EUROPÄISCHER
DATENSCHUTZBEAUFTRAGTER

Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Kommission für eine Vorabkontrolle der Sicherheitsgutachten über Drittstaatsangehörige mit Zugang zu den Standorten der Gemeinsamen Forschungsstelle

Brüssel, 22. Juli 2014 (Fall 2013-1020)

1. Verfahren

Am 17. September 2013 erhielt der Europäische Datenschutzbeauftragte („EDSB“) vom Datenschutzbeauftragten („DSB“) der Kommission eine Meldung für eine Vorabkontrolle der Verarbeitungen im Zusammenhang mit Sicherheitsgutachten über Drittstaatsangehörige („DSA“), die Zugang zu den Standorten der Gemeinsamen Forschungsstelle („GFS“) haben.

Die GFS entwickelte das DSA-Verfahren in enger Zusammenarbeit mit der Direktion der Kommission für Sicherheit (Referat HR.DS.2) aus zweierlei Anlass:

- die Abschaffung des *Nulla-osta*-Verfahrens (Sicherheitsüberprüfungsverfahren) der GFS ab dem 1. September 2012[1], woraus sich eine Lücke in der GFS-Sicherheitspolitik hinsichtlich unter anderem der Überprüfung von DSA mit Zugang zu allen GFS-Standorten außer *Karlsruhe* ergab;
- die Anweisung der GD HR, eine angemessene Überprüfung von DSA mit Zugang zu den Räumlichkeiten der Kommission unverzüglich sicherzustellen.

Nach der Abschaffung des *Nulla-osta*-Verfahrens unterbreitete die Kommission ein GFS-Sicherheits- und -Vertrauenswürdigkeitskontrollverfahren (Fall 2012-1090), das die Verarbeitung von personenbezogenen Daten für alle Mitarbeiter abdeckt, die unbeaufsichtigten Zugang zu nukleartechnischen und ähnlichen sensiblen Bereichen bzw. unbeaufsichtigten Zugriff auf Informationen des *Ispra*-Standorts benötigen.

Das DSA-Verfahren wurde ab dem 1. September 2013 und somit vor seiner Meldung am 17. September 2013 implementiert, so dass es sich bei der Analyse um eine Ex-post-Kontrolle einer Verarbeitung handelt.

Der EDSB übersandte den Entwurf der Stellungnahme am 19. Juni 2014 mit der Bitte um Stellungnahme an den DSB. Die Rückmeldung ging am 7. Juli 2014 ein.

[1] Beschluss des Generaldirektors der GFS vom 11. Juli 2012. Dieser Beschluss erging nach u. a. einer Inspektion der GFS im Jahre 2010 (Fall 2010-0832), bei der der EDSB die Rechtmäßigkeit des *Nulla-osta*-Verfahrens in der GFS in Frage stellte.

Postanschrift: rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: 02-283 19 00 – Fax : 02-283 19 50

2. Sachverhalt

Der ***Zweck*** der Verarbeitung besteht darin, dass die GFS-Hierarchie eine Entscheidung über Gewährung oder Verweigerung von Zugangsrechten zu den GFS-Standorten für DSA treffen kann. In dem DSA-Verfahren wird nicht nur definiert, unter welchen Umständen eine Sicherheitsüberprüfung angefordert wird, sondern es werden auch Vorsorge- und Gegenmaßnahmen festgelegt, die in diesem Zusammenhang eingeführt werden können. Die GFS unterhält Arbeitskontakte zu wissenschaftlichen Einrichtungen in verschiedenen Ländern. Das kann bedeuten, dass von diesen Einrichtungen abgeordnete Mitarbeiter an GFS-Standorten anwesend sind und häufig Besucher zugelassen werden müssen, die an GFS-Aktivitäten, die an ihren jeweiligen Standorten stattfinden, teilnehmen oder dabei assistieren. Aufgrund der Spezifizität der GFS-Aufgaben kann es auch erforderlich sein, dass externe Auftragnehmer (oder Bieter – im Stadium der Vertragsvorbereitung oder -aushandlung) an den verschiedenen GFS-Standorten anwesend sind, die von der GFS in Auftrag gegebene Dienstleistungen erbringen. Viele von ihnen sind DSA. Manche DSA sind mögliche Mitarbeiter, die beispielsweise zu einem Einstellungsgespräch eingeladen wurden (wie Stipendiaten oder Gastwissenschaftler usw.).

Bei dem ***Verfahren*** geht es um die Verarbeitung personenbezogener Daten im Sinne der Verordnung (EG) Nr. 45/2001 (die Verordnung). Jeder GFS-Mitarbeiter, der für einen DSA den Zugang zu einem GFS-Standort beantragt, füllt ein Antragsformular aus, das alle für die Tätigkeit (siehe unten) relevanten personenbezogenen Daten enthält. Auf der Grundlage der bereitgestellten Informationen ergeht ein Sicherheitsgutachten durch den Örtlichen Sicherheitsdienst. Vor dem Ergehen des Sicherheitsgutachtens kann der Örtliche Sicherheitsdienst die Direktion der Kommission für Sicherheit (Referat HR.DS.2) der Kommission konsultieren. Die GFS-Hierarchie trifft ihre Entscheidung über Gewährung/Verweigerung von Zugang auf der Basis der Stellungnahme.

Hinsichtlich der ***Rechtsgrundlage*** wurde von der GFS Folgendes gekennzeichnet:

- Beschluss der Kommission vom 29. November 2001 – 2001/844/EG/EGKS/EURATOM;
- Beschluss der Kommission über Alarmstufen der Kommission und Krisenmanagement 2007/65/EG vom 15. Dezember 2006, insbesondere Abschnitt 4 des Anhangs in Bezug auf die GFS;
- Vereinbarung zwischen GD HR/DS und GFS über im Bereich Sicherheit durchgeführte Aufgaben, Ares (2010)884864 – 30/11/2010**;**
- „*Mit der Anwesenheit von Drittstaatsangehörigen ohne Dienstverhältnis in der Kommission verbundene Sicherheitsmaßnahmen*“, Ares(2012)251857), 16.11.2012.

Wie im Fall 2012-1090 festgestellt, fasst die Kommission einen neuen Sicherheitsbeschluss, auf dessen Grundlage eine neue Vereinbarung zwischen der GD HR/DS und der GFS geschlossen wird. Durch diesen Beschluss und diese Vereinbarung werden die Zuständigkeiten der verschiedenen beteiligten Dienststellen geklärt, und sie bilden die Rechtsgrundlage verschiedener Verarbeitungen, einschließlich des DSA-Verfahrens. Bis jetzt wurde jedoch weder der Beschluss gefasst noch die Vereinbarung geschlossen.

Die ***für die Datenverarbeitung Verantwortliche*** ist die Kommission, vertreten durch den Direktor für Ressourcen der GFS. Unterauftragnehmer von Sicherheitsdienststellen, die den Örtlichen Sicherheitsbeauftragten jedes GFS-Standorts angeschlossen sind, können die Daten als ***Auftragsverarbeiter*** im Namen der für die Datenverarbeitung Verantwortlichen verarbeiten.

Bei den ***betroffenen Personen*** handelt es sich um natürliche Personen (nicht juristische Personen, Verbände, Stiftungen usw.), die Zugang zu den GFS-Standorten haben und DSA sind.

Bei den ***verarbeiteten Daten***, die von der betroffenen Person auch in Form von Nachweisdokumenten bereitgestellt werden, handelt es sich um Folgendes:

- Vorname, Nachname, Staatsangehörigkeit, Passnummer und -ausstellungsdatum, Liste von Ländern, in denen sich die betroffene Person in den 12 Monaten vor dem Antrag auf Zugang zu den GFS-Standorten aufgehalten hat, Gründe für den Aufenthalt und Aufenthaltsdauer in diesen Ländern, Liste von GFS-Standorten, die bereits aufgesucht wurden, bevor der Antrag zum erneuten Zugang zu dem/den GFS-Standort/en gestellt wurde, Gründe für den/die Besuch/e und Länge des Aufenthalts an diesen Standorten;
- personenbezogene Daten enthaltende Schriftstücke: Lebenslauf, Auszug aus dem Strafregister und Stellungnahme des Örtlichen Sicherheitsbeauftragten der GFS-Standorte/HR Direktion für Sicherheit.

Unabhängig von den Sicherheitsdienstkompetenzen und den an den verschiedenen GFS-Standorten verwendeten Instrumenten werden die Daten manuell oder per Computer zu einer Datei verarbeitet, die aus dem Antragsformular und dem DSA-Sicherheitsgutachten besteht.

Was den ***Aufbewahrungszeitraum*** angeht, wird in der Meldung betont, dass für die GFS-Standorte nationales Recht gilt, nach dem für die Aufbewahrung personenbezogener Daten von Personen, die Zugang zu ihren Räumlichkeiten haben, andere Regelungen zutreffen; eine Rolle spielt dabei auch das Sicherheitsniveau des Bereichs, zu dem Zugang beantragt wird. Gemäß der Meldung gilt Folgendes:

- *Ispra*[2]: Zugangskontrollsystemtransaktionen und Anomaliedaten werden 24 Monate lang aufbewahrt; in Bezug auf den Zugang zu kontrollierten Zonen oder nukleartechnischen Bereichen beträgt der Aufbewahrungszeitraum aufgrund von rechtlichen Anforderungen 30 Jahre (z. B. zur Speicherung personenbezogener Daten in Bezug auf Strahlendosimetrie aus gesundheitlichen Gründen).

- *Petten*[3]: Dateien werden 3 Monate lang aufbewahrt. Bei einem Vorfall werden die Daten, falls notwendig, zur Analyse länger aufbewahrt, um bei einer rechtsanhängigen Klage ein Recht zu etablieren, auszuüben oder zu verteidigen.

- *Sevilla*[4]: Die Identitäts- und Zugangs*profil*daten von Bediensteten werden während der Dauer des entsprechenden Vertrags aufbewahrt (d. h. in Verbindung mit einem gültigen Mitarbeiterausweis); für andere Mitarbeiter werden die Daten 24 Monate aufbewahrt. Zugangs*profil*daten von Mitarbeitern externer Auftragnehmer werden während der Dauer des entsprechenden Vertrags aufbewahrt (d. h. in Verbindung mit einem gültigen Mitarbeiterausweis). Zugangsdaten werden 5 Jahre lang aufbewahrt. Personenbezogene Daten von Teilnehmern an Workshops/Meetings (von Wissenschaftlichen Referaten verwaltet) sind mit dem Projektprofil verbunden und werden entsprechend den Anforderungen des Projekts aufbewahrt. Der Sicherheitsbeauftragte verwahrt eine Kopie für maximal 6 Monate nach der Veranstaltung.

- *Geel*[5]: Der Aufbewahrungszeitraum beträgt mindestens 30 Jahre für nukleartechnische Kontrollbereiche und kann auf Antrag von Personen, die keinen Zugang zu nukleartechnischen Kontrollbereichen benötigen, auf 5 Jahre verkürzt werden[6].

[2] DSB-2734.1 - GFS: Zugangskontrollsystem am GFS-Standort *Ispra*.
[3] DSB-1534.3 - GFS: Zugangsverwaltungssystem bei GFS-IE in *Petten.*
[4] DSB-1426.5 - GFS: Zugangskontrolle bei GFS-IPTS in *Sevilla.*
[5] DSB-1177.6 - GFS: Zugangskontrolle in GFS-*Geel.*

– *Karlsruhe*[7]: Personenbezogene Daten von Mitarbeitern und Auftragnehmern werden 5 Jahre nach dem Ablaufdatum der Sicherheitsprüfung gelöscht. Für Besucher, die keinen Zugang zu nukleartechnischen Bereichen haben, beträgt der maximale Aufbewahrungszeitraum 5 Jahre nach dem letzten Besuch. Für Personen, die Zugang zu nukleartechnischen Bereichen haben und mit Dosimeterdaten registriert sind, beträgt der maximale Aufbewahrungszeitraum gemäß der Meldung 95 Jahre nach dem Geburtsdatum der betroffenen Person[8].

Hinsichtlich der ***Empfänger*** der Daten unterscheidet die GFS zwischen internen und externen Empfängern:

– *Interne Empfänger*: die GFS-Mitarbeiter, die Zugang für den DSA beantragen, ihre Hierarchie, die Örtlichen Sicherheitsbeauftragten, der GFS-Sicherheitskoordinator, die GD HR für Sicherheit.
– *Externe Empfänger*: Auftragnehmer, die mit der Implementierung der Sicherheitsbestimmungen und deren Überwachung betraut sind (Standortwachpersonal) – die Informationen, über die das Wachpersonal verfügt, sind auf den Vornamen, den Nachnamen, die Passnummer und die Entscheidung „Zugang gewährt“ beschränkt. Der Text des Sicherheitsgutachtens und die im Antragsformular enthaltenen Informationen (außer dem oben Erwähnten) werden nicht an das Wachpersonal weitergegeben.

Hinsichtlich des ***Auskunftsrechts*** geht jeder betroffenen Person, bevor die GFS mit der Erhebung der zum Ausfüllen des Formulars notwendigen Informationen beginnt, per E-Mail eine Datenschutzerklärung durch den Mitarbeiter zu, der den Zugang zu dem GFS-Standort für den DSA beantragt. Sie ist ebenfalls auf Anfrage erhältlich und auf der Internet-Website der GFS öffentlich zugänglich. Die Datenschutzerklärung enthält Angaben zum Zweck der Verarbeitung (mit einer kurzen Beschreibung), zu den erfassten personenbezogenen Daten, zur Identität des für die Datenverarbeitung Verantwortlichen, Informationen über die relevante Rechtsgrundlage, zu den Empfängern der Daten, die Sicherheit der Datenspeicherung und zu den Aufbewahrungsfristen für die Daten (mit Hinweis darauf, dass die Aufbewahrung personenbezogener Daten von dem für jeden GFS-Standort geltenden nationalen Recht sowie vom Sicherheitsniveau des Bereichs, zu dem Zugang beantragt wird, abhängig ist; es wird ein Link zu den Aufbewahrungszeiträumen aller Standorte bereitgestellt). Ferner enthält sie Informationen über das Auskunfts- und Berichtigungsrecht. Erwähnt wird dort schließlich auch das Recht, sich an den Europäischen Datenschutzbeauftragten zu wenden.

Hinsichtlich der ***Auskunfts- und Berichtigungsrechte*** können die betroffenen Personen die folgenden Rechte ausüben, indem sie eine E-Mail mit einem begründeten Antrag an ein funktionales Postfach schicken:

– das Recht auf Auskunft über ihre von dem für die Datenverarbeitung Verantwortlichen aufbewahrten Daten (jederzeit innerhalb von drei Monaten ab dem Eingang des Antrags und kostenlos von dem für die Datenverarbeitung Verantwortlichen);

---

[6] Die Mitteilung bezieht sich auf Artikel 30(1) des Königlichen Erlasses vom 20. Juli 2001, in dem die Allgemeine Verordnung, in der geänderten Fassung, für den Schutz von Öffentlichkeit, Arbeitnehmern und Umwelt gegen die Gefahren von ionisierenden Strahlen festgelegt ist.

[7] DSB-1460.2 - GFS: Zugangserfassung und Zugangskontrolle für den physischen Schutz (ZES+ZKS) bei GFS-ITU in *Karlsruhe.*

[8] Die Mitteilung bezieht sich auf §42 der deutschen *Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung – StrlSchV)*, wo es wie folgt heißt: „*Die Aufzeichnungen sind so lange aufzubewahren, bis die überwachte Person das 75. Lebensjahr vollendet hat oder vollendet hätte, mindestens jedoch 30 Jahre nach Beendigung der jeweiligen Beschäftigung. Sie sind spätestens 100 Jahre nach der Geburt der betroffenen Person zu löschen*“.

– das Recht auf Berichtigung von dem für die Datenverarbeitung Verantwortlichen aufbewahrter unrichtiger oder unvollständiger personenbezogener Daten; die Daten werden innerhalb von höchstens 14 Tagen berichtigt oder geändert.

Hinsichtlich ***Sicherheitsmaßnahmen***
...

3. Rechtsliche Prüfung

3.1. Vorabkontrolle

Diese Stellungnahme bezieht sich auf die Verarbeitung personenbezogener Daten im Zusammenhang des DSA-Verfahrens. 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 (EG) Nr. 45/2001, „die 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 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 Ansicht des EDSB fällt eine solche Verarbeitung von Daten unter Artikel 27 Absatz 2 Buchstabe a der Verordnung, 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 oder strafrechtliche Verurteilungen betreffen.

Obwohl dies in der Meldung nicht erwähnt wird, fällt die Meldung nach Ansicht des EDSB gleichfalls unter Artikel 27 Absatz 2 Buchstabe b der Verordnung, 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 bewertet, um zu bestimmen, ob Zugang zu den GFS-Standorten gewährt werden kann; damit ist Artikel 27 Absatz 2 Buchstabe b der Verordnung anzuwenden, wie es für das „Vertrauenswürdigkeitskontroll"-Verfahren der Fall war[9].

Da die Vorabkontrolle für Situationen gedacht ist, die mit hoher Wahrscheinlichkeit mit gewissen Risiken verbunden sind, sollte die Stellungnahme des EDSB vor dem Beginn der Verarbeitung ergehen. In diesem Fall bestand die Verarbeitung durch die Kommission bereits. Die Empfehlungen des EDSB sollten jedoch vollständig umgesetzt werden. Da dies jedoch als eine Ex-post-Meldung gilt, gilt die Zweimonatsfrist, innerhalb derer der EDSB eine Stellungnahme gemäß Artikel 27 Absatz 4 der Verordnung abgeben muss, nicht für diese Meldung, die auf der Grundlage bestmöglichen Bemühens behandelt wurde.

[9] Siehe EDSB-Stellungnahme vom 19. Juni 2013 zu einer Meldung des Datenschutzbeauftragten der Kommission für eine Vorabkontrolle der Sicherheits- und Vertrauenswürdigkeitskontrolle in der Gemeinsamen Forschungsstelle Ispra (Fall 2012-1090).

3.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe nach Artikel 5 der Verordnung vorliegen.

Nach Auffassung des EDSB fällt die Verarbeitung sowohl unter Artikel 5 Buchstabe a der Verordnung, 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"* als auch Artikel 5 Buchstabe b der Verordnung, da die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die GFS unterliegt. Das nationale Recht unterschiedlicher Mitgliedstaaten stellt nämlich andere Anforderungen an Sicherheitsprüfungen von Personen mit Zugang zu den GFS-Standorten auf dem jeweiligen Staatsgebiet[10]. Insbesondere sind im jeweiligen nationalen Recht unterschiedliche Aufbewahrungsfristen für die personenbezogenen Daten vorgeschrieben, wie im Sachverhalt beschrieben.

Der EDSB berücksichtigt die folgenden EU-Rechtsinstrumente[11], die für eine gewisse Rechtsgrundlage für stattfindende Verarbeitungen sorgen:

- Beschluss der Kommission über Alarmstufen der Kommission und Krisenmanagement 2007/65/EG vom 15. Dezember 2006, insbesondere Abschnitt 4 des Anhangs in Bezug auf die GFS;
- Vereinbarung zwischen GD HR/DS und GFS über im Bereich Sicherheit durchgeführte Aufgaben, Ares (2010)884864 – 30/11/2010, **nach der Aktualisierung;**
- Mit der Anwesenheit von Drittstaatsangehörigen ohne Dienstverhältnis in der Kommission verbundene Sicherheitsmaßnahmen, Ares(2012)251857), 16.11.2012;
- Ferner trägt nationales Recht, durch das spezifische Maßnahmen auferlegt werden, zur Rechtsgrundlage bei, weil den GFS-Standorten dadurch spezifische Verfahren auferlegt werden.

Wie jedoch vom EDSB in dem Fall betreffend die „Vertrauenswürdigkeitskontrolle" (Fall 2012-1090)[12] bereits erwähnt, 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 derartiger Sicherheitsüberprüfungen zu übertragen. Beides stärkt auch die Rechtmäßigkeit und Legitimität der Verarbeitungen für Sicherheitsgutachten über DSA, die Zugang zu GFS-Standorten haben. Wenn dieser Beschluss nicht angenommen und diese Vereinbarung nicht geschlossen wird, kann die Rechtsgrundlage für die Verarbeitung personenbezogener Daten nicht als vollständig gelten. **Der EDSB empfiehlt daher dringend die Annahme des neuen Sicherheitsbeschlusses der Kommission und den Abschluss der aktualisierten Vereinbarung.**

Im Hinblick auf die Notwendigkeit der Verarbeitung stellt der EDSB fest, dass die Verarbeitung personenbezogener Daten im Zusammenhang des DSA-Verfahrens zur

[10] Wie im Fall „Sicherheits- und Vertrauenswürdigkeitsüberprüfung" angemerkt (2012-1090), bestehen beispielsweise spezifische Pflichten zur Implementierung anderer Sicherheitsmaßnahmen für den GFS-Standort *Ispra* als kerntechnischer Betrieb und Inhaber einer kerntechnischen Lizenz nach italienischem Recht.

[11] Der in der Meldung erwähnte Beschluss der Kommission C(2001)3031 (sowie 2001/844/EG) gilt in diesem Fall als irrelevant.

[12] Bereits zum Zeitpunkt der Analyse des Falls 2012-1090 betonte der EDSB, dass es notwendig sei, bei derartigen Sicherheitsverfahren von dem neuen Sicherheitsbeschluss und der neuen Sicherheitsvereinbarung auszugehen.

Einhaltung von für die GFS-Standorte geltenden EU- und nationalen Bestimmungen für notwendig gehalten wird.

3.3. Verarbeitung besonderer Datenkategorien

Unter Berücksichtigung des Verarbeitungszwecks könnten bestimmte Unterlagen unter Artikel 10 der Verordnung fallen. In diesem Zusammenhang verweist der EDSB auf die Anwendung von Artikel 10 Absatz 5 der Verordnung, 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 kann diese Ausnahme aufgrund der rechtlichen Verpflichtungen, denen die GFS-Standorte unterliegen, gelten (siehe die im Sachverhalt und in Punkt 3.2 oben erwähnten Rechtsinstrumente).

3.4. Datenqualität

Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung *„dürfen [personenbezogene Daten] nur den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen*“. Die personenbezogenen Daten, die im vorliegenden Fall verarbeitet werden, dürften auf das begrenzt sein, was für das Erreichen des Zwecks des DSA-Verfahrens erforderlich ist; damit dürfte Artikel 4 Absatz 1 Buchstabe c der Verordnung Genüge getan werden.
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 über einen bestimmten Zeitraum hinaus aufbewahrt werden muss (siehe auch nachstehenden Punkt 3.5).

3.5. Datenaufbewahrung/Datenspeicherung

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung 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, je nach dem für den jeweiligen GFS-Standort gültigen nationalen Recht und dem Sicherheitsniveau des Zugangsbereichs, wie im Sachverhalt beschrieben. Im Lichte der über das für den jeweiligen GFS-Standort gültige nationale Recht vorgelegten Informationen besteht nach Ansicht des EDSB bezüglich der Notwendigkeit und Verhältnismäßigkeit der angewandten Aufbewahrungszeiträume angesichts des durch das DSA-Verfahren verfolgten Ziels kein Anlass zur Sorge.
Wie bereits ausgeführt, sind Daten aus einem Auszug aus dem Strafregister nur sehr 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 (Fall 2011-0482). Zur dementsprechenden

Berücksichtigung empfiehlt der EDSB die Modifizierung des für Auszüge aus dem Strafregister geltenden Aufbewahrungszeitraums.

3.6. Verarbeitung im Auftrag des für die Datenverarbeitung Verantwortlichen

Im Einzelnen ist in dem Verfahren vorgesehen, dass Verarbeiter Daten im Auftrag des für die Datenverarbeitung Verantwortlichen verarbeiten können, da Sicherheitsdienstunterauftragnehmer, die den Örtlichen Sicherheitsbeauftragten jedes GFS-Standorts beigeordnet sind, die Daten im Namen des für die Datenverarbeitung Verantwortlichen verarbeiten dürfen.
Der EDSB erinnert daran, dass die Verarbeitung personenbezogener Daten im Auftrag des für die Datenverarbeitung Verantwortlichen auf der Grundlage eines Vertrags oder Rechtsakts erfolgen muss, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem die folgenden Mindestanforderungen gemäß Artikel 23 der Verordnung erfüllt sein müssen: Im Vertrag muss festgelegt sein, dass der Auftragsverarbeiter nur auf Weisung des für die Verarbeitung Verantwortlichen handelt, und der Auftragsverarbeiter muss für die zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen ausreichende Gewähr bieten und für die Einhaltung dieser Maßnahmen sorgen.
Der EDSB empfiehlt daher, dass die GFS sicherstellt, dass die Anforderungen gemäß Artikel 23 erfüllt werden, und fordert die GFS auf, dem EDSB die entsprechenden Unterlagen zu übersenden.

3.7. Auskunftsrecht und Berichtigung

In Artikel 13 der Verordnung werden ein Auskunftsrecht sowie die Modalitäten seiner Ausübung durch die betroffene Person nach Antrag festgelegt. Er umfasst das Recht, darüber informiert zu werden, dass Informationen, die sich auf die betroffene Person beziehen, von dem für die Datenverarbeitung Verantwortlichen verarbeitet werden, sowie die Übermittlung derartiger Daten in verständlicher Form zu erhalten. Gemäß Artikel 14 der Verordnung hat die betroffene Person das Recht, dass unrichtige oder unvollständige personenbezogene Daten unverzüglich berichtigt werden. Aus der Datenschutzerklärung geht als spezifische Anlaufstelle zur Ausübung dieser Rechte eine funktionale E-Mail-Adresse hervor, und es wird darin festgelegt, dass die Daten nach Einreichung eines begründeten Antrags über die funktionale E-Mail-Adresse innerhalb von höchstens 14 Tagen berichtigt oder modifiziert werden. Einhaltung der Anforderungen gemäß Artikeln 13 und 14 der Verordnung stellt für den EDSB keinen Anlass zur Sorge dar.

3.8. Informationspflicht gegenüber der betroffenen Person

Die Informationspflicht gegenüber betroffenen Personen ist in Artikeln 11 und 12 der Verordnung verankert. Als Teil des DSA-Verfahrens wird vor Erfassung der zum Ausfüllen des DSA-Formulars notwendigen Informationen eine Datenschutzerklärung bereitgestellt.
Der EDSB möchte hier anmerken, dass in der Datenschutzerklärung Links oder interne Schriftstücke der Kommission oder der GFS erwähnt werden, die u. U. für betroffene Personen, die möglicherweise keinen direkten Zugriff auf diese Ressourcen haben, nicht verfügbar sind. Beispielsweise sind der Datenschutzerklärung Informationen über die nationalen Rechtsvorschriften, die für jeden GFS-Standort gelten, und die jeweiligen Aufbewahrungszeiträume lediglich über einen Link zum Register des DSB der Kommission zu entnehmen. Nach Ansicht des EDSB ist die Bereitstellung eines derartigen Links zum Register des DSB nicht hinreichend, um zu gewährleisten, dass die betroffenen Personen richtig informiert werden, da sie möglicherweise keinen Zugriff auf dieses Register haben.

Daher fordert der EDSB die Kommission auf sicherzustellen, dass die betroffenen Personen leichteren Zugriff auf Informationen über die für jeden GFS-Standort geltenden nationalen Rechtsvorschriften und die jeweiligen Aufbewahrungszeiträume haben. Ferner müssen nach der Annahme des neuen Sicherheitsbeschlusses der Kommission und der Vereinbarung Verweise darauf mit aufgenommen werden.
Die anderen Informationselemente in der Datenschutzerklärung enthalten nach Ansicht des EDSB die Angaben, die gemäß Artikeln 11 und 12 der Verordnung erforderlich sind.

3.9. Sicherheitsmaßnahmen

...

4. Schlussfolgerungen

Der EDSB äußert seine Besorgnis hinsichtlich der Tatsache, dass der angekündigte neue Sicherheitsbeschluss der Kommission und die Vereinbarung, die für diese Verarbeitung und die Verarbeitung in Fall 2012-1090 relevant sind, noch nicht angenommen worden sind. Beide sind als Rechtsgrundlage für mehrere Verarbeitungen von größter Bedeutung. Deshalb weist der EDSB besonders darauf hin, dass dringend umfassende Anstrengungen zur Annahme dieses Beschlusses und dieser Vereinbarung unternommen werden müssen, um zu verhindern, dass die Rechtmäßigkeit der betroffenen Verarbeitungen in irgendeiner Weise kompromittiert wird. **Der EDSB fordert daher die Kommission auf, den neuen Sicherheitsbeschluss und die Vereinbarung so schnell wie möglich anzunehmen.**

Die folgenden Empfehlungen sind von der Kommission zu berücksichtigen. Die Kommission muss:

- sicherstellen, dass der neue Sicherheitsbeschluss der Kommission und die Vereinbarung so schnell wie möglich angenommen werden, und diese dem EDSB dann umgehend zustellen;
- den für Strafregisterauszüge geltenden Aufbewahrungszeitraum modifizieren;
- sicherstellen, dass die Datenschutzerklärung ihrerseits umfassende Informationen enthält;

...

Brüssel, den 22. Juli 2014

(unterzeichnet)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter