Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission zur Vorabkontrolle der „Risikoanalyse zur Verhütung und Aufdeckung von Betrug in der Verwaltung des ESF und des EFRE“ - ARACHNE

Brüssel, 17. Februar 2014 (2013-0340)

1. VERFAHREN

Am 17. Mai 2013 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) eine Meldung des Datenschutzbeauftragten (**DSB**) der Europäischen Kommission zur Vorabkontrolle der Verarbeitung personenbezogener Daten bei der „Risikoanalyse zur Verhütung und Aufdeckung von Betrug in der Verwaltung des ESF und des EFRE“ – ARACHNE.

Am 4. Juni 2013 gestellte Fragen wurden vom DSB der Kommission am 26. Juni 2013 beantwortet. In der Zwischenzeit hatte eine Sitzung von EDSB und Kommissionsdienststellen am 7. Juni 2013 stattgefunden. Weitere Fragen wurden am 27. Juni 2013 übermittelt; die Antworten hierauf gingen am 30. Oktober 2013 ein. Der Entwurf der Stellungnahme wurde dem DSB am 18. November 2013 zur Kommentierung übersandt. Eine Antwort hierauf erhielt der EDSB am 26. November 2013, aufgrund derer er noch am gleichen Tag eine überarbeitete Meldung anforderte, die am 29. November 2013 einging. Am 9. Dezember 2013 beantragte der EDSB eine Sitzung, die am 9. Januar 2014 stattfand und in deren Nachgang am 17. Januar 2014 weitere Unterlagen eingereicht wurden. Der überarbeitete Entwurf der Stellungnahme wurde dem DSB am 24. Januar 2014 zur Kommentierung übersandt, der jedoch am 13. Februar 2014 mitteilte, er habe keine Bemerkungen vorzutragen.

2. SACHVERHALT

Das ARACHNE-System ist Bestandteil der Strategie der Kommission zur Verhütung und Aufdeckung von Betrug im Bereich der Strukturfonds (Europäischer Sozialfonds (ESF) und Europäischer Fonds für regionale Entwicklung (EFRE)). Die Unterstützung aus den Strukturfonds erfolgt über ein System der „geteilten Mittelverwaltung“, in dem die Mitgliedstaaten für die Durchführung der Hilfe verantwortlich sind, die Kommission aber letztendlich die finanzielle Verantwortung trägt. Die Direktion H der Generaldirektion (GD) Beschäftigung, Soziales und Integration und die Direktion J der GD Regionalpolitik der Kommission tragen die Hauptverantwortung für die Validierung der Informationen, die von den für den ESF und den EFRE tätigen Behörden vorgelegt werden[1], die in den EU-Mitgliedstaaten externe Audits durchführen, zeitnah Berichte und Stellungnahmen verfassen

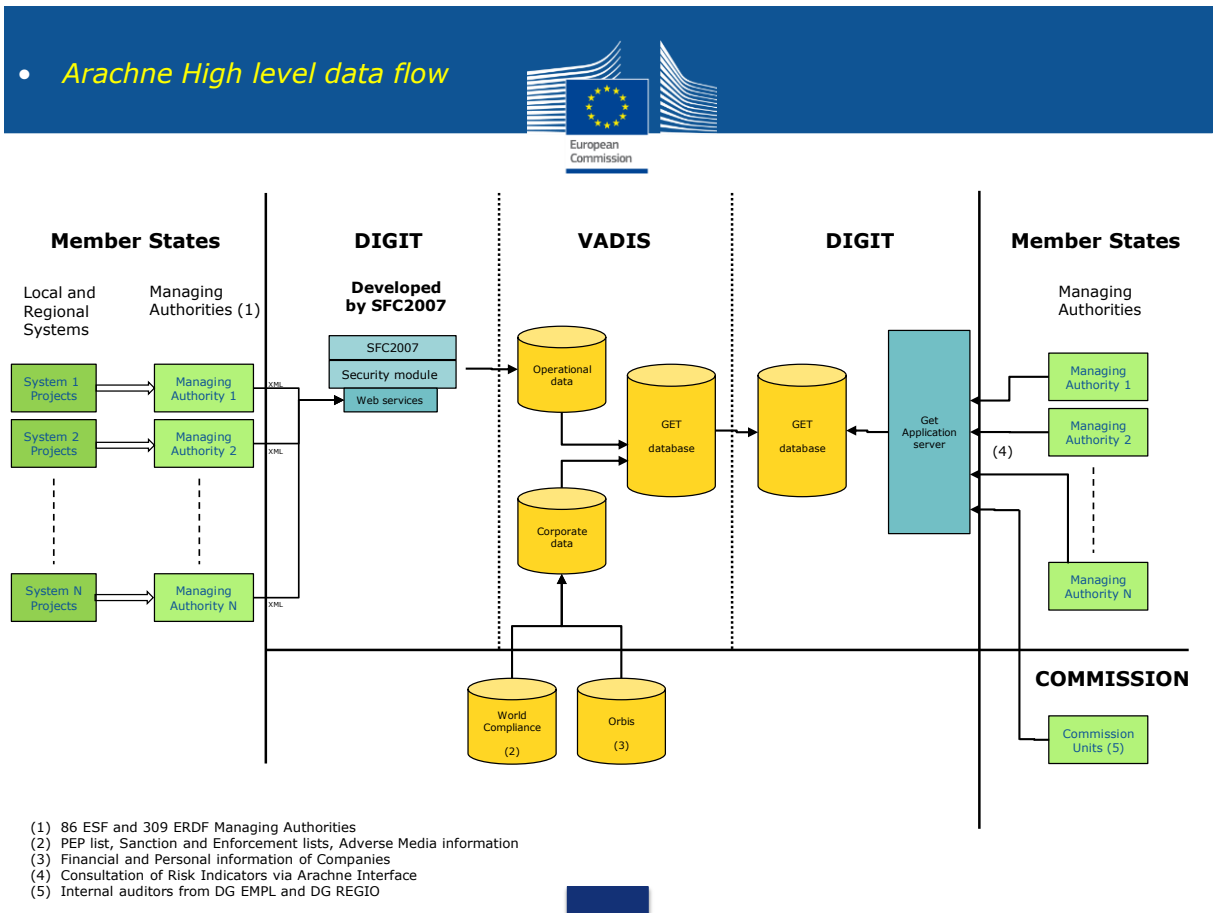
[1] Beschreibung des Verwaltungs- und Kontrollsystems, Audit-Strategie, Jahreskontrollbericht/Jahresstellungnahme, nationale Audit-Berichte, jährliche Zusammenfassungen.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (02) 283 19 00 – Fax: +32 (02) 283 19 50

und eine Risikoeinstufungstabelle auf dem neuesten Stand halten, um eine ordnungsgemäße Verwaltung der Fonds zu ermöglichen.

Zweck des ARACHNE-Systems ist die Aufdeckung von Betrug. Während der Sitzung am 9. Januar 2014 bekräftigte die Kommission noch einmal ausdrücklich, dass ARACHNE nicht das Ziel verfolgt, das individuelle Verhalten von Begünstigten zu beurteilen und als solches auch nicht dazu dient, Begünstigte von den Fonds auszuschließen. ARACHNE ergänzt eine bereits bestehende Datenbank mit Projekten, die aus den Strukturfonds durchgeführt werden (SFC), und die öffentlich zugängliche Informationen enthält, damit anhand einer Reihe von Risikoindikatoren die mit den größten Risiken behafteten Projekte ermittelt werden können. In der Sitzung am 9. Januar 2014 wurde unterstrichen, dass die Risikoeinstufung keine automatischen Entscheidungen gegen Begünstigte zur Folge hat. Risikoeinstufungen helfen Auditoren bei der Auswahl/Ermittlung künftiger Audit-Kandidaten. ARACHNE als System stützt sich auf die Integration und Anpassung eines bestehenden Risikobewertungsinstruments, der Anwendung GET von *VADIS Consulting SA/NV*, mit operativen Daten, die von den Verwaltungsbehörden des ESF und des EFRE stammen, um Risikoeinstufungen für die Ermittlung der risikoreichsten Projekte und konkreter Risikobereiche bereitzustellen.

In der ersten Phase des **Verfahrens** wird die bestehende SFC2007-Infrastruktur, eine Webservice-Implementierung für die Übermittlung operativer Projektdaten von den ESF- und EFRE-Verwaltungsbehörden der Mitgliedstaaten an die Kommission, verwendet, um operative Daten in ARACHNE einzugeben. In einer zweiten Phase werden die Projektdaten durch Informationen aus öffentlich zugänglichen Quellen ergänzt. In einer dritten Phase berechnet ARACHNE individuelle Risikoindikatoren (Risikoeinstufungsbögen für die einzelnen Projekte) um so eine ordnungsgemäße Verwaltung der Fonds einschließlich des laufenden Monitorings für Zwecke von Projekt-Audits zu ermöglichen.



Arachne High level data flow	Arachne High level data flow (Datenverkehr auf oberster Ebene)
Member States	Mitgliedstaaten
Local and Regional Systems	Lokale und regionale Systeme
Managing Authorities (1)	Verwaltungsbehörden (1)
System 1 Projects	System 1-Projekte
System 2 Projects	System 2-Projekte
System N Projects	System N-Projekte
Managing Authority 1	Verwaltungsbehörde 1
Managing Authority 2	Verwaltungsbehörde 2
Managing Authority N	Verwaltungsbehörde N
DIGIT	DIGIT
Developed by SFC2007	Entwickelt von SFC2007
Security module	Sicherheitsmodul
Web servicies	Webdienste
VADIS	VADIS
Operational data	Operative Daten
Get database	GET Datenbank
Corporate data	Unternehmensdaten
World Compliance (2)	World Compliance (2)
Orbis (3)	Orbis (3)
DIGIT	DIGIT
Get application server (4)	GET Anwendungsserver (4)
COMMISSION	KOMMISSION
Commission Units (5)	Referate der Kommission (5)
(1) 86 ESF and 309 ERDF Managing Authorities	(1) 86 ESF- und 309 EFRE-Verwaltungsbehörden
(2) PEP list, Sanction and Enforcement lists, Adverse Media information	(2) PEP-Liste, Listen für Sanktionen und Durchsetzung, Informationen über negativ berichtende Medien (Adverse Media information)
(3) Financial and Personal information of Companies	(3) Finanz- und Personalinformationen von Unternehmen
(4) Consultation of Risk Indicators via Arachne Interface	(4) Konsultation von Risikoindikatoren über Arachne-Schnittstelle
(5) Internal auditors from DG EMPL and DG REGIO	(5) Interne Prüfer von GD EMPL und GD REGIO

Für die Verarbeitung Verantwortliche ist die Kommission, hier gemeinsam vertreten durch den Direktor der Direktion H der GD Beschäftigung, Soziales und Integration und den Direktor der Direktion J der GD Regionalpolitik. Den am 26. November 2013 eingegangenen weiteren Informationen ist zu entnehmen, dass die Kommission selber keine Daten erhebt, sondern dass alle Daten aus einer bestehenden Projektdatenbank der Strukturfonds (SFC) oder von dem externen Dienstleister stammen. *VADIS SA/NV* als Unterauftragnehmer von *ATOS Belgium NV/SA* führt die Verarbeitung im Auftrag der Kommission im Sinne von Artikel 23 der Verordnung (EG) Nr. 45/2001 („Verordnung“) durch. *VADIS SA/NV* als **Auftragsverarbeiter** stellt die daraus resultierende GET-Datenbank der Kommission zur Verfügung, die als Host für die GET-Anwendung für die Endnutzer fungiert. Wie auf der Sitzung von 9. Januar 2014 bestätigt wurde, übermittelt *VADIS SA/NV* keine individuellen Einträge und auch keine anderen Informationen. Diese Tätigkeit ist in einem am 17. Januar 2014 vorgelegten schriftlichen Vertrag geregelt, der insbesondere vorsieht, dass der Auftragsverarbeiter auf Anweisung des für die Verarbeitung Verantwortlichen tätig wird, und der Klauseln bezüglich der in Artikel 21 und 22 der Verordnung niedergelegten Verpflichtungen des für die Verarbeitung Verantwortlichen enthält.

Betroffene Personen sind natürliche Personen wie die Begünstigten bzw. die Geschäftsführer und öffentlich bekannten Anteilseigner von Begünstigten, die juristische Personen sind und Unterstützung aus dem ESF und/oder dem EFRE erhalten, sowie möglicherweise andere, zu ihnen in einer Beziehung stehende Personen.

Laut Meldung umfasst die **Rechtsgrundlage** des ARACHNE-Systems folgende Bestimmungen:

- Artikel 60, 61, 62, 69 und Kapitel IV, Abschnitte 1 und 2 der Verordnung (EG) Nr. 1083/2006[2];
- Artikel 13, 14, 16, 19, 37 sowie Abschnitt 7 der Verordnung (EG) Nr. 1828/2006[3] ;
- Kapitel 2.2.3 der Mitteilung der Kommission „Die Betrugsbekämpfungsstrategie der Kommission“ vom 22. Juni 2011[4];
- Verordnung (EU, Euratom) Nr. 966/2012[5] vor dem Hintergrund von Artikel 325 und 317 des Vertrags über die Funktionsweise der Europäischen Union (AEUV).
-

Laut Meldung werden folgende **Datenkategorien** verarbeitet:
1) von den ESF- und EFRE-Verwaltungsbehörden (durch die SFC2007-Infastruktur):
- Begünstigte: Name, Anschrift, MwSt-Nummer, Funktion;
- leitende Mitarbeiter: Name, Funktion;
- Auftragnehmer: Name, Anschrift, MwSt-Nummer;
- wichtigste Experten für Dienstleistungsverträge: Name, Geburtsdatum.

2) Von externen öffentlichen Datenquellen, die von VADIS SA/NV bereitgestellt werden:
a) vom kommerziellen Anbieter ORBIS (http://www.bvdinfo.com/Products/Company-Information/International/Orbis):

- umfassende Informationen über Unternehmen;
- Anteilseigner/Management/leitende Mitarbeiter: Name, Funktion;

b) vom kommerziellen Anbieter WORLD COMPLIANCE:

- Profile politisch exponierter Personen (PEP) sowie die ihrer Familienmitglieder und von ihnen nahestehenden Personen;
- Sanktionsliste, auf der natürliche Personen und Unternehmen verzeichnet sind, die die höchste Risikoeinstufung haben;
- Durchsetzungsliste mit Informationen von Regulierungsstellen und Behörden und dem Inhalt von Warnungen vor und Klagen gegen Personen und Unternehmen;
- Durchschau von Zeitungen und Zeitschriften auf risikorelevante Informationen (einschließlich Informationen der großen Online-Zeitungen in den Mitgliedstaaten der Europäischen Union und in Drittländern).

Empfänger sind die ARACHNE-Nutzer:

- die Verwaltungsbehörden und ihre zwischengeschalteten Stellen in den Mitgliedstaaten, ihre Bescheinigungsbehörden und die Prüfbehörden;
- die GD Beschäftigung, Soziales und Integration und die GD Regionalpolitik der Kommission (jeweils beschränkt auf das Audit-Referat), mit Ausnahme der Direktion H

[2] Verordnung (EG) Nr. 1083/2006 des Rates vom 11. Juli 2006 mit allgemeinen Bestimmungen über den Europäischen Fonds für regionale Entwicklung, den Europäischen Sozialfonds und den Kohäsionsfonds, ABl. L 210 vom 31.7.2006, S. 25.

[3] Verordnung (EG) Nr. 1828/2006 der Kommission vom 8. Dezember 2006 zur Festlegung von Durchführungsvorschriften zur Verordnung (EG) Nr. 1082/2006 des Rates mit allgemeinen Bestimmungen über den Europäischen Fonds für regionale Entwicklung, den Europäischen Sozialfonds und den Kohäsionsfonds und der Verordnung (EG) Nr. 1080/2006 des Europäischen Parlaments und des Rates über den Europäischen Fonds für regionale Entwicklung, ABl. L 371 vom 27.12.2006, S. 1.

[4] KOM(2011) 376 endgültig, siehe http://ec.europa.eu/anti_fraud/documents/preventing-fraud-documents/ec_antifraud_strategy_de.pdf.

[5] Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, ABl. L 298 vom 26.10.2012, S. 1.

der GD Beschäftigung, Soziales und Integration und der Direktion J der GD Regionalpolitik;
- der Europäische Rechnungshof und OLAF (auf deren Ersuchen).

Lese- und Schreibzugriff haben nur die Verwaltungsbehörde und ihre zwischengeschalteten Stellen. Bei technischen Problemen haben Zugriff auch die für IT-Fragen zuständige GD der Kommission sowie *VADIS SA/NV*.

Betroffene Personen werden über die Verarbeitung mit Hilfe einer Datenschutzerklärung auf der Website des Europäischen Sozialfonds **informiert**, die zum einen die vorgeschriebenen Angaben gemäß Artikel 11 und 12 der Verordnung enthält, zum anderen aber auch erläutert, wie im Zusammenhang mit ARACHNE das Risikomanagement funktioniert und vorgenommen wird, und die Rechtsgrundlage nennt.

Im Hinblick auf das **Recht** betroffener Personen **auf Auskunft und Berichtigung** ist zu unterscheiden zwischen a) Daten im Besitz der für den ESF und den EFRE tätigen Verwaltungsbehörden und ihrer zwischengeschalteten Stellen in den Mitgliedstaaten oder anderer einzelstaatlicher zuständiger Behörden, die der Richtlinie 95/46/EG unterworfen sind, und b) Daten im Besitz der Kommission, für die die Verordnung gilt:

a) Wie es in der (am 29. November 2013 erneut gemeldeten) Datenschutzerklärung heißt, können betroffene Personen ihr Recht auf Auskunft und Berichtigung der Daten über das von ihnen vertretene Unternehmen oder ihrer personenbezogenen Daten mit einem Antrag an die für den ESF und den EFRE tätigen Verwaltungsbehörden und deren zwischengeschaltete Stellen oder andere nationale zuständige Behörden ausüben. Ändern sich Projektdaten, können die Behörden der Mitgliedstaaten die Daten in der Datenbank der im Rahmen der Strukturfonds durchgeführten Projekte (SFC) sofort ändern. Betroffene Personen werden ferner darüber unterrichtet, dass sie sich bei Schwierigkeiten oder bei Fragen zur Verarbeitung dieser Daten auch an ihre nationale Datenschutzbehörde wenden können. In der Meldung heißt es hierzu: „*Die Mitgliedstaaten verfahren so, wie es in der Richtlinie 95/46/EG vorgesehen ist"*.

b) Bezüglich der Informationen aus externen Medienquellen, die die Kommission nicht selber erhebt, sondern verarbeitet, geht der EDSB davon aus, dass „*die betroffene Person nach der Informationsquelle fragen sollte, wenn sie ihre Rechte <u>über</u> das ARACHNE-System <u>hinaus</u> wahrnehmen möchte*" (Hervorhebung durch uns). Die Gewährung des Rechts auf Auskunft und Berichtigung im Rahmen des ARACHNE-Systems geht aber nicht *über* dieses System *hinaus*.

Laut Datenschutzerklärung gilt für die Kommission „*Artikel 20 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 45/20001. Das Recht betroffener Person auf Auskunft gemäß Artikel 13 wird fallweise bewertet und seine Ausübung wird aufgeschoben, falls diese Ausübung potenziellen Betrügern die Möglichkeit geben sollte, mögliche Schwachstellen im Risikobewertungsprozess zu entdecken und diesen somit zu umgehen. Auskunft wird in solchen Fällen erteilt, wenn kein Audit beschlossen wurde bzw. zum Zeitpunkt des Audits*". In der Meldung heißt es hierzu, dass *„…aus dem gleichen Grund nicht die Logik offengelegt wird, die zum Ergebnis der Risikobewertung geführt hat. Dies bedeutet jedoch keine Einschränkung von Artikel 13, da Entscheidungen nur vom System unterstützt, aber nicht von ihm automatisiert werden*".

Bezüglich der von den kommerziellen Anbietern gewonnenen Daten aus externen öffentlichen Quellen besagt die Meldung (in der Fassung vom 29. November 2013), dass das System aktualisiert wird:

- vierteljährlich mit einem komplett neuen Datensatz des kommerziellen Anbieters (der sich auf die Jahresabschlüsse von Begünstigten stützt und von der Kommission bei der nächsten Risikoeinstufung herangezogen werden kann);
- wöchentlich mit neuen Daten von den Mitgliedstaaten (durch SFC oder die Rückkopplungsschleife). Die Mitgliedstaaten können die Risikoeinstufung oder andere importierte Daten nicht direkt in ARACHNE ändern, können aber in ARACHNE einen Kommentar einstellen, um Anträge betroffener Personen nachverfolgen zu können.
- Stellt ein ARACHNE-Nutzer, also die Kommission oder ein Mitgliedstaat, einen Fehler oder eine Unstimmigkeit fest (unrichtige Angaben zur Geschäftsführung, unrichtige Angaben zu Anteilseignern, unrichtige Informationen in der Presse / den Medien, fehlende Namensübereinstimmung zwischen Datenquellen), kann er dies mit Hilfe eines „Rückkopplungsschleife" (feedback loop) genannten Verfahrens an *VADIS SA/NV* melden. Die von *VADIS SA/NV* über die Rückkopplungsschleife eingegebenen Änderungen schlagen sich nur auf das ARACHNE-System nieder, nicht jedoch auf die ursprüngliche Informationsquelle. Die Meldung besagt: „*Die betroffene Person sollte nach der Informationsquelle fragen, wenn sie ihre Rechte über das ARACHNE-System hinaus wahrnehmen möchte*".

In der Datenschutzerklärung werden betroffene Personen ferner darüber aufgeklärt, dass sie sich bei allen Problemen oder bei Fragen zur Verarbeitung dieser Daten an den Datenschutzbeauftragten der Kommission (dessen E-Mail-Adresse angegeben ist) wenden und nähere Informationen über diese Verarbeitung personenbezogener Daten im öffentlichen Register der Meldungen unter der Meldung Nr. 3580 erhalten können.

Zur **Aufbewahrung der Daten** ist anzumerken, dass sie drei Jahre nach dem Abschluss eines operationellen Programms und im Einklang mit den Bedingungen in Artikel 90 der Verordnung (EG) Nr. 1083/2006 gespeichert werden. Laut Datenschutzerklärung werden keine Daten für statistische Zwecke gespeichert.

Definition der geplanten technischen Architektur des Systems: (...)

3. RECHTLICHE ANALYSE

3.1. Vorabkontrolle

Die gemeldeten Verarbeitungsvorgänge sind eine Verarbeitung personenbezogener Daten („*alle Informationen über eine bestimmte oder eine bestimmbare natürliche Person*") im Sinne von Artikel 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 („Verordnung"). Sie wird durch eine Einrichtung der EU im Rahmen von Tätigkeiten vorgenommen, die in den Anwendungsbereich des EU-Rechts fallen. Die Verarbeitung der Daten wird zumindest teilweise automatisch vorgenommen. Somit ist die Verordnung anzuwenden.

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. Unter Buchstabe a wird unter anderem die Verarbeitung von Daten erwähnt, die Verdächtigungen, Straftaten und strafrechtliche Verurteilungen betreffen. Buchstabe b spricht von Verarbeitungen, die dazu bestimmt sind,

die Persönlichkeit der betroffenen Person zu bewerten, einschließlich ihres Verhaltens. Gegenstand von Buchstabe c sind Verarbeitungen, die eine in den nationalen oder Unionsrechtsvorschriften nicht vorgesehene Verknüpfung von Daten ermöglichen, die zu unterschiedlichen Zwecken verarbeitet werden. Buchstabe d schließlich befasst sich mit Verarbeitungen, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen. In der Meldung wurden alle diese Punkte als Gründe für die Vorabkontrolle aufgeführt.

Auf der Sitzung vom 9. Januar 2014 bestätigte die Kommission ausdrücklich, dass ARACHNE nicht der Bewertung des individuellen Verhaltens von Begünstigten im Sinne von Artikel 27 Absatz 2 Buchstabe b dient. Wie jedoch bereits in Abschnitt 2 dargestellt, können personenbezogene Daten über Verdächtigungen und Straftaten im Sinne von Artikel 27 Absatz 2 Buchstabe a verarbeitet werden (Sanktionsliste von WORLD COMPLIANCE). Aus diesem Grund ist die Verarbeitung einer Vorabkontrolle zu unterziehen.

Die Meldung des DSB ging am 17. Mai 2013 ein. Der Entwurf der Stellungnahme wurde dem DSB am 18. November 2013 zur Kommentierung übersandt. Beim EDSB gingen am 26. November 2013 eine Antwort und am 29. November 2013 eine überarbeitete Meldung sowie eine überarbeitete Datenschutzerklärung ein. Am 9. Dezember 2013 beantragte der EDSB eine Sitzung, die am 9. Januar 2014 stattfand und in deren Nachgang am 17. Januar 2014 weitere Unterlagen eingereicht wurden. Der Entwurf der überarbeiteten Stellungnahme wurde dem DSB am 24. Januar 2014 zur Kommentierung übersandt. Nach Artikel 27 Absatz 4 der Verordnung hat die Stellungnahme des EDSB innerhalb von zwei Monaten zu ergehen. Der Fall wurde für insgesamt 216 Tage ausgesetzt. Unter Berücksichtigung aller Aussetzungszeiträume muss die Stellungnahme daher spätestens am 17. Februar 2014 angenommen werden.

3.2. Rechtmäßigkeit der Verarbeitung

Gemäß Artikel 5 Buchstabe a der Verordnung[6], ist in zwei Schritten Folgendes zu bewerten: Erstens, ob entweder im Vertrag oder in anderen Rechtsakten die Wahrnehmung einer Aufgabe im öffentlichen Interesse vorgesehen ist, aufgrund derer die Datenverarbeitung stattfindet (Rechtsgrundlage), und zweitens, ob die Verarbeitungen für die Wahrnehmung dieser Aufgabe tatsächlich erforderlich sind.

In der Meldung gibt die Kommission die Bestimmungen der Verordnung (EG) Nr. 1083/2206 und der Verordnung (EG) Nr. 1828/2006, die Mitteilung der Kommission zur Betrugsbekämpfungsstrategie sowie die Verordnung (EU, Euratom) Nr. 966/2012 als mögliche Rechtsgrundlagen an. Wie nachstehend erörtert, sind mehrere dieser Bestimmungen keine angemessene Rechtsgrundlage für die gemeldete Verarbeitung.

- Die **Verordnung (EU, Euratom) Nr. 966/2012** enthält die Finanzvorschriften betreffend den Gesamthaushaltsplan der Union. Allein aus ihrem Wortlaut lassen sich die Tätigkeiten der Kommission im Zusammenhang mit ARACHNE nicht ableiten. So würden beispielsweise betroffene Personen nicht erfassen können, in welchem Umfang personenbezogene Daten über sie erhoben und im ARACHNE-System weiter verarbeitet

[6] Gemäß Artikel 5 Buchstabe a der Verordnung dürfen personenbezogene Daten nur verarbeitet werden, „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“.

werden könnten. Die Verordnung (EU, Euratom) Nr. 966/2012 ist somit zu allgemein gehalten, um als Rechtsgrundlage gemäß Artikel 5 Buchstabe a dienen zu können.

- **Verordnung (EG) Nr. 1083/2006**: Gemäß Artikel 60 Buchstabe c der Verordnung (EG) Nr. 1083/2006 ist die Verwaltungsbehörde dafür zuständig, insbesondere „*die elektronische Aufzeichnung und Erfassung von Buchführungsdaten zu jedem im Rahmen eines operationellen Programms durchgeführten Vorhaben sowie die Erfassung der erforderlichen Durchführungsdaten für Finanzverwaltung, Begleitung, Überprüfungen, Prüfungen und Bewertung zu gewährleisten; …*". Gemäß Artikel 61 Buchstabe e der Verordnung (EG) Nr. 1083/2006 ist es Aufgabe der Bescheinigungsbehörde eines operationellen Programms, insbesondere „*über die bei der Kommission geltend gemachten Ausgaben in elektronischer Form Buch zu führen…*". In beiden Bestimmungen ist zwar von einem IT-gestützten Überwachungssystem die Rede, doch werden die Verwaltungs- und die Bescheinigungsbehörde, also Stellen der Mitgliedstaaten gemäß Artikel 59 Buchstabe a der Verordnung (EG) Nr. 1083/2006, und nicht die Kommission mit ihrem Betrieb betraut. Der EDSB ist jedoch der Ansicht, dass die Rechtsgrundlage für den Zweck von Artikel 5 Buchstabe a in Rechtsvorschriften zu suchen ist, die unmittelbar auf die Kommission anzuwenden sind.

  Artikel 66 der Verordnung (EG) Nr. 1083/2006 sieht im Hinblick auf die ordnungsgemäße Durchführung des operationellen Programms vor: „*Der (...) Datenaustausch zwischen der Kommission und den Mitgliedstaaten erfolgt elektronisch gemäß den Durchführungsbestimmungen zu dieser Verordnung, die von der Kommission nach dem in Artikel 103 Absatz 3 genannten Verfahren angenommen werden*". Diese Bestimmung könnte zwar als Rechtsgrundlage für die derzeitige SFC2007-Infrastruktur (Webservices-Implementierung) für die Übermittlung operativer Daten des Projekts von den Verwaltungsbehörden der Mitgliedstaaten an die Kommission herangezogen werden, doch findet sich darin kein Bezug auf das mit ARACHNE verfolgte Ziel der Betrugsverhütung.

- **Verordnung (EG) Nr. 1828/2006**: Artikel 19 Absatz 1 der Verordnung (EG) Nr. 1828/2006 (mit dem Titel „*Aufbewahrung von Unterlagen*") besagt: „*Für die Zwecke von Artikel 90 der Verordnung (EG) Nr. 1083/2006 stellt die Verwaltungsbehörde sicher, dass Aufzeichnungen verfügbar sind, die Angaben zu den Einrichtungen, die die Belege für Ausgaben und Prüfungen – einschließlich aller für einen hinreichenden Prüfpfad erforderlichen Unterlagen – führen, sowie zu deren Standort enthalten*". Liegen Unterlagen nur in elektronischer Form vor, besagt Artikel 19 Absatz 6 der Verordnung (EG) Nr. 1828/2006: „*… so muss das verwendete EDV-System anerkannten Sicherheitsstandards genügen, die die Gewähr bieten, dass die aufbewahrten Unterlagen den nationalen Rechtsvorschriften entsprechen und dass sie für Rechnungsprüfungszwecke glaubwürdig sind*". Zwar ist in diesen Bestimmungen von einem IT-gestützten Überwachungssystem die Rede, doch werden die Verwaltungsbehörden, also Stellen der Mitgliedstaaten, und nicht die Kommission mit ihrem Betrieb betraut. Der EDSB ist jedoch der Ansicht, dass die Rechtsgrundlage für den Zweck von Artikel 5 Buchstabe a in Rechtsvorschriften zu suchen ist, die unmittelbar auf die Kommission anzuwenden sind.

  Artikel 34 der Verordnung (EG) Nr. 1828/2006 lautet: „*Die Kommission kann alle allgemeinen und operativen Informationen, die die Mitgliedstaaten ihr im Rahmen dieser Verordnung mitteilen, verwenden, um Risikoanalysen durchzuführen sowie Berichte und Frühwarnsysteme zu erarbeiten, die eine effizientere Risikoermittlung ermöglichen*" (Hervorhebung durch uns). **Abschnitt 7** der Verordnung (EG)

Nr. 1828/2006 („*Elektronischer Datenaustausch*“) sieht die Einrichtung eines computergestützten Systems für den Austausch aller Daten im Zusammenhang mit dem operationellen Programm vor (Artikel 39 Absatz 1), und: „*Der Zugriff der Mitgliedstaaten und der Kommission (…) erfolgt entweder direkt oder über eine die automatische Synchronisierung und Dateneinspeisung gewährleistende Schnittstelle zu den nationalen, regionalen und lokalen computergestützten Verwaltungssystemen*“ (Artikel 42 Absatz 1).
Zwar könnte dies möglicherweise eine hinreichende Rechtsgrundlage für die Entwicklung von computergestützten Risikobewertungsinstrumenten sein, doch besteht eine Einschränkung, weil nur von den Mitgliedstaaten *im Zusammenhang mit der derzeitigen SFC2007-Infrastruktur* (Webservices-Implementierung) für die Übermittlung der operativen Daten der Projekte von den Verwaltungsbehörden an die Kommission gewonnenen Informationen gemeint sind („*Informationen verwenden*…“). ARACHNE geht jedoch über diese Informationen hinaus, weil, wie es in der Meldung heißt, die Projektdaten noch durch Daten aus öffentlich zugänglichen Quellen ergänzt werden. Daher ist Artikel 34 der Verordnung (EG) Nr. 1828/2006 gemäß Artikel 5 Buchstabe a für das ARACHNE-System keine umfassende Rechtsgrundlage.

- In der **Mitteilung der Kommission zur Betrugsbekämpfungsstrategie** heißt es in Kapitel 2.2.3: „*Die Kommissionsdienststellen werden prüfen, inwieweit es erforderlich ist, die Betrugsrisikobewertung durch ein systematischeres, formalisiertes Vorgehen bei der Ermittlung von Bereichen, in denen Betrugsrisiken bestehen, zu verbessern. Zugleich sollten sie unter optimaler Nutzung der vorhandenen Ressourcen intelligente Kontrollen durchführen und dabei auf die IT-Werkzeuge zurückgreifen, die von einigen Dienststellen in Zusammenarbeit mit dem OLAF entwickelt worden sind, und diese an ihre Erfordernisse anpassen. Diese Werkzeuge ermöglichen beispielsweise das Zusammentragen aller vorhandenen Daten zu abgeschlossenen oder noch laufenden Projekten, die mit EU-Mitteln finanziert werden. Dies ist nicht nur für die Betrugsbekämpfung nützlich, sondern auch für die Aufdeckung von Plagiaten und betrügerischen Doppelfinanzierungen. Gleichwohl können diese Werkzeuge nur dann in vollem Umfang nützlich sein, wenn die in den betreffenden Informationssystemen gespeicherten Daten über EU-Gelder vollständig, in sich stimmig und zuverlässig sind. Bei der Festlegung der technischen Anforderungen an neue IT-Systeme sollte auch die Fähigkeit zur Datenanalyse zu Betrugsverhütungszwecken berücksichtigt werden*“.

In Anbetracht dessen ist der EDSB der Auffassung, dass die Kombination von Artikel 34 und Abschnitt 7 der Verordnung (EG) Nr. 1828/2006 sowie Kapitel 2.2.3 der Mitteilung der Kommission zur Betrugsbekämpfungsstrategie eine ausreichende Rechtsgrundlage für die Zwecke von Artikel 5 Buchstabe a bieten.

Grundsätzlich dürften die gemeldeten Verarbeitungen auch für Zwecke der Aufdeckung und Verhütung von Betrug erforderlich sein. Ohne Risikoeinstufungen zur Ermittlung der risikoreichsten Projekte und konkreter Risikobereiche mit Hilfe der aus allen Quellen in ARACHNE eingegebenen Informationen für das laufende Monitoring wäre die Kommission kaum in der Lage, im gleichen Umfang Betrug im Bereich der Strukturfonds aufzudecken und zu verhüten. Es sollte jedoch bedacht werden, dass Erforderlichkeit ein relatives Kriterium ist, und die Kommission hat zu gewährleisten, dass eine solche Überwachung nicht über das hinausgeht, was für das angestrebte Ziel angebracht ist und dazu in einem angemessenen Verhältnis steht. Auf diese Aspekte soll weiter unten in Abschnitt 3.4 eingegangen werden.

3.3. Verarbeitung besonderer Datenkategorien

Artikel 10 Absatz 1 untersagt die Verarbeitung personenbezogener Daten, aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von Daten über Gesundheit oder Sexualleben. Die Verarbeitung dieser besonderen Datenkategorien ist untersagt, sofern nicht eine der Ausnahmen gemäß Artikel 10 Absatz 2 greift. Zu berücksichtigen wäre auch Artikel 10 Absatz 4 der Verordnung, der besagt: *„Vorbehaltlich angemessener Garantien können aus Gründen eines wichtigen öffentlichen Interesses andere als die in Absatz 2 genannten Ausnahmen durch die [EU-Verträge] oder andere auf der Grundlage dieser Verträge erlassener Rechtsakte oder, falls notwendig, im Wege einer Entscheidung des Europäischen Datenschutzbeauftragten vorgesehen werden"*.

Der für die Verarbeitung Verantwortliche erwähnt in der Meldung keine der in Artikel 10 Absatz 1 aufgeführten besonderen Datenkategorien[7].

Auch wenn die Verarbeitung besonderer Datenkategorien nicht das Hauptziel der Verarbeitung ist, kann nicht ganz ausgeschlossen werden, dass derartige Daten verarbeitet werden. Bei Verwendung der Sanktionsliste können beispielsweise durchaus politische Meinungen und religiöse oder philosophische Überzeugungen enthüllt werden. Der EDSB weist darauf hin, dass in derartigen Fällen das Verbot gemäß Artikel 10 Absatz 1 einzuhalten oder andernfalls streng zu bewerten ist, ob eine Ausnahme zur Anwendung kommen muss. Die Empfänger sind auf jeden Fall auf diese Vorschrift hinzuweisen und haben die Verarbeitung besonderer Datenkategorien zu vermeiden, sofern nicht eine der in Artikel 10 Absatz 2 oder Artikel 10 Absatz 4 aufgeführten Ausnahmen greift.

Artikel 10 Absatz 5 erlaubt „*die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, [...] nur, wenn sie durch die Verträge [...] oder andere auf der Grundlage dieser Verträge erlassene Rechtsakte oder, falls notwendig, vom Europäischen Datenschutzbeauftragten vorbehaltlich geeigneter besonderer Garantien genehmigt wurde*". Die Verordnung (EG) Nr. 1828/2006 oder auch die anderen in der Meldung als Rechtsgrundlage genannten Rechtsakte enthalten keinen Hinweis darauf, dass die Kommission im Zusammenhang mit Straftaten stehende Daten gemäß Artikel 10 Absatz 5 erhebt oder verarbeitet. Die Mitteilung der Kommission zur Betrugsbekämpfungsstrategie[8] ist zwar kein Rechtsakt, doch setzt sie die der Kommission gemäß Artikel 32 Absatz 4 Buchstabe a der Verordnung (EU) Nr. 966/2012 obliegende Verpflichtung zur „*Umsetzung einer angemessenen Risikomanagement- und*

[7] In der Meldung heißt es im Hinblick auf PEP, ihre Familienangehörigen und ihnen nahestehende Personen: „Es werden keine Daten betreffend die Mitgliedschaft in einer politischen Partei oder andere Daten verarbeitet, deren Verarbeitung gemäß Artikel 10 der Verordnung (EG) Nr. 45/2001 untersagt ist (so kann beispielsweise der Name eines Staatspräsidenten aufgrund dessen offizieller Funktion, nicht jedoch aufgrund seiner Zugehörigkeit zu einer bestimmten politischen Partei verarbeitet werden)…".

[8] In ihrem Kapitel 2.2.3 heißt es ausdrücklich: „Die Kommissionsdienststellen werden prüfen, inwieweit es erforderlich ist, die Betrugsrisikobewertung durch ein systematischeres, formalisiertes Vorgehen bei der Ermittlung von Bereichen, in denen Betrugsrisiken bestehen, zu verbessern. Zugleich sollten sie unter optimaler Nutzung der vorhandenen Ressourcen intelligente Kontrollen durchführen und dabei auf die IT-Werkzeuge zurückgreifen, die von einigen Dienststellen in Zusammenarbeit mit dem OLAF entwickelt worden sind, und diese an ihre Erfordernisse anpassen. Diese Werkzeuge ermöglichen beispielsweise das Zusammentragen aller vorhandenen Daten zu abgeschlossenen oder noch laufenden Projekten, die mit EU-Mitteln finanziert werden. Dies ist nicht nur für die Betrugsbekämpfung nützlich, sondern auch für die Aufdeckung von Plagiaten und betrügerischen Doppelfinanzierungen. Gleichwohl können diese Werkzeuge nur dann in vollem Umfang nützlich sein, wenn die in den betreffenden Informationssystemen gespeicherten Daten über EU-Gelder vollständig, in sich stimmig und zuverlässig sind. Bei der Festlegung der technischen Anforderungen an neue IT-Systeme sollte auch die Fähigkeit zur Datenanalyse zu Betrugsverhütungszwecken berücksichtigt werden".

Kontrollstrategie, die mit allen maßgeblichen Akteuren der Kontrollkette abgestimmt wird" sowie die nach Artikel 60 Buchstabe c der Verordnung (EG) Nr. 1083/2006 bestehende Verpflichtung um, „*die elektronische Aufzeichnung und Erfassung von Buchführungsdaten zu jedem im Rahmen eines operationellen Programms durchgeführten Vorhaben sowie die Erfassung der erforderlichen Durchführungsdaten für Finanzverwaltung, Begleitung, Überprüfungen, Prüfungen und Bewertung zu gewährleisten* ". Auf diese Verpflichtungen wird noch umfassender in Artikel 325 und 317 AEUV eingegangen.

Der EDSB schlägt der Kommission daher vor, eine eigene Rechtsgrundlage zu schaffen (einen Beschluss auf der angemessenen Verwaltungsebene), der die Kommission dazu ermächtigt, Daten im Einklang mit Artikel 10 Absatz 5 in Anwendung der einschlägigen Bestimmungen der Verordnung (EU) Nr. 966/2012 und der Verordnung (EG) Nr. 1083/2006 zu verarbeiten. Die Verarbeitung besonderer Datenkategorien sollte auf jeden Fall auf das zur Einhaltung der gesetzlichen Verpflichtungen aus beiden Verordnungen erforderliche Maß beschränkt werden. Zur Gewährleistung von Erforderlichkeit, Verhältnismäßigkeit und Datenqualität sollten diesbezüglich angemessene Garantien vorgesehen werden (siehe hierzu auch nachstehenden Abschnitt 3.4).

3.4. Auftragsverarbeitung

VADIS SA/NV nimmt als Auftragsverarbeiter die Erhebung und Aufbereitung der Daten vor. Diese Tätigkeit ist in einem schriftlichen Vertrag geregelt, der insbesondere in seinem Anhang I Artikel II.6 vorsieht, dass der Auftragsverarbeiter auf Anweisung des für die Verarbeitung Verantwortlichen tätig wird, und der Klauseln bezüglich der in Artikel 21 und 22 der Verordnung niedergelegten Verpflichtungen des für die Verarbeitung Verantwortlichen enthält (Anhang I Artikel II.6.6).

Grundsätzlich tut die Kommission somit Artikel 23 der Verordnung Genüge. Der EDSB würde jedoch eine Datenschutzklausel ausschließlich zu den Verpflichtungen des Auftragsverarbeiters befürworten. Der Auftragsverarbeiter sollte über die Bedingungen der Verarbeitung seiner Daten durch die Kommission eher im Wege einer Datenschutzerklärung aufgeklärt werden. Für eine Verarbeitung unter Einsatz komplexer Technik könnte außerdem eine gesonderte Datenschutzerklärung von Vorteil sein (siehe z. B. unsere Empfehlung unter Punkt 3.6).

3.5. Qualität der Daten

Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung dürfen personenbezogene Daten nur den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, müssen dafür erheblich sein und dürfen nicht darüber hinausgehen. Das bedeutet auch, dass sie sachlich richtig sein und auf dem neuesten Stand gehalten werden müssen; es müssen alle angemessenen Maßnahmen getroffen werden, damit unrichtige oder unvollständige Daten berichtigt oder gelöscht werden (Artikel 4 Absatz 1 Buchstabe d der Verordnung).

In dem hier zu prüfenden Fall kann man bei einigen Datenkategorien wohl davon ausgehen, dass sie von ausreichend guter Qualität sind, so z. B. bei den Identifizierungsdaten, die die betroffenen Personen selber den Verwaltungsbehörden des ESF und des EFRE gegeben haben (abrufbar in ARACHNE über die SFC2007-Infrastruktur), oder bei den Auszügen aus den Sanktions- und Durchsetzungslisten.

Bei den aus externen öffentlich zugänglichen Quellen stammenden Daten kann davon nicht mit Sicherheit ausgegangen werden. Im Zusammenhang mit der hier zu prüfenden

Verarbeitung stammen sie von zwei kommerziellen Anbietern (die unter anderem auch Zeitungen und Zeitschriften auf risikorelevante Informationen durchsuchen). Hier hat die Kommission mit geeigneten Maßnahmen für ein hohes Maß an sachlicher Richtigkeit zu sorgen.

a) Der EDSB begrüßt das Verfahren der so genannten „Rückkopplungsschleife". Er weist jedoch darauf hin, dass laut Meldung ein ARACHNE-Nutzer, der in den externen Daten auf einen Fehler oder eine Unstimmigkeit stößt, dies *VADIS SA/NV* melden *kann*. Es besteht also augenscheinlich für ARACHNE-Nutzer *keine Verpflichtung* zur Meldung von Fehlern oder Unstimmigkeiten. Dies reicht nicht aus, um ein angemessenes Maß an sachlicher Richtigkeit der personenbezogenen Daten zu gewährleisten. Der EDSB empfiehlt daher, für ARACHNE-Nutzer die Meldung von Fehlern oder Unstimmigkeiten in den externen Daten bei *VADIS SA/NV* verpflichtend zu machen.

b) Bezüglich der Informationen aus externen Medienquellen geht der EDSB davon aus, dass „*die betroffene Person nach der Informationsquelle fragen sollte, wenn sie ihre Rechte <u>über</u> das ARACHNE-System <u>hinaus</u> wahrnehmen möchte*" (Hervorhebung durch uns). Der EDSB räumt ein, dass die Gewährung des Rechts auf Auskunft und Berichtigung im Rahmen des ARACHNE-Systems nicht *über* dieses System *hinausgeht*.

Mit Blick auf die aus externen Medienquellen stammenden Informationen empfiehlt der EDSB jedoch der Kommission, im Rahmen ihrer vertraglichen Beziehung mit dem Auftragsverarbeiter (*VADIS SA/NV*) wirksame Maßnahmen zu entwerfen und umzusetzen, um bei der Datenqualität ein hohes Niveau zu gewährleisten, das über das als „Rückkopplungsschleife" bezeichnete Verfahren hinausgeht. Diese Maßnahmen könnten z. B. folgendermaßen aussehen[9]:

- Personen, die externe Medienquellen überwachen, sollten darin geschult werden, dies im Einklang mit den Datenschutzvorschriften zu tun und dabei vor allem klar und eindeutig den Grundsatz der Zweckbindung anzuwenden;
- Beschreibung, ob und wie zwischen Faktendaten, Meinungsdaten, Intelligence-Daten und den für verschiedene Kategorien betroffener Personen erhobenen Daten unterschieden wird;
- als weitere Maßnahmen wären der Verzicht auf die Verwendung unzuverlässiger Presseberichte und der Abgleich von Informationen aus Presseberichten mit zuverlässigen unabhängigen Quellen vorstellbar.

3.6. Datenaufbewahrung / Datenspeicherung

Wie in Abschnitt 2 dieser Stellungnahme dargestellt, werden die Daten im Einklang mit Artikel 90 der Verordnung (EG) Nr. 1083/2006 drei Jahre aufbewahrt und ist keine Weiterverarbeitung für statistische Zwecke vorgesehen. Vor diesem Hintergrund hat der EDSB keinen Grund zu der Annahme, dass personenbezogene Daten länger, als für die Erreichung der Zwecke, für die die Daten erhoben und/oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die eine Identifizierung betroffener Personen zulässt (Artikel 4 Absatz 1 Buchstabe e der Verordnung). Dessen ungeachtet empfiehlt der EDSB, in dem schriftlichen Vertrag mit *VADIS SA/NV* die Verpflichtung vorzusehen, personenbezogene Daten nach Ablauf der Speicherfrist zu löschen.

[9] Siehe ähnliche Empfehlungen in der Stellungnahme des EDSB im Fall 2012-0326 zur AML-CFT-Datenverarbeitung bei der Europäischen Investitionsbank.

3.7. Datenübermittlung

Übermittlungen von Daten an Empfänger, die der Verordnung unterliegen, sind in Artikel 7 der Verordnung geregelt, Übermittlungen an Empfänger, die den aufgrund der Richtlinie 945/46EG erlassenen nationalen Rechtsvorschriften unterliegen, sind in Artikel 8 der Verordnung geregelt.

- Artikel 7 Absatz 1 besagt, dass Daten innerhalb der Organe oder Einrichtungen der Union oder an andere Organe oder Einrichtungen der Union nur übermittelt werden, wenn die Daten *„für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen*". Übermittlungen gemäß Artikel 7 finden sowohl innerhalb der Kommission als auch an andere Organe oder Einrichtungen der Union statt. Interne Übermittlungen können insoweit vorgenommen werden, als dies für Finanzierungsentscheidungen und interne Kontrollfunktionen erforderlich ist. Der Meldung ist zu entnehmen, dass Übermittlungen an andere Organe und Einrichtungen der EU an OLAF und den Europäischen Rechnungshof erfolgen. Soweit diese Übermittlungen im Zusammenhang mit der Untersuchung konkreter Fälle stehen, fallen sie grundsätzlich unter Artikel 7 Absatz 1 der Verordnung. Es ist jedoch in jedem Einzelfall zu bewerten, ob die Bedingungen für die Übermittlung tatsächlich erfüllt sind.

- Übermittlungen an die Verwaltungsbehörden und ihre zwischengeschalteten Stellen in den Mitgliedstaaten, ihre Bescheinigungsbehörden und die Prüfbehörden unterliegen Artikel 8 der Verordnung. Gemäß Artikel 8 Buchstabe a sind Übermittlungen personenbezogener Daten an solche Empfänger zulässig, „*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 ist".* Diese Bestimmung deckt auch Übermittlungen an solche mitgliedstaatlichen Behörden im Zusammenhang mit der Aufdeckung und Verhütung von Betrug im Einklang mit der Mitteilung der Kommission zur Betrugsbekämpfungsstrategie ab.

Der Meldung ist zu entnehmen, dass keine anderen Übermittlungen gemäß Artikel 9, beispielsweise an Drittländer, geplant sind.

3.8. Auskunfts- und Berichtigungsrecht

Artikel 13 und 14 der Verordnung besagen, dass die betroffene Person das Recht hat, jederzeit Auskunft über die sie betreffenden Daten zu erhalten und diese zu berichtigen.
Die Kommission erwähnt in ihrer Meldung, dass diese Rechte gemäß Artikel 20 Absatz 1 Buchstabe b der Verordnung unter Umständen eingeschränkt werden können. Der EDSB weist darauf hin, dass eine Einschränkung des Rechts auf Auskunft und Berichtigung nur fallweise und nur so lange Anwendung finden darf, wie dies für diesen Zweck *erforderlich* ist. Es sollten angemessene Verfahren eingeführt werden, damit diese Rechte in diesen Fällen ausgeübt werden können. Artikel 20 Absatz 3 der Verordnung ist von der Kommission auf jeden Fall Genüge zu tun: „*Findet eine Einschränkung nach Absatz 1 Anwendung, ist die betroffene Person gemäß dem Gemeinschaftsrecht über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden*."

Laut Datenschutzerklärung wird „*das Recht betroffener Personen auf Auskunft gemäß Artikel 13 fallweise bewertet und wird seine Ausübung aufgeschoben, falls diese Ausübung potenziellen Betrügern die Möglichkeit geben sollte, mögliche Schwachstellen im*

Risikobewertungsprozess zu entdecken und diesen somit zu umgehen. Auskunft wird in solchen Fällen erteilt, wenn kein Audit beschlossen wurde bzw. zum Zeitpunkt des Audits".

In Anbetracht dieser betroffenen Personen gegebenen Erläuterungen nimmt der EDSB das fallweise Vorgehen zur Kenntnis und sieht keinen Anlass zu der Annahme, dass die Kommission das Recht auf Auskunft und Berichtigung länger als erforderlich einschränkt.

3.9. Informationspflicht gegenüber der betroffenen Person

Werden wie im Fall des ARACHNE-Systems die Daten nicht bei der betroffenen Person erhoben, müssen der betroffenen Person gegenüber zumindest folgende Angaben gemacht werden (siehe Artikel 12 der Verordnung):

- Identität des für die Verarbeitung Verantwortlichen
- Zwecke der Verarbeitung
- Empfänger oder Empfängerkategorien
- Kategorien erhobener Daten
- Bestehen des Auskunfts- und Berichtigungsrechts
- Rechtsgrundlage der Verarbeitung
- Aufbewahrungsfristen
- das Recht, sich an den EDSB zu wenden
- die Herkunft der Daten; ausgenommen sind Fälle, in denen der für die Verarbeitung Verantwortlich aus Gründen der Geheimhaltung diese Herkunft nicht offenlegen kann.

Bezüglich der Wege, auf denen diese Informationen bereitgestellt werden, ist der EDSB der Ansicht, dass die Einstellung der Datenschutzerklärung in die Website des Europäischen Sozialfonds für sich genommen nicht gewährleistet, dass betroffene Personen diese Informationen auch wirklich erhalten. Denn vermutlich lesen nicht alle potenziell betroffenen Personen die auf die Website gestellten Informationen. Nach Ansicht des EDSB sollte diese Veröffentlichung nach Möglichkeit durch eine eher individuelle Vermittlung der nach Artikel 11 und 12 der Verordnung erforderlichen Angaben ergänzt werden.

Stammen Daten von den Verwaltungsbehörden von ESF und EFRE (über die SFC2007-Infrastruktur), wurden sie zuvor zumindest teilweise bei den betroffenen Personen erhoben. Der EDSB empfiehlt daher, an dieser Stelle die in Artikel 12 der Verordnung geforderten erforderlichen Angaben bereitzustellen.

3.10. Automatisierte Einzelentscheidungen

Artikel 19 der Verordnung lautet: „*Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die für sie rechtliche Folgen nach sich zieht oder sie erheblich beeinträchtigt und die ausschließlich aufgrund einer automatischen Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens, es sei denn, die Entscheidung ist ausdrücklich aufgrund einzelstaatlicher oder gemeinschaftlicher Rechtsvorschriften zulässig oder wird, falls notwendig, vom Europäischen Datenschutzbeauftragten ausdrücklich genehmigt. In beiden Fällen müssen Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person getroffen werden wie etwa Gewährleistung der Möglichkeit, ihren Standpunkt geltend zu machen*".

Wie es in der Meldung heißt und auch auf der Sitzung vom 9. Januar 2014 ausdrücklich bestätigt wurde, werden keine automatisierten Entscheidung ausschließlich auf der Grundlage

der von ARACHNE berechneten Risikoindikatoren getroffen, da das System nicht automatisch den Schluss zulässt, dass etwas falsch oder irregulär ist[10].

3.11. Sicherheitsmaßnahmen

(...)

4. SCHLUSSFOLGERUNG

Es besteht kein Grund zu der Annahme, dass die Bestimmungen der Verordnung (EG) Nr. 45/2001 verletzt werden, sofern die in dieser Stellungnahme enthaltenen Erwägungen vollständig berücksichtigt werden. Die Kommission sollte insbesondere

- eine eigene Rechtsgrundlage in Erwägung ziehen (einen Beschluss auf der angemessenen Verwaltungsebene), der die Kommission dazu ermächtigt, Daten im Einklang mit Artikel 10 Absatz 5 in Anwendung der einschlägigen Bestimmungen der Verordnung (EU, Euratom) Nr. 966/2012 und der Verordnung (EG) Nr. 1083/2006 zu verarbeiten. Die Verarbeitung besonderer Datenkategorien sollte auf jeden Fall auf das zur Einhaltung der gesetzlichen Verpflichtungen aus beiden Verordnungen erforderliche Maß beschränkt werden. Zur Gewährleistung von Erforderlichkeit, Verhältnismäßigkeit und Datenqualität sollten diesbezüglich angemessene Garantien vorgesehen werden;
- im Zusammenhang mit der „Rückkopplungsschleife“ für ARACHNE-Nutzer die Meldung entdeckter Fehler oder Unstimmigkeiten in den externen Daten an *VADIS SA/NV* verpflichtend zu machen;
- gemäß den Empfehlungen in Abschnitt 3.4 wirksame Maßnahmen ausarbeiten und umsetzen, mit denen ein hohes Maß an Datenqualität bei den aus externen Medienquellen gewonnenen Informationen gewährleistet wird;
- gewährleisten, dass Übermittlungen an OLAF und den Europäischen Rechnungshof gemäß Artikel 7 der Verordnung nach einer fallweisen Prüfung erfolgen;
- in den schriftlichen Vertrag mit *VADIS SA/NV* die Verpflichtung zum Löschen personenbezogener Daten nach Ablauf der Speicherfrist aufnehmen;
- für von den Verwaltungsbehörden von ESF und EFRE stammende Daten (über die SFC2007-Infrastruktur) der Informationspflicht über die Verarbeitung im ARACHNE-System nachkommen, wie in Artikel 12 der Verordnung vorgesehen, in dem es um nicht bei der betroffenen Person erhobene Daten geht;
- die Nutzerverwaltungsprozesse und alle vom ARACHNE-System verwendeten Nutzerkonten überprüfen und den Mitgliedstaaten Leitlinien für eine kohärente Nutzerverwaltung an die Hand geben.

Brüssel, den 17. Februar 2014

(fall)

Giovanni Buttarelli

[10] In der Meldung heißt es weiter ausdrücklich: „die Logik, die zum Ergebnis der Risikobewertung geführt hat, wird nicht offengelegt. Dies bedeutet jedoch keine Einschränkung von Artikel 13, da Entscheidungen nur vom System unterstützt, aber nicht von ihm automatisiert werden“.