



Stellungnahme zu einer Meldung des Datenschutzbeauftragten des Europäischen Auswärtigen Dienstes für eine Vorabkontrolle von Sicherheitsuntersuchungen

Brüssel, 1. Februar 2013 (Fall 2011-1059)

1. Verfahren

Am 21. November 2011 erhielt der Europäische Datenschutzbeauftragte (EDSB) eine Meldung des Datenschutzbeauftragten (DSB) des Europäischen Auswärtigen Dienstes (EAD) zur Vorabkontrolle von Sicherheitsuntersuchungen der Abteilung Sicherheit und Sicherheitspolitik des EAD. Der Meldung war eine Datenschutzerklärung beigelegt.

Am 20. Dezember 2011 wurden Fragen gestellt, die der EAD am 14. Juni 2012 beantwortete. Weitere Auskunftsersuchen wurden am 21. Juni bzw. 9. August versendet und am 23. Juli bzw. 31. August beantwortet. In der Zwischenzeit war am 23. Juli 2012 eine überarbeitete Meldung eingereicht worden. Am 10. September verlängerte der EDSB im Einklang mit Artikel 27 Absatz 4 die Frist für die Annahme der Stellungnahme zur Vorabkontrolle um zwei Wochen (24. September), danach noch einmal wegen der Komplexität des Falls bis zum 8. Oktober. Weitere Informationen/Klarstellungen wurden am 8. Oktober angefordert (Antwort am 14. Dezember 2012). Am 17. Dezember 2012 verlängerte der EDSB die Frist um einen weiteren Monat. Der Entwurf der Stellungnahme wurde dem DSB am 16. Januar 2013 zur Kommentierung vorgelegt; seine Bemerkungen gingen beim EDSB am 31. Januar 2013 ein.

2. Sachverhalt

2.1 Zwecke

Der Meldung ist zu entnehmen, dass der Hauptzweck der Verarbeitung der Daten die Untersuchung von Verletzungen und vermuteten Verletzungen der Sicherheitsvorschriften, von Fällen der Kenntnisnahme durch Unbefugte oder Verlust von EU-Verschlusssachen (EU-VS) und von Sicherheitszwischenfällen oder Bedrohungen der Sicherheitsinteressen des EAD ist. Diesem allgemeinen Zweck dienen verschiedene Verarbeitungsvorgänge, die nachstehend näher beschrieben werden.

Für die Verarbeitung Verantwortlicher ist der EAD, hier vertreten durch den Leiter der Abteilung Sicherheit der Zentrale und EAD Sicherheitspolitik (Division for HQ Security and EEAS Security Policy).

Die **Rechtsgrundlage** für die unter diesen Zweck fallenden Verarbeitungsvorgänge besteht aus folgenden Rechtsakten:

1. Beschluss des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes (2010/427/EU), Artikel 10 („Sicherheit“) Absatz 2.
2. Beschluss des Rates vom 31. März 2011 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2011/292/EU), insbesondere Artikel 1, 7, 12 und 13¹.
3. Beschluss der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik vom 15. Juni 2011 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst, insbesondere Artikel 1, 7, 8, 9 und 10² (2011/C 304/05).
4. Beschluss der Europäischen Kommission vom 8. September 1994.
5. Beschluss der Kommission 2001/844 vom 29. November 2001³ und Euratom-Verordnung Nr. 3 vom 31. Juli 1958⁴.
6. Verwaltungsinformation Nr. 45/2006 der Europäischen Kommission vom 15. September 2006.

Während der Abfassung der Stellungnahme war der EAD dabei, einen konsolidierten⁵ „Beschluss der Hohen Repräsentantin der Europäischen Union für die Außen- und Sicherheitspolitik [...] über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst“ („Entwurf des konsolidierten Beschlusses“) zu formulieren. Nach Angaben des für die Verarbeitung Verantwortlichen werden in diesem Beschluss die zu untersuchenden vorhersehbaren Ereignisse dargestellt und folgende Ereignisse abgedeckt:

- Verletzungen oder vermutete Verletzungen der Sicherheitsvorschriften (Artikel 8);
- Kenntnisnahme oder vermutete Kenntnisnahme durch Unbefugte oder Verlust von EU-Verschlusssachen (EU-VS) (Artikel 8);
- Sicherheitszwischenfälle oder vermutete Sicherheitszwischenfälle oder Bedrohungen der Sicherheitsinteressen des EAD (Artikel 2).

Zweck der Verarbeitung und Arten von Verarbeitungsvorgängen

Unter dem Dach des vorstehend beschriebenen allgemeinen Zwecks deckt das EAD-Verfahren mehrere Verarbeitungsvorgänge ab:

2.1.1) Untersuchung von Sicherheitszwischenfällen, Verletzungen der Sicherheitsvorschriften oder Bedrohungen von Sicherheitsinteressen des EAD

Artikel 9 des Entwurfs des konsolidierten Beschlusses besagt zur Untersuchung von Sicherheitszwischenfällen, zu Verletzungen der Sicherheitsvorschriften und/oder zur der Kenntnisnahme durch Unbefugte sowie zu Abhilfemaßnahmen Folgendes:

¹ Der Beschluss enthält die grundlegenden Prinzipien und die Mindestsicherheitsnormen für den Schutz von EU-Verschlusssachen.

² Der Beschluss legt die Vorschriften für den Schutz und die Sicherheit des EAD fest. Er schafft den allgemeinen Regelungsrahmen, um den Risiken für das Personal, die materiellen Vermögenswerte wirksam entgegenzuwirken und den Fürsorgepflichten und der Verantwortung des EAD in dieser Hinsicht nachzukommen.

³ Der Beschluss der Kommission vom 29. November 2001 sieht die Einrichtung eines Sicherheitsbüros der Kommission und die Einsetzung lokaler Sicherheitsbeauftragter in den einzelnen Dienststellen der Kommission vor. Ferner enthält der Beschluss die Sicherheitsbestimmungen der Kommission. In diesen Bestimmungen sind unter anderem die wichtigsten Sicherheitsgrundsätze und -anforderungen festgelegt.

⁴ Die Verordnung Nr. 3 des Euratom-Rates vom 31. Juli 1958 legt unter anderem die Sicherheitsmaßnahmen für von der Gemeinschaft verarbeitete Informationen fest. Darüber hinaus sieht er die Einrichtung eines Sicherheitsbüros und die Einsetzung von Sicherheitsbeauftragten vor.

⁵ Die ersten diesbezüglichen Vorschriften des EAD finden sich in dem Beschluss der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik vom 15. Juni 2011 mit Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst (2011/C 304/05).

Untersuchungen oder Überprüfungen dürfen in folgenden Fällen durchgeführt werden:

- I) wenn bekannt ist oder wenn berechtigter Grund zu der Annahme besteht, dass für den EAD relevante Verschlussachen Unbefugten zur Kenntnis gelangt oder verloren gegangen sind;
- II) bei tatsächlichen oder vermuteten Verletzungen der Sicherheitsvorschriften oder anderen Sicherheitszwischenfällen oder Bedrohungen der Sicherheitsinteressen des EAD.

Bei Eintreten der genannten Ereignisse wird eine Akte mit allen Elementen angelegt, die der Wahrheitsfindung, der Schadensbeurteilung und der Ermittlung des mutmaßlichen Täters dienen. Dazu gehören die Erklärungen der Beschwerdeführer, von Zeugen und potenziellen Tätern, aber auch sachdienliche Beweismittel. Ziel ist es, einen Bericht zu erstellen, der gegebenenfalls der für den Fall zuständigen Behörde übersandt wird. Artikel 9 besagt ferner: „Wird auf persönliche Daten in Kommunikations- und Informationssystemen zugegriffen, erfolgt dieser Zugriff im Einklang mit der Verordnung (EG) Nr. 45/2001“.

2.1.2) Falldatenbank

Der Meldung ist zu entnehmen, dass eine Datenbank mit (offenen und abgeschlossenen) Fällen eingerichtet werden soll, die hilfreiche Informationen aus den einzelnen Akten enthalten und das Auffinden und den Abruf bestimmter Daten erleichtern soll, um so Präventivmaßnahmen und die Erstellung anonymisierter Statistiken zu ermöglichen. Nach Auskunft des für die Verarbeitung Verantwortlichen besteht der Zweck der Datenbank darin, die Unterlagen mit Unterstützung eines automatisierten Werkzeugs aufzubewahren, das eine leichtes Finden/Wiederauffinden von Akten für zulässige Untersuchungszwecke ermöglicht (Suche nach ähnlichen Fällen, Vorgehensweisen in diesen Fällen, wiederholte Verletzungen der Sicherheitsvorschriften durch eine bestimmte Person, Erleichterung der Sicherheitsüberprüfung von Personal durch befugte Dienststellen usw.).

2.1.3) Zugangsliste

Eine weitere Verarbeitung ist die Erstellung, Pflege und Aktualisierung einer Liste von Personen, denen aufgrund von in den einschlägigen Akten vermerkten Informationen der Zugang zu den Räumlichkeiten des EAD untersagt ist. Artikel 11 des Entwurfs des konsolidierten Beschlusses besagt: „Läuft eine Untersuchung der Verletzung der Sicherheitsvorschriften und/oder der Kenntnisnahme durch Unbefugte, kann der Leiter der Direktion Sicherheit des EAD einer Person vorübergehend den Zugang zu EU-VS und den Zutritt zu den Räumlichkeiten untersagen“.

Diese Liste wird folgendermaßen erstellt: Läuft eine zulässige Untersuchung einer Kenntnisnahme von EU-VS durch Unbefugte, kann nach den derzeitigen Vorschriften der Person, die im Verdacht steht, für den Verstoß verantwortlich zu sein, von der EAD-Sicherheitsbehörde der Zugang zu EU-VS entzogen werden. Folglich muss der betreffenden Person der Zutritt zu den Räumlichkeiten des EAD (Sicherheitsbereiche und/oder möglicherweise alle Räumlichkeiten) verweigert werden.

2.1.4) e-Überwachung

In seiner Meldung weist der EAD darauf hin, dass im Hinblick auf die Untersuchung konkreter Fälle der Nutzung von Computern und/oder Kommunikationsmöglichkeiten (wie E-Mail, Internet, Festnetz- oder Mobiltelefonen und Fax) die annehmbare Nutzung sowie Kontrollmaßnahmen und Untersuchungen in der Verwaltungsinformation Nr. 45/2006 vom 15. September 2006 mit Vorschriften für die Nutzung von IKT-Diensten beschrieben sind. In dieser Verwaltungsinformation geht es um die elektronische Überwachung (e-Überwachung) der Arbeit der Mitarbeiter.

Vor dem Hintergrund dieser Verwaltungsinformation stellt der EAD klar, dass im Rahmen einer Untersuchung die Anonymität bestimmter, beschränkter Daten (Verkehrsdaten und/oder Inhalte einer elektronischen Mailbox, Zugang zu Websites, Gespräche mit Festnetz- und Mobiltelefon, Faxübermittlungen usw.) aufgehoben werden kann.

2.2 Kategorien betroffener Personen

Betroffene Personen sind alle Bediensteten des EAD, sonstige Bedienstete, Vertragsbedienstete, ehemalige Beamte, Dienstleister, Auftragnehmer, Besucher, Dritte, die sich von sich aus per Post, E-Mail, Telefon, Fax usw. an den EAD und seine Mitarbeiter wenden oder die Opfer, Zeugen oder Täter bei einer Verletzung der Sicherheitsvorschriften oder einem Ereignis sind, das den Interessen des EAD oder seiner Bediensteten abträglich ist.

2.3 Kategorien von Daten

Welche Daten bei Sicherheitszwischenfällen verarbeitet werden, hängt von dem während der Untersuchung festgestellten Sachverhalt ab. Grundsätzlich können personenbezogene Daten einschließlich Vor- und Nachname, möglicherweise Geburtsort und Geburtsdatum, Anschrift, Telefon- und Mobiltelefonnummer wie auch die Art des Falls, seine näheren Umstände (was geschah wann und wo usw.). die erhobenen Beweismittel und die Verbindungen zwischen diesen Elementen und Personen verarbeitet werden.

In der Fall-Datenbank sind folgende Daten gespeichert:

Aktennummer; Datum der Einrichtung der Akte; Vorname/Familiename/Geburtsdatum des Meldenden; Vorname/Familiename/Geburtsdatum des Opfers; Stadt des Ereignisses; Gemeinde des Ereignisses; Ort des Ereignisses, Datum des Ereignisses; Tageszeit; Art des Ereignisses (nach Möglichkeit nach Kategorien); eigenes Feld für Verletzungen der Sicherheitsvorschriften; eigenes Feld für die Kenntnisnahme von EU-VS durch Unbefugte; eigenes Feld für den Verlust der Akkreditierung/von Parkausweisen, Schlüsseln, PCS, Handys oder anderen Geräten des EAD; kurze Darstellung der Vorgehensweise; erfolgte eine Anzeige bei der belgischen Bundespolizei oder nicht; Ergebnisse der Untersuchungen; Feld für das Melden verdächtigen Verhaltens/verdächtiger Handlungen von Personen/Autos/Bediensteten; ergriffene Maßnahmen.

Nach Angaben des für die Verarbeitung Verantwortlichen sind die verarbeiteten personenbezogenen Daten die Daten, die erforderlich sind, um in der Datenbank mit Hilfe eines Schlüsselwortes nach einer Akte zu suchen. Zur Suche in der Datenbank mit Hilfe von Schlüsselwörtern merkt der für die Verarbeitung Verantwortliche weiter an, die Schlüsselwörter⁶ würden vom EAD verwendet, um *„künftig einen bestimmten Fall aufzufinden oder Akten mit demselben modus operandi zusammenzufassen oder Ereignisse zu finden, die sich am selben Ort ereignet haben, auf dieselbe Person zurückgehen, sich am selben Wochentag ereignet haben usw.“*. In der Datenbank werden nach ihrem Bekanntwerden ebenfalls alle Sicherheitszwischenfälle erfasst, für die eine Akte angelegt wurde.

Im Zusammenhang mit der Zugangsliste und e-Überwachung umfasst das Verfahren die Abfrage der Datenbanken Sysper, Sysper2, Gestel und IOLAN, den Zugriff auf Dienstaussweise und Zugangsberechtigungen einschließlich Fotos, auf Daten über Pensionäre,

⁶ Gemäß der Definition des für die Verarbeitung Verantwortlichen ist ein Schlüsselwort ein in der Meldung aufgeführtes Datenfeld, das Identifizierungszwecken dienen kann.

Angaben zu den nächsten Familienangehörigen⁷, auf Sicherheitsüberprüfungen, das Abrufen, Kopieren und Speichern von Bildern aus kameraüberwachten Gebäuden, Anfragen an die GD DIGIT (E-Mail-Verkehr und Web-Logs, Telefonnummern, die von Räumlichkeiten des EAD und Gebäuden, in denen er seiner Tätigkeit nachgeht, angerufen wurden) nach einem festgelegten Verfahren.

2.4 Erhebung und Speicherung von Daten

Personenbezogene Daten werden sowohl manuell als auch automatisiert in Akten und digitalen Dateien verarbeitet. Papierunterlagen werden in einem Safe, die elektronischen Dateien in einem gesicherten Speichersystem aufbewahrt.

2.5 Datenübermittlungen

Die verarbeiteten Daten können an folgende Empfänger weitergeleitet werden:

- Innerhalb des EAD wird die Liste der Personen, denen der Zugang untersagt ist, an die EAD-Beamten weitergegeben, die bei der Wahrnehmung ihrer beruflichen Aufgaben über diese Liste Bescheid wissen müssen;
- innerhalb anderer Organe und Einrichtungen der EU gehen Daten an befugte natürliche Personen, die im Rahmen ihrer Zuständigkeiten (bei IDOC, OLAF usw.) diese Daten unbedingt benötigen;
- innerhalb der EU-Mitgliedstaaten gehen Daten an befugte natürliche Personen oder Justizbehörden oder die Polizei oder an beauftragte Unternehmen, die diese Daten unbedingt benötigen;
- an Drittländer und internationale Organisationen im Einklang mit konkreten Abkommen oder Vereinbarungen über den gegenseitigen Schutz von Verschlusssachen. Der für die Verarbeitung Verantwortliche weist darauf hin, dass es Drittländer und internationale Organisationen gibt, mit denen die EU Informationssicherheitsabkommen oder ähnliche Vereinbarungen ausgehandelt hat. Der für die Verarbeitung Verantwortliche hat dem EDSB einen Informationsvermerk des Rates der Europäischen Union über den „Austausch von EU-Verschlusssachen (EU-VS) mit ihnen („Derzeitige Fassung des EAD vom 22. Juni 2012 – 11766/12“) vorgelegt. Dieser Vermerk enthält eine Auflistung der Drittländer und internationalen Organisationen, mit denen derartige Abkommen und Vereinbarungen unterzeichnet wurden⁸. Der Informationsaustausch in diesem Zusammenhang betrifft nur Verletzungen der Sicherheitsvorschriften und/oder Gefährdungen der Sicherheit im Umgang mit Verschlusssachen, die zwischen der EU (insbesondere dem EAD) einerseits und dem betreffenden Drittland oder der betreffenden internationalen Organisation andererseits ausgetauscht wurden. Er erfolgt auf der Rechtsgrundlage der Bestimmungen über die Zusammenarbeit von Parteien bei Sicherheitsuntersuchungen in dem betreffenden Abkommen.

⁷ Jeder Bedienstete hat eine Person anzugeben, die im Fall eines Unfalls benachrichtigt werden soll. Der Name und die Kontaktdaten dieses Familienangehörigen werden von der Personalabteilung in der Personalakte aufbewahrt.

⁸ Auf der Liste stehen derzeit folgende Staaten: Australien, Bosnien-Herzegowina, Kroatien, Ehemalige Jugoslawische Republik Mazedonien, Island, Israel, Liechtenstein, Montenegro, Norwegen, Schweiz, Ukraine und Vereinigte Staaten von Amerika. Mit anderen Staaten laufen die Verhandlungen noch. Es bestehen Abkommen mit folgenden internationalen Organisationen: NATO, ICC, ESA. Mit den Vereinten Nationen bestehen Ständige Verwaltungsvereinbarungen.

Nach Angaben des für die Verarbeitung Verantwortlichen wird über einen solchen Austausch fallweise entschieden und zuvor überprüft, ob der Partner und das System sowie die bestehenden Verfahren vertrauenswürdig sind und ob die andere Seite wirklich über die Informationen verfügen muss.

In diesem Rahmen würde eine Offenlegung personenbezogener Daten ausschließlich in Ausnahmefällen erwogen, wenn

1. eine solche Offenlegung für die Zusammenarbeit mit dem Dritten in der betreffenden Sicherheitsuntersuchung unbedingt erforderlich ist;
2. die Angemessenheit des vom Dritten gebotenen Schutzniveaus ordnungsgemäß bewertet und mit Blick auf das fragliche Sicherheitsinteresse als ausreichend gilt.

Sind diese Bedingungen erfüllt, würden nach Angaben des für die Verarbeitung Verantwortlichen die betreffenden personenbezogenen Daten auf der Grundlage von Artikel 9 Absatz 6 Buchstabe d der Verordnung (EG) Nr. 45/2001 weitergegeben.

Der für die Verarbeitung Verantwortliche wies ferner darauf hin, dass zum Schutz der Sicherheitsinteressen des EAD ein Austausch personenbezogener Daten auch mit Drittländern und internationalen Organisationen erforderlich sein könnte, mit denen keine derartigen Sicherheitsabkommen oder Vereinbarungen bestehen. Auch hier würde eine Weitergabe personenbezogener Daten nur in Ausnahmefällen in Erwägung gezogen, und zwar nach sorgfältiger Bewertung der Angemessenheit des von dem Dritten gebotenen Schutzniveaus betreffend

1. das lebenswichtige Interesse der betreffenden betroffenen Person oder
2. das in Frage stehende Sicherheitsinteresse.

Sind diese Bedingungen erfüllt, würden nach Angaben des für die Verarbeitung Verantwortlichen die betreffenden personenbezogenen Daten auf der Grundlage von Artikel 9 Absatz 6 Buchstabe e und/oder d der Verordnung (EG) Nr. 45/2001 offengelegt.

Schließlich heißt es, dass jeder Empfänger den Verpflichtungen nachzukommen hat, die sich aus EU-Verordnungen, internationalen Abkommen und/oder Verwaltungsvereinbarungen und einzelstaatlichen Gesetzen ergeben, wenn Aufgaben wahrzunehmen sind, die in die Zuständigkeit der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik und/oder des EAD fallen.

2.6 Datenaufbewahrung

Für die Aufbewahrung gilt Folgendes: Personenbezogene Daten in Papierform und/oder in digitalen Dateien sowie in der Datenbank dürfen von der Verwaltung nach Schließen der Akte höchstens zehn Jahre aufbewahrt werden. Dieser Zeitraum entspricht den gesetzlich festgelegten allgemeinen Fristen für Akten in Strafverfahren. Die Sachbearbeiter können zur Aussage vor den zuständigen Gremien aufgefordert werden.

Personenbezogene Daten in der Liste von Personen, denen der Zutritt zu den Räumlichkeiten des EAD untersagt ist, werden solange aufbewahrt, wie es für die Anwendung des Zutrittsverbots erforderlich ist, jedoch keinesfalls länger als fünf Jahre nach Durchführung der Maßnahme.

2.7 Informationspflicht gegenüber der betroffenen Person

Im Abschnitt „Sicherheit“ des Intranets des EAD ist eine Datenschutzerklärung einsehbar. Sie enthält Angaben zur Identität des für die Verarbeitung Verantwortlichen, zum Zweck der

Sicherheitsuntersuchung, der Rechtsgrundlage der Verarbeitung, den Datenempfängern, dem Bestehen des Rechts auf Auskunft und Berichtigung, zur Aufbewahrungsfrist und dem Recht, sich jederzeit an den EDSB zu wenden.

Je nach betroffenen Personen werden weitere spezifische Angaben über andere Kanäle bereitgestellt.

- Person, die Gegenstand einer Untersuchung ist (betroffene Person)

Kann die betroffene Person kontaktiert werden, wird sie bei Einholung ihrer schriftlichen Aussage aufgeklärt und erhält sofort ein Exemplar der Datenschutzerklärung. Andernfalls erhält sie die Informationen beim ersten Kontakt nach der Aufzeichnung. Nach Auffassung des EAD sollte in den Fällen, in denen eine Information der möglicherweise betroffenen Person entweder durch die zuständigen Stellen des EAD oder durch die Justizbehörden die Untersuchung gefährden würde, die Erteilung der Auskünfte so lange aufgeschoben werden, bis keine Gefährdung mehr besteht.

- Informanten, Zeugen und interne Hinweisgeber

Meldet eine Person einen Tatbestand per E-Mail, erhält sie die Datenschutzerklärung automatisch. Wird die Meldung in Anwesenheit der Person schriftlich aufgenommen, wird ihr unverzüglich ein Exemplar der Datenschutzerklärung ausgehändigt. Erfolgt die Meldung telefonisch, wird die Person mündlich aufgeklärt. Der für die Verarbeitung Verantwortliche weist darauf hin, dass solche Anrufe zur Gewährleistung ihrer Echtheit aufgezeichnet werden sollen (zum Zeitpunkt der Prüfung der Notwendigkeit einer Vorabkontrolle waren die technischen Voraussetzungen für eine Aufzeichnung allerdings noch nicht gegeben).

Zeugen erhalten die Datenschutzerklärung während ihrer Befragung und bekommen außerdem eine Kopie ihrer Aussage.

Wie der für die Verarbeitung Verantwortliche erläutert, kann es auch bei Sicherheitsuntersuchungen interne Hinweisgeber⁹ geben, die in die Kategorie „Informanten“ fallen. Weiter wird erläutert, dass derartige Fälle durch Artikel 8 „Verletzungen der Sicherheit und Kenntnisnahme von Verschlusssachen durch Unbefugte“ des Beschlusses der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik vom 15. Juni 2011 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst (2011/C 304/05) abgedeckt sind, der besagt: „Verletzungen oder vermutete Verletzungen der Sicherheitsvorschriften werden unverzüglich der Direktion „Sicherheit“ des EAD gemeldet, die erforderlichenfalls die zuständigen Stellen der Kommission, des Generalsekretariats des Rates oder die zuständigen Behörden in den Mitgliedstaaten hiervon in Kenntnis setzt“.

- Personen, denen der Zutritt zu den Räumlichkeiten des EAD untersagt ist

Den von dem für die Verarbeitung Verantwortlichen vorgelegten Unterlagen ist zu entnehmen, dass Personen, die in einer Sicherheitsuntersuchung Verdächtige sind, nicht vorab

⁹ Artikel 22 des Statuts besagt: „Erhält ein Beamter in Ausübung oder anlässlich der Ausübung seines Dienstes Kenntnis von Tatsachen, die die Möglichkeit rechtswidriger Handlungen, einschließlich Betrug oder Korruption, zum Nachteil der Interessen der Gemeinschaften oder Verhaltensweisen im Zusammenhang mit der Ausübung dienstlicher Pflichten, die eine schwerwiegende Verletzung der Dienstpflichten der Beamten der Gemeinschaften darstellen können, vermuten lassen, so unterrichtet er unverzüglich seinen unmittelbaren Vorgesetzten oder Generaldirektor oder, falls er dies für zweckdienlich hält, den Generalsekretär oder Personen in vergleichbaren Positionen bzw. direkt das Europäische Amt für Betrugsbekämpfung (OLAF)“.

darüber in Kenntnis gesetzt werden, dass sie auf der Liste stehen, weil dies die Untersuchung behindern könnte. Sie werden informiert, wenn sie tatsächlich an einer Zutrittsstelle vorstellig werden. Nach Angaben des für die Verarbeitung Verantwortlichen wird am Ende des Untersuchungsverfahrens 1) die Person darüber in Kenntnis gesetzt, dass ihr im Rahmen der möglicherweise ergriffenen Verwaltungsmaßnahmen der Zutritt untersagt ist, und 2) in dem Fall, dass bei Abschluss der Untersuchung keine Beweise gegen den Verdächtigen vorliegen, die Daten der Person unverzüglich von der Ausschlussliste gelöscht. Nach Auffassung des für die Verarbeitung Verantwortlichen kann es gerechtfertigt sein, die Person nicht darüber zu informieren, dass sie Verdächtiger war, da sich die Person vielleicht gar nicht der gegen sie laufenden Untersuchung bewusst war und die Untersuchung ohne Konsequenzen für die betreffende Person abgeschlossen worden ist.

2.8 Auskunfts- und Berichtigungsrecht

Betroffene Personen haben das Recht, sofort oder später durch Abgabe oder Übersenden einer weiteren Aussage, die zur Akte genommen wird, von ihnen eingereichte Daten zu berichtigen. Auf diese Möglichkeit werden die betreffenden Personen im Verlauf ihrer Befragung immer hingewiesen; sie wird aber auch in der Datenschutzerklärung im Abschnitt Sicherheit des Intranets des EAD erwähnt.

Nach Angaben des für die Verarbeitung Verantwortlichen kann gestützt auf die in Artikel 20 der Verordnung (EG) Nr. 45/2001 aufgeführten Ausnahmen der Zugang zu Daten abgelehnt, eingeschränkt oder mit Verzögerung gewährt werden, wenn sich dieser Zugang nachteilig auf die Untersuchung oder die Rechte und Freiheiten anderer Personen auswirken kann. Die betroffene Person kann sich dann an den EDSB wenden, der die diese Person betreffenden Daten überprüfen und sie erforderlichenfalls berichtigen oder bei Vorliegen eines berechtigten Grundes löschen kann.

2.9 Sicherheit

[...]

3. Rechtliche Analyse

3.1. Vorabkontrolle

Anwendbarkeit der Verordnung (EG) Nr. 45/2001 („Verordnung“): Erstens ist die hier zu prüfende Datenverarbeitung eine Verarbeitung personenbezogener Daten („*alle Informationen über eine bestimmte oder eine bestimmbare natürliche Person*“ – Artikel 2 Buchstabe a der Verordnung). Wie in der Meldung beschrieben, werden nämlich personenbezogene Daten von an dem Sicherheitszwischenfall beteiligten Personen (mutmaßlichen Tätern, Zeugen usw.) erhoben. Zweitens werden die erhobenen personenbezogenen Daten „automatisiert und manuell verarbeitet“, wie in Artikel 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 definiert. Wird beispielsweise ein Bericht mit Informationen aus Datenbanken, Bildern aus einer Videoüberwachung usw. erstellt und später in einer elektronischen Datenbank gespeichert, werden personenbezogene Daten verarbeitet. Schließlich wird die Datenverarbeitung von einer Einrichtung der EU, dem EAD, bei Sicherheitsuntersuchungen im Zuge der Wahrnehmung seiner Aufgaben, die in den Anwendungsbereich des Unionsrechts fallen, vorgenommen. Der EDSB ist daher der Auffassung, dass bei der vom EAD vorgenommenen Datenverarbeitung alle Elemente gegeben sind, die die Anwendung der Verordnung auslösen.

Der „Entwurf eines Beschlusses der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst“ (**Beschlussentwurf**) sieht in seinem Artikel 9 Absatz 3 Folgendes vor: „Wird auf personenbezogene Daten in Kommunikations- und Informationssystemen zugegriffen, erfolgt dieser Zugriff gemäß der Verordnung (EG) Nr. 45/2001“. Der EDSB stellt fest, dass diese Einschränkung der Anwendbarkeit der Verordnung im Widerspruch zur Verordnung steht. Laut Artikel 3 der Verordnung (EG) Nr. 45/2001 gilt die Verordnung nämlich „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“. Die Verordnung (EG) Nr. 45/2001 ist daher nicht nur auf die Verarbeitung personenbezogener Daten durch Kommunikations- und Informationssysteme anzuwenden. Der Beschlussentwurf sollte so geändert werden, dass er dies deutlich macht.

Bewertung der Frage, ob die Verarbeitungsvorgänge unter Artikel 27 der Verordnung fallen. Nach Auffassung des EDSB fällt die Datenverarbeitung eindeutig unter die in Artikel 27 Absatz 2 der Verordnung (EG) Nr. 45/2001 aufgeführten Fälle.

Erstens fällt eine solche Verarbeitung nach Auffassung des EDSB unter Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001, dem zufolge Verarbeitungen, die „*Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen*“ betreffen, vom EDSB vorab zu kontrollieren sind. Im vorliegenden Fall verarbeitet der EAD bei Untersuchungen von Zwischenfällen wie Unfällen, Verletzungen der Sicherheitsvorschriften, Diebstahl oder unbefugtem Zutritt Daten, die mit mutmaßlichen Straftaten und Straftaten und anderen schweren Verfehlungen in Verbindung stehen können. Bekräftigt wird dies noch, wenn man berücksichtigt, dass der Zweck der Verarbeitung letztendlich darin besteht, einen Bericht über ein Vorkommnis zu verfassen und ihn möglicherweise an Strafverfolgungs- und Justizbehörden weiterzuleiten.

Der für die Verarbeitung Verantwortliche hat die Meldung auch mit Blick auf Artikel 27 Absatz 2 Buchstabe d eingereicht, in dem es um Verarbeitungen geht, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen. Der EDSB ist allerdings der Auffassung, dass nur die Verarbeitung unter diesen Artikel fällt, die darauf abzielt, Personen den Zutritt zu den Räumlichkeiten des EAD zu verwehren. Seiner Ansicht nach dienen Verarbeitungen im Zusammenhang mit der Abfassung eines Berichts und die Eingabe in Datenbanken an sich nicht dem Zweck, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen, obwohl sie dies möglicherweise nach sich ziehen können. Artikel 27 Absatz 2 Buchstabe d gilt also nur für bestimmte Verarbeitungsvorgänge.

Die Meldung des DSB ging am 21. November 2011 ein. Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten abzugeben. Am 23. Juli 2012 ging eine überarbeitete Meldung über einen kleineren Geltungsbereich ein. Das Verfahren wurde für insgesamt 297 bzw. 15 Tage ausgesetzt, um den für die Verarbeitung Verantwortlichen Gelegenheit zu geben, weitere Auskünfte zu erteilen und Bemerkungen zu machen. Aufgrund der Komplexität des Falls wurde das Verfahren um insgesamt zwei Monate verlängert. Daher muss diese Stellungnahme spätestens am 1. Februar 2013 vorgelegt werden.

3.2. Rechtmäßigkeit der Verarbeitung

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

In der Meldung des EAD sind Artikel 5 Buchstabe a, b, d, und e der Verordnung als Rechtsgrundlage angegeben. 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 a, demzufolge 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“*.

Bei der Prüfung der Frage, ob Verarbeitungen im Einklang mit Artikel 5 Buchstabe a der Verordnung (EG) Nr. 45/2001 stehen, sind drei Elemente zu berücksichtigen. Es geht darum, ob erstens der Vertrag oder andere Rechtsinstrumente die Datenverarbeitungen durch den EAD vorsehen, zweitens die Verarbeitungen im öffentlichen Interesse durchgeführt werden und drittens die Verarbeitungen für die Wahrnehmung dieser Aufgabe tatsächlich erforderlich sind. Diese drei Anforderungen sind natürlich eng miteinander verknüpft.

Einschlägige Rechtsgrundlagen im Vertrag oder in anderen Rechtsinstrumenten. Der EDSB nimmt die im Abschnitt „Sachverhalt“ aufgeführten Rechtsinstrumente zur Kenntnis, die vom Allgemeinen zum Besonderen hin die Rechtsgrundlage für die legitimen Verarbeitungsvorgänge im Rahmen von Untersuchungen abgeben.

Bezüglich Artikel 10 („Sicherheit“) Absatz 2 des Beschlusses des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes (2010/427/EU) stellt der EDSB fest, dass gemäß diesem Artikel der EAD bis zur Annahme seiner eigenen Sicherheitsvorschriften im Jahr 2011 hinsichtlich des Schutzes von Verschlussachen die im Anhang des Beschlusses 2001/264/EG festgelegten Sicherheitsmaßnahmen und hinsichtlich anderer Sicherheitsaspekte die im einschlägigen Anhang der Geschäftsordnung der Kommission festgelegten Sicherheitsvorschriften angewandt hat.

Wie bereits unter Punkt 2 ausgeführt, erteilte der für die Verarbeitung Verantwortliche dem EDSB mit dem Beschlusssentwurf weitere Auskünfte über die Rechtsgrundlage. Nach den vorliegenden Informationen soll dieser konsolidierte Beschluss alle relevanten Aspekte von Untersuchungen abdecken und die derzeitige Rechtsgrundlage ersetzen. Bei der Prüfung der Rechtmäßigkeit der Verarbeitung sind unter anderem Artikel 9 über die Untersuchung von Sicherheitszwischenfällen und Artikel 12 über die Organisation der Sicherheit des EAD relevant.

Nach Auffassung des EDSB sehen die genannten Rechtsgrundlagen im Allgemeinen und im Besonderen die Existenz des Sicherheitsdienstes des EAD vor und regeln seine Befugnisse zur Durchführung von Untersuchungen oder Überprüfungen. Des Weiteren sehen die genannten Rechtsgrundlagen die in der Meldung beschriebenen Arten von Verarbeitungsvorgängen vor. Die oben zitierten Rechtsakte ermächtigen den Sicherheitsdienst des EAD zu Verarbeitungen, mit denen Informationen gewonnen werden, die dem EAD sichere Bedingungen für seine Tätigkeit gewährleisten, sowie Informationen über ungesetzliche Handlungen in seinen Abteilungen, die bei Untersuchungen der Justiz oder Disziplinarmaßnahmen Verwendung finden. Diesbezüglich hält der EDSB fest, dass diese Rechtsakte eine gültige Rechtsgrundlage für die Datenverarbeitungen darstellen, mit denen Informationen über Zwischenfälle innerhalb des EAD gewonnen werden sollen.

Die Verarbeitungen werden im öffentlichen Interesse vorgenommen. Der EDSB stellt fest, dass der EAD die Verarbeitungen im Rahmen der legitimen Ausübung seiner öffentlichen Gewalt vornimmt. Die Aufgabenbeschreibung des EAD besagt, dass er befugt und verpflichtet ist, zum Schutz von Personal, materiellen Vermögenswerten und Informationen innerhalb des EAD und bei der Wahrnehmung von Aufgaben gemäß Titel V Kapitel 2 EUV Untersuchungen durchzuführen. Bedenkt man den Charakter dieser Aktivitäten, steht fest, dass sie insofern im öffentlichen Interesse erfolgen, als dem öffentlichen Interesse gedient ist, wenn in Untersuchungen nach dem Urheber solcher Ereignisse gesucht und deren Wiederholung in der Zukunft verhindert wird.

Erforderlichkeitsprüfung. Im Rahmen von Untersuchungen, bei denen Informationen über Zwischenfälle in Räumlichkeiten des EAD gewonnen werden sollen, dürfte die Verarbeitung personenbezogener Daten erforderlich sein. Ohne die Verarbeitung solcher Daten könnte der EAD seinen Pflichten nicht nachkommen. Allgemein betrachtet ist die Verarbeitung also für die Untersuchungen erforderlich. Es ist jedoch zu berücksichtigen, dass die „Erforderlichkeit“ der Datenverarbeitung auch im konkreten Einzelfall, also bei jeder Untersuchung zu prüfen ist. Hierbei ist zu bedenken, dass die Verarbeitung personenbezogener Daten im Rahmen der Verarbeitung von Informationen über Zwischenfälle (wie sie im Abschnitt „Sachverhalt“ beschrieben werden) in einem angemessenen Verhältnis zum allgemeinen Zweck der Verarbeitung (Gewährleistung der Sicherheit von Personen, Gebäuden) und zum speziellen Zweck der Verarbeitung in dem hier zu prüfenden Fall stehen muss. Die Verhältnismäßigkeit ist also fallweise zu bewerten.

3.3. Verarbeitung besonderer Datenkategorien

In Anbetracht der Tatsache, dass der Zweck der Verarbeitung darin besteht, die Erhebung von Informationen über Zwischenfälle, denen ein mutmaßliches Fehlverhalten zugrunde liegt, zu erleichtern, kann erwartet werden, dass in vielen Fällen diese Informationen im Zusammenhang mit Straftaten, strafrechtlichen Verurteilungen oder Sicherungsmaßnahmen stehen. 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 Sicherungsmaßnahmen 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 ist die Verarbeitung der erwähnten Daten nach den unter Punkt 3.2 bereits genannten Rechtsakten zulässig.

Zu besonderen Datenkategorien heißt es in Artikel 10 Absatz 1 der Verordnung (EG) Nr. 45/2001: *„Die Verarbeitung personenbezogener Daten, aus denen die rassistische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von Daten über Gesundheit oder Sexualleben sind untersagt.“*

Aus der Meldung zur Vorabkontrolle geht nicht hervor, dass im Rahmen der Untersuchungen Daten aus den in Artikel 10 Absatz 1 der Verordnung (EG) Nr. 45/2001 genannten Kategorien verarbeitet werden. Mit Blick auf den Gesamtzweck, den der EAD mit den Datenverarbeitungsvorgängen verfolgt, geht der EDSB davon aus, dass die Erhebung besonderer Datenkategorien nicht das Hauptziel des EAD ist.

Der EDSB ist jedoch der Ansicht, dass der EAD im Zuge seiner Untersuchungen unter Umständen besondere Datenkategorien erhebt und, vielleicht unabsichtlich, auch verarbeitet. Die Erhebung und Weiterverarbeitung sensibler Daten ist nur dann zulässig, wenn sie im vorliegenden Fall für einen der in Artikel 10 Absatz 2 geregelten Zwecke *erforderlich* ist. Da die Verarbeitung sensibler Daten eher als Ausnahme und nicht als Regel zu betrachten ist, ist hier das Kriterium der Erforderlichkeit restriktiv anzuwenden.

In diesem Zusammenhang verweist der EDSB auf die Anwendung des Grundsatzes der Datenqualität (auf den weiter unten noch näher eingegangen wird), dem zufolge die Daten den Zwecken entsprechen müssen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein müssen und nicht darüber hinausgehen dürfen (Artikel 4 Absatz 1 Buchstabe c). Sollten also besondere Datenkategorien, die für die Untersuchung eines Zwischenfalls eindeutig nicht erheblich sind, trotzdem erhoben werden, sollten sie nach diesem Grundsatz nicht in den schriftlichen Bericht eingehen. Sicherheitsbeauftragte sollten auf diese Vorschrift hingewiesen werden.

3.4. 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“*. Dies wird als Grundsatz der Datenqualität bezeichnet.

In den Unterlagen einer Untersuchung von Zwischenfällen werden immer bestimmte Standarddaten wie Name, Geburtsdatum, Anschrift usw. zu finden sein, doch dürfte der genaue Inhalt einer solchen Akte von Fall zu Fall sehr verschieden ausfallen. Es sind daher Garantien dafür vorzusehen, dass der Grundsatz der Datenqualität eingehalten wird. In der Entscheidung über die Eröffnung einer Untersuchung sollten Gegenstand und Umfang der Ermittlungen festgelegt sein. Damit ließe sich die Menge der erhobenen Daten auf das beschränken, was zum Umfang der Untersuchung gehört. Zweitens vertritt der EDSB die Auffassung, dass Untersuchungsbeauftragte vor Beginn der Untersuchung Weisungen erhalten sollten, in denen auf Artikel 4 Absatz 1 Buchstabe c der Verordnung (EG) Nr. 45/2001 hingewiesen wird, um sie zu größerer Vorsicht bei der Erhebung von Beweismitteln oder Eingabe von Daten in die Untersuchungsakte zu veranlassen. Bedienstete, die eine Untersuchung durchführen und einen Bericht abfassen sollen, sind mit diesen Weisungen zu versehen und haben sich an diese zu halten.

Gemäß Artikel 4 Absatz 1 Buchstabe d der Verordnung müssen personenbezogene Daten *„sachlich richtig sein und, wenn nötig, auf den neuesten Stand gebracht werden“*, und *„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.“*

Dieser Grundsatz ist eng mit der Ausübung des Rechts auf Auskunft, Berichtigung, Sperrung und Löschung verknüpft (siehe weiter unten Punkt 3.7).

3.5. 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.

Der EDSB ist mit der Fünfjahresfrist für personenbezogene Daten in der Liste von Personen einverstanden, denen der Zugang zu Räumlichkeiten des EAD untersagt ist.

Ferner nimmt der EDSB die Frist von zehn Jahren nach Schließung der Akte zur Kenntnis, die für personenbezogene Daten gilt, die von der Verwaltung in Papierform und/oder in digitalen Dateien sowie in der Datenbank aufbewahrt werden.

3.6. Datenübermittlung

In den Artikel 7, 8 und 9 der Verordnung (EG) Nr. 45/2001 sind bestimmte Pflichten geregelt, die Anwendung finden, wenn für die Verarbeitung Verantwortliche personenbezogene Daten an Dritte übermitteln. Die Vorschriften fallen unterschiedlich aus, je nachdem ob die Übermittlung gemäß Artikel 7 an Organe oder Einrichtungen der Gemeinschaft, gemäß Artikel 8 am Empfänger, die der Richtlinie 95/46/EG unterworfen sind, oder gemäß Artikel 9 an andere Arten von Empfängern erfolgt.

Den Angaben des für die Verarbeitung Verantwortlichen ist zu entnehmen, dass Daten an befugte Personen in den Organen und Einrichtungen der EU und der EU-Mitgliedstaaten oder an Justizbehörden oder die Polizei oder betroffene Auftragnehmer übermittelt werden dürfen, sofern diese die Daten unbedingt benötigen. Daten könnten auf der Grundlage von Abkommen oder Vereinbarungen über den gegenseitigen Schutz von Verschlusssachen auch an Drittländer und internationale Organisationen übermittelt werden, sollte dieser Fall auftreten und sollten an ihm das besagte Drittland oder die besagte internationale Organisation beteiligt sein.

Die Artikel 7, 8 und 9 sind daher anzuwenden und sollten einer näheren Betrachtung unterzogen werden.

Übermittlung personenbezogener Daten innerhalb von oder zwischen Organen und Einrichtungen der Gemeinschaft. Aus dem in den Meldungen zur Vorabkontrolle beschriebenen Sachverhalt geht hervor, dass Daten an Organe und Einrichtungen der EU übermittelt werden können. Dabei handelt es sich im Wesentlichen um OLAF, IDOC, den EDSB oder den Ombudsmann in ihren jeweiligen Zuständigkeitsbereichen.

Artikel 7 Absatz 1 der Verordnung besagt: *„Personenbezogene Daten werden innerhalb der Organe oder Einrichtungen der Gemeinschaft oder an andere Organe oder Einrichtungen der Gemeinschaft nur übermittelt, wenn die Daten für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen“.*

Gemäß der Meldung werden Berichte und damit zusammenhängende Unterlagen (personenbezogene Daten) an die genannten Organe und Einrichtungen der EU nur bei Bedarf übermittelt und wenn sie unbedingt benötigt 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. Hierbei ist auf die Verhältnismäßigkeit zu achten und sind beispielsweise die Art der erhobenen und weiterverarbeiteten Daten und der Zuständigkeitsbereich des Empfängers zu berücksichtigen.

Der Empfänger innerhalb eines Organs oder einer Einrichtung der EU ist auf jeden Fall darauf hinzuweisen, dass personenbezogene Daten nur für den Zweck verarbeitet werden dürfen, für den sie erhoben wurden.

Übermittlung personenbezogener Daten an Mitgliedstaaten. Nach Angaben der Meldung können Daten an nationale Strafverfolgungs- und Justizbehörden übermittelt werden. In den Mitgliedstaaten sind hier zwei Szenarien denkbar: a) Mitgliedstaaten, in denen die einzelstaatlichen Datenschutzvorschriften zur Umsetzung der Richtlinie 95/46/EG alle Bereiche der nationalen Rechtsordnung einschließlich des Justizwesens abdecken, und b) Mitgliedstaaten, in denen die einzelstaatlichen Datenschutzvorschriften zur Umsetzung der Richtlinie 95/46/EG nicht alle Bereiche und insbesondere nicht den Justizsektor abdecken. Im Hinblick auf das erste Szenario besagt Artikel 8 der Verordnung Folgendes: *„Unbeschadet der Artikel 4, 5, 6 und 10 werden personenbezogene Daten an Empfänger, die den aufgrund der Richtlinie 95/46/EG erlassenen nationalen Rechtsvorschriften unterliegen, nur übermittelt, wenn der Empfänger nachweist, dass die Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Ausübung der öffentlichen Gewalt gehört, erforderlich sind [...].“* Wenn der Mitgliedstaat bei der Umsetzung der Richtlinie 95/46/EG in innerstaatliches Recht für diese Behörden nationale Durchführungsbestimmungen erlassen hat, ist Artikel 8 der Richtlinie Rechnung zu tragen, auch wenn Justizbehörden nicht in den Anwendungsbereich der Richtlinie 95/46/EG fallen. Für die Länder, die für Justizbehörden keine nationalen Vorschriften zur Umsetzung der Richtlinie 95/46/EG erlassen haben, gilt Artikel 9 der Verordnung. In diesen Fällen gilt das Übereinkommen Nr. 108 des Europarates, das für die hier zu prüfende Frage grundsätzlich von der Annahme eines angemessenen Schutzniveaus ausgeht, auf jeden Fall für Justizbehörden.

Übermittlungen personenbezogener Daten an Drittländer und internationale Organisationen

Für Empfänger, die nicht der Richtlinie 95/46/EG unterworfen sind, sieht Artikel 9 Absatz 1 der Verordnung Folgendes vor: *„Personenbezogene Daten werden an Empfänger, die nicht Organe oder Einrichtungen der Gemeinschaft sind und die nicht den aufgrund der Richtlinie 95/46/EG erlassenen Rechtsvorschriften unterliegen, nur übermittelt, wenn ein angemessenes Schutzniveau in dem Land des Empfängers oder innerhalb der empfangenden internationalen Organisation gewährleistet ist und diese Übermittlung ausschließlich die Wahrnehmung von Aufgaben ermöglichen soll, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen“.* Grundsätzlich dürfen also keine Daten an Empfänger in nicht dem ERW angehörenden Ländern übermittelt werden, die kein angemessenes Schutzniveau gewährleisten. Artikel 9 Absatz 6 und 7 sehen jedoch Ausnahmen von dieser Regelung vor.

Den von dem für die Verarbeitung Verantwortlichen vorgelegten Unterlagen entnimmt der EDSB, dass zwischen dem Europäischen Rat und Drittländern und internationalen Organisationen Vereinbarungen über den Austausch von Verschlusssachen unterzeichnet wurden. Diese Vereinbarungen gelten auch für den EAD. Diese Vereinbarungen sehen lediglich Übermittlungen von Informationen aus EU-VS vor, die personenbezogene Daten enthalten können oder auch nicht. Für den Fall, dass die zu übermittelnden Informationen aus EU-VS personenbezogene Daten enthalten sollten, fordert der EDSB daher den EAD auf, Artikel 9 der Verordnung Genüge zu tun.

Artikel 9 sollte auch bei Übermittlungen an Drittländer und internationale Organisationen eingehalten werden, mit denen der EAD keine Vereinbarung über den Austausch von Verschlusssachen unterzeichnet hat.

Bezüglich der Anwendbarkeit von Artikel 9 Absatz 6 Buchstabe d bzw. e in solchen Fällen akzeptiert der EDSP vorläufig die vorgeschlagene Ausnahme, doch tut er dies unbeschadet seiner Schlussfolgerung der Prüfung dieser Frage in einem „Positionspapier über die Anwendung von Artikel 9 der Verordnung (EG) Nr. 45/2001: Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen“, das derzeit erarbeitet wird.

3.7. Recht auf Auskunft und Berichtigung

Als Recht auf Auskunft bezeichnet man das Recht der betroffenen Person, von dem für die Verarbeitung Verantwortlichen Auskunft über alle in dessen Besitz befindlichen sie betreffenden Daten zu erhalten. 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. Diese Informationen können der betroffenen Person direkt oder, unter gewissen Umständen, wie im vorliegenden Fall, dem EDSB erteilt werden.

Laut Datenschutzerklärung haben betroffene Personen das Recht, Auskunft über die im Besitz des EAD befindlichen sie betreffenden Informationen zu erhalten. Für die Ausübung dieses Rechts steht eine funktionale Mail-Box zur Verfügung. Die in der Datenschutzerklärung beschriebene Vorgehensweise steht generell im Einklang mit Artikel 13 der Verordnung (EG) Nr. 45/2001.

In der Datenschutzerklärung ist zwar nicht die Möglichkeit vorgesehen, in bestimmten Fällen die Auskunftserteilung/Berichtigung zum Schutz der Untersuchung aufzuschieben, doch wird diese Möglichkeit in der Meldung erwähnt, wo es heißt, dass bestimmte Daten unter die in Artikel 20 (insbesondere Absatz 1 Buchstabe a und c) der Verordnung (EG) Nr. 45/2001 aufgeführten Ausnahmen fallen können. Dies könnte beispielsweise immer dann der Fall sein, wenn nach Auffassung des EAD die Offenlegung von Informationen die Identität des internen Hinweisgebers oder Informanten enthüllen könnte. Vor einer Entscheidung über die Inanspruchnahme einer Ausnahme muss der EAD in jedem Einzelfall die Umstände der betreffenden Datenverarbeitung bewerten.

Das Recht auf Auskunft gilt ferner, wenn eine betroffene Person Einsicht in die Akten anderer Personen verlangt, die sie betreffende Informationen enthalten könnten. Dies gälte z. B. für interne Hinweisgeber, Informanten oder Zeugen, die Auskunft über die sie betreffenden Daten in einer Untersuchung gegen eine andere Person verlangen. Die Auskunft kann direkt der betroffenen Person erteilt werden (so genannte „Direktauskunft“), oder, unter bestimmten Umständen, einer Behörde (so genannte „indirekte Auskunft“), üblicherweise der Datenschutzbehörde, im vorliegenden Fall also dem EDSB.

Aufgrund der ihm in der Datenschutzerklärung und der Meldung vorliegenden Informationen ist der EDSB der Auffassung, dass der EAD, sollte er sich in Untersuchungen auf eine Ausnahme beziehen und die Unterrichtung aufschieben, berücksichtigen sollte, dass die Einschränkung eines Grundrechts nicht systematisch angewandt werden darf. Der EAD hat in jedem Einzelfall zu beurteilen, ob die Bedingungen für die Anwendung einer der in Artikel 20 Absatz 1 Buchstabe a oder c genannten Ausnahmen erfüllt sind. Gemäß Artikel 20 der Verordnung muss die Maßnahme außerdem „notwendig“ sein. Das heißt, dass für jeden Fall die „Erforderlichkeitsprüfung“ durchgeführt werden muss. Beruft sich der EAD auf eine Ausnahme, hat dies im Einklang mit Artikel 20 Absatz 3 zu geschehen, dem zufolge *„die betroffene Person gemäß dem Gemeinschaftsrecht über die wesentlichen Gründe für diese*

Einschränkung und darüber zu unterrichten ist, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden“. Der EAD kann sich jedoch auf Artikel 20 Absatz 5 berufen, um die Unterrichtung, wie in diesem Artikel geregelt, aufzuschieben: *„Die Unterrichtung nach den Absätzen 3 und 4 kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt“.*

In Anbetracht dessen und anders als in der Meldung des EAD ausgesagt, darf die Unterrichtung nur vorübergehend aufgeschoben werden. Der EAD darf die Auskunft über die Daten nicht endgültig „verweigern“. Das Wort „verweigern“ sollte daher aus der Datenschutzerklärung gestrichen werden.

Darüber hinaus ist angemessen zu berücksichtigen, dass die Verarbeitung personenbezogener Daten nach Treu und Glauben in einer Untersuchung und einem anschließenden Strafverfahren die Ausübung des Rechts auf Verteidigung impliziert. Um dieses Recht ausüben zu können, muss die betroffene Person normalerweise erfahren können, ob gegen sie ein Verfahren eingeleitet wurde. Ausnahmen müssen daher streng begrenzt und dürfen nur fallweise angewandt werden.

3.8. Informationspflicht gegenüber der betroffenen Person

Die Verordnung besagt, dass die betroffene Person darüber informiert werden muss, wo ihre personenbezogenen Daten erhoben werden, und sie enthält eine Reihe von Angaben, die in den Informationen enthalten sein müssen, damit eine Verarbeitung der personenbezogenen Daten nach Treu und Glauben gewährleistet ist. Im vorliegenden Fall können die Daten unmittelbar bei der betroffenen Person, aber auch mittelbar erhoben werden, beispielsweise mit Hilfe von Informanten.

Es ist zu berücksichtigen, dass alle in Artikel 11 Absatz 1 sowie Artikel 12 Absatz 1 aufgeführten Angaben einschließlich Buchstabe f gemacht werden müssen, da die betroffenen Personen in Anbetracht der Sensibilität der Fälle, um die es bei den hier zu prüfenden Verarbeitungen normalerweise geht, alle Garantien kennen müssen, auf die sie Anspruch haben.

Zur Beantwortung der Frage, ob der für die Verarbeitung Verantwortliche im vorliegenden Fall die betroffenen Personen unterrichtet, sind zwei Aspekte zu prüfen: Erstens inwieweit die Informationen tatsächlich gegeben werden, und zweitens, inwieweit die Informationen inhaltlich im Einklang mit der Verordnung (EG) Nr. 45/2001 stehen.

Kommunikationskanal: Laut Meldung werden die betroffenen Personen mit Hilfe der im Abschnitt „Sicherheit“ des Intranets des EAD eingestellten Datenschutzerklärung unterrichtet. Außerdem erhalten laut Meldung alle Personen einschließlich des Anzeigenden, die betroffenen Personen, Zeugen oder internen Hinweisgeber bei schriftlichen oder mündlichen Aussagen automatisch die Datenschutzerklärung in schriftlicher oder mündlicher Form. Das heißt, dass ohne Befragung oder schriftliche Aussage diese Personen die Datenschutzerklärung nicht erhalten¹⁰.

Nach Auffassung des EDSB ist die Veröffentlichung im Abschnitt „Sicherheit“ des Intranets des EAD ein erster Schritt zur Unterrichtung betroffener Personen. Im vorliegenden Fall kann dies jedoch nicht als ausreichend gelten. Der EDSB empfiehlt daher dem EAD, ein Verfahren

¹⁰ Die Meldung besagt, dass betroffene Personen, die nicht kontaktiert werden können, die Datenschutzerklärung beim ersten Kontakt nach der Erfassung erhalten.

zu entwickeln, mit dem die Datenschutzerklärung den betroffenen Personen zugeleitet wird, deren personenbezogene Daten erhoben werden.

Im Hinblick auf Informanten, Zeugen und interne Hinweisgeber empfiehlt der EDSB, sie unabhängig davon, ob sie befragt werden oder nicht, ebenfalls individuell zu unterrichten.

Der EDSB hält jedoch fest, dass der EAD in Fällen, in denen er telefonisch informiert wird, dieser Anruf aufgezeichnet werden soll, um die Echtheit des Berichts zu gewährleisten. Diese technische Möglichkeit besteht zum Zeitpunkt der Abfassung dieser Stellungnahme noch nicht, ist jedoch in der Meldung bereits vorgesehen. In derartigen Fällen sind die betroffenen Personen auch über die Aufzeichnung aufzuklären. Dieser Aspekt wird allerdings in den Informationen für den EDSB nicht erwähnt. Der EDSB fordert den EAD auf, die für eine ordnungsgemäße Information betroffener Personen, deren Anrufe aufgezeichnet werden können, erforderlichen Maßnahmen zu ergreifen.

Bezüglich der Anwendbarkeit von Artikel 20 der Verordnung, dem zufolge der EAD die Unterrichtung aufschieben kann, verweist der EDSB auf seine vorstehenden Kommentare im Zusammenhang mit dem Auskunftsrecht und auf die Tatsache, dass die Einschränkung eines Grundrechts nicht systematisch erfolgen darf. In einem solchen Fall muss der EAD fallweise die Umstände der betreffenden Datenverarbeitung prüfen.

Schließlich gilt: Beruft sich der EAD auf eine Ausnahme, hat dies im Einklang mit Artikel 20 Absatz 3 zu geschehen, dem zufolge *„die betroffene Person gemäß dem Gemeinschaftsrecht über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten ist, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden“*. Der EAD kann sich jedoch auf Artikel 20 Absatz 5 berufen, um die Unterrichtung, wie in diesem Artikel geregelt, aufzuschieben: *„Die Unterrichtung nach den Absätzen 3 und 4 kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt“* (gemäß Absatz 3 hat die betroffene Person das Recht, über die wesentlichen Gründe für eine Einschränkung und darüber unterrichtet zu werden, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden; gemäß Absatz 4 besteht für die betroffene Person das Recht auf indirekte Unterrichtung über den EDSB und auf Mitteilung der Ergebnisse seiner Anfrage).

Folglich kann sich der EDSB nicht der Auffassung des EAD anschließen, dass eine betroffene Person nicht unterrichtet werden muss, wenn am Ende der Untersuchung gegen den Verdächtigen keine Beweise vorliegen. Aus diesem Grund kann der EDSB auch nicht die Aussage des EAD hinnehmen, der zufolge *„es gerechtfertigt sein kann, die Person nicht darüber zu informieren, dass sie Verdächtiger war, da sich die Person vielleicht gar nicht der gegen sie laufenden Untersuchung bewusst war und die Untersuchung ohne Konsequenzen für die betreffende Person abgeschlossen worden ist“*.

Ein solches Verfahren ohne jegliche Information der betroffenen Person widerspräche der Verordnung (EG) Nr. 45/2001 und dem Recht auf Unterrichtung der betroffenen Personen über eine von dem Organ vorgenommene Verarbeitung personenbezogener Daten und könnte unter Umständen Beschwerden gegen das Organ zur Folge haben. Der EAD sollte daher diesen Aspekt seines Verfahrens unbedingt ändern.

Inhalt der Datenschutzerklärung: Die Meldung sagt zur Informationspflicht gegenüber der betroffenen Person und zu den Mitteln, mit denen diese Informationen gegeben werden, Folgendes aus: *„Die Existenz der Datenbanken und die Kontrolle der in ihnen enthaltenen Daten sowie gegebenenfalls deren Berichtigung, sofern sie unrichtig sind, ist Gegenstand*

einer in den Abschnitt „Sicherheit“ des Intranets des EAD eingestellten Erklärung“. Nach Auffassung des EDSB ist diese Formulierung mit Blick auf die Anforderungen von Artikel 11 und 12 unvollständig. Sie sollte daher entsprechend geändert 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 zur Identität des für die Verarbeitung Verantwortlichen, zu den Empfängern der Daten, zum Recht auf Auskunft und Berichtigung einschließlich des Namens der Kontaktperson, an die man sich wenden muss, um diese Rechte auszuüben. Erwähnt wird auch das Recht, sich an den Europäischen Datenschutzbeauftragten zu wenden. Nach Ansicht des EDSB sollten allerdings die Aufbewahrungsfristen um die Fristen für Berichte ergänzt werden, die weder zu einer wirksamen Maßnahme führen noch an nationale Strafverfolgungsbehörden übergeben werden. Er fordert daher den EAD auf, die Datenschutzerklärung diesbezüglich zu ergänzen (siehe weiter oben Punkt 3.5). Außerdem sollte nach seiner Auffassung der Zweck näher beschrieben werden. Derzeit heißt es nämlich in der Erklärung hierzu lediglich: „Die Verarbeitung dient der Durchführung von Sicherheitsuntersuchungen“.

3.9. Vertraulichkeit des Kommunikationsverkehrs

In Artikel 36 der Verordnung heißt es: *„Die Organe und Einrichtungen der Gemeinschaft gewährleisten unter Beachtung der allgemeinen Grundsätze des Gemeinschaftsrechts die Vertraulichkeit der Kommunikation über Telekommunikationsnetze und Endgeräte.“* Das Konzept der „allgemeinen Grundsätze des Gemeinschaftsrechts“ bezieht sich auf die grundlegenden Menschenrechte, die insbesondere in der Europäischen Menschenrechtskonvention verankert sind. Jede Einschränkung der Vertraulichkeit des Kommunikationsverkehrs muss also im Einklang mit Artikel 8 Absatz 2 dieses Instruments stehen: *„Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“.*

Diese Bestimmung ist bei der e-Überwachung, insbesondere bei der Prüfung von E-Mails einzuhalten. Der EAD verweist auf die Verwaltungsinformation Nr. 45/2006 der Kommission vom 15. September 2006, die auch beim EAD angewandt wird. Der Verweis auf die Verwaltungsinformation der Kommission gibt jedoch keinen Aufschluss darüber, ob der EAD selber die „Nachforschungen“ durchführen würde, oder ob, wie es in der Information heißt, diese Aufgabe auch vom Untersuchungs- und Disziplinaramt der Kommission (IDOC) übernommen würde. Auch der dem EDSB vorgelegte Entwurf des konsolidierten Beschlusses stellt nur klar, dass es die Direktion „Sicherheit“ des EAD ist, die Untersuchungen oder Überprüfungen vornimmt und etwaige sich aus den Untersuchungen ergebende Abhilfemaßnahmen durchführt¹¹.

¹¹ Artikel 9 des Beschlussentwurfs lautet:

1. Die Direktion „Sicherheit“ des EAD nimmt, gegebenenfalls mit Unterstützung durch Experten aus Mitgliedstaaten und/oder anderen EU-Organen, und bei Bedarf mit Genehmigung des Chief Operating Officer folgende Aufgaben wahr:

a) Gegebenenfalls Durchführung von Untersuchungen oder Überprüfungen:

i) wenn bekannt ist oder wenn berechtigter Grund zu der Annahme besteht, dass für den EAD relevante Verschlusssachen Unbefugten zur Kenntnis gelangt oder verloren gegangen sind;

Der EDSB fordert daher den EAD auf, ein eigenes Verfahren für eventuell durchzuführende e-Überwachung auszuarbeiten.

Unter Berücksichtigung der Anforderungen in Artikel 8 Absatz 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten müssen Einschränkungen des Grundsatzes der Vertraulichkeit auf jeden Fall anhand folgender Kriterien geprüft werden¹²:

- Ist die Einschränkung durch eine gesetzliche Bestimmung oder eine gleichwertige Maßnahme vorgesehen?
- Ist die Einschränkung notwendig? Könnte dasselbe Ergebnis ohne eine Verletzung des Vertraulichkeitsgrundsatzes erreicht werden? Nur unter außergewöhnlichen Umständen ist die Überwachung des persönlichen Gebrauchs von E-Mail (abgesehen vom Virenscreening) oder Telefon durch einen Mitarbeiter als notwendig anzusehen.
- Steht die Einschränkung im Verhältnis zu den zugrunde liegenden Bedenken? Der Grundsatz der Verhältnismäßigkeit beinhaltet, dass Einschränkungen der Vertraulichkeit des Kommunikationsverkehrs unterschiedlich angewendet werden, je nachdem, ob es sich um den persönlichen oder den geschäftlichen Kommunikationsverkehr handelt. Er beinhaltet ferner, dass, falls es notwendig sein sollte, die E-Mail-Konten von Mitarbeitern in deren Abwesenheit zu kontrollieren, dies sich grundlegend auf E-Mails beschränken sollte, die nicht als privat oder persönlich gekennzeichnet sind, bzw. auf E-Mails, die an das Organ gerichtet sind.

Im Bereich e-Überwachung verfasst der EDSB derzeit Leitlinien für die Verarbeitung des elektronischen Kommunikationsverkehrs durch Organe und Einrichtungen der EU.

3.9. 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.

[...]

II) bei tatsächlichen oder vermuteten Verletzungen der Sicherheitsvorschriften oder anderen Sicherheitszwischenfällen oder Bedrohungen der Sicherheitsinteressen des EAD;

b) gegebenenfalls Durchführung aller erforderlichen Abhilfemaßnahmen, die sich aus Untersuchungen ergeben.

2. Die Untersuchungsbeauftragten haben Zugang zu allen für die Durchführung solcher Untersuchungen erforderlichen Informationen und werden diesbezüglich von allen Dienststellen des EAD umfassend unterstützt.

Die Untersuchungsbeauftragten können zum Schutz der Beweismittel angemessene Maßnahmen einer Art ergreifen, die in einem angemessenen Verhältnis zur Schwere der zu untersuchenden Angelegenheit steht.

¹² Es sei darauf hingewiesen, dass die Frage der Überwachung oder Kontrolle des elektronischen Kommunikationsverkehrs (e-Überwachung) Gegenstand eigener horizontaler Leitlinien des EDSB sein wird.

Für den EDSB besteht kein Grund zu der Annahme, dass der EAD nicht angemessene technische und organisatorische Maßnahmen durchgeführt hat, die ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist, und die im Einklang mit den in anderen EU-Organen durchgeführten Maßnahmen stehen.

Schlussfolgerung:

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. Der EAD sollte insbesondere Folgendes beachten:

- Der EAD sollte im Entwurf eines Beschlusses der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst die Beschreibung des Anwendungsbereichs der Verordnung (EG) Nr. 45/2001 ändern, die sich derzeit in dessen Artikel 9 befindet;
- es ist zu gewährleisten, dass nur Daten, die für die Untersuchungszwecke erheblich sind, erhoben werden und in den schriftlichen Bericht eingehen. Besondere Aufmerksamkeit ist besonderen Datenkategorien zu widmen. Die für die Durchführung der Untersuchungen und das Abfassen der Berichte zuständigen Sicherheitsbeauftragten sollten hierauf hingewiesen werden;
- werden Daten innerhalb von Organen und Einrichtungen der EU, an nationale (Polizei- und Justiz-)Behörden sowie an Drittländer und internationale Organisationen übermittelt, sollten die Empfänger in einem Vermerk darauf hingewiesen werden, dass die Daten nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden;
- werden Daten übermittelt, sollte gewährleistet sein, dass die Übermittlung wirklich erforderlich ist. Diese Erforderlichkeit sollte in einer begründeten Stellungnahme bestätigt werden;
- der EAD sollte die Verfahren dokumentieren, die für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gelten, mit denen EU-VS-Vereinbarungen bestehen. Der EDSB behält sich eine Klarstellung seiner Haltung zu diesen Übermittlungen nach der Annahme seines Strategiepapiers über Übermittlungen vor;
- der EAD sollte Verfahren für die Information der verschiedenen Kategorien von betroffenen Personen annehmen, geeignete Maßnahmen bezüglich des Inhalts der Unterrichtung ergreifen und seine Meldung im Lichte der vorstehenden Kommentare ändern;
- die Datenschutzerklärung sollte in Anlehnung an die unter verschiedenen Punkten dieser Stellungnahme gemachten Anregungen geändert werden.
- [...]

Brüssel, den 1. Februar 2013

(unterzeichnet)

Giovanni BUTTARELLI