**Stellungnahme zu Meldungen des Datenschutzbeauftragten des Europäischen Amtes für Betrugsbekämpfung für eine Vorabkontrolle der Verarbeitungen „Virtual Operational Cooperation Unit“, „Mutual Assistance Broker“ und Zollinformationssystem**

Brüssel, den 17. Oktober 2011 (Verbundene Fälle 2010-0797, 2010-0798, 2010-0799)

## 1. Verfahren

Am 11. Oktober 2010 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) vom Datenschutzbeauftragten (**DSB**) des Europäischen Amtes für Betrugsbekämpfung (**OLAF**) drei Meldungen zur Vorabkontrolle der Verarbeitungen personenbezogener Daten im Rahmen des „Virtual Operational Cooperation Unit“ (Virtuelle Einheit für operative Zusammenarbeit) (**V-OCU**), des „Mutual Assistance Broker“ (Makler für gegenseitige Amtshilfe) (**MAB**) und des Zollinformationssystems (**ZIS**).

Den Meldungen waren folgende Unterlagen beigefügt:

- für V-OCU:
  - Handbuch für den V-OCU-Helpdesk
  - Datenschutzerklärung
  - Musterbildschirme für die verschiedenen Module (Consur, Marsur, Viasur)
- für MAB:
  - Datenschutzerklärung
  - Anhang I zu den Verfahren von MAR-/YAC-INFO
- für ZIS:
  - Datenschutzerklärung
- allen Meldungen war beigefügt:
  - AFIS Sicherheitskonzeptdokument (AFIS-SEC-POL)

Der EDSB stellte eine Reihe von Fragen, die vom OLAF am 20. Oktober 2010 beantwortet wurden. Eine zweite Fragenreihe wurde dem OLAF am 26. November 2010 übermittelt; die Antworten hierauf gingen am 26. Mai 2011 ein. Während dieser Zeit war die Frist für die Stellungnahme zur Vorabkontrolle ausgesetzt.

Den Antworten waren die folgenden zusätzlichen Unterlagen beigefügt.

- für V-OCU:
  - operativer Plan für JCO Sirocco
  - Virtual OCU Schulung Consur
  - Handbuch für den OCU-Helpdesk
  - Liste von Drittländern und internationalen Organisationen
- für ZIS:
  - Nutzerhandbuch für das Instrument für die Nutzerregistrierung
  - ZIS und V-OCU Qualitätsanforderungen
- zum AFIS Sicherheitskonzeptdokument (AFIS-SEC-POL):

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

- AFIS Terminalsicherheitsleitlinien
- AFIS „Operations Handling Procedure“ (Verfahrenshandbuch) (Anhang 1 des Hauptdokuments des AFIS Sicherheitskonzepts)
- AFIS UNIX „Security Baseline“ (Sicherheitskonzept)
- AFIS Windows „Security Baseline“ (Sicherheitskonzept)

Am 10. Juni 2011 lud der EDSB das OLAF zu einer Besprechung der offenen Fragen ein, auf die in den Antworten nicht eingegangen worden war. Diese Sitzung fand am 1. Juli 2011 statt. Bis dahin wurde der Fall erneut ausgesetzt. Im Nachgang zu der Sitzung legte das OLAF dem EDSB ein Exemplar des MAB „Case User Manual“ (Benutzerhandbuch) vor. In Anbetracht der Komplexität der zu prüfenden Fälle beschloss der EDSB am 1. Juli 2011, die Frist für die Vorlage seiner Stellungnahme um zwei Monate zu verlängern.

Der Entwurf der Stellungnahme wurde dem DSB am 27. September 2011 zur Kommentierung vorgelegt; seine Bemerkungen gingen beim EDSB am 10. Oktober 2011 ein.

## 2. Sachverhalt

### 2.1. Allgemeine Bemerkungen

Gegenstand dieser Stellungnahme sind drei Meldungen des DSB des OLAF für eine Vorabkontrolle, die alle die Zusammenarbeit bei der Bekämpfung von Betrug in den Bereichen Zoll und Landwirtschaft betreffen. Da diese Meldungen inhaltlich miteinander verbunden sind, beschloss der EDSB, sie in einer einzigen Stellungnahme zu behandeln.

Alle drei Anwendungen verfolgen auf das Engste miteinander verknüpfte Zwecke, unterliegen demselben Sicherheitskonzept und sind teilweise integriert, weshalb eine ganzheitliche Herangehensweise angebracht ist. Die Meldungen für V-OCU und MAB aktualisieren eine frühere Meldung zum Datenaustausch im Rahmen der Amtshilfe, während die Meldung zum ZIS eine frühere Meldung zum selben System auf den neuesten Stand bringt. Zu diesen älteren Meldungen hat der EDSB am 19. Oktober 2007 bzw. 24. Juli 2007 Stellungnahmen abgegeben (EDSB-Vorgangsnummern 2007-0202 bzw. 2007-0177). Die vorliegende Stellungnahme knüpft also an die oben genannten Stellungnahmen an und wird sich insbesondere mit den neuen Aspekten der gemeldeten Verarbeitung befassen. Zunächst soll auf die allen Meldungen gemeinsamen Punkte eingegangen werden, danach sollen Fragen in Zusammenhang mit den einzelnen Meldungen diskutiert werden. Bei Bedarf wird auf die früheren Stellungnahmen zur Vorabkontrolle und die darin formulierten Empfehlungen verwiesen.

*Beschreibung und Zweck der Verarbeitung*
Zwar bestehen zwischen den Anwendungen Unterschiede, doch verfolgen sie alle generell den Zweck der Intensivierung der Zusammenarbeit in Zollsachen zwischen Mitgliedstaaten und Kommission und heben auf die Verhinderung, Ermittlung und Verfolgung von Zuwiderhandlungen gegen die Zoll- und die Agrarregelung ab. Die Anwendungen ermöglichen den Austausch von Informationen zwischen den Mitgliedstaaten – sowohl in strukturierter als auch in unstrukturierter Form (als Freitext) – über Personen, die der Beteiligung an solchen Zuwiderhandlungen verdächtigt werden oder darin verwickelt sind, sowie über die Beamten, die in diesen Fällen ermitteln. Der Zugriff erfolgt in allen Fällen über das AFIS-Portal, eine Browseranwendung, die eine einheitliche Schnittstelle zu einer Reihe von Datenbanken und Anwendungen bietet. Unter bestimmten Umständen kann die

Behörde, die Daten in das System eingegeben hat, auch Übermittlungen an Drittländer genehmigen.

Jedes System besteht aus einer zentralen Datenbank, auf die die Kommission, eine Reihe zuständiger Behörden in den Mitgliedstaaten und in einigen Fällen bestimmte Drittländer, internationale Organisationen sowie Europol und Eurojust zugreifen können. Der Zugriff für Drittländer und internationale Organisationen[1] ist in Amthilfeabkommen mit entsprechenden Klauseln geregelt.[2] Europol und Eurojust kann im Rahmen ihrer Zuständigkeiten Zugriff gewährt werden, doch dürfen sie keine Daten hochladen. V-OCU unterscheidet sich von den anderen Systemen insofern, als nur ein zeitlich begrenzter Zugang für Behörden in den Ländern gewährt wird, die an einer im jeweiligen operativen GZA-Plan aufgeführten gemeinsamen Zollaktion (GZA) beteiligt sind. Die Verarbeitung erfolgt im Wesentlichen automatisch. Die Entscheidung über die Aufnahme oder den Ausschluss von Daten erfolgt jedoch manuell. Eine detailliertere Beschreibung folgt in den Abschnitten über die einzelnen Systeme.

*Rechtsgrundlagen*
Alle drei Anwendungen haben ihre Rechtsgrundlage zumindest teilweise in der Verordnung (EG) Nr. 515/97[3], zuletzt geändert durch die Verordnung (EG) Nr. 766/2008.[4] Das ZIS unterliegt besonderen Bestimmungen des Titels V (Artikel 23 bis 41) der genannten Verordnung, während die Rolle der Kommission (in diesem Fall des OLAF) bei MAB und V-OCU in Titel III (Artikel 17 und 18) festgelegt ist. Wie in Titel IV (Artikel 19 bis 22) der Verordnung (EG) Nr. 515/97 bestimmt, können die Anwendungen auch die Übermittlung personenbezogener Daten in Länder außerhalb der EU beinhalten. Der früher zum dritten Pfeiler gehörende Teil des ZIS unterliegt dem Beschluss 2009/917/JI des Rates[5] seit dessen Inkrafttreten am 27. Mai 2011. Das OLAF selber wurde mit der Verordnung (EG) Nr. 1073/99 errichtet.[6]

*Verantwortung für die Verarbeitung und Zuständigkeiten*
Die drei gemeldeten Anwendungen werden alle vom OLAF verwaltet; laut den Meldungen ist ein Beamter im Referat C.3 (Amtshilfe und Intelligence) des OLAF mit der Wahrnehmung der Aufgaben des für die Verarbeitung Verantwortlichen beauftragt. Die Anwendungen laufen auf Servern, die in den Räumlichkeiten des OLAF stehen und von OLAF verwaltet werden.

Daten werden von Behörden in den Mitgliedstaaten (und in einigen Fällen in Drittländern) eingegeben, geändert und verwendet. Nur die Behörde, die Daten eingegeben hat, kann sie auch ändern. Diese Behörden fungieren als für die Verarbeitung Mitverantwortliche. Auf dieses Thema wird in Abschnitt 3.4näher eingegangen.

*Nutzer und Nutzerverwaltung*
Die Nutzer aller drei Anwendungen werden mit Hilfe eines einheitlichen Instruments, des *User Registration Tool* (URT), verwaltet. Dem EDSB liegt ein Exemplar des Nutzerhandbuchs für dieses Instrument vor. Es gibt unterschiedliche Nutzerkategorien mit unterschiedlichen Rechten. Diese Kategorien sind: normale Nutzer, Verbindungsbeamte,

[1] Nach Angaben von OLAF kann die Weltzollorganisation (WZO) anonymisierte Daten von MAB zu Marinfo-, Ciginfo- und Yachtinfo-Fällen erhalten (S. 23, 28 des MAB-Nutzerhandbuchs); Teile der Informationen in MAB sind auch MarInfo-Mitgliedern zugänglich, von denen nicht alle EU-Mitgliedstaaten sind. Interpol nahm als Beobachter an mindestens einer GZA teil (S. 13 in Anhang 2 von Q12).
[2] Siehe das Verzeichnis unter http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html.
[3] ABl. L 82 vom 22.3.1997, S. 1.
[4] ABl. L 218 vom 13.8.2008, S. 48.
[5] ABl. L 323 vom 10.12.2009, S. 20.
[6] ABl. L 136 vom 31.5.1999, S. 1.

gesetzlicher Bevollmächtigter, IT-Helpdesk. Normale Nutzer erscheinen als institutionelle oder persönliche Konten. Diese Nutzer werden vom nationalen Verbindungsbeamten eingerichtet und verwaltet. Dieser Beamte kann Ersuchen für neue Nutzer und Organisationen stellen und ihre Vorrechte verwalten. Ersuchen, bei denen eine gesetzliche Genehmigung erforderlich ist, werden vom gesetzlich Bevollmächtigten – einem Beamten des OLAF - geprüft und validiert und vom IT-Helpdesk, ebenfalls einem OLAF-Mitarbeiter, umgesetzt. Ersuchen, bei denen keine gesetzliche Genehmigung erforderlich ist, werden auf Ersuchen des Verbindungsbeamten vom Helpdesk unmittelbar umgesetzt.

*Datenkategorien und betroffene Personen*
Laut Meldungen verarbeiten alle drei Systeme personenbezogene Daten von zwei verschiedenen Kategorien betroffener Personen:

Kategorie I: Personen, die in Fällen erwähnt werden, über die Daten gespeichert sind oder ausgetauscht werden.

Hierbei handelt es sich um Personen, die in den Meldungen erwähnt werden, die zwischen dem OLAF und Mitgliedstaaten oder Drittländern im Rahmen der gemeldeten Anwendungen ausgetauscht werden, sowie um Personen, über die Daten gespeichert sind. Gemeint sind insbesondere Personen, die an aufgedeckten oder geplanten Vorgängen beteiligt oder vermutlich beteiligt sind, die der Zoll- und der Agrarregelung zuwiderlaufen.

Kategorie II: Die diese Fälle bearbeitenden Beamten.

Bei V-OCU und MAB können dies Beamte aus Mitgliedstaaten oder Drittländern sein, die an den Fällen arbeiten, während beim ZIS nur Beamte von Mitgliedstaaten in Frage kommen. Für V-OCU und MAB können auch Beamte bestimmter internationaler Organisationen Zugriff haben, doch werden deren Bedienstete in den Meldungen nicht in dieser Kategorie aufgeführt.

In der ersten Kategorie variiert die Menge der verarbeiteten Daten je nach gemeldetem System, doch handelt es sich mindestens um Namen, Anschriften, Geburtsdatum und Geburtsort sowie Angaben zu Personaldokumenten. Erschöpfende Aufzählungen finden sich in den nachstehenden Unterabschnitten zu den einzelnen Systemen. In einigen Fällen enthalten diese auch Felder für Freitext oder Felder für Angaben zu Kennzeichen, in denen theoretisch auch Angaben gemacht werden können, die Rückschlüsse auf die rassische oder ethnische Herkunft, Religionszugehörigkeit, gesundheitsbezogene Daten oder andere besondere Arten von Daten zulassen. Die Handbücher für alle Systeme informieren die Nutzer über den für diese Art von Daten geltenden besonderen Schutz und klären sie darüber auf, dass derartige Daten in den Systemen nicht gespeichert werden dürfen.

Bezüglich der zweiten Kategorie betroffener Personen - Beamte, die die fraglichen Fälle bearbeiten – verwenden alle drei Systeme dieselbe Liste von Datenfeldern:

1) Familienname, Vorname
2) Dienststelle
3) Telefon, Mobiltelefon, Fax und E-Mail-Adresse[7].

[7] In der ZIS-Meldung ist an dieser Stelle von „Kontaktdaten“ die Rede. Inhaltlich dürfte hier kein Unterschied bestehen.

*Information und Rechte betroffener Personen*
Betroffene Personen der Kategorie I werden über die mögliche Erhebung ihrer personenbezogenen Daten durch Datenschutzhinweise aufgeklärt, die in den öffentlich zugänglichen Teil der Website des OLAF und des AFIS-Portals eingestellt werden.

Die Datenschutzhinweise der drei Systeme weisen große Ähnlichkeiten auf. Sie informieren mögliche betroffene Personen über die Zwecke und Rechtsgrundlagen der Verarbeitung sowie über Stellen, an die die Daten weitergegeben werden können und über Aufbewahrungsfristen. In den Hinweisen für V-OCU und MAB wird erwähnt, dass Daten unter bestimmten Voraussetzungen auch an Drittländer und internationale Organisationen übermittelt werden können. Lediglich der Hinweis für das ZIS enthält eine Aufzählung der Datenfelder, die möglicherweise verarbeitet werden. Das in den Hinweisen erwähnte Recht auf Auskunft, Berichtigung und Löschung gilt für alle drei Anwendungen gleichermaßen. Betroffene Personen können eine Kopie der über sie gespeicherten Daten anfordern, indem sie sich an den für die Verarbeitung Verantwortlichen wenden, dessen Name und Kontaktdaten angegeben sind, und sie können die Berichtigung sachlich nicht korrekter Daten verlangen.

Betroffene Personen werden darüber in Kenntnis gesetzt, dass die in Artikel 20 der Verordnung (EG) Nr. 45/2001 aufgeführten Einschränkungen zum Tragen kommen können. In den Hinweisen für V-OCU und MAB heißt es zusätzlich, dass bei Daten, die von einem Mitgliedstaat bereitgestellt wurden, diesem Mitgliedstaat die Möglichkeit eingeräumt wird, seine Haltung zu dem Ersuchen geltend zu machen, bevor Auskunft erteilt wird. Diese beiden Hinweise besagen ferner, dass bei der Verwendung von Daten in umfassenden Übermittlungen zwischen Einrichtungen zur Aufdeckung von Tendenzen und ungewöhnlicher Aktivität kein individueller Hinweis auf ihre Verwendung erfolgt.

Die Frist für die Sperrung/Löschung von Daten auf begründeten Antrag beträgt in allen drei Datenbanken einen Monat. In allen drei Datenschutzhinweisen werden betroffene Personen über ihr Recht aufgeklärt, sich an den EDSB zu wenden.

Beim OLAF bestehen Verfahren, in denen personenbezogene Daten bereitgestellt werden, die über das hinausgehen, was in den Datenschutzhinweisen für betroffene Personen genannt wird.[8] Derartige Daten werden nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen des operativen Partners bereitgestellt, der die Daten in das betreffende System eingegeben hat. Darüber hinaus können Ausnahmen nach Artikel 20 der Verordnung (EG) Nr. 45/2001 gelten. In den geltenden Leitlinien wird darauf hingewiesen, dass diese Ausnahmen nur fallweise Anwendung finden können.

Bei betroffenen Personen der Kategorie II fordert das OLAF die jeweiligen Behörden in den Mitgliedstaaten auf, ihm die entsprechenden Daten zu liefern. Betroffene Personen der Kategorie II, die Bedienstete des OLAF sind, können ferner die „Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen“ einsehen, die vom Generaldirektor des OLAF im Oktober 2010 angenommen wurden.

*Datenaufbewahrung*
Das OLAF wendet auf alle drei Systeme dieselben Grundverfahren für die Datenaufbewahrung an. Den Meldungen ist zu entnehmen, dass personenbezogene Daten in den Systemen für höchstens zehn Jahre aufbewahrt werden dürfen. Schon in seiner Stellungnahme vom 19. Oktober 2007, in der es um die Vorgängersysteme von V-OCU und

[8] Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen, Oktober 2010, Titel 1.5. Anhang 5 des OLAF-Handbuchs, öffentlich zugänglich unter http://ec.europa.eu/dgs/olaf/legal/manual/annexes/Guidelines-October2010.pdf.

MAB ging, sowie in einigen Fragen vom 26. November 2010 hatte der EDSB das OLAF aufgefordert, diesen Aufbewahrungszeitraum zu begründen.

In seinen Antworten führte das OLAF aus, Fälle seien im Jahrestakt daraufhin zu prüfen, ob eine Fortsetzung der Aufbewahrung erforderlich ist oder nicht. Nach elf Monaten werden die Nutzer über die anstehende Prüfung der Daten informiert. Falls innerhalb des Prüfzeitraums (ein Monat) keine weitere Aufbewahrung der Daten beschlossen wird, werden die Daten gelöscht. Nach Angaben des OLAF können solche positiven Entscheidungen nur in ZIS-Fällen getroffen werden. Das OLAF teilte dem EDSB ferner mit, es gäbe keine zusätzlichen Leitlinien für die Beamten heraus, die diese Entscheidung treffen.

Die Zugangsprotokolle („Access Logs“) zu Systemen, die über das AFIS-Portal zugänglich sind, werden für 15 Jahre aufbewahrt. Es besteht ein Verfahren, nach dem den zuständigen Behörden in den Mitgliedstaaten zu Auditzwecken Zugang zu diesen Logs gewährt werden kann. Der DSB von Eurojust hat um einen monatlichen Auszug aus den AFIS-Logs ersucht; diesem Ersuchen wurde stattgegeben. Es wird ein Verfahren eingeführt, das dem EDSB gemeldet wird. Der EDSB hat von OLAF erfahren, dass der DSB von Europol ein ähnliches Ersuchen eingereicht hat.

*Sicherheitsaspekte*

[...]

Bisher ging es um die wichtigsten Aspekte, die allen drei Anwendungen gemeinsam sind. Eine detailliertere Darstellung der Merkmale der einzelnen Systeme folgt in den spezifischen Bemerkungen.

## 2.2. Spezifische Bemerkungen

### 2.2.1. V-OCU

V-OCU ist ein Instrument für den Austausch von Informationen über unbestätigte Verdachtsfälle und Anträge anderer zuständiger Behörden auf Tätigwerden. Dem EDSB war schon früher eine ältere Version von V-OCU gemeldet worden, zu der er am 19. Oktober 2007 eine Stellungnahme mit einer Reihe von Empfehlungen abgab (Fall 2007-0202).

*Beschreibung der Verarbeitung*
V-OCU ist eine über das AFIS-Portal zugängliche Browseranwendung, mit der für Mitgliedstaaten, aber auch für Drittländer und internationale Organisationen, mit denen die EU Amtshilfeabkommen mit entsprechenden Klauseln abgeschlossen hat, Daten über Bewegungen und Kontrollen von Waren und Personen erhoben und geprüft werden. Diese Daten betreffen unbestätigte Verdachtsfälle, die von Beamten in Mitgliedstaaten und denjenigen Drittländern oder internationalen Organisationen eingegeben werden können, die an einer bestimmten gemeinsamen Zollaktion (GZA) und ähnlichen kurzfristigen Einsätzen teilnehmen. GZA sind koordinierte Einsätze, die von Behörden in Mitgliedstaaten und möglicherweise Drittländern durchgeführt werden. Für jede GZA besteht eine eigene Zugriffsmöglichkeit auf Daten im V-OCU, die nur den Ländern gewährt wird, die an der betreffenden GZA beteiligt sind. Als Beispiel wurde dem EDSB der Entwurf des Einsatzplans für eine bereits durchgeführte GZA vorgelegt.

Die Datenverarbeitung beginnt mit der Eingabe von Daten (Bewegungsaufzeichnungen) in das System durch die zuständigen Behörden von Mitgliedstaaten und anderen Behörden mit Zugriff auf das V-OCU. Diese Bewegungsaufzeichnungen enthalten Angaben zu verdächtigen Bewegungen (gestützt auf eine Reihe von Indikatoren wie bekannte Versender/Empfänger, unstimmige Dokumente usw.) von Waren und können auch personenbezogene Daten beispielsweise von Lkw-Fahrern enthalten. Mit diesen Einträgen können auch bestimmte Maßnahmen beantragt werden, z. B. Kontrollen und Durchleuchtungen von Sendungen. Andere Parteien können Freitextkommentare zu Einträgen abgeben, etwa „Diese Person ist im Zusammenhang mit der Fälschung von Markenwaren bekannt“, oder sie können Kontrollergebnisse eingeben. Diese Daten werden in einer zentralen Datenbank gespeichert[9] und sind anderen Parteien in einem befristeten Zeitfenster während des Lebenszyklus konkreter GZA zugänglich. Dieser Lebenszyklus lässt sich üblicherweise in drei Phasen unterteilen: „vor dem Einsatz“ (Auswahl von Zielen, die besonders beobachtet werden sollen), „Einsatz“ (Durchführung von Kontrollen) und „nach dem Einsatz“ (Follow-up).

Je nach Art des Eintrags sehen die Bildschirme – „Module“ genannt – verschieden aus; sie enthalten Informationen zur betreffenden Ladung oder zur betreffenden Feststellung sowie die Anmerkungen anderer Parteien. Folgende Module sind zu unterscheiden:

- **Viasur** befasst sich mit der Sammlung von *Intelligence* zum Straßenverkehr;
- **Consur** erfüllt die gleiche Funktion beim Container-Seeverkehr;
- **Marsur** dient demselben Zweck beim nichtgewerblichen Seeverkehr.

Das OLAF hat dem EDSB Bildschirmfotos dieser Module vorgelegt. Der Informationsaustausch erfolgt in Form strukturierter Nachrichten in der Mailing-Anwendung des AFIS-Systems, d. h. MAB-mail (siehe nachstehenden Abschnitt 2.2.2 zu MAB). Darüber hinaus enthält V-OCU eine Nachrichtenanwendung für den Austausch von Freitextnachrichten zwischen Teilnehmern.

*Rechtsgrundlage*
In der Meldung wird nur allgemein die Verordnung (EG) Nr. 515/97 als Rechtsgrundlage genannt. Im Einzelnen gilt: Die Mitwirkung der Kommission fußt auf Artikel III dieser Verordnung (Artikel 17 und 18). Der Zugang für Drittländer ist in Titel IV der Verordnung und in den bestehenden Amtshilfeabkommen geregelt. V-OCU soll Ersuchen um „sorgfältige Überwachung“ nach Artikel 7 der Verordnung (EG) Nr. 515/97 erleichtern.

*Datenkategorien*
Die Auflistung personenbezogener Daten von betroffenen Personen der Kategorie I (siehe Abschnitt 2.1 „Allgemeine Bemerkungen“), die in V-OCU gespeichert werden, enthält folgende Angaben:

1) Familienname, Vorname
2) Geburtsdatum und Geburtsort
3) Staatsangehörigkeit
4) Personaldokument
5) Daten zur Verwicklung in den Fall (Freitext)

[9] Hier liegt der Hauptunterschied zu den sogenannten herkömmlichen Austauschformaten, bei denen keine zentrale Datenspeicherung stattfand.

Das OLAF bestätigte, dass Daten über Familienangehörige von Verdächtigen nur in das Freitextfeld für Daten zur Verwicklung in den Fall eingetragen werden, wenn sie für den betreffenden Fall erheblich sind; Geburtsnamen von Frauen können aus demselben Grund dort eingetragen werden. Dies war in den Empfehlungen der früheren Stellungnahme zur Vorabkontrolle gefordert worden. Die Nutzer von V-OCU werden vor Anlaufen einer GZA sowohl schriftlich als auch in Schulungen (E-Learning oder praktische Schulung) über die anzuwendenden Grundsätze der Datenqualität aufgeklärt.

*Datenempfänger*
Als potenzielle Empfänger werden in der Meldung benannte Beamte der zuständigen Behörden bei der Kommission und in den Mitgliedstaaten genannt, die für die Anwendung der Verordnung (EG) Nr. 515/97 zuständig sind. Im Datenschutzhinweis ist die Rede von benannten Beamten in den *„zuständigen Verwaltungs-, Gesetzgebungs- und Justizbehörden der Mitgliedstaaten, in Organen, Einrichtungen, Ämtern und Agenturen der EU, in internationalen Organisationen und/oder Verwaltungsbehörden in Drittländern*". Sowohl die Meldung als auch der Datenschutzhinweis erwähnen, dass Daten an Behörden in Drittländern übermittelt werden können, sofern zwischen der Union und diesen Ländern Amtshilfeabkommen bestehen.[10] Internationale Organisationen als Empfänger werden zwar in der Beschreibung der Verarbeitung in der Meldung erwähnt, nicht jedoch in dem Empfängerfeld. Auf die technischen Aspekte der Nutzerverwaltung wurde bereits im vorstehenden allgemeinen Abschnitt eingegangen.

Laut dem der Meldung beigefügten Datenschutzhinweis *„werden die Daten mittels eines IT-Tools analysiert und können vom OLAF zu Intelligence-Zwecken verwendet werden (siehe Meldungen DPO-88: Information und Intelligence-Datenpool und DPO-89: Intelligence-Datenbanken)"*. Diese Meldungen waren Anlass für die gemeinsame Stellungnahme zur Vorabkontrolle vom 21. November 2007.

*Rechte der betroffenen Person*
Eine Aufstellung der Rechte der betroffenen Person findet sich in dem Abschnitt über das Datenschutzkonzept in den allgemeinen Bemerkungen. In seinen Antworten vom 26. Mai 2011 unterstrich das OLAF, dass Auskunftsersuchen während der Dauer der GZA (normalerweise 10-14 Tage) wahrscheinlich abgelehnt werden.

### 2.2.2. MAB

MAB ist ein Fallverwaltungssystem für den Informationsaustausch zwischen einer Reihe von Datenbanken im Bereich Zoll. Eine frühere Version von MAB wurde dem EDSB bereits gemeldet. Eine Stellungnahme zur Vorabkontrolle dieses Systems mit einer Reihe von Anregungen, die OLAF umsetzen sollte, um der Verordnung (EG) Nr. 45/2001 zu entsprechen, wurde am 19. Oktober 2007 abgegeben (Fall 2007-0202).

*Rechtsgrundlage*
Die die Mitwirkung der Kommission betreffende Rechtgrundlage ist dieselbe wie für V-OCU, nämlich Titel III der Verordnung (EG) Nr. 515/97.

*Beschreibung der Verarbeitung*
MAB bietet eine gemeinsame Schnittstelle für fünf Informationsaustauschsysteme: Yachtinfo, Marinfo, Ciginfo, MAB Mail und ZIS.

[10] Siehe http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html.

- **Yachtinfo** enthält Informationen über nichtgewerbliche Schiffe und deren bestätigte Beschlagnahmen. [...].
- **Marinfo** enthält Informationen über Schiffe im Container-Seeverkehr und deren bestätigte Beschlagnahmen. [...].
- **Ciginfo** enthält Informationen über Zigaretten und Tabakwaren sowie nachgeahmte Waren und deren bestätigte Beschlagnahmen.
- **ZIS** hilft den teilnehmenden Zollbehörden bei der Zusammenarbeit durch den Austausch von Informationen über (vermutete) Zuwiderhandlungen gegen die Zoll- und die Agrarregelung. Eine nähere Beschreibung folgt weiter unten, da das System für sich Gegenstand einer der drei Meldungen ist.
- **MAB Mail** ermöglicht den Versand unstrukturierter Nachrichten (Freitext) an andere Teilnehmer des Systems. Es handelt sich um dasselbe System wie das frühere AFIS-Mail. Wie bereits erwähnt, wird es auch für den Austausch von Nachrichten bei V-OCU verwendet.

Die vier erstgenannten Subsysteme werden für die Anlage von Fällen und den Austausch strukturierter Information genutzt[11]; mit dem letztgenannten können zwischen Teilnehmern Freitextnachrichten ausgetauscht werden.

Bei der Anlage eines Falls können die Beamten zwischen zahlreichen Fallarten wählen und beispielsweise einen Marinfo-Fall mit einem Ciginfo-Fall kombinieren. Die in der Anlagephase des Falls eingegebenen Daten werden dann automatisch in alle Fälle übertragen, sofern gemeinsame Datenfelder vorhanden sind.[12] Nach ihrer Anlage sind die Fälle jedoch voneinander völlig unabhängig und es findet auch kein Datenaustausch zwischen ihnen statt. Die Daten sind zentral beim OLAF gespeichert.

*Datenkategorien*
In den strukturierten Teil von MAB (die drei ersten der vorstehend genannten Subsysteme; auf ZIS wird unter Punkt 2.2.3 eingegangen) können folgende Datenfelder aufgenommen werden:

1) Name, Vorname, Geburtsname, angenommene Namen, Geschlecht
2) Kennzeichen
3) Geburtsort und Geburtsdatum
4) Staatsangehörigkeit
5) Beruf
6) Warnhinweis zu etwaigen früheren Erfahrungen wie Bewaffnung, Gewalttätigkeit, Drogenabhängigkeit, Selbstmordgefährdung u. ä. (aus einer Liste auszuwählen sowie Freitexteingabe)
7) Personaldokument (Art, Nummer, Datum und Ort der Ausstellung)
8) Anschrift (Postfach, Straße, Hausnummer, Briefkasten, PLZ, Stadt, Land)
9) Beschreibung der Verwicklung (aus einer Liste auszuwählen sowie Freitexteingabe, einschließlich einer Bewertung der Qualität der Information)
10) vorgeschlagene Vorgehensweise.

In das Feld mit Warnungen können auch Angaben zum Drogenkonsum und zu Selbstmordneigungen eingetragen werden, die in der früheren Meldung zum Informationsaustausch im Rahmen der Amtshilfe (EDSB Fall 2007-0202) noch nicht genannt

[11] Dieser Austausch erfolgt in Form strukturierter Nachrichten in der AFIS-Mailing-Anwendung (d. h. MAB Mail).
[12] So könnten beispielsweise die in einem Container auf einem Seeschiff geschmuggelten Zigaretten in ZIS, MarInfo und CigInfo eingegeben werden, während das Konossement nur in MarInfo gespeichert würde.

wurden. In das Feld „Merkmale“ könnten grundsätzlich auch Daten eingegeben werden, die Rückschlüsse auf rassische oder ethnische Herkunft, Religionszugehörigkeit oder Gesundheit zulassen.

MAB Mail wiederum ist eine Nachrichtenanwendung, mit der die Nutzer unstrukturierte Nachrichten (also Freitextnachrichten) austauschen können. Vor der Gewährung des Zugangs werden die Nutzer in Schulungen angewiesen, in diese Freitextnachrichten und die anderen Felder keine sensiblen Daten einzugeben.

*Datenempfänger*
Als potenzielle Empfänger werden in der Meldung benannte Beamte der zuständigen Behörden bei der Kommission und in den Mitgliedstaaten genannt, die für die Anwendung der Verordnung (EG) Nr. 515/97 zuständig sind. Im Datenschutzhinweis ist die Rede von benannten Beamten in den „*zuständigen Verwaltungs-, Gesetzgebungs- und Justizbehörden der Mitgliedstaaten, in Organen, Einrichtungen, Ämtern und Agenturen der EU, in internationalen Organisationen und/oder Verwaltungsbehörden in Drittländern*“. Außerdem können Daten mit den Mitgliedern der MarInfo- bzw. YachtInfo-Gruppe ausgetauscht werden, von denen nicht alle EU-Mitgliedstaaten sind. Daten können ferner auch an Behörden in anderen Drittländern übermittelt werden, sofern zwischen der Union und diesen Drittländern Amtshilfeabkommen bestehen. Informationen aus Yachtinfo-, MarInfo- und CigInfo-Fällen können auch an die Weltzollorganisation (WZO) weitergegeben werden; in diesem Fall wird jedoch nur eine anonymisierte Teilmenge der Informationen[13] versandt. Internationale Organisationen werden hingegen als Empfänger personenbezogener Daten in der Meldung nicht erwähnt.

Laut dem der Meldung beigefügten Datenschutzhinweis können die Daten auch zu *Intelligence*-Zwecken verwendet werden. Am 21. November 2007 veröffentlichte der EDSB eine gemeinsame Stellungnahme zur Vorabkontrolle von zwei Meldungen über Verarbeitungen zu *Intelligence*-Zwecken („*Information and intelligence data pool*“ und „*Intelligence databases*“) (EDSB Fälle 2007-0027 und 2007-0028).

*Rechte der betroffenen Person*[14]
Es sei darauf hingewiesen, dass der Datenschutzhinweis für MAB keine Auflistung der zu speichernden Datenelemente enthält. Bezüglich der Nutzung des ZIS im Anwendungsbereich von MAB wird im Datenschutzhinweis auf das ZIS in der Form verwiesen, die in DPO-17, also der alten Fassung der Meldung, gemeldet worden war, und nicht wie sie in der aktualisierten Fassung DPO-17-2 gemeldet wurde, die Gegenstand dieser Vorabkontrolle ist.

### 2.2.3. ZIS

Eine ältere Version dieses Systems war bereits Gegenstand einer Stellungnahme zur Vorabkontrolle vom 24. Juli 2007 (EDSB Fall 2007-0177). Da seine Rechtsgrundlage jedoch in der Zwischenzeit durch die Verordnung (EG) Nr. 766/2008 geändert worden ist und sich die Verarbeitung personenbezogener Daten innerhalb des Systems geändert hat, ist eine neue Stellungnahme zur Vorabkontrolle durchaus angebracht.

*Beschreibung der Verarbeitung*
Zweck des ZIS ist es, die zuständigen nationalen Behörden und die Kommission („ZIS-Partner“) bei der Verhinderung, Ermittlung und Verfolgung von Vorgängen zu unterstützen, die der Zoll- und der Agrarregelung zuwiderlaufen. Zu diesem Zweck gibt es den ZIS-

[13] Siehe MAB Benutzerhandbuch, S. 23.
[14] Siehe die Diskussion über Datenschutzhinweise in den allgemeinen Bemerkungen.

Partnern die Möglichkeit, Warnmeldungen in das System einzustellen, mit denen andere ZIS-Partner um bestimmte Maßnahmen ersucht werden. Im Einzelnen handelt es sich dabei um Feststellung und Unterrichtung, verdeckte Registrierung, gezielte Kontrolle und operative Analyse. Diese Warnmeldungen können sich auf Waren, Transportmittel, Unternehmen und Personen beziehen. Für die Nutzer ist kein Unterschied zwischen dem ZIS nach der Verordnung (EG) Nr. 515/97 bzw. nach dem Beschluss 2009/917/JI des Rates erkennbar.

*Rechtsgrundlage*
Grundlage des ZIS sind Titel V der Verordnung (EG) Nr. 515/97 und der ZIS-Beschluss des Rates (2009/917/JI), der am 27. Mai 2011 das ZIS-Übereinkommen ersetzte. Artikel 23 Absatz 2 der Verordnung (EG) Nr. 515/97 besagt: *„Zweck des ZIS ist es, (…) die Verhinderung, Ermittlung und Bekämpfung von Handlungen, die der Zoll- oder der Agrarregelung zuwiderlaufen, zu unterstützen und hierfür durch eine raschere Verbreitung von Informationen die Effizienz von Kooperations- und Kontrollmaßnahmen der zuständigen Behörden im Sinne dieser Verordnung zu steigern“*. Artikel 25 Absatz 2 enthält eine erschöpfende Aufzählung von Datenkategorien, die aufgenommen werden dürfen, und die, wie nachstehend aufgeführt, der in der Datenbank entspricht. Die Beziehungen zu Drittländern sind in Titel IV (Artikel 19 bis 22) dieser Verordnung geregelt. Der ZIS-Beschluss des Rates enthält entsprechende Bestimmungen.

Formal betrachtet besteht das ZIS aus zwei getrennten Teilen: einem Teil, der mit der Verordnung (EG) Nr. 515/97 eingerichtet wurde („ZIS EU“), und einem Teil, der auf dem Beschluss 2009/917/JI des Rates fußt („ZIS MS“). Der Unterschied liegt in den Waren, mit denen sie sich befassen: Thema des ZIS nach dem Ratsbeschluss sind Drogen, Waffen und einige andere Kategorien wie Geldwäsche und gestohlene Fahrzeuge, während alle anderen Kategorien zum ZIS nach der Verordnung (EG) Nr. 515/97 gehören. Die bereits erwähnte frühere Stellungnahme des EDSB zur Vorabkontrolle befasste sich lediglich mit dem ZIS nach der Verordnung (EG) Nr. 515/97.

*Datenkategorien*
Daten können von den benannten Behörden der Mitgliedstaaten eingegeben werden. Wegen der verschiedenen Rechtsgrundlagen gibt es je nach Art der betroffenen Waren zwei Arten von Fällen, nämlich „ZIS EU“ und „ZIS MS“. Bei Fällen, in denen es um Waren, Transportmittel, Unternehmen und Personen geht, können die folgenden Datenfelder aufgenommen werden:

1) Name, Geburtsname, Vornamen, frühere Familiennamen und angenommene Namen
2) Geburtsdatum und Geburtsort
3) Staatsangehörigkeit
4) Geschlecht
5) Anzahl der Personalpapiere (Pässe, Personalausweise, Führerscheine) sowie Ort und Datum ihrer Ausstellung
6) Anschrift
7) besondere objektive und ständige Kennzeichen
8) Warncode mit Hinweis auf frühere Erfahrungen hinsichtlich Bewaffnung, Gewalttätigkeit oder Fluchtgefahr
9) Grund für die Aufnahme von Daten
10) vorgeschlagene Maßnahmen
11) amtliches Kennzeichen des Transportmittels

In Fällen, in denen es um vorläufig oder endgültig beschlagnahmte Barmittel oder Waren geht, werden nur die Punkte 1 bis 4 sowie 6 der obigen Liste aufgenommen. In Fällen schließlich, in denen Sachverständige hinzugezogen werden, werden nur die Namen und Vornamen dieser Experten gespeichert.

Sobald eine ersuchte Maßnahme durchgeführt worden ist, kann der ZIS-Partner, der die Kontrolle vorgenommen oder eine andere Maßnahme durchgeführt hat, dies dem ersuchenden ZIS-Partner mitteilen.

*Nutzer und Nutzerverwaltung*
Wie schon im allgemeinen Teil erwähnt, erfolgt die Nutzerverwaltung über URT. Beim ZIS besteht nach Artikel 29 Absatz 2 der Verordnung (EG) Nr. 515/97 zusätzlich die Verpflichtung, das Verzeichnis der zuständigen Behörden, die Zugang zum ZIS haben, im Amtsblatt der Europäischen Union zu veröffentlichen. Das OLAF teilte dem EDSB mit, das Verzeichnis werde derzeit überarbeitet. Dieses Verzeichnis hat nichts mit dem über URT aufgestellten zu tun; für die Zukunft hat das OLAF angekündigt, das Verzeichnis regelmäßig zu aktualisieren und zu veröffentlichen.

*Datenempfänger und Datenübermittlungen*
Laut Meldung haben Zugang nur Beamte der Europäischen Kommission und der für die Anwendung der Verordnung (EG) Nr. 515/97 zuständigen Behörden in den Mitgliedstaaten. Davon erhalten direkten Zugang nur Beamte mit einer Nutzerkennung und einem Passwort. Mit vorheriger Einwilligung des ZIS-Partners, der die Daten hochgeladen hat, und vorbehaltlich seiner Bedingungen können Informationen auch an andere Behörden der Mitgliedstaaten übermittelt werden. OLAF lädt keine eigenen Daten in das System hoch und ist daher nicht in der Lage, solche Übermittlungen zu genehmigen. Sowohl in der Meldung als auch im Datenschutzhinweis heißt es, dass die Übermittlung von im ZIS gespeicherten personenbezogenen Daten an Drittländer möglich ist, doch bekräftigte OLAF in seinen Antworten an den EDSB vom 26. Mai 2011, es übermittle Daten weder an Drittländer oder andere Organe, Einrichtungen oder Agenturen der EU noch an Mitgliedstaaten; wie bereits erwähnt, können nach Genehmigung durch den Mitgliedstaat, der Daten hochgeladen hat, Datenübermittlungen an Drittländer vorkommen.

*Rechte der betroffenen Person*[15]
Im Gegensatz zum MAB-Datenschutzhinweis enthält dieser Hinweis eine Liste von Datenkategorien. Anders als in der Liste in der Meldung werden hier Informationen über Personaldokumente und Anschriften nicht erwähnt.

## 3. Rechtliche Prüfung

### 3.1. Allgemeine Bemerkungen

In der folgenden Analyse werden Aspekte, die alle drei Meldungen gleichermaßen betreffen, gemeinsam abgehandelt. Dabei handelt es sich im Wesentlichen um die Anwendbarkeit der Verordnung (EG) Nr. 45/2001[16] („Verordnung"), die Frage der Verantwortung („controllership"), das Recht auf Auskunft und Berichtigung sowie die Sicherheitsmaßnahmen. Die Aspekte, die sich in den Meldungen unterscheiden, werden jeweils für sich abgehandelt.

[15] Siehe die Diskussion im Teil „Allgemeine Bemerkungen".
[16] ABl. L 8 vom 18.12.2000, S. 1.

### 3.2. Vorabkontrolle

#### 3.2.1. Anwendbarkeit der Verordnung

Artikel 3 Absatz 1 der Verordnung besagt, dass diese „*auf die Verarbeitung personenbezogener Daten durch alle Organe und Einrichtungen der Gemeinschaft Anwendung [findet], soweit die Verarbeitung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen.*" In Artikel 2 Buchstabe a der Verordnung werden personenbezogene Daten definiert als „*alle Informationen über eine bestimmte oder eine bestimmbare natürliche Person*". Laut Artikel 3 Absatz 2 gilt die Verordnung „*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 Verarbeitung von Daten in den drei Anwendungen stellt eine Verarbeitung personenbezogener Daten dar. Die Datenverarbeitung erfolgt durch eine Einrichtung der EU, und zwar im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen (Artikel 3 Absatz 1 der Verordnung, gelesen im Licht des Vertrags von Lissabon). Die Verarbeitung der Daten erfolgt zumindest teilweise automatisch. Dies gilt für alle drei gemeldeten Systeme. Somit ist die Verordnung anzuwenden.

#### 3.2.2. Begründung der Vorabkontrolle

In Artikel 27 Absatz 1 der Verordnung ist festgelegt, dass alle „*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. Diese Liste umfasst unter anderem Verarbeitungen „*von Daten, die Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen*" (Artikel 27 Absatz 2 Buchstabe a). Solche Daten können bei allen drei gemeldeten Anwendungen verarbeitet werden. Wie OLAF in den Meldungen ausführte, dienen diese Verarbeitungen auch dazu, „*die Persönlichkeit der betroffenen Person zu bewerten*" (Artikel 27 Absatz 2 Buchstabe b). Daten über die Verwicklung in einen Fall dienen der Bewertung des Verhaltens betroffener Personen dahingehend, ob sie Zuwiderhandlungen gegen die Zoll- und die Agrarregelung begangen haben. Die Anwendungen sind daher einer Vorabkontrolle durch den EDSB zu unterziehen.

Da die Vorabkontrolle dazu dient, sich mit Situationen zu befassen, die gewisse Risiken beinhalten können, gibt der EDSB seine Stellungnahme idealerweise vor Aufnahme der Verarbeitungen ab. Im vorliegenden Fall wurden die Verarbeitungen jedoch bereits eingeleitet. Dies stellt jedoch kein schwerwiegendes Problem dar, da alle Empfehlungen des EDSB auch jetzt noch übernommen werden können.

#### 3.2.3. Verfahren

Die Meldung des DSB ging am 11. Oktober 2010 ein. Nach Artikel 27 Absatz 4 der Verordnung muss der EDSB seine Stellungnahme innerhalb von zwei Monaten abgeben. Insgesamt wurde die Frist für die Abgabe der Stellungnahme um 215 Tage ausgesetzt, in denen Antworten auf Ersuchen um weitere Auskünfte erwartet, eine Sitzung abgehalten und Anmerkungen zum endgültigen Entwurf der Stellungnahme abgegeben wurden. Aufgrund der Komplexität der Fälle wurde die Frist um zwei Monate verlängert. Darüber hinaus wurden die Fälle im August 2011 ausgesetzt. Unter Berücksichtigung dieser Aussetzungen und der

Verlängerung hätte die Stellungnahme am 15. Oktober 2011 abgegeben werden müssen; da dieses Datum auf einen Samstag fällt, legt der EDSB seine Stellungnahme am 17. Oktober 2011 vor.

### 3.3. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dafür rechtliche Gründe nach Artikel 5 der Verordnung vorliegen. In den zu prüfenden Fällen ist Artikel 5 Buchstabe a anzuwenden. Danach ist eine Verarbeitung rechtmäßig, die *„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 [...]“*. Diese Bestimmung enthält drei Bedingungen, die alle erfüllt sein müssen: 1) Die Verarbeitung muss sich auf einen Rechtsakt stützen (entweder die Verträge oder andere Rechtakte), 2) sie muss im öffentlichen Interesse ausgeführt werden und muss 3) für die Wahrung dieses öffentlichen Interesses erforderlich sein.

Alle drei Anwendungen stützen sich zumindest teilweise auf die Verordnung (EG) Nr. 515/97. Für V-OCU und MAB ist sie die einzige Rechtsgrundlage, während es für das ZIS eigene Bestimmungen in dieser Verordnung, aber auch im Beschluss 2009/917/JI des Rates gibt. Die Rechtsgrundlage von V-OCU und MAB kann daher zusammen diskutiert werden.

#### 3.3.1. V-OCU und MAB

Rechtsgrundlage dieser beiden Anwendungen ist die Verordnung (EG) Nr. 515/97. Artikel 17 und 18 dieser Verordnung bilden die Grundlage für die Mitwirkung der Kommission an dem Datenaustausch und besagen, dass die zuständigen Behörden in den Mitgliedstaaten der Kommission zweckdienliche Informationen übermitteln.

Nach Artikel 17 übermitteln die zuständigen Behörden der Mitgliedstaaten der Kommission alle ihnen zweckdienlich erscheinenden Informationen über die Waren, die Gegenstand von Vorgängen waren oder vermutlich waren, die der Zoll- oder der Agrarregelung zuwiderlaufen, die Ersuchen um Amtshilfe, die ergriffenen Maßnahmen und die aufgrund der Artikel 4 bis 16 der Verordnung (EG) Nr. 515/97 ausgetauschten Informationen (Amtshilfe ohne Antrag und Amtshilfe auf Antrag).[17] Die Kommission wiederum übermittelt alle Informationen, die geeignet sind, die Einhaltung der Zoll- und der Agrarregelung durch die zuständigen Behörden der Mitgliedstaaten zu gewährleisten, sobald sie ihr zur Verfügung stehen.[18]

Nach Artikel 18 Absatz 1 sind die Mitgliedstaaten verpflichtet, der Kommission über Handlungen, die der Zoll- und der Agrarregelung zuwiderlaufen oder zuwiderzulaufen

[17] Artikel 17 Absatz 1 der Verordnung (EG) Nr. 515/97 lautet: *„Die zuständigen Behörden der einzelnen Mitgliedstaaten übermitteln der Kommission, sobald sie vorliegen,*
*a) alle ihnen zweckdienlich erscheinenden Informationen über*
*- die Waren, die Gegenstand von Vorgängen waren oder vermutlich waren, die der Zoll- oder der Agrarregelung zuwiderlaufen; [...]*
*- die Ersuchen um Amtshilfe, die getroffenen Maßnahmen und die aufgrund der Artikel 4 bis 16 ausgetauschten Informationen, die Tendenzen bei den Betrugspraktiken im Zoll- oder im Agrarbereich sichtbar machen könnten; [...]“.*

[18] Artikel 17 Absatz 2 der Verordnung (EG) Nr. 515/97 lautet: *„Die Kommission übermittelt den zuständigen Behörden der einzelnen Mitgliedstaaten alle Informationen, die geeignet sind, die Einhaltung der Zoll- und der Agrarregelung durch diese Behörden zu gewährleisten, sobald sie ihr zur Verfügung stehen“*.

scheinen, Auskunft zu erteilen, und ist die Kommission verpflichtet, diese Auskünfte den zuständigen Behörden aller Mitgliedstaaten mitzuteilen.[19]

Artikel 7 der Verordnung (EG) Nr. 515/97 legt fest, dass zuständige Behörden in den Mitgliedstaaten auf Antrag Bewegungen von Personen oder Beförderungsmitteln *„besonders sorgfältig überwachen“*, bei denen begründeter Anlass zu der Annahme besteht, dass sie zu Vorgängen benutzt werden, die der Zoll- oder der Agrarregelung zuwiderlaufen.[20] V-OCU dient der Umsetzung dieses Artikels.

Die Beziehungen zu Drittländern sind in Artikel 19 der Verordnung sowie in den zwischen der Union und Drittländern bestehenden Amtshilfeabkommen geregelt. Mögliche Übermittlungen an Drittländer erfolgen direkt durch die Mitgliedstaaten, die personenbezogene Daten aufgenommen haben, und den Drittländern; OLAF ist hieran nicht beteiligt.

### 3.3.2. ZIS

Das ZIS unterscheidet sich von den anderen gemeldeten Verarbeitungen insofern, als es in der Verordnung (EG) Nr. 515/97 eine eigene, explizite Rechtsgrundlage hat. Sein Zweck ist in Artikel 23 Absatz 2 beschrieben, der folgendermaßen lautet:

> „Zweck des ZIS ist es, nach Maßgabe dieser Verordnung die Verhinderung, Ermittlung und Verfolgung von Handlungen, die der Zoll- oder der Agrarregelung zuwiderlaufen, durch eine rasche Bereitstellung von Informationen zu unterstützen und dadurch die Effizienz von Kooperations- und Kontrollmaßnahmen der zuständigen Behörden im Sinne dieser Verordnung zu steigern“.

Zum Erreichen dieses Ziels umfasst das ZIS laut Artikel 24 *„ausschließlich die für den Zweck des ZIS nach Artikel 23 Absatz 2 erforderlichen Daten, einschließlich personenbezogener Daten*“ einer Reihe von Kategorien, die in Artikel 25 im Einzelnen aufgeführt werden.

Der zweite Teil der Rechtsgrundlage des ZIS findet sich im Beschluss 2009/97/JI des Rates und hier in Artikel 1 Absatz 2, der folgendermaßen lautet:

> „Zweck des Zollinformationssystems ist es, nach Maßgabe dieses Beschlusses die Verhinderung, Ermittlung und Verfolgung schwerer Zuwiderhandlungen gegen einzelstaatliche Rechtsvorschriften zu unterstützen, indem die Daten schneller zur Verfügung gestellt werden und auf diese Weise die Effizienz der Kooperations- und Kontrollverfahren der Zollverwaltungen der Mitgliedstaaten gesteigert wird“.

---

[19] Artikel 18 Absatz 1 der Verordnung (EG) Nr. 515/97 lautet: *„Wenn von den zuständigen Behörden eines Mitgliedstaats festgestellte Handlungen, die der Zoll- und der Agrarregelung zuwiderlaufen oder zuwiderzulaufen scheinen, von besonderem Interesse auf Gemeinschaftsebene sind, insbesondere - wenn sie sich auf andere Mitgliedstaaten erstrecken oder erstrecken könnten oder - wenn die genannten Behörden der Ansicht sind, dass ähnliche Handlungen auch in anderen Mitgliedstaaten erfolgt sein könnten, erteilen diese Behörden der Kommission [...] so rasch wie möglich alle zweckdienlichen Auskünfte [...]. Die Kommission teilt diese Auskünfte den zuständigen Behörden der anderen Mitgliedstaaten mit“*.

[20] *„Besonders sorgfältige Überwachung*“ kann auch für Bewegungen von Waren und für Warenlager beantragt werden; in diesen Fällen reicht es aus, wenn *„zu ihnen mitgeteilt wird, dass sie Vorgängen dienen können, die der Zoll- und der Agrarregelung zuwiderlaufen*“ oder wenn *„Warenlager unter Umständen eingerichtet werden, die begründeten Anlass zu der Annahme geben*“, dass sie Vorgängen dienen, die der Zoll- und der Agrarregelung zuwiderlaufen.

Artikel 4 Absatz 2 dieses Beschlusses bietet eine erschöpfende Liste von Kategorien personenbezogener Daten, die in das ZIS aufgenommen werden können.

### 3.3.3. Öffentliches Interesse und Notwendigkeit

Damit eine Verarbeitung gemäß Artikel 5 Buchstabe a rechtmäßig ist, muss sie im öffentlichen Interesse ausgeführt werden. Ziel der drei dem EDSB gemeldeten Anwendungen ist die Intensivierung der Zusammenarbeit zwischen Kommission, Behörden der Mitgliedstaaten und in einigen Fällen auch Behörden von Drittländern bei der Verhinderung, Ermittlung und Verfolgung von Zuwiderhandlungen gegen die Zoll- und die Agrarregelung. Die Gewährleistung einer wirksamen Anwendung der Zoll- und der Agrarregelung schützt die finanziellen Interessen der Kommission und der Mitgliedstaaten und liegt auch im öffentlichen Interesse. Die Verarbeitungen sollten daher als im öffentlichen Interesse liegend angesehen werden.

Abstrakt betrachtet hilft ein solcher Datenaustausch beim Schutz der finanziellen Interessen der Kommission und der Mitgliedstaaten. Ohne diesen Austausch wäre die Durchsetzung der Rechtsvorschriften in den Bereichen Zoll und Landwirtschaft ernsthaft erschwert. Die Erfüllung von Anträgen auf „*besonders sorgfältige Überwachung*“ wäre bei Bewegungen, die sich auf mehrere Länder erstrecken, vermutlich nicht effizient. In diesem Sinne können also V-OCU, MAB und ZIS als für die Betrugsbekämpfung erforderliche Instrumente gelten. Ob nun die Aufnahme von Daten in diese Systeme in einem bestimmten Fall erforderlich ist oder nicht, kann abstrakt nicht beurteilt werden. Hier ist die Notwendigkeit also konkret in jedem Einzelfall nachzuweisen.

## 3.4. Verantwortlichkeit

In Artikel 2 Buchstabe d der Verordnung ist der „*für die Verarbeitung Verantwortliche*“ folgendermaßen definiert: „*das Organ oder die Einrichtung der Gemeinschaft, die Generaldirektion, das Referat oder jede andere Verwaltungseinheit, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet*“. Als für die Verarbeitung Verantwortlicher gilt derjenige, der diese Aufgabe tatsächlich wahrnimmt.

In der Meldung wird lediglich ein Beamter des OLAF als für die Verarbeitung Verantwortlicher bezeichnet. Aus der Beschreibung der Verarbeitungsvorgänge geht jedoch hervor, dass neben dem OLAF auch die zuständigen Behörden in den Mitgliedstaaten als für die Verarbeitung Verantwortliche gelten sollten.

Die Systeme sind so angelegt, dass einige der Aufgaben eines für die Verarbeitung Verantwortlichen nicht vom OLAF, sondern nur von den zuständigen Behörden in den Mitgliedstaaten wahrgenommen werden können. So hat beispielsweise nach Artikel 4 Absatz 2 der Verordnung der für die Verarbeitung Verantwortliche für die Einhaltung des Grundsatzes der Datenqualität zu sorgen. OLAF kann hierzu einen Beitrag leisten, indem es das System so gestaltet, dass keine eindeutig unerheblichen Daten verarbeitet werden können und indem es über die ordnungsgemäße Nutzung des Systems aufklärt, doch sind es die zuständigen Behörden in den Mitgliedstaaten, die letztendlich Daten hochladen und ändern, die darüber entscheiden, ob die Speicherfrist bei ZIS-Fällen verlängert wird[21], sowie im

[21] Siehe nachstehenden Abschnitt 3.7.1.

konkreten Fall bestimmen, welche Daten hochgeladen werden sollen. Und da sie auch als einzige von ihnen hochgeladene Daten ändern dürfen, haben sie das Recht auf Berichtigung zu gewährleisten, das gemäß Artikel 14 bei dem für die Verarbeitung Verantwortlichen liegt. Sie und nicht das OLAF genehmigen Übermittlungen in Drittländer, sofern diese möglich sind.[22]. Dies alles zeigt, dass sie nicht nur als reine Nutzer des Systems betrachtet werden dürfen, da sich ihre Entscheidungen erheblich auf die Zwecke der Verarbeitung auswirken.

Für das ZIS wird dieses Konzept in Artikel 34 Absatz 3 der Verordnung (EG) Nr. 515/97 bekräftigt, demzufolge die Mitgliedstaaten und die Kommission *„das ZIS als ein System zur Verarbeitung personenbezogener Daten, das den nationalen Bestimmungen zur Umsetzung der Richtlinie 95/46/EG, den Bestimmungen der Verordnung (EG) Nr. 45/2001 und allen strengeren Bestimmungen der vorliegenden Verordnung unterliegt*" betrachten. Wäre das OLAF allein der für die Verarbeitung Verantwortliche, wäre der Verweis auf die nationalen Bestimmungen zur Umsetzung der Richtlinie 95/46/EG überflüssig. Dementsprechend spricht die Verordnung (EG) Nr. 515/97 von den zuständigen Behörden und der Kommission als „ZIS-Partnern".

Diesbezüglich entsprechen V-OCU, MAB und ZIS anderen IT-Großsystemen wie Eurodac oder dem Informationssystem für den Binnenmarkt, bei denen die Kommission für die Einrichtung und die operative Verwaltung zuständig ist, nicht jedoch für den Inhalt der in das System hochgeladenen Daten. Das OLAF ist die Partei, die das System aufbaut und der Genehmigung in der Rechtsgrundlage konkrete Form verleiht. In diesem Sinne bestimmt es (teilweise) Mittel und Zwecke der Verarbeitung. Die zuständigen Behörden wiederum sind mehr als nur Nutzer des Systems und entscheiden teilweise über den Zweck der Verarbeitung. Es ist also durchaus angebracht, die an die Systeme angeschlossenen zuständigen Behörden und OLAF als gemeinsam für die Verarbeitung Verantwortliche zu bezeichnen. Dies hat natürlich auch Auswirkungen auf die Zuständigkeiten, wobei jeder einzelne für die Verarbeitung Verantwortliche für seine eigenen Verarbeitungen verantwortlich ist. OLAF ist für die Verwaltung des Zentralsystems, einschließlich dessen Sicherheit, verantwortlich. Die zuständigen Behörden in den Mitgliedstaaten sind für das Hochladen und die Änderung von Daten sowie für ihre eigene Nutzung der Systeme verantwortlich.

### 3.5. Verarbeitung besonderer Datenkategorien

Gemäß Artikel 10 Absatz 1 der Verordnung ist die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von Daten über Gesundheit oder Sexualleben generell untersagt, es sei denn, es ist eine der in Artikel 10 Absatz 2 bis 5 aufgeführten Ausnahmen gegeben. Artikel 10 Absatz 2 enthält Ausnahmen für alle besonderen Kategorien; Artikel 10 Absatz 3 sieht eine Ausnahme für die Verarbeitung von Gesundheitsdaten zu medizinischen Zwecken durch ärztliches Personal oder durch sonstige Personen vor, die einer entsprechenden Geheimhaltungspflicht unterliegen; nach Artikel 10 Absatz 4 können vorbehaltlich angemessener Garantien aus Gründen eines „*wichtigen öffentlichen Interesses*" durch die Verträge oder andere auf der Grundlage dieser Verträge erlassenen Rechtsakte oder durch eine Entscheidung des EDSB andere Ausnahmen vorgesehen werden. Gemäß Artikel 10 Absatz 5 darf die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, nur gestützt auf eine besondere Rechtsgrundlage oder nach Genehmigung durch den EDSB erfolgen.

[22] Siehe nachstehenden Abschnitt 3.8.3.

Bei allen drei gemeldeten Verarbeitungen sind besondere Kategorien von Daten betroffen; die jeweiligen Kategorien und der genaue Umfang der Verarbeitung fallen allerdings je nach Anwendung unterschiedlich aus. Auf sie wird noch im Einzelnen eingegangen.

### 3.5.1. V-OCU

V-OCU kann für den Austausch von Informationen über vermutete Zuwiderhandlungen gegen die Agrar- und die Zollregelung verwendet werden, d. h., es werden Daten über (mutmaßliche) Straftaten ausgetauscht. Die Verarbeitung solcher besonderen Daten durch OLAF ist nach Artikel 1 Absatz 2 der Verordnung (EG) Nr. 1073/99 und den entsprechenden Bestimmungen der Verordnung (EG) Nr. 515/97 zulässig; somit wird den Bestimmungen von Artikel 10 Absatz 5 der Verordnung Genüge getan.

### 3.5.2. MAB

Im Zusammenhang mit MAB können mehrere besondere Datenkategorien verarbeitet werden. Nach Auskunft von OLAF können in die Felder für Warnhinweise nun auch Angaben zum Drogenkonsum und zu Selbstmordneigungen eingetragen werden, also gesundheitsbezogene Daten. In der früheren Meldung über den Datenaustausch im Rahmen der Amtshilfe waren diese Elemente nicht erwähnt (EDSB Fall 2007-0202). Aus dem MAB *Case User Manual* geht hervor, dass neben diesen Warnhinweisen, die aus einer Liste ausgewählt werden können, noch ein Freitextfeld für weitere Warnhinweise zur Verfügung steht. Außerdem könnten in das Feld „Kennzeichen“ grundsätzlich auch Daten eingegeben werden, die Rückschlüsse auf rassische oder ethnische Herkunft, Religionszugehörigkeit oder Gesundheit zulassen. Schließlich kann das Feld mit Angaben zur Verwicklung in den Fall durchaus auch Daten zu Verdächtigungen enthalten.

Aufgrund der vorliegenden Informationen besteht kein Grund zu der Annahme, dass auf die neuen Warnhinweise in der Auswahlliste eine der Ausnahmen nach Artikel 10 der Verordnung Anwendung findet. Die in Artikel 10 Absatz 2 der Verordnung genannten Ausnahmen dürften ebenfalls nicht gelten. Auch die Ausnahme in Artikel 10 Absatz 3 greift nicht. Nach dieser Ausnahme ist die Verarbeitung von Gesundheitsdaten zum Zweck der Gesundheitsvorsorge und Behandlung und zu bestimmten anderen medizinischen Zwecken durch ärztliches Personal oder sonstige Personen möglich, die einer entsprechenden Geheimhaltungspflicht unterliegen. Selbst wenn die Geheimhaltungspflicht der Beamten von OLAF und Mitgliedstaaten als der der Angehörigen der Gesundheitsberufe entsprechend angesehen würde, hätte dies noch nicht die Anwendbarkeit der Ausnahme auf die Verarbeitung durch OLAF zur Folge, da seine Beamten mit der Gesundheitsvorsorge nicht das Geringste zu tun hätten. Artikel 10 Absatz 4 lässt vorbehaltlich angemessener Garantien weitere, durch die Verträge oder andere auf der Grundlage dieser Verträge erlassene Rechtsakte vorgesehene oder vom EDSB genehmigte Ausnahmen zu, falls ein wichtiges öffentliches Interesse besteht. Anders als die Warnungen vor Gewalttätigkeit, Bewaffnung oder Fluchtgefahr werden die neuen Felder für Warnhinweise in der Rechtsgrundlage nicht erwähnt. Daher gilt hier auch nicht die in den Verträgen oder in auf deren Grundlage erlassenen Rechtsakten vorgesehene weitere Ausnahme bei der Verarbeitung gemäß Artikel 10 Absatz 4 der Verordnung. Laut MAB *Case User Manual* gibt es ferner ein Freitextfeld für weitere Warnhinweise, in das möglicherweise besondere Datenkategorien eingetragen werden könnten.

Bezüglich des Felds „Kennzeichen“ erhalten die Nutzer dieses Systems eine Schulung, in der sie darüber aufgeklärt werden, dass Daten, die einen Rückschluss auf den rassischen oder ethnischen Hintergrund oder andere besondere Datenkategorien zulassen, dort nicht eingetragen werden dürfen.[23] Den Nutzern des gemeldeten Systems stehen auch Unterlagen mit diesen Informationen zur Verfügung. Damit soll sichergestellt werden, dass keine unter Artikel 10 Absatz 1 fallenden Daten verarbeitet werden. In Anbetracht der vielfältigen Datenfelder, die in MAB eingegeben werden können (siehe Abschnitt 2.2.2), ist nicht klar, ob dieses zusätzliche Datenfeld für die Identifizierung von Personen tatsächlich erforderlich ist. In Anbetracht der Risiken, die das Feld mit sich bringt (also Fehlinterpretation dessen, was gesundheitsbezogene Daten sind, oder einfache Nichtbefolgung von Weisungen), empfiehlt der EDSB dem OLAF eine Bewertung der Notwendigkeit dieses Feldes. Hierzu sollte OLAF Statistiken über die Nutzung dieses Feldes erheben und den EDSB innerhalb von sechs Monaten von den Ergebnissen in Kenntnis setzen.

Die Verarbeitung besonderer Daten - wie der Daten über die Verwicklung in einen Fall - durch OLAF ist nach Artikel 1 Absatz 2 der Verordnung (EG) Nr. 1073/99 und den entsprechenden Bestimmungen der Verordnung (EG) Nr. 515/97 zulässig; somit wird den Bestimmungen von Artikel 10 Absatz 5 der Verordnung Genüge getan.

OLAF sollte in Erwägung ziehen, die Felder „Drogensucht“ und „Selbstmordneigung“ aus der Liste der Warnhinweise zu streichen. Es sollte ferner die Aufnahme des Freitextfeldes für Warnhinweise begründen und dessen Entfernung in Erwägung ziehen, sollten die vorformulierten Warnhinweise als ausreichend erachtet werden.

### 3.5.3. ZIS

Die Liste der in Artikel 25 Absatz 2 der Verordnung (EG) Nr. 515/97 aufgeführten Daten, die in das ZIS aufgenommen werden können, enthält unter g) „*besondere objektive und ständige Kennzeichen*“. In Absatz 5 dieses Artikels heißt es: „*In keinem Fall dürfen personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über die Gesundheit oder das Sexualleben aufgenommen werden*“. OLAF erläuterte hierzu, dass die Nutzer in Schulungen auf diese Einschränkungen hingewiesen werden, bevor sie Zugang zum System erhalten. Diese Einschränkungen werden auch in den Nutzern zugänglichen Unterlagen wiederholt. Damit soll sichergestellt werden, dass keine unter Artikel 10 Absatz 1 der Verordnung fallenden Daten in diesem Feld verarbeitet werden. In Anbetracht der vielfältigen Datenfelder, die in das ZIS eingegeben werden können (siehe Abschnitt 2.2.3), ist nicht klar, ob dieses zusätzliche Datenfeld für die Identifizierung von betroffenen Personen tatsächlich erforderlich ist. In Anbetracht der Risiken, die das Feld mit sich bringt (also Fehlinterpretation dessen, was gesundheitsbezogene Daten sind, oder einfache Nichtbefolgung von Weisungen), empfiehlt der EDSB dem OLAF eine Bewertung der Notwendigkeit dieses Feldes. Hierzu sollte OLAF Statistiken über die Nutzung dieses Feldes erheben und den EDSB innerhalb von sechs Monaten von den Ergebnissen in Kenntnis setzen.

Buchstabe i) der Liste in Artikel 25 Absatz 2 lautet: „*Grund für die Aufnahme der Daten*“. Diese Bestimmung bietet eine explizite Rechtsgrundlage für die Verarbeitung von Daten über Verdächtigungen, womit die Ausnahme nach Artikel 10 Absatz 5 der Verordnung gilt.

[23] Siehe auch die Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen, S. 8f.

Artikel 4 Absatz 2 Buchstaben g und h und Artikel 4 Absatz 5 des Beschlusses 2009/917/JI des Rates enthalten ähnliche Bestimmungen und bilden eine Rechtsgrundlage für die Verarbeitung von Daten über Verdächtigungen in dem auf der Grundlage dieses Beschlusses eingerichteten Teils des ZIS.

### 3.6. Datenqualität

Artikel 4 Absatz 1 der Verordnung enthält den Grundsatz der Datenqualität. Genauer heißt es in Artikel 4 Absatz 1 Buchstabe c: Personenbezogene Daten dürfen nur „*den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen*". Außerdem müssen Daten, wenn nötig, auf den neuesten Stand gebracht werden (Artikel 4 Absatz 1 Buchstabe d).

#### 3.6.1. V-OCU und MAB

Der Grundsatz der Datenqualität wird bei V-OCU und MAB insofern eingehalten, als i) die Liste der Datenkategorien dem Erreichen der jeweiligen Zwecke angemessen sein dürfte, ii) in den internen Leitlinien von OLAF gefordert wird, dass Daten zu Personen nur aufgenommen werden dürfen, wenn diese „*im Verdacht stehen, von der Unregelmäßigkeit oder dem Betrug betroffen zu sein*" (Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen, S. 7), und iii) in denselben Leitlinien von OLAF-Bediensteten verlangt wird, „*alle sinnvollen Schritt zu unternehmen [...], um sicherzustellen, dass die von einzelstaatlichen Behörden stammenden und von OLAF verwendeten und gespeicherten Daten sowie die von OLAF erhobenen Daten, die an die einzelstaatlichen Behörden weitergegeben werden, sachlich richtig und auf dem neuesten Stand sind*" (S. 7), indem beispielsweise aktualisierte Daten rasch übermittelt werden. Für Beamte von Mitgliedstaaten, die Daten hinzufügen, hält OLAF Material mit den gleichen Informationen bereit.

Der EDSB kann also nicht ohne konkreten Fall beurteilen, ob diese Datenkategorien in allen Einzelfällen aufgenommen werden sollten. Die Entscheidung über die Aufnahme einzelner Datenkategorien muss fallweise getroffen werden. Für die Fallbearbeiter hat OLAF Hilfestellung bei der Erfüllung dieser Anforderungen herausgegeben, auch zur Aktualisierung von Daten (Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen, Titel 1.3).

Der EDSB stellt fest, dass die Anweisungen in den Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen den Empfehlungen zur Datenqualität in den bereits zitierten früheren Stellungnahmen zur Vorabkontrolle entsprechen.

#### 3.6.2. ZIS

Die Meldung enthält eine Liste von Datenkategorien, die in das ZIS aufgenommen werden dürfen (Feld 17). Sie ist mit der Liste in Artikel 25 Absatz 2 der Verordnung (EG) Nr. 515/97 deckungsgleich.

Der Grundsatz der Datenqualität wird beim ZIS insofern eingehalten, als i) die Liste der Datenkategorien dem Erreichen der jeweiligen Zwecke angemessen sein dürfte, ii) Daten nur dann aufgenommen werden dürfen, „*wenn es - insbesondere aufgrund früherer illegaler Handlungen oder aufgrund von Informationen im Rahmen der gegenseitigen Amtshilfe - tatsächliche Anhaltspunkte dafür gibt, dass die betreffende Person Handlungen begangen hat,*

*begeht oder begehen wird, die der Zoll- oder der Agrarregelung zuwiderlaufen und die von besonderem Interesse auf Gemeinschaftsebene sind*" (Artikel 27 Absatz 2 der Verordnung (EG) Nr. 515/97) und iii) den ZIS-Nutzern dieselben Informationen über die Datenaktualisierung wie den Nutzern von V-OCU und MAB zur Verfügung gestellt werden.

Wie bei V-OCU und MAB kann der EDSB also auch hier nicht ohne konkreten Fall beurteilen, ob diese Datenkategorien in allen Einzelfällen aufgenommen werden sollten. Auch hier muss fallweise entschieden werden. Die bereits genannten Leitlinien gelten auch für das ZIS.

### 3.7. Datenaufbewahrung

In Artikel 4 Absatz 1 Buchstabe e der Verordnung heißt es, dass personenbezogene Daten „*so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht"*. In der Verordnung (EG) Nr. 515/97 sind Aufbewahrungsfristen nur für das ZIS festgelegt. OLAF teilte dem EDSB mit, dass in der Praxis die für ZIS festgelegten Verfahren auch für die anderen gemeldeten Anwendungen gelten. Aus diesem Grund steht am Anfang dieses Abschnittes die Diskussion über ZIS; die anderen Systeme werden danach abgehandelt. In seinen am 26. Mai 2011 eingegangenen Antworten kündigte OLAF an, dem EDSB künftig eine weitere Meldung einer Verarbeitung personenbezogener Daten im Zusammenhang mit den AFIS Logs zu übermitteln.

#### 3.7.1. ZIS

Rechtlich ist in Artikel 33 der Verordnung (EG) Nr. 515/97 festgelegt, dass in das ZIS eingegebene Daten nur so lange zu speichern sind, wie es zur Erfüllung des Zwecks, zu dem sie eingegeben wurden, notwendig ist. Die die Daten eingebenden Partner haben mindestens einmal pro Jahr zu überprüfen, ob die Daten noch benötigt werden. Erfolgt keine Antwort des Daten eingebenden Partners innerhalb des Überprüfungszeitraums für das ZIS, werden die Daten in einen Teil des ZIS mit begrenztem Zugang sowohl im Hinblick auf die Zugangsberechtigten als auch auf die Verwendungszwecke der Daten (Artikel 33 Absatz 4) übertragen. Der Zugang wird auf die Vertreter des Ausschusses, der die Kommission unterstützt (Artikel 43), und zwar bei der Prüfung der Maßnahmen zur Sicherung des Systems, des Erfordernisses der Speicherung der Daten oder der Vertraulichkeit der gespeicherten Informationen (Artikel 43 Absatz 4 Spiegelstriche 7, 8 und 9), sowie auf die von den Mitgliedstaaten benannten Aufsichtsbehörden (Artikel 37) beschränkt. Die in diesem Teil des ZIS gespeicherten Daten dürfen nur zum Zweck der Überprüfung ihrer Richtigkeit und der Rechtmäßigkeit der Verarbeitung abgefragt werden und müssen nach einem Jahr gelöscht werden (Artikel 33 Absatz 4). Sind die Daten nach Auffassung der Partner weiterhin notwendig, werden sie bis zur nächsten Überprüfung aufbewahrt.

Bezüglich der praktischen Umsetzung dieser Anforderungen teilte OLAF dem EDSB mit, es gebe ein Verfahren zur jährlichen Überprüfung. Nach 11 Monaten werden die Fallbesitzer darüber unterrichtet, dass der Fall zur Überprüfung ansteht, und sie werden um Auskunft dazu gebeten, ob eine weitere Speicherung der Daten erforderlich ist. Wird im Überprüfungszeitraum (ein Monat) nicht angegeben, dass die Aufbewahrungsfrist verlängert werden soll, werden die Daten gelöscht. Die Aufbewahrungsfrist beträgt höchstens zehn Jahre und mindestens ein Jahr. Wird eine längere Speicherung nicht für nötig erachtet, kann der die Daten eingebende ZIS-Partner überdies jederzeit Fälle löschen. Diese Möglichkeit besteht nur beim ZIS, nicht jedoch bei den anderen Systemen.

In seiner Stellungnahme zur ersten ZIS-Meldung hatte der EDSB OLAF um nähere Auskunft dazu gebeten, wie dafür gesorgt wird, dass die Möglichkeit einer längeren Aufbewahrungsfrist nur bei Bedarf genutzt wird. OLAF hatte dem EDSB mitgeteilt, es gebe für die Fallbesitzer diesbezüglich keine besonderen Entscheidungshilfen.

Der EDSB fordert OLAF daher auf, einen Leitfaden mit methodologischen Hinweisen zur Beantwortung der Frage herauszugeben, wann eine längere Aufbewahrung notwendig ist.

#### 3.7.2. V-OCU

Wie bereits erwähnt, setzte OLAF den EDSB darüber in Kenntnis, dass die für das ZIS geltenden grundlegenden Verfahren auch für V-OCU gelten. Es wird jedoch schon nach Abschluss der postoperativen Phase der Zugriff gesperrt und die Daten sind nicht länger zugänglich. Auch eine Verlängerung der Aufbewahrungsfrist ist nicht möglich. Das bedeutet in der Praxis, dass die Daten nach einem Jahr gelöscht werden.

Es dürfte besser sein, die Daten unmittelbar nach dem Abschluss der postoperativen Phase zu löschen, da offensichtlich kein Grund für eine längere Speicherung besteht: Kontrollen, die eine Zuwiderhandlung gegen die Zoll- oder die Agrarregelung erbringen, führen zur Schaffung eines Beschlagnahmeberichts in einem der anderen Systeme, und Kontrollen, die keine positiven Ergebnisse erbringen, sind nicht länger von Bedeutung. In beiden Fällen dürfte eine längere Speicherung in V-OCU nicht erforderlich sein.

OLAF sollte zum einen diese Aufbewahrungsfrist begründen, denn nach Abschluss einer GZA ist eine weitere Speicherung wohl kaum erforderlich, und es sollte zum anderen den EDSB über Möglichkeiten für eine Kürzung des Zeitraums informieren.

#### 3.7.3. MAB

Die ZIS-Regeln gelten auch für andere Arten von MAB-Fällen. Wie bei V-OCU besteht keine Möglichkeit zur Verlängerung der Aufbewahrungsfrist, was in der Praxis auf einen Zeitraum von einem Jahr hinausläuft. Der EDSB begrüßt diese deutliche Änderung der Aufbewahrungsfrist von zehn Jahren in der älteren Mitteilung zur Vorabkontrolle des Datenaustauschs im Rahmen der Amtshilfe.

### 3.8. Datenübermittlung

Übermittlungen personenbezogener Daten an andere Organe, Einrichtungen und Agenturen der EU, andere Mitgliedstaaten sowie Drittländer und internationale Organisationen sind in Artikel 7, 8 bzw. 9 der Verordnung geregelt.

#### 3.8.1. Weitergabe an andere Organe, Einrichtungen oder Agenturen der EU

Beim OLAF bestehen allgemeine Verfahren für Übermittlungen an andere EU-Organe und Mitgliedstaaten. Sollten derartige Übertragungen in Zukunft im Anwendungsbereich der gemeldeten Systeme vorkommen, würden diese Verfahren angewandt. Nach diesen Verfahren haben die OLAF-Bediensteten zu überprüfen, i) ob der beabsichtigte Empfänger über die entsprechende Zuständigkeit verfügt, und ii), ob die Übermittlung erforderlich ist. Diese Anforderungen müssen in jedem Einzelfall und bei jeder Übermittlung erfüllt sein. Der Test muss auch dann vorgenommen werden, wenn die Übermittlung in einschlägigen

Rechtsvorschriften vorgesehen ist (Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen, S. 15). Dieses Verfahren gilt auch für Übermittlungen an andere Referate innerhalb von OLAF. Es ist nach den Empfehlungen im älteren zur Vorabkontrolle gemeldeten Fall 2007-0202 gestaltet.

OLAF erwähnt in der Meldung, dass die DSB von Eurojust und Europol Zugriff auf die Log-Dateien für das AFIS-Portal beantragt haben, zu dem ja auch die Systeme gehören, die Gegenstand dieser Stellungnahme sind. Dadurch hat OLAF erst erkannt, dass in den Logs personenbezogene Daten verarbeitet werden. OLAF hat dem EDSB mitgeteilt, dass ein Verfahren eingeführt werden soll, um den beiden DSB, die den Zugriff beantragt haben, allmonatlich einen Auszug aus den Log-Dateien zur Verfügung zu stellen. Der EDSB fordert OLAF nachdrücklich auf, dafür zu sorgen, dass bei diesen Übermittlungen die Bedingungen der Verordnung erfüllt werden, und dass dies auch dokumentiert wird.

### 3.8.2. Weitergabe an Mitgliedstaaten

In den Meldungen wird zwar die Möglichkeit solcher Übermittlungen erwähnt, doch weist OLAF darauf hin, dass sie in der Praxis nicht stattfinden.

In den Datenschutzhinweisen für MAB und V-OCU heißt es, dass Daten an die „*zuständigen Verwaltungs-, Gesetzgebungs- und Justizbehörden in den Mitgliedstaaten*“ weitergegeben werden dürfen. In Artikel 1 Absatz 1 der Verordnung (EG) Nr. 515/97 wird als Ziel dieser Verordnung eindeutig die Zusammenarbeit zwischen Verwaltungsbehörden in den Mitgliedstaaten und zwischen ihnen und der Kommission genannt. Auch in den Meldungen werden als potenzielle Empfänger in den Mitgliedstaaten „*die in den Mitgliedstaaten [...] für die Anwendung der Verordnung (EG) Nr. 515/97 zuständigen Behörden*“ genannt. In den Datenschutzhinweisen werden deutlich mehr Behördenkategorien erwähnt, als in der Rechtsgrundlage vorgesehen ist. Im Datenschutzhinweis für ZIS heißt es hingegen, dass Daten an die „*zuständigen Verwaltungsbehörden der Mitgliedstaaten*“ übermittelt werden dürfen, was im Einklang mit der Rechtsgrundlage steht.

Gemäß Artikel 30 Absatz 4 der Verordnung (EG) Nr. 515/97 dürfen personenbezogene Daten aus dem ZIS mit vorheriger Zustimmung des ZIS-Partners, der sie in das System eingegeben hat, und zu den von ihm festgesetzten Bedingungen an andere nationale Behörden oder Drittländer übermittelt werden. Sollte in Zukunft OLAF Daten eingeben, würden die Verfahren aus den Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen (S. 14-17) Anwendung finden.

Das gemäß der Verordnung (EG) Nr. 515/97 erstellte Verzeichnis von Behörden mit Zugang zum ZIS wird nach Artikel 29 Absatz 2 dieser Verordnung im Amtsblatt veröffentlicht. Dies ist bisher noch nicht geschehen. Neben diesen amtlichen Verzeichnissen hat das OLAF interne Verzeichnisse für die Nutzerverwaltung auf technischer Ebene zusammengestellt, auf die vorstehend im allgemeinen Teil (2.1 „Nutzer und Nutzerverwaltung“) bereits verwiesen wurde. Zwischen diesen Verzeichnissen besteht formal keine Verbindung.

OLAF sollte das Verfahren für die Erstellung interner Verzeichnisse von Behörden mit Zugang zum ZIS für die Nutzerverwaltung auf technischer Ebene dokumentieren. Diese Verzeichnisse sollten regelmäßig auf den neuesten Stand gebracht werden. Darüber hinaus sollte OLAF sich nach Möglichkeit aktiv für die Aktualisierung und Veröffentlichung der amtlichen Verzeichnisse einsetzen. Die in den Datenschutzhinweisen für MAB und V-OCU aufgeführten Behördenarten sollten auf den neuesten Stand gebracht werden, damit sie der Rechtsgrundlage entsprechen und die Behörden umfassen, die Zugang haben.

### 3.8.3. Weitergabe an Drittstaaten und internationale Organisationen

Aus den Meldungen und den sie begleitenden Unterlagen geht hervor, dass Übermittlungen an Drittländer bei allen drei Anwendungen vorkommen können. In seinen Antworten vom 26. Mai 2011 wies OLAF darauf hin, dass beim ZIS solche Übermittlungen nicht vorkommen. Übermittlungen an Drittländer sind in Artikel 9 der Verordnung geregelt.

Bei Daten, die von Mitgliedstaaten in das System eingegeben wurden, können laut Artikel 30 Absatz 4 der Verordnung (EG) Nr. 515/97 Übermittlungen aus dem ZIS „*mit vorheriger Zustimmung*“ des Mitgliedstaats, der sie in das System eingegeben hat, „*und zu den von ihm festgesetzten Bedingungen*“ vorgenommen werden. Das OLAF spielt hierbei keine Rolle. Eine Beurteilung der bestehenden Verfahren würde somit über den Gegenstand dieser Stellungnahme zur Vorabkontrolle hinausgehen. Im zweiten Unterabsatz der genannten Bestimmung heißt es jedoch, dass diese entsprechend für die Kommission gilt, wenn diese die Daten in das System eingegeben hat. Wie in der Darstellung des Sachverhalts ausgeführt, werden Daten nur von den Mitgliedstaaten eingegeben. Sollte sich hieran etwas ändern und sollte auch OLAF damit beginnen, Informationen in die Systeme einzugeben, die dann möglicherweise an Drittländer übermittelt werden könnten, müsste auch OLAF mit angemessenen Maßnahmen dafür sorgen, dass den Anforderungen von Artikel 9 der Verordnung Genüge getan wird.

Die Frage von Datenübermittlungen an Drittländer und internationale Organisationen wird horizontal in den Fällen 2005-0154 und 2006-0493 abgehandelt. Die vorliegende Stellungnahme ist nicht der Ort, um diesen Aspekt weiter zu vertiefen.

## 3.9. Auskunftsrecht und Berichtigung

In Artikel 13 und 14 der Verordnung wird betroffenen Personen das Recht auf Auskunft und Berichtigung gewährt. Dieses Recht unterliegt gewissen Ausnahmen und Einschränkungen, die in Artikel 20 der Verordnung dargestellt sind. Da die einschlägigen Bestimmungen in den Datenschutzhinweisen der gemeldeten Anwendungen praktisch identisch sind, können sie zusammen betrachtet werden.

Alle drei Datenschutzhinweise enthalten fast deckungsgleiche Bestimmungen, denen zufolge betroffenen Personen Auskunft über ihre Daten erteilt werden „*kann*“, sofern nicht die Ausnahmen nach Artikel 20 der Verordnung greifen. Der einzige Unterschied liegt darin, dass bei MAB und V-OCU auf Artikel 20 im Allgemeinen verwiesen wird, während beim ZIS ausgeführt wird, dass die Ausnahmen nach Artikel 20 Absatz 1 Buchstaben a, b und c angewandt werden können.

Die beim OLAF bestehenden Verfahren für den Umgang mit derartigen Ersuchen sind Gegenstand von Titel 1.5 der Leitlinien für OLAF-Bedienstete zur praktischen Umsetzung von Datenschutzanforderungen. Die darin enthaltenen Anweisungen setzen die Empfehlungen des EDSB in seinen beiden älteren Stellungnahmen zum ZIS und zum Datenaustausch im Rahmen der Amtshilfe um (Fälle 2007-0177 und 2007-0202).

Bezüglich V-OCU teilte OLAF dem EDSB in seinen Antworten vom 26. Mai 2011 mit, dass in der operativen Phase einer GZA vermutlich keine Auskunft erteilt wird. Nach Artikel 20 Absatz 1 Buchstabe a der Verordnung sind solche Einschränkungen möglich, wenn sie für „*die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten*“ notwendig sind. In

Artikel 36 Absatz 2 zweiter Unterabsatz der Verordnung (EG) Nr. 515/97 heißt es dazu näher: „*Auf jeden Fall können Personen, deren Daten verarbeitet werden, Auskünfte während des Zeitraums verweigert werden, in welchem Maßnahmen zum Zweck der Feststellung und Unterrichtung oder der verdeckten Registrierung durchgeführt werden, sowie während des Zeitraums, in welchem eine operationelle Analyse der Daten durchgeführt wird oder eine behördliche oder strafrechtliche Ermittlung läuft*“. Außerdem erhält die Behörde, die die Daten eingegeben hat, Gelegenheit zur Stellungnahme, bevor betroffenen Personen Auskunft erteilt wird. Die Erteilung von Auskünften an betroffene Personen während laufender Ermittlungen könnte den Erfolg dieser Ermittlungen gefährden, und daher könnte in solchen Fällen die Verweigerung von Auskünften gerechtfertigt sein. Über eine solche Auskunftsverweigerung ist jedoch fallweise zu entscheiden. Diese Bestimmungen dürfen nicht systematisch herangezogen werden, um Auskünfte zu verweigern. Der betroffenen Person ist Auskunft zu erteilen, sobald diese Ausnahmen nicht mehr gelten. Selbst wenn eine der Ausnahmen nach Artikel 20 Absatz 1 Anwendung findet, ist der für die Verarbeitung Verantwortliche gemäß Artikel 20 Absatz 3 verpflichtet, die betroffene Person über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden. Artikel 20 Absatz 4 besagt, dass in diesen Fällen der EDSB bei Prüfung der Beschwerde die betroffene Person nur darüber unterrichtet, ob die Daten richtig verarbeitet wurden und, falls dies nicht der Fall ist, ob alle erforderlichen Berichtigungen vorgenommen wurden. Laut Artikel 20 Absatz 5 kann diese Unterrichtung so lange aufgeschoben werden, wie sie die Einschränkung gemäß Artikel 20 Absatz 1 ihrer Wirkung beraubt.

OLAF sollte klarstellen, dass betroffene Personen so schnell wie möglich zu unterrichten sind und dass die in Artikel 20 der Verordnung vorgesehenen Einschränkungen nur fallweise Anwendung finden.

### 3.10. Informationspflicht gegenüber der betroffenen Person

Bei betroffenen Personen der Kategorie I kann davon ausgegangen werden, dass die Informationen über ihre mutmaßlichen rechtswidrigen Handlungen nicht von ihnen, sondern aus anderen Quellen stammen. In ihrem Fall ist daher Artikel 12 der Verordnung die anzuwendende Bestimmung. Nach diesem Artikel hat die betroffene Person Anspruch auf folgende Informationen: Identität des für die Verarbeitung Verantwortlichen, Zwecke der Verarbeitung, die Datenkategorien, die verarbeitet werden, die Empfänger oder Kategorien von Empfängern, das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, die Rechtsgrundlage der Verarbeitung, für die die Daten bestimmt sind, die zeitliche Begrenzung der Speicherung der Daten, das Recht, sich jederzeit an den Europäischen Datenschutzbeauftragten zu wenden, und die Herkunft der Daten, außer wenn der für die Verarbeitung Verantwortliche diese aufgrund der beruflichen Geheimhaltungspflicht nicht offen legen kann. Wenn betroffene Personen nicht wissen, dass Daten über sie erhoben werden, können sie ihr Recht auf Auskunft und Berichtigung nicht wahrnehmen; daher ist eine angemessene Unterrichtung für die Wahrung ihrer Rechte von entscheidender Bedeutung.

Betroffene Personen werden über die mögliche Verarbeitung sie betreffender personenbezogener Daten in den Datenschutzhinweisen informiert, die auf der Website des OLAF veröffentlicht sind. Die Datenschutzhinweise erfüllen die meisten der in Artikel 12 genannten Bedingungen. Sie weisen jedoch auch einige Mängel auf:

- die Datenschutzhinweise für MAB und V-OCU enthalten keine Liste der Datenkategorien, die in die Systeme aufgenommen werden können;

- im Datenschutzhinweis für MAB wird auf das ZIS verwiesen, wie es in DPO-17 gemeldet wurde, also nicht auf die Version, die bei dieser Vorabkontrolle geprüft wird;
- der Datenschutzhinweis für das ZIS enthält zwar eine Liste von Datenkategorien, doch ist diese nicht genau: Es fehlen Personaldokumente und Anschriften;
- in allen Meldungen könnten die Verweise auf die Rechtsgrundlagen präziser ausfallen.

Zu personalisierten Daten, also nicht allgemeinen Informationen darüber, dass Daten verarbeitet werden können, sondern Informationen über den Inhalt der über eine bestimmte betroffene Person verarbeiteten Daten, teilte OLAF dem EDSB mit, dass solche Informationen nur *„gegebenenfalls"* und mit vorheriger Zustimmung des die Daten eingebenden Partners gegeben werden. Einschränkungen nach Artikel 20 der Verordnung dürfen nur fallweise vorgenommen werden. Die Verfahren für eine proaktive Unterrichtung von betroffenen Personen sind in Anhang 5 des OLAF-Handbuchs (Titel 1.5 und 2) niedergelegt. Werden die Einschränkungen nach Artikel 20 Absatz 1 angewandt, sind die betroffenen Personen dennoch über die wesentlichen Gründe für die Einschränkung und darüber zu unterrichten, dass sie sich an den EDSB wenden können. Diese Unterrichtung kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt. Diese Bestimmungen dürfen nicht herangezogen werden, um unbegrenzt die Auskunft zu verweigern; sobald keine stichhaltigen Gründe mehr für die Auskunftsverweigerung bestehen, muss Auskunft erteilt werden.

Von den Behörden der Mitgliedstaaten eingegebene Daten sollten von den Behörden stammen, die dabei ihren Pflichten als für die Verarbeitung Mit-Verantwortliche nachzukommen haben.[24]

Bezüglich betroffener Personen der Kategorie II in Mitgliedstaaten informiert OLAF die betreffenden Behörden in den Mitgliedstaaten darüber, dass sie ihre Beamten vor Beginn der Nutzung der Systeme entsprechend unterrichten. Bei betroffenen Personen der Kategorie II, die Beamte internationaler Organisationen sind, geht aus den vorliegenden Unterlagen nicht hervor, ob sie ähnliche Informationen erhalten. Ebenso wenig ist klar, wie OLAF-Bedienstete, die mit diesen Systemen arbeiten, über ihre Rechte und die Verarbeitung ihrer Daten aufgeklärt werden, die sich ja von der der betroffenen Personen der Kategorie I unterscheidet.[25] Sie haben zwar Zugang zu den Leitlinien für OLAF-Bedienstete für die praktische Umsetzung von Datenschutzanforderungen, die auch Angaben zu ihren Rechten anhalten, doch deuten die dem EDSB vorliegenden Unterlagen darauf hin, dass es für sie keinen Datenschutzhinweis gibt, in dem sie genau über ihre Rechte und deren Wahrnehmung aufgeklärt werden.

OLAF sollte daher die Datenschutzhinweise für V-OCU und MAB mit vollständigen Listen von Datenkategorien aktualisieren. Ferner sollte es in den Datenschutzhinweis für MAB einen aktualisierten Verweis auf die ZIS-Meldung sowie in den Datenschutzhinweis für das ZIS eine korrekte Liste von Datenkategorien aufnehmen. Alle drei Hinweise sollten mit genaueren Verweisen auf die Rechtsgrundlagen auf den neuesten Stand gebracht werden. Die aktualisierten Datenschutzhinweise sollten unverzüglich auf die Website des OLAF eingestellt werden. Weiter sollte OLAF dafür Sorge tragen, dass betroffene Personen der Kategorie II unter seinen eigenen Bediensteten und denen internationaler Organisationen angemessene Informationen erhalten.

[24] Siehe vorstehenden Abschnitt 3.4.

[25] So ist z. B. die Aufbewahrungsfrist für Audit-Logs für betroffene Personen der Kategorie I unerheblich, nicht jedoch für betroffene Personen der Kategorie II.

### 3.11. Sicherheitsmaßnahmen

[...]

## 4. Schlussfolgerung:

Es besteht kein Grund zu der Annahme, dass ein Verstoß gegen die Bestimmungen der Verordnung (EG) Nr. 45/2001 vorliegt, sofern die oben angestellten Erwägungen in vollem Umfang berücksichtigt werden.

Die Empfehlungen des EDSB lassen sich folgendermaßen zusammenfassen:

Empfehlungen zu V-OCU:

- Aktualisierung des Datenschutzhinweises mit einer erschöpfenden Liste von Datenkategorien und Aktualisierung des Verzeichnisses der Behörden, um der Rechtsgrundlage zu entsprechen. Ferner Aufnahme eines präziseren Verweises auf die Rechtsgrundlage. Unverzügliche Veröffentlichung des aktualisierten Datenschutzhinweises auf der Website des OLAF.
- Formulierung klarer Regeln für Aufbewahrungsfristen und Angabe von Gründen für die Aufbewahrungsfrist, da GZA im Allgemeinen in einem kleinen Zeitfenster stattfinden, sowie Information des EDSB über Möglichkeiten zur Kürzung der Frist.
- Angemessene Information von betroffenen Personen der Kategorie II unter den OLAF-Bediensteten und den Bediensteten internationaler Organisationen.

Empfehlungen zu MAB:

- Die Streichung von „drogenabhängig“ und „selbstmordgefährdet“ aus der Liste der Warnhinweise in Erwägung ziehen, die in MAB eingegeben werden können, um der Rechtsgrundlage zu entsprechen. Ferner Aufnahme eines präziseren Verweises auf die Rechtsgrundlage. Unverzügliche Veröffentlichung des aktualisierten Datenschutzhinweises auf der Website des OLAF.
- Angabe von Gründen für das Freitextfeld „Sonstige Warnhinweise“ und Streichung dieses Feldes, falls die vorformulierten Warnhinweise als ausreichend erachtet werden. Prüfung der Frage, ob das Feld „Kennzeichen“ notwendig ist. Hierzu sollte OLAF Statistiken über die Nutzung dieses Feldes erheben und den EDSB innerhalb von sechs Monaten von den Ergebnissen in Kenntnis setzen.
- Aktualisierung des Datenschutzhinweises mit der erschöpfenden Liste von Datenkategorien und Aufnahme eines aktualisierten Verweises auf die ZIS-Meldung. Außerdem Aktualisierung des Behördenverzeichnisses im Datenschutzhinweis, um der Rechtsgrundlage zu entsprechen.
- Angemessene Information von betroffenen Personen der Kategorie II unter den OLAF-Bediensteten und den Bediensteten internationaler Organisationen.

Empfehlungen zum ZIS:

- Berichtigung der Liste von Datenkategorien im Datenschutzhinweis. Ferner Aufnahme eines präziseren Verweises auf die Rechtsgrundlage. Unverzügliche Veröffentlichung des aktualisierten Datenschutzhinweises auf der Website des OLAF. Auch angemessene Information von in dem System arbeitenden OLAF-Bediensteten.

- Prüfung der Frage, ob das Feld „Kennzeichen“ notwendig ist. Hierzu sollte OLAF Statistiken über die Nutzung dieses Feldes erheben und den EDSB innerhalb von sechs Monaten von den Ergebnissen in Kenntnis setzen.
- Prüfung der Möglichkeit von Leitlinien für Beamte, die über eine Verlängerung von Aufbewahrungsfristen entscheiden.
- Das Verfahren für die Erstellung interner Verzeichnisse von Behörden mit Zugang zum ZIS für die Nutzerverwaltung auf technischer Ebene sollte dokumentiert werden. Diese Verzeichnisse sollten regelmäßig auf den neuesten Stand gebracht werden.
- Bezüglich des Verfahrens für die Erstellung von Verzeichnissen von Behörden mit Zugang zum ZIS gemäß Artikel 29 Absatz 2 der Verordnung 515/97 sollte OLAF sich nach Möglichkeit für die Veröffentlichung der amtlichen Verzeichnisse einsetzen. Auch diese Verzeichnisse sollten regelmäßig auf den neuesten Stand gebracht werden.

Empfehlungen betreffend die Sicherheit der an AFIS angeschlossenen Systeme:

- [...]

Brüssel, den 17. Oktober 2011

**(gezeichnet)**

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter