Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Kommission für eine Vorabkontrolle der Sicherheits- und Vertrauenswürdigkeitskontrolle („Security Trustworthiness Check“) in der Gemeinsamen Forschungsstelle Ispra

Brüssel, den 19. Juni 2013 (Fall 2012-1090)

1. Verfahren

Am 20. Dezember 2012 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) der Kommission eine Meldung für eine Vorabkontrolle der Verarbeitungen im Zusammenhang mit dem *Security Trustworthiness Check* (Sicherheits- und Vertrauenswürdigkeitsüberprüfung) in der GD Gemeinsame Forschungsstelle in Ispra („GFS Ispra“).

Die hier zu prüfende Meldung stützt sich auf die Entscheidung des Generaldirektors der GFS vom 11. Juli 2012, das (auf einer Unbedenklichkeitsbescheinigung beruhende) *Nulla-osta*-Screeningverfahren für die Einstellung ausgewählter Bewerber an den GFS-Standorten abzuschaffen. Diese Entscheidung wurde im Anschluss an eine Inspektion bei der GFS im Jahr 2010 (Fall 2010-0832) getroffen, bei der der EDSB die Rechtmäßigkeit des bei der GFS geltenden *Nulla-osta*-Verfahrens infrage gestellt hatte.

Als Ersatz reicht die GFS nunmehr den Entwurf eines Verfahrens für die Sicherheitsüberprüfung (anhand der Vertrauenswürdigkeit) mit der Bezeichnung „Security Trustworthiness Check“ ein. Dieses Verfahren ist nicht länger mit der Einstellung von Bediensteten an allen GFS-Standorten[1] mit Ausnahme von Karlsruhe verknüpft, sondern gilt für den unbegleiteten Zugang zu kerntechnischen Anlagen und den dazugehörenden sensiblen Bereichen innerhalb des Standorts Ispra. Damit sind von dem Verfahren deutlich weniger Menschen und Flächen betroffen. Der Meldung waren zehn Anlagen beigefügt. Eine der Anlagen enthält einen Aktenvermerk mit Angaben zur Umsetzung einiger der Empfehlungen des Inspektionsberichts, der Anlass für die Entwicklung des *Trustworthiness Security Checks* war.

Wie es in dem Aktenvermerk heißt, können die Direktoren die zur Aufrechterhaltung spezifischer Sicherheitsmaßnahmen für Hochrisikobereiche erforderlichen Sicherheitsscreenings vornehmen lassen. Diese Möglichkeit ist jedoch sehr beschränkt, denn sie kann nur genutzt werden
- bezüglich des Zugangs zu als kerntechnisch bezeichneten Sperrgebieten (im Gegensatz zu dem abgeschafften Verfahren mit der Unbedenklichkeitsbescheinigung, das bei der Einstellung von Bediensteten zum Einsatz kam), und wenn

[1] Aufgegeben hat die GFS das *Nulla-osta*-Verfahren an ihren Standorten Petten, Sevilla, Geel und Brüssel, und sie hat es auch in Ispra aufgehoben, allerdings unter Beibehaltung eines Sicherheitsscreenings für den Zugang zu „sensiblen Bereichen“ (einschließlich kerntechnischer Bereiche).

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
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

- dies in Standards der Kommission und/oder anwendbaren lokalen, regionalen und/oder nationalen Sicherheitsauflagen verlangt wird und
- im Einklang mit den Datenschutzvorschriften steht.

Im Schriftwechsel erläuterte die GFS, dass sie in einer Vereinbarung zwischen der Generaldirektion Humanressourcen und Sicherheit/Direktion Sicherheit („GD.HR/DS“) und der Gemeinsamen Forschungsstelle konkret mit der Durchführung bestimmter Sicherheitsuntersuchungen beauftragt worden ist.

Nach einer ersten Analyse der Meldung nahm der EDSB Kontakt sowohl mit dem DSB als auch mit der GFS als dem für die Verarbeitung Verantwortlichen auf und wies darauf hin, dass die Meldung nicht im Einklang mit dem dritten Follow-up-Bericht des EDSB an die GFS steht. In diesem Schreiben unterstrich der EDSB die Notwendigkeit, das Verfahren auf die Grundlage des neuen Sicherheitsbeschlusses und der Vereinbarung zu stellen. Es trifft zu, dass, wie in der E-Mail behauptet, der Sicherheitsbeschluss C(94)2129 der Kommission über die allgemeinen Aufgaben des Sicherheitsdienstes zum Zeitpunkt der Analyse überarbeitet wurde. Wie es in dem Aktenvermerk heißt, enthält der Entwurf dieses neuen Beschlusses einen Artikel über „*die Sicherheitsmaßnahmen, die die Kommission – unter strenger Wahrung der Grundrechte und der Grundsätze der Rechtmäßigkeit, Transparenz, Rechenschaftspflicht, Subsidiarität und Verhältnismäßigkeit – ergreifen kann. Zu den beschriebenen Maßnahmen gehören unter anderem systematische Vorabsicherheitsüberprüfungen, um Bedrohungen der Sicherheit von Personen, die zu ihren Räumlichkeiten Zutritt haben, zu vermeiden und abzuwehren“.* Der Entwurf enthält ferner eine Bestimmung, der zufolge bestimmte Sicherheitskontrollen im Wege der Unterzeichnung eines Durchführungsrechtsakts auf lokaler Ebene vorgenommen werden dürfen, beispielsweise vom Sicherheitsdienst der GFS Ispra. Aus diesem Grund wird eine neue Vereinbarung unterzeichnet werden.

Zum Zeitpunkt der Abfassung dieser Stellungnahme waren die Gespräche zwischen der GD HR/DS und der GFS allerdings noch nicht abgeschlossen.

Gleichzeitig befindet sich die GFS in einer Lage, in der sie verpflichtet ist, vorgeschriebene Sicherheitsscreenings für den Zugang zu kerntechnischen Sperrbereichen durchzuführen. Die GFS unterliegt der *Empfehlung 4.26 des Dokuments (INFCIRC/225/fifth) der Internationalen Atomenergieagentur (IAEA), die besagt, dass „unbegleiteten Zutritt zum Sperrbereich nur Personen haben sollten, deren Vertrauenswürdigkeit belegt ist“,* sowie dem per Dekret des italienischen Industrieministeriums gebilligten Plan für den physischen Schutz.

Der EDSB hat daher beschlossen, um eine Sicherheitslücke zu vermeiden, seine rechtliche Analyse auf der Grundlage der bei ihm eingegangenen Informationen vorzunehmen, auch wenn der neue Kommissionsbeschluss und die Vereinbarung noch nicht fertiggestellt sind. Dank des Vermerks der GFS hatte der EDSB Einsicht in die relevanten Teile des Beschlussentwurfs, und er erfuhr von der GFS, dass sich die neue Vereinbarung von der alten nur geringfügig unterscheiden wird.

Daher erfolgt diese Stellungnahme unbeschadet weiterer Kommentare, die der EDSB möglicherweise vorträgt, wenn der neue Sicherheitsbeschluss und die neue Vereinbarung angenommen sein werden.

Am 31. Mai 2013 sandte der EDSB den Entwurf seiner Stellungnahme an den Datenschutzbeauftragten zur Kommentierung. Die Reaktion ging am 14. Juni 2013 ein.

2. Prüfung des Gegenstands

2.1 Sachverhalt

Zweck der Verarbeitung personenbezogener Daten ist die Überprüfung und Bestätigung der Vertrauenswürdigkeit von Personen, die unbegleiteten Zutritt zu den kerntechnischen und den dazu gehörenden sensiblen Bereichen in der GFS Ispra benötigen.

Zu den Unterlagen, die bei einem *Security Trustworthiness Check* verarbeitet werden, gehören ein aktueller Lebenslauf oder ein Bewerbungsformular; eine Ausnahme bilden externe Mitarbeiter, die einen Liefer- oder Dienstleistungsvertrag mit der Europäischen Kommission abgeschlossen haben, die auch einen Auszug aus dem Strafregister einreichen müssen. Für Nichtitaliener ist ferner ein „Permesso di soggiorno" (Aufenthaltsgenehmigung) vorzulegen.

Im Zuge des neuen *Security Trustworthiness Check* wenden Personalabteilungen und Einstellungsreferate Artikel 28 Buchstabe c des Statuts der Beamten der Europäischen Gemeinschaften an, in dem es um die für die Ausübung des Amtes zu stellenden sittlichen Anforderungen geht. Gleichlautende Artikel finden auch auf andere Kategorien von Bediensteten Anwendung.

In der Mitteilung wird unterstrichen, dass Daten über die Anwesenheit von Personen vor Ort zwecks Anwendung des Beschlusses der Kommission C(2004) 1597 über die Höchstdauer der Beschäftigung nicht ständiger Bediensteter in Dienststellen der Kommission vom Sicherheitsdienst nicht länger erhoben und verarbeitet werden.

Betroffene Personen sind alle Mitarbeiter, die unbegleiteten Zugang zu kerntechnischen und den dazu gehörenden sensiblen Bereichen oder Informationen am Standort Ispra benötigen (die sich also einem *Security Trustworthiness Check* unterziehen müssen). Es sei darauf hingewiesen, dass dies nicht Tagesbesucher betrifft, die den Standort nur gelegentlich betreten; sie werden beim Betreten sensibler Bereiche des Standorts Ispra auf jeden Fall begleitet, und ihre Daten werden nur im Rahmen von SECPAC (2007-0381) gespeichert.

Die ***verarbeiteten Daten*** werden in die folgenden Kategorien eingeteilt: Personen, Dokumente und Dokumentenarten.

- PERSONEN: Vorname, echter Vorname, Nachname, echter Nachname, Künstlername, Geschlecht, Titel, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, Pseudonym, Personalnummer, Quellen-ID, Quelle, E-Mail, Telefon, Datum Besuchsbeginn und Datum Besuchsende, [Universal-ID]

- DOKUMENTENARTEN: Bewerbungsformular bzw. Lebenslauf, neuerer Auszug aus dem Strafregister (nur für externe Mitarbeiter, die mit der Europäischen Kommission einen Liefer- oder Dienstleistungsvertrag abgeschlossen haben), Kopie des entsprechenden Liefer- oder Dienstleistungsvertrags (Referenznummer) (für externe Mitarbeiter), Vertragsverlängerung, Ablauf des Vertrags, *Permesso di Soggiorno* (für Nichtitaliener), Selbstzertifizierung, Genehmigung, Datenerhebungsformular und Befreiung.

Die Meldung besagt, dass die Datenfelder den vorgelegten Unterlagen zugeordnet sind und im Wesentlichen nicht unter Artikel 10 der Verordnung fallen. Einige Unterlagen könnten hingegen möglicherweise durchaus unter Artikel 10 fallen.

Zur Tatsache, dass diese Informationen vorgelegt werden müssen, sagt die Meldung aus, dass Mitarbeiter bei der Einstellung vom Manager Humanressourcen darüber in Kenntnis gesetzt

werden, dass sie bestimmte Unterlagen einzureichen haben, und dass sie darauf hingewiesen werden, dass ihre Daten zwecks Anwendung des Statuts sowie vom Sicherheitsdienst zwecks Durchführung eines *Security Trustworthiness Checks* verwendet werden dürfen, falls an ihrem Arbeitsplatz der Zugang zu kerntechnischen und den dazu gehörenden sensiblen Bereichen oder Informationen erforderlich ist.

Dieses Thema und einige andere werden regelmäßig in den zweimonatlich erscheinenden „Newcomer's Security Briefings" (Sicherheitsinformationen für neue Mitarbeiter) näher erläutert und erklärt.

Für die ***Verarbeitung Verantwortlicher*** ist ***in der Hauptsache*** das Referat Sicherheit der GFS Ispra. Es berichtet direkt an den Direktor des Ispra Site Management.

Zum ***Aufbewahrungszeitraum*** besagt die ***Meldung***, dass Daten so lange aufbewahrt werden müssen, wie ein Vertragsverhältnis mit der betreffenden Person besteht, und dass sie darüber hinaus für zwei weitere Jahre nach Beendigung des Vertragsverhältnisses (Ruhestand, Ablauf eines befristeten Vertrags usw.) aufbewahrt werden sollten.

Alle personenbezogenen Daten und Unterlagen im Zusammenhang mit dem *Trustworthiness Check* werden also nach Ablauf dieser Zeit gelöscht oder anonymisiert. In gut begründeten Ausnahmefällen können solche Daten auch länger aufbewahrt werden, wenn in Zusammenhang mit einer Person nach deren Weggang vom Standort Ispra Untersuchungen von Verstößen gegen die Sicherheitsregeln oder Zwischenfällen angestellt werden.

Die Daten von Bewerbern, die ihre Bewerbung zurückgezogen haben oder nicht eingestellt wurden, aber schon einem *Security Trustworthiness Check* mit Verarbeitung ihrer Daten unterzogen worden sind, werden für ein Jahr aufbewahrt.

Die erhobenen personenbezogenen Daten und alle Angaben zu der oben genannten Verarbeitung werden auf eigenen Servern des Sicherheitsdienstes der GFS Ispra gespeichert, für deren Betrieb die IT-Sicherheitsbeschlüsse und Bestimmungen für diese Art von Servern und Diensten der Kommission gelten.

Der Zugriff auf die Daten erfolgt mit einem einmaligen, individuellen Zugang, der durch einen Benutzernamen/ein Passwort geschützt ist. Der Kernmitarbeiterstab des Sicherheitsdienstes umfasst verschiedene Profile, unter anderem den *Sicherheitsbeauftragten* und den *Sicherheitsarchivar und Administrator*. Sicherheitsbeauftragte haben Zugriff auf personenbezogenen Daten. *Sicherheitsarchivare* haben Zugriff auf alle registrierten Informationen einschließlich Dokumente. *Administratoren* haben umfänglichen Zugriff auf die ARDOS-Funktionalität, zu der auch die Verwaltung solcher Profile gehört.

Derzeit kommt aufgrund der vielfältigen und zahlreichen denkbaren Szenarios bei der Analyse des Aufbewahrungszeitraums eine Reihe halbautomatischer Verfahren zum Einsatz, das Löschen von Dokumenten in ARDOS, die nur in digitaler Form vorliegen, muss jedoch manuell geschehen.

Laut Meldung hat der Sicherheitsdienst alle seine Unterlagen in Papierform, die länger als oben ausgeführt aufbewahrt wurden und nicht länger benötigt werden, aussortiert und kontrolliert. Die GFS stellte klar, dass sie alle in ihrem Besitz befindlichen in der Vergangenheit im Rahmen des *Nulla-osta*-Verfahrens eingereichten Unterlagen in Papierform zerstört hat. Zu eventuellen anderen elektronischen Unterlagen, die für das *Nulla-osta*-Verfahren benötigt wurden, teilte die GFS mit, dass bis Ende 2013 ein Verfahren entwickelt und fertiggestellt

werden soll, das alle Daten löscht, die eindeutig als nur dem *Nulla-osta*-Verfahren zugehörig identifiziert werden können (z. B. Bewerbungsformulare, Lebensläufe usw.).

Zu den ***Empfängern*** der Daten ist anzumerken, dass die Unterlagen, die für die Verarbeitung von *Security Trustworthiness Checks* benötigt werden und in ARDOS gespeichert sind, nur für den internen Gebrauch des Sicherheitsdienstes bestimmt sind. Daten werden niemals direkt übermittelt, und ein Zugriff ist außerhalb des Sicherheitsdienstes nicht möglich, da ein solches Informationssystem in einem physisch getrennten Netz untergebracht ist.

Ein *Security Trustworthiness Check* ist ein internes Verfahren des Sicherheitsdienstes, weshalb an andere Personen keine Daten weitergegeben werden. Zugriff auf die Daten haben nur sicherheitsüberprüfte Kernmitarbeiter des Sicherheitsdienstes. In Notfällen oder bei Sicherheitsuntersuchungen kann der Direktor des Standortes Ispra zusätzliche Informationen anfordern.

Bezüglich des ***Rechts auf Information*** wurde der Meldung eine Datenschutzerklärung beigefügt und darauf hingewiesen, dass betroffene Personen Auskunft über diese Verarbeitung verlangen können. Entsprechende Anträge können an den für die Verarbeitung Verantwortlichen über eine funktionale E-Mail-Adresse gerichtet werden, die als einzige Kontaktstelle fungiert; die Meldung enthält die entsprechenden Kontaktdaten. Der Zweck der Verarbeitung personenbezogener Daten bestehe darin, im Zusammenhang mit dem entsprechenden Antrag auf langfristige Genehmigung die Vertrauenswürdigkeit von Personen zu überprüfen und zu bestätigen.

Die Datenschutzerklärung enthält Angaben zum Zweck der Verarbeitung (mit einer kurzen Beschreibung), zur Identität des für die Verarbeitung Verantwortlichen, zur Rechtsgrundlage, zu den Empfängern der Daten, zur Datenaufbewahrung und zu den Aufbewahrungsfristen für die Daten. Ferner enthält sie Informationen über das Auskunfts- und Berichtigungsrecht. Erwähnt wird dort schließlich auch das Recht, sich an den Europäischen Datenschutzbeauftragten zu wenden.

Im Sinne der Transparenz hat der Sicherheitsdienst der GFS Ispra zur Wahrnehmung des ***Rechts auf Auskunft und Berichtigung*** ein Verfahren vorgesehen, mit dem betroffene Personen auf Antrag überprüfen können, welche sie betreffenden Daten gespeichert sind. Die einzige Kontaktstelle des Sicherheitsdienstes der GFS Ispra ist für die Erteilung von Auskünften über personenbezogene Daten oder deren Berichtigung zuständig. Für die Aktualisierung oder Rückgabe eines „Originalauszugs aus dem Polizeiregister“ wurde ein besonderes Verfahren eingeführt. Ein solcher Antrag ist unter Verwendung des „Formulars für die Aktualisierung oder Rückgabe des Originalauszugs aus dem Polizeiregister“ zu stellen. Derzeit sind hiervon nur externe Mitarbeiter betroffen.

Auf begründeten Antrag der betroffenen Person werden spätestens nach 14 Tagen Daten geändert, eingefroren oder möglicherweise gelöscht.

Zum Thema ***Sicherheitsmaßnahmen*** verweist die Meldung auf die detaillierten Antworten auf die Fragen nach der Durchführung der für ARDOS angenommenen technischen und organisatorischen Maßnahmen.

[...]

2.2. Rechtliche Aspekte

2.2.1. Vorabkontrolle

Gegenstand dieser Stellungnahme im Rahmen der Vorabkontrolle ist die Verarbeitung personenbezogener Daten im Zusammenhang mit *Security Trustworthiness Checks* der GFS Ispra. Die Verarbeitung erfolgt durch ein EU-Organ im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen (Artikel 3 Absatz 1 der Verordnung). Die Verarbeitung personenbezogener Daten erfolgt, zumindest teilweise, automatisiert (Artikel 3 Absatz 2 der Verordnung). Damit ist die Verordnung anzuwenden.

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. Artikel 27 Absatz 2 der Verordnung enthält eine Liste der Verarbeitungen, die solche Risiken beinhalten können.

Nach Angaben der GFS als für die Verarbeitung Verantwortlichem fällt die Verarbeitung der Daten unter Artikel 27 bei a) strafrechtlichen Verurteilungen oder Sicherungsmaßregeln, b) Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten, insbesondere ihr Verhalten, c) Verarbeitungen, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen.

Erstens fällt eine solche Verarbeitung unter Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001, dem zufolge Verarbeitungen, die „*Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln*“ betreffen, vom EDSB vorab zu kontrollieren sind. Im vorliegenden Fall kann es vorkommen, dass der Sicherheitsdienst bei der Verarbeitung der oben genannten Daten auch Daten verarbeitet, die mutmaßliche Straftaten/strafrechtliche Verurteilungen betreffen. Der Verweis auf Sicherungsmaßregeln gemäß Artikel 27 Absatz 2 Buchstabe a) ist nicht relevant, da die Auslegung von Sicherungsmaßregeln nicht so verstanden wird wie die beschriebenen Maßnahmen.[2]

Die Meldung fällt gleichfalls unter Artikel 27 Absatz 2 Buchstabe b) der Verordnung (EG) Nr. 45/2001, dem zufolge Verarbeitungen, die dazu bestimmt sind, *„die Persönlichkeit der betroffenen Person zu bewerten, einschließlich(….) ihres Verhaltens“,* einer Vorabkontrolle durch den EDSB zu unterziehen sind. Im hier zu prüfenden Fall wird das Verhalten von Personen zwecks Feststellung ihrer Vertrauenswürdigkeit bewertet; damit ist Artikel 27 Absatz 2 Buchstabe b) anzuwenden.

Nach Auffassung des EDSB ist schließlich Artikel 27 Absatz 2 Buchstabe d) hier nicht anzuwenden. Diese Bestimmung betrifft Verarbeitungen, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen (ein typisches Beispiel hierfür sind schwarze Listen). Dies dürfte kaum der Zweck des *Trustworthiness Check* sein, der ja im Gegenteil den unbegleiteten Zugang zum GFS-Standort ermöglichen soll.

Ex-ante-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 soll die Verarbeitung an die Stelle des abgeschafften *Nulla-osta*-Verfahrens treten und ist daher vorab zu prüfen; vor der Einführung des Verfahrens sollten alle Empfehlungen umgesetzt worden sein.

[2] Der Verweis in Artikel 27 Absatz 2 Buchstabe a) bezeichnet tatsächlich sogenannte „safety measures“ oder „mesures de sûreté“, wie es in der französischen Fassung der Verordnung heißt.

Meldung und Frist für die Stellungnahme des EDSB. Die Meldung des DSB ging am 20. Dezember 2012 ein. Zwischen dem 9. Januar 2013 und dem 23. April 2013 war die Prüfung ausgesetzt. Der Entwurf der Stellungnahme wurde am 31. Mai 2013 zur Kommentierung übermittelt; die Kommentare gingen am 14. Juni 2013 ein. Der Zeitraum von zwei Monaten, innerhalb dessen der EDSB seine Stellungnahme annehmen muss, wurde also für 104 sowie weitere 14 Tage ausgesetzt, in denen dem DSB und der GFS als für die Verarbeitung Verantwortlichem Gelegenheit gegeben wurde, sich zum Entwurf der Stellungnahme des EDSB zu äußern. Die Stellungnahme muss daher spätestens am 19. Juni 2013 angenommen werden.

2.2.2. Rechtmäßigkeit der Verarbeitung

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

Laut Meldung ist die Verarbeitung rechtmäßig gemäß Artikel 5 Buchstabe a), b), d) und e) der Verordnung. Nach Auffassung des EDSB fällt die im vorliegenden Fall zur Vorabkontrolle gemeldete Verarbeitung von den in Artikel 5 der Verordnung (EG) Nr. 45/2001 aufgeführten Gründen lediglich unter Artikel 5 Buchstabe b) – „*die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich*“, der die GFS unterliegt – sowie 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 (...) ausgeführt wird*“.

Wie im Abschnitt „Verfahren“ dargestellt, unterliegt die GFS der *Empfehlung 4.26 des Dokuments (INFCIRC/225/fifth) der Internationalen Atomenergieagentur (IAEA), die besagt, dass „unbegleiteten Zutritt zum Sperrbereich nur Personen haben sollten, deren Vertrauenswürdigkeit belegt ist“,* sowie dem per Dekret des italienischen Industrieministeriums gebilligten Plan für den physischen Schutz; somit findet Artikel 5 Buchstabe b) der Verordnung Anwendung. Die GFS Ispra als Betreiberin einer kerntechnischen Anlage und Inhaberin einer entsprechenden Lizenz nach italienischem Recht ist zu zahlreichen Sicherheitsmaßnahmen verpflichtet.

In seinem dritten Follow-up-Bericht zur Inspektion mit Datum vom 5. Dezember 2012 empfahl der EDSB, dieser gesetzlichen Auflage mit dem neuen Sicherheitsbeschluss der Kommission und der aktualisierten Vereinbarung nachzukommen. Sowohl im italienischen Dekret als auch in der IAEA-Empfehlung wird eine Überprüfung der Vertrauenswürdigkeit verlangt, doch besagt keiner der beiden Texte, wie und von wem (GFS-Sicherheitsdienst oder DG.HR/DS) diese Überprüfung vorgenommen werden soll. Der IAEA-Empfehlung kann zwar entnommen werden, dass die Überprüfung der Vertrauenswürdigkeit die Erhebung und Verarbeitung personenbezogener Daten zur Folge hat, doch schreibt die Empfehlung an sich die Verarbeitung personenbezogener Daten nicht vor.

Daher sind der künftige neue Sicherheitsbeschluss der Kommission und die aktualisierte Vereinbarung zwischen der GD GFS und der GD HR von allergrößter Bedeutung, um der GFS mehr Befugnisse zur Durchführung von Sicherheitsüberprüfungen zu übertragen und damit die Rechtmäßigkeit und Legitimität der Verarbeitungen im Rahmen von *Security Trustworthiness Checks* zu stärken.

Sowohl der neue Sicherheitsbeschluss der Kommission als auch die neue Vereinbarung sind dem EDSB zur Analyse vorzulegen, da sie die derzeitige Rechtsgrundlage Artikel 5 Buchstabe b) (italienisches Recht) mit der Rechtsgrundlage Artikel 5 Buchstabe a) ergänzen.

Folglich nimmt der EDSB die folgenden Rechtsakte zur Kenntnis, die als Rechtsgrundlage für Verarbeitungen im Zusammenhang mit der Durchführung von Untersuchungen dienen:

- italienisches Gesetz 906/1960 über die Einrichtung der Gemeinsamen Forschungsstelle Ispra;
- Plan für den physischen Schutz (gebilligt in einem Dekret des italienischen Industrieministeriums), der alle Maßnahmen enthält, die über die in dem Dokument IAEA INFCIRC/225 [3] genannten hinausgehen und stillschweigend als Grundlage eines solchen Dokuments gelten;
- Beschluss der Kommission vom 8. September 1994 über die Aufgaben der Sicherheitsbüros der Europäischen Kommission[4], **nach der Überarbeitung**;
- Vereinbarung zwischen der Generaldirektion „Humanressourcen und Sicherheit“ und der „Gemeinsamen Forschungsstelle“ über die im Sicherheitsbereich wahrzunehmenden Aufgaben (eine aktualisierte Fassung wird es nach der Annahme des erwarteten neuen Sicherheitsbeschlusses der Europäischen Kommission geben), **nach der Aktualisierung**.

Bezüglich der Notwendigkeit der Verarbeitung verweist der EDSB nicht nur auf den neuen Sicherheitsbeschluss der Kommission und die neue Vereinbarung, sondern vertritt auch die Ansicht, dass die Verarbeitung zur Einhaltung internationaler und italienischer Rechtsvorschriften über Nuklearstandorte erforderlich ist.

In Anbetracht des anstehenden Beschlusses und der neuen Vereinbarung ist der EDSB der Auffassung, dass die Rechtsgrundlage, gestützt auf die bei der Europäischen Kommission geltenden Vorschriften, durchaus die Aufgaben der Sicherheitsdienste an GFS-Standorten regelt.

2.2.3. Verarbeitung besonderer Datenkategorien

In Anbetracht der Tatsache, dass der Zweck der Verarbeitung darin besteht, die Vertrauenswürdigkeit von Personen zu überprüfen und zu bestätigen, die unbegleiteten Zutritt zu kerntechnischen und den dazu gehörenden Bereichen in der GFS Ispra benötigen, könnten bestimmte Unterlagen unter Artikel 10 fallen.

In diesem Zusammenhang verweist der EDSB auf die Anwendung von Artikel 10 Absatz 5 der Verordnung (EG) Nr. 45/2001, der besagt: „*Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur erfolgen, wenn sie durch die Verträge zur Gründung der Europäischen Gemeinschaften oder andere auf der Grundlage dieser Verträge erlassene Rechtsakte oder, falls notwendig, vom Europäischen Datenschutzbeauftragten vorbehaltlich geeigneter besonderer Garantien genehmigt wurde.*“ Im vorliegenden Fall sieht Artikel 10 Absatz 5 eine Ausnahme vor, d. h., die Verarbeitung der Daten ist wegen der gesetzlichen Verpflichtung für die Gemeinsame Forschungsstelle zur Durchführung des „Plans für den physischen Schutz“ (siehe die vorstehend unter Punkt 2.2.2 aufgeführten Rechtsakte) zulässig.

[3] http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

[4] Die in der Meldung erwähnte Entscheidung der Kommission C(2001)3031 (auch 2001/844/EG) und die Entscheidung der Kommission C(2007)513/Euratom gilt im vorliegenden Fall nicht als das ausschlaggebende Dokument.

2.2.4. Datenqualität

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, dafür erheblich sein und nicht darüber hinausgehen*".

Die Daten, die im Rahmen des *Security Trustworthiness Check* verarbeitet werden, dürften auf das begrenzt sein, was für das Erreichen des Zwecks der Verarbeitung erforderlich ist; damit dürfte Artikel 4 Absatz 1 Buchstabe c) der Verordnung (EG) Nr. 45/2001 Genüge getan werden.

Bei den Auszügen aus dem Strafregister erwähnt die GFS den Begriff „Polizeiregister". Bereits in seinem Bericht über die Inspektion bei der GFS (2010-0834) unterstrich der EDSB, dass dieser Begriff besser nicht verwendet werden sollte. Es kann nur ein von der zuständigen Behörde des betreffenden Landes ausgestellter Auszug aus dem Strafregister verwendet werden. Daher sollten Dokumente wie „Führungszeugnis" oder Ähnliches nicht verlangt werden, es sei denn, es gibt in dem betreffenden Land kein Strafregister. Der EDSB erinnert ferner daran, dass die GFS für alle Mitgliedstaaten in den Originalsprachen eine Liste sogenannter „Auszüge aus dem Strafregister" erstellt hat. Eben dieses Dokument sollte verlangt werden. Der EDSB fordert die GFS daher auf, die in dem geplanten Verfahren verwendeten Begriffe zu ändern. In Anbetracht der vielen betroffenen Ausländer sollten die Bewerber auch darüber in Kenntnis gesetzt werden, ob der Auszug aus dem Strafregister von ihrem derzeitigen und/oder früheren Wohnsitzland und/oder dem Land ihrer Staatsangehörigkeit ausgestellt werden soll.

Gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten *„sachlich richtig [sein] und, wenn nötig, auf den neuesten Stand gebracht"* werden; ferner *„sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, unrichtige oder unvollständige Daten berichtigt oder gelöscht werden."*

Auszüge aus dem Strafregister sind mitunter nur für kurze Zeit zutreffend. Der EDSB fordert daher die GFS zur Überprüfung der Frage auf, ob ein solcher Auszug lange aufbewahrt werden muss (siehe auch nachstehenden Punkt 2.2.5).

2.2.5. Datenaufbewahrung / Datenspeicherung

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

Bei der Verarbeitung sind unterschiedliche Aufbewahrungszeiträume vorgesehen.

1) Laut GFS sollen die Daten so lange aufbewahrt werden, wie ein Vertragsverhältnis mit der betreffenden Person besteht (interner oder externer Mitarbeiter). Nach Beendigung dieses Vertragsverhältnisses (also Ruhestand, Ablauf befristeter Verträge usw.) ist ein Aufbewahrungszeitraum von zwei weiteren Jahren vorgesehen.

Der EDSB nimmt zur Kenntnis, dass die GFS diese Zeiträume als für die Verarbeitung im Rahmen der *Security Trustworthiness Checks* erforderlich hält. Wie bereits ausgeführt, sind

Daten aus einem Auszug aus dem Strafregister nur befristet korrekt. Der EDSB hinterfragt daher die Aufbewahrungsfrist für den Auszug aus dem Strafregister; seiner Auffassung nach sollte sie höchstens zwei Jahre nach der Ausstellung betragen. Dies entspräche auch dem Zeitraum, innerhalb dessen der Rechnungshof ein solches Dokument prüfen würde (zur Weiterverarbeitung). Aufzeichnungen, die vom Rechnungshof vor Ablauf dieser Frist geprüft wurden, können auch früher vernichtet werden. Diese Lesart wurde vom Rechnungshof offiziell akzeptiert. Die in der Meldung und in der Datenschutzerklärung vorgesehene Aufbewahrungsfrist sollte entsprechend geändert werden.

2) Es ist vorgesehen, dass nach Ablauf des unter 1) angegebenen Zeitraums alle personenbezogenen Daten und Unterlagen im Zusammenhang mit dem *Trustworthiness Check* gelöscht oder anonymisiert werden, dass aber in gut begründeten Ausnahmefällen die Daten länger aufbewahrt werden dürfen, damit Verletzungen der Sicherheitsvorschriften oder Zwischenfälle im Zusammenhang mit der betroffenen Person nach deren Ausscheiden aus dem Standort Ispra untersucht werden können.

Der EDSB nimmt zur Kenntnis, dass die GFS Ispra diesen Aufbewahrungszeitraum für weitere Verarbeitungen im Rahmen von Untersuchungen erforderlich hält. Der EDSB weist nachdrücklich darauf hin, dass eine solche Aufbewahrung nur in gut begründeten Ausnahmefällen erfolgen darf.

Die Daten von Bewerbern, die ihre Bewerbung zurückgezogen haben oder nicht eingestellt wurden, aber schon einem *Security Trustworthiness Check* mit Verarbeitung ihrer Daten unterzogen worden sind, werden für ein Jahr aufbewahrt. Der EDSB nimmt diese Aufbewahrungsfrist zur Kenntnis.

In der Meldung der GFS heißt es ferner, dass der Sicherheitsdienst alle seine Unterlagen in Papierform, die länger als oben ausgeführt aufbewahrt worden waren und nicht länger benötigt werden, aussortiert und kontrolliert hat. Nach Auffassung des EDSB gilt dieses Verfahren auch für die *Nulla-osta*-Unterlagen, die jahrelang erhoben wurden, bevor der Generaldirektor der GFS die Abschaffung dieses Verfahrens beschloss. Der EDSB begrüßt zwar, dass ein Verfahren für alle neuen Daten vorgesehen ist, die im Rahmen des *Security Trustworthiness Check* erhoben werden, doch ist es ebenso wichtig, dass die GFS Regeln für bereits vorhandene Daten aufstellt.

2.2.6. Datenübermittlung

Gestützt auf die vorliegenden Informationen gilt nur Artikel 7 der Verordnung (EG) Nr. 45/2001. Daten werden niemals direkt übermittelt, und ein Zugriff ist außerhalb des Sicherheitsdienstes nicht möglich, da ein solches Informationssystem in einem physisch getrennten Netz untergebracht ist. Außerdem haben nur sicherheitsüberprüfte Kernmitarbeiter des Sicherheitsdienstes Zugang zu den Daten, und der Direktor des Standorts Ispra kann in Notfällen oder bei Sicherheitsuntersuchungen weitere Informationen anfordern. Dies ist in den erhaltenen Unterlagen ausgeführt (Datenschutzerklärung). Der für die Regelung des Zugangs zum Standort Ispra verantwortliche Sicherheitsdienst kann aus Sicherheitsgründen ebenfalls Daten an die Direktion Sicherheit (GD HR/DS) der Kommission übermitteln.

Daten können an Organe und Einrichtungen der Europäischen Union wie OLAF, IDOC, den EDSB oder den Europäischen Bürgerbeauftragten innerhalb ihrer jeweiligen Zuständigkeiten übermittelt werden.

In Anbetracht der Zuständigkeitsbereiche der empfangenden Stellen dürften solche Datenübermittlungen für die rechtmäßige Erfüllung der Aufgaben erforderlich sein, die in den Zuständigkeitsbereich der Empfänger fallen. In den neuen Sicherheitsvorschriften wird darüber hinaus eindeutig zwischen den Zuständigkeiten der GFS und denen der GD HR.DS für Sicherheit und die Fälle zu unterscheiden sein, in denen solche Übermittlungen stattfinden könnten.

Der Empfänger ist auf jeden Fall darüber zu unterrichten, dass personenbezogene Daten gemäß Artikel 7 Absatz 3 nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden.

Es ist keine Übermittlung personenbezogener Daten an Mitgliedstaaten oder Drittländer vorgesehen.

2.2.7. Auskunftsrecht und Berichtigung

Das Recht auf Auskunft ist das Recht der betroffenen Person, über alle sie betreffenden Daten informiert zu werden, die der für die Verarbeitung Verantwortliche verarbeitet. Gemäß Artikel 13 der Verordnung (EG) Nr. 45/2001 hat die betroffene Person das Recht, frei und ungehindert 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.

Die Datenschutzerklärung besagt, dass betroffene Personen Anfragen (zwecks Auskunft über die gespeicherten Daten, ihre Änderung, Berichtigung oder Löschung) zu dieser Verarbeitung an den für die Verarbeitung Verantwortlichen richten können. Für die Ausübung dieses Rechts wird eine funktionale Mail-Box aufgeführt.

2.2.8. Informationspflicht gegenüber der betroffenen Person

Gemäß Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 ist der für die Verarbeitung Verantwortliche verpflichtet, betroffene Personen darüber zu unterrichten, dass ihre Daten erhoben und verarbeitet werden. Artikel 11 bezieht sich auf Angaben in Fällen, in denen die Daten bei der betroffenen Person direkt erhoben wurden, und Artikel 12 deckt Angaben bei Daten ab, die nicht von der betroffenen Person stammen. Die betroffenen Personen haben überdies das Recht, u. a. über die Zwecke der Verarbeitung, die Empfänger der Daten und ihre Rechte als betroffene Personen unterrichtet zu werden.

Die GFS als für die Verarbeitung Verantwortlicher hat eine Datenschutzerklärung für den *Security Trustworthiness Check* eingereicht. Die Meldung enthält jedoch keinerlei Angaben dazu, wie diese Datenschutzerklärung den betroffenen Personen zur Kenntnis gebracht werden soll. Die Meldung besagt hierzu Folgendes: „Die Mitarbeiter werden bei der Einstellung vom Manager Humanressourcen darüber in Kenntnis gesetzt, dass sie bestimmte Unterlagen einzureichen haben, und dass sie sich der Tatsache bewusst sein müssen, dass ihre Daten zwecks Anwendung des Statuts und vom Sicherheitsdienst zwecks Durchführung eines *Security Trustworthiness Check* verwendet werden dürfen, falls an ihrem Arbeitsplatz der Zugang zu kerntechnischen und damit zusammenhängenden sensiblen Bereichen oder Informationen erforderlich ist. Der EDSB weist darauf hin, dass die Datenschutzerklärung bei dieser Gelegenheit ausgehändigt werden sollte. Dies sollte im Verfahren klargestellt werden. Bei externen Mitarbeitern eines Unterauftragnehmers sollte die Datenschutzerklärung bei der Datenerhebung ausgehändigt werden.

Der EDSB hat auch inhaltlich die Informationen in der Datenschutzerklärung geprüft und ist zu der Auffassung gelangt, dass sie größtenteils die in Artikel 11 und 12 der Verordnung (EG) Nr. 45/2001 geforderten Angaben enthalten. So finden sich dort Angaben zum Zweck der Verarbeitung (mit einer kurzen Beschreibung), zur Identität des für die Verarbeitung Verantwortlichen, zur Rechtsgrundlage, zu den Empfängern der Daten, zur Datenaufbewahrung und den entsprechenden Fristen und eine funktionale E-Mail-Adresse für Anfragen. Nach Annahme des neuen Sicherheitsbeschlusses der Kommission und der neuen Vereinbarung sollte allerdings auch auf diese Dokumente hingewiesen werden.

2.2.9. Sicherheitsmaßnahmen

Gemäß Artikel 22 und 23 der Verordnung (EG) Nr. 45/2001 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. Diese Maßnahmen müssen insbesondere einer unbefugten Weitergabe, einem unbefugten Zugriff sowie einer zufälligen oder unrechtmäßigen Vernichtung, einem zufälligen Verlust oder einer Veränderung sowie jeder anderen Form der unrechtmäßigen Verarbeitung personenbezogener Daten vorbeugen.

[...]

Für den EDSB besteht kein Grund zu der Annahme, dass die GFS keine angemessenen technischen und organisatorischen Maßnahmen ergriffen hat, um ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

3. Schlussfolgerungen

Es gibt keinen 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. Die GFS Ispra sollte insbesondere Folgendes umsetzen:

- Einhaltung der Aufbewahrungszeiten für die Verarbeitung von Auszügen aus dem Strafregister;
- rechtzeitige Aushändigung der Datenschutzerklärung an die verschiedenen betroffenen Personen (interne sowie externe Mitarbeiter) und Änderung der Datenschutzerklärung, wie vorstehend erläutert;
- Einreichung der die Rechtsgrundlage ausmachenden Dokumente (neuer Sicherheitsbeschluss der Europäischen Kommission und neue Vereinbarung), sobald diese vorliegen.

Brüssel, den 19. Juni 2013

(**unterzeichnet**)

Giovanni Buttarelli
Stellvertretender Europäischer Datenschutzbeauftragter