisse.

Der EDSB ist der Ansicht, dass im vorliegenden Fall die Fehlermarge in Anbetracht der relativ niedrigen Zahl von Vorlagen (rund 400) sehr klein ist, doch sollte seiner Auffassung nach grundsätzlich besser der Suchmodus „Eins-zu-eins" angewandt werden. Der Suchmodus „Eins-zu-eins" erbringt nicht nur genauere Informationen, sondern verringert auch das Ausmaß der Datenverarbeitung, da das System nur zwei zu einer Person gehörende Datensätze abgleichen muss (und nicht einen Datensatz mit den Vorlagen zahlreicher Personen vergleichen muss). Somit bedeutet dieser Suchmodus von Natur aus einen weniger starken Eingriff in die Privatsphäre. Bei der Entscheidung für den Suchmodus „Eins-zu-eins" ist zu berücksichtigen, dass Systeme, die biometrische Vorlagen auf Chips und nicht in zentralen Datenbanken speichern, datenschutzfreundlicher sind. Die Speicherung auf Chips ist insofern ein geringerer Eingriff in die Privatsphäre, als die Vorlage auf einem Träger (z. B. einem Dienstausweis mit Chip) gespeichert wird, der der jeweiligen betroffenen Person gehört. Damit hat die betroffene Person unmittelbar die Kontrolle über ihre Vorlage und trägt dafür die Verantwortung. Niemand sonst hat Zugriff auf ihre Vorlage oder besitzt sie. Ein weiteres Problem der Speicherung in Datenbanken besteht darin, dass damit das Risiko so genannter „Fishing Expeditions" entsteht, bei denen auf die Datenbank zu anderen Zwecken zugegriffen wird als denen, für die sie konzipiert wurde. Ein dezentrales System beseitigt dieses Risiko, ohne dass jedoch das Sicherheitsniveau gesenkt wird.

In Anbetracht dessen fordert der EDSB das JRC-ITU auf, seine weiter oben bereits erörterte Entscheidung für eine bestimmte Technologie zu überdenken und sich für die beste verfügbare Technik zu entscheiden. Eine solche Neubewertung ist für den EDSB von Bedeutung, damit er beurteilen kann, ob das EPACPP im Einklang mit Artikel 4 Absatz 1 Buchstabe d der Verordnung steht.

III.4. Datenaufbewahrung/Datenspeicherung

Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001 enthält den Grundsatz, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht, *„so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist. Die Organe oder Einrichtungen der Gemeinschaft sehen für personenbezogene Daten, die für ... statistische Zwecke über längere Zeiträume aufbewahrt werden sollen, vor, dass diese Daten entweder überhaupt nur in anonymisierter Form oder, wenn dies nicht möglich ist, nur mit verschlüsselter Identität der Betroffenen gespeichert werden".*

Gemäß der Meldung werden Daten von Besuchern, die keinen Zutritt zu den eigentlichen kerntechnischen Anlagen haben, nach dem letzten Besuch fünf Jahre aufbewahrt. Diese Informationen werden aus folgendem Grund für diesen Zeitraum aufbewahrt: Bei den meisten Besuchern handelt es sich um Fachkräfte oder hochrangige Wissenschaftler, die regelmäßig, normalerweise über mehrere Jahre hinweg, das JRC-ITU besuchen. Deshalb hat das JRC-ITU beschlossen, die Daten für fünf Jahre aufzubewahren, um die Verlängerung der Unbedenklichkeitsbescheinigungen beantragen zu können, ohne von der betreffenden Person bei jedem Besuch im JRC-ITU die Daten erheben zu müssen. Auch aus der Sicht des EDSB ist es erforderlich, in Anbetracht der für eine erneute Ausstellung einer Unbedenklichkeitsbescheinigung benötigten Daten die Daten für diesen Zeitraum aufzubewahren.

Bei Besuchern und ITU-Mitarbeitern, die Zutritt zu den eigentlichen Nuklearbereichen haben und mit dosimetrischen Daten registriert sind, werden die Daten 95 Jahre nach dem Geburtsdatum der betroffenen Person aufbewahrt. Mit Ausnahme der [...]-Codes gilt dies für alle Daten. Sie werden aufbewahrt, um alle Zwischenfälle oder Fragen im Zusammenhang mit den Dosimetrie-Werten zurückverfolgen und die betreffende Person identifizieren und kontaktieren zu können. Dieser Zeitraum ist sehr lang. Da jedoch die Speicherung genauer Dosimetrie-Daten später für die medizinische Behandlung der betreffenden Person und/oder im Hinblick auf mögliche Ansprüche aufgrund einer Berufskrankheit von großem Belang sein kann, ist der EDSB der Auffassung, dass dieser Zeitraum noch vertretbar ist.

Der EDSB entnimmt der Meldung, dass nach Ablauf der Aufbewahrungsfrist die personenbezogenen Daten nicht mehr für Statistiken verwendet werden dürfen. Dessen ungeachtet weist der EDSB darauf hin, dass bei einer Verwendung nach Ablauf der Aufbewahrungsfrist die Daten anonymisiert werden müssen (Artikel 4 Absatz 1 Buchstabe e der Verordnung).

III.5. Datenübermittlung

Die Meldung besagt, dass bei einem Sicherheitszwischenfall die Daten an die DS der GD ADMIN übermittelt werden. Der EDSB erinnert daran, dass nach Artikel 7 der Verordnung (EG) Nr. 45/2001 personenbezogene Daten nur übermittelt werden dürfen, wenn sie *„für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den*

Zuständigkeitsbereich des Empfängers fallen". Zur Einhaltung dieser Vorschrift hat der für die Verarbeitung Verantwortliche bei der Übermittlung personenbezogener Daten zu gewährleisten, dass i) der Empfänger die entsprechende Zuständigkeit hat und ii) die Übermittlung erforderlich ist.

Der Meldung ist zu entnehmen, dass die genannten Übermittlungen für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des jeweiligen Empfängers fallen. Die DS der GD ADMIN ist nämlich unter anderem für den Schutz von Personen, den Schutz von Gebäuden und Eigentum sowie den Schutz von Informationen sowie der Übermittlung und Verarbeitung von Daten zuständig. Damit Artikel 7 der Verordnung in vollem Umfang Genüge getan wird, empfiehlt der EDSB, allen Empfängern in Erinnerung zu rufen, dass sie die Daten nur für die Zwecke verarbeiten dürfen, für die sie übermittelt wurden.

Bei einem Sicherheitszwischenfall können diese Daten auch an die zuständigen nationalen Behörden in Deutschland weitergegeben werden; in solchen Fällen gilt Artikel 8 der Verordnung (EG) Nr. 45/2001. Artikel 8 der Verordnung (EG) Nr. 45/2001 bietet mehrere Rechtsgrundlagen für die Übermittlung personenbezogener Daten. Angesichts der im vorliegenden Fall gegebenen Umstände kann sich der für die Verarbeitung Verantwortliche auf Artikel 8 Buchstabe a berufen, dem zufolge personenbezogene Daten übermittelt werden dürfen, wenn die Daten für die Wahrnehmung einer Aufgabe, die zur Ausübung der öffentlichen Gewalt gehört, erforderlich sind, oder wenn die Datenübermittlung im berechtigten Interesse der betroffenen Person erfolgt. Gemäß Artikel 8 Buchstabe a der Verordnung (EG) Nr. 45/2001 hat zwar der Empfänger sein Interesse zu belegen, doch versteht der EDSB diese Bestimmung dahingehend, dass für den Fall, dass die Datenübermittlung nicht auf Ersuchen des Empfängers erfolgt, der Übermittelnde den Bedarf nachweisen muss.

Folglich hat der für die Verarbeitung Verantwortliche die Notwendigkeit der Datenübermittlung nachzuweisen, falls diese nicht auf Ersuchen des Empfängers vorgenommen wird. Zur Umsetzung dieser Vorschrift schlägt der EDSB dem für die Verarbeitung Verantwortlichen vor, in einer begründeten Stellungnahme alle Datenübermittlungen aufzulisten, die im Zusammenhang mit einem Fall durchgeführt werden sollen oder bereits durchgeführt worden sind, und ihre Notwendigkeit zu beschreiben. Diese Verfahren sollten allen zuständigen Mitarbeitern mitgeteilt werden.

III.6. Auftragsverarbeitung im Auftrag des für die Verarbeitung Verantwortlichen

Gemäß Artikel 23 der Verordnung kann eine Verarbeitung personenbezogener Daten im Auftrag eines für die Verarbeitung Verantwortlichen durch einen Auftragsverarbeiter nur auf der Grundlage eines Vertrags zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen durchgeführt werden. Im Vertrag muss geregelt sein, dass der Auftragsverarbeiter (bei der Datenverarbeitung) auf Weisung des für die Verarbeitung Verantwortlichen handelt. Der Auftragsverarbeiter hat zu gewährleisten, dass die geltenden Sicherheitsverpflichtungen eingehalten werden, die in diesem Fall in den nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG niedergelegt sind.

Im vorliegenden Fall greift der für die Verarbeitung Verantwortliche auf zwei Auftragsverarbeiter zurück, einen, der Aufgaben im Bereich des physischen Schutzes wahrnimmt (bezeichnet als „Gruppe Physischer Schutz"), und einen anderen, der die für die Datenverarbeitung verwendete Software und Hardware entwickelt. In Anbetracht des höchst sensiblen Charakters der Daten weist der EDSB nachdrücklich darauf hin, dass der für die

Verarbeitung Verantwortlich ein hohes Maß an Sicherheit zu gewährleisten hat. Nach Auffassung des EDSB hat der für die Verarbeitung Verantwortliche entsprechende Vereinbarungen abgeschlossen und wird somit nicht gegen Artikel 23 der Verordnung verstoßen.

III.7. Auskunftsrecht und Berichtigung

Gemäß Artikel 13 der Verordnung (EG) Nr. 45/2001 hat die betroffene Person das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags von dem für die Verarbeitung Verantwortlichen eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten zu erhalten. Artikel 14 der Verordnung gewährt der betroffenen Person das Recht, unrichtige oder unvollständige Daten zu berichtigen.

In der Meldung wird die Möglichkeit der Auskunft über personenbezogene Daten und deren Berichtigung durch Mitarbeiter erwähnt und beschrieben. In der dem EDSB zur Überprüfung vorgelegten Datenschutzerklärung wird eine E-Mail-Adresse angegeben, über die diese Rechte ausgeübt werden können. Der EDSB erinnert daran, dass diese Rechte nicht nur auf die von der Person stammenden Informationen (Identifizierungsdaten und [biometrische] Vorlagen), sondern auch auf die Daten anzuwenden sind, die bei jedem Betreten des JRC-ITU durch die Person generiert werden. Aufgrund der ihm vorliegenden Informationen sieht der EDSB keinen Anlass für den Schluss, dass die Vorgaben von Artikel 13 und 14 der Verordnung nicht eingehalten werden.

III.8. Informationspflicht gegenüber der betroffenen Person

Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 führen Informationen auf, die der betroffenen Person zu geben sind. Diese beiden Artikel enthalten eine Reihe obligatorischer und nicht obligatorischer Informationspunkte. Im vorliegenden Fall stammen alle Daten von der betroffenen Person; damit ist Artikel 11 (Informationspflicht bei Erhebung der Daten bei der betroffenen Person) anzuwenden.

Die Meldung besagt, dass im Intranet des JRC-ITU sowie bei den Wachposten am Eingang zu den Räumlichkeiten des ITU eine Datenschutzerklärung zur Verfügung gestellt wird. Die Datenschutzerklärung enthält Folgendes: i) Erläuterung des Zutrittsgenehmigungs- und Zugangskontrollsystems des ITU; ii) Angaben dazu, welche personenbezogenen Daten für welchen Zweck und mit welchen technischen Mitteln erfasst wurden; iii) Angaben zum Schutz der Daten und zu Garantien; iv) Aufbewahrungsfrist; v) Hinweise auf die Rechte der betroffenen Person (auf Auskunft, Berichtigung und Löschung) und das Recht, sich an den EDSB zu wenden. Der DSB hatte die Datenschutzerklärung der Meldung beigefügt. Dem EDSB wurde ein Exemplar der Datenschutzerklärung zur Verfügung gestellt.

Die Datenschutzerklärung enthält Angaben zu den Zwecken der Verarbeitung, zur Form der Verarbeitung, zu den Bedingungen für die Ausübung des Rechts auf Auskunft und Berichtigung, zu den Fristen für die Datenaufbewahrung und zur Möglichkeit, sich an den EDSB zu wenden. Nach Auffassung des EDSB enthält die Datenschutzerklärung die meisten der in Artikel 11 und 12 der Verordnung verlangten Angaben. Allerdings würden seiner Meinung nach einige Änderungen dazu beitragen, dass Artikel 11 und 12 in vollem Umfang Genüge getan wird; er regt insbesondere Folgendes an:

- Mit Blick auf die Erfassung biometrischer Daten sollten den Mitarbeitern weitere Informationen gegeben werden, auch über die Funktionsweise des Systems insgesamt und über die praktischen Konsequenzen einer Erfassung bzw. Nicht-Erfassung.

- Es sollte besser über die Zwecke der Verarbeitung informiert werden; die Datenschutzerklärung erwähnt beispielsweise nicht, dass die Daten für die Ausstellung einer Unbedenklichkeitsbescheinigung durch die DS der GD ADMIN benötigt werden.

Bezüglich der Form dieser Unterrichtung ist der EDSB der Auffassung, dass die Datenschutzerklärung natürlichen Personen in der Erfassungsphase ausgehändigt werden sollte. Es dürfte nicht ausreichen, diese Erklärung ins Intranet zu stellen oder am Eingang zu den Sicherheitsbereichen bereitzustellen. In einer anderen Stellungnahme zu einer Vorabkontrolle[5], äußerte der EDSB Anerkennung für das bei der Europäischen Zentralbank bei der Erfassung geltende Verfahren (z. B. wird die Datenschutzerklärung im Ausdruck ausgehändigt und die Betroffenen werden aufgefordert, sie zu unterzeichnen und damit zu bestätigen, dass sie die Erklärung gelesen und verstanden haben). Nach Ansicht des EDSB handelt es sich hierbei um eine angemessene Methode der Information, und er schlägt vor, den Betroffenen eine Kopie der Datenschutzerklärung auszuhändigen, damit sie die Datenschutzerklärung erneut lesen können, wenn sie beispielsweise in Erfahrung bringen möchten, wie sie ihre Rechte wahrnehmen können oder wie die Daten verarbeitet werden.

III.9. Sicherheitsmaßnahmen

Gemäß Artikel 22 der Verordnung, in dem es um die Sicherheit der Verarbeitung geht, *„hat der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, damit ein Schutzniveau gewährleistet ist, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist*“. Nach Überprüfung der in den dem EDSB vorliegenden Informationen beschriebenen Sicherheitsvorkehrungen besteht kein Anlass zu der Annahme, dass die im Rahmen des gemeldeten Verfahrens durchgeführten Maßnahmen gegen Artikel 22 der Verordnung verstoßen.

IV. Schlussfolgerungen:

Es gibt keinerlei Grund zu der Annahme, dass die Bestimmungen der Verordnung (EG) Nr. 45/2001 verletzt werden, sofern die in dieser Stellungnahme enthaltenen Erwägungen vollständig berücksichtigt werden. Der für die Verarbeitung Verantwortliche sollte insbesondere

- seine Entscheidung über die Einrichtung des Systems der Zugangskontrolle für physischen Schutz in der dem EDSB geschilderten Form überdenken und vor allem der Frage nachgehen, ob er die richtigen Technologien (Verwendung [biometrischer] Daten, Verwendung des Suchmodus „Eins-zu-viele“, Anzahl der betroffenen Personen) und die beste verfügbare Technik ausgewählt hat; vor dem geschilderten Hintergrund erneut prüfen, ob die Anwendung der Maßnahmen auf alle Mitarbeiter des JRC-ITU angemessen ist;
- im Zusammenhang mit der genannten Bewertung die Möglichkeit des Einsatzes anderer Technologien bei künftigen Änderungen des Systems zu prüfen;
- dem EDSB diese Bewertung (Bericht) innerhalb von acht bis zehn Monaten vorlegen;
- Empfänger von Daten darüber in Kenntnis setzen, dass die personenbezogenen Daten nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden, und in einer begründeten Stellungnahme alle Datenübermittlungen an Behörden auflisten und

[5] Siehe Stellungnahme zur Zugangskontrolle bei der Europäischen Zentralbank (2007-501).

ihre Notwendigkeit belegen. Diese Verfahren sollten den zuständigen Mitarbeitern mitgeteilt werden;

- die Datenschutzerklärung in Anlehnung an die Empfehlungen in dieser Stellungnahme ändern und dafür sorgen, dass den Betroffenen eine Kopie der Datenschutzerklärung ausgehändigt oder ihnen leicht zugänglich zur Verfügung gestellt wird.

Brüssel, den 24. Juli 2012

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter