Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Investitionsbank für eine Vorabkontrolle der Verarbeitung von AML-CFT-Daten

Brüssel, 7. Februar 2013 (Fall 2012-0326)

1. VERFAHREN

Am 3. April 2012 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) vom Datenschutzbeauftragten (**DSB**) der Europäischen Investitionsbank (**EIB**) eine Meldung für eine Vorabkontrolle der Verarbeitung personenbezogener Daten „AML-CFT".

Der Meldung waren zur Information folgende Unterlagen beigefügt:

- Draft Compliance Policy on Counterparty Acceptance and Monitoring, Covering Integrity, Money Laundering and Financing of Terrorism (Integrity and AML-CFT Policy) (Entwurf einer Strategie für die Einhaltung der Vorschriften über die Akzeptanz und Überwachung von Gegenparteien in Bezug auf Integrität, Geldwäsche und Terrorismusfinanzierung (Strategie Integrität und AML-CFT) [und dazugehörende Unterlagen];
- [...]
- Kodex für gute Verwaltungspraxis in den Beziehungen der Mitarbeiter der Europäischen Investitionsbank zur Öffentlichkeit.

Am 13. April 2012 wurden dem DSB der EIB Fragen übermittelt, die dieser am 23. Mai 2012 beantwortete; seinen Antworten waren folgende weitere Unterlagen beigefügt:

- Integritätscharta der EIB;
- Baseler Ausschuss für Bankenaufsicht: „Compliance and the Compliance Function in Banks";
- Satzung der EIB;
- Auszug aus dem Bericht 2009 des Prüfungsausschusses an den Rat der Gouverneure;
- Auszug aus dem Bericht 2010 des Prüfungsausschusses an den Rat der Gouverneure;
- []
- AML-CFT-Fragebogen;
- Compliance Procedure on Counterparty Acceptance and Monitoring, Covering Integrity, Money Laundering and Financing of Terrorism (Integrity and AML-CFT Policy) (Compliance-Verfahren für die Akzeptanz und Überwachung von Gegenparteien in Bezug auf Integrität, Geldwäsche und Terrorismusfinanzierung (Strategie Integrität und AML-CFT) [und dazugehörende Unterlagen];
- [...]

Weitere Fragen wurden am 26. Juni, 6. August und 8. Oktober 2012 übermittelt; die Antworten gingen am 30. Juli, 1. Oktober bzw. 5. Dezember 2012 ein. Der Entwurf der Stellungnahme wurde dem DSB am 6. Dezember 2012 zur Kommentierung übersandt. Am

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

15. Januar 2013 ging beim EDSB eine Antwort ein; daraufhin wurde für den 4. Februar 2013 eine Sitzung zwischen EIB und EDSB anberaumt.

2. SACHVERHALT

In Anwendung bewährter Praktiken im Bankwesen bei der Bekämpfung von Geldwäsche (AML) und Terrorismusfinanzierung (CFT, zusammen AML-CFT) und zur Minimierung der Risiken für Integrität und Ansehen führt die EIB-Gruppe (bestehend aus der Europäischen Investitionsbank und dem Europäischen Investitionsfonds) bezüglich ihrer (künftigen) Geschäftspartner eine sorgfältige Prüfung (Counterparty Due Diligence (CDD)) durch.

Vor der Aufnahme neuer Geschäftsbeziehungen führt die EIB einen „Counterparty Acceptance Process" zur Prüfung der Frage durch, ob hierdurch eines der vorstehend genannten Risiken entstehen könnte. Gegenparteien, bei denen *a priori* keine besonderen Bedenken bezüglich der Integrität bestehen, werden einer vereinfachten CDD unterzogen. Dies gilt beispielsweise für Gegenparteien wie Kredit- oder Finanzinstitute innerhalb der Best Practice Area[1], in der Best Practice Area notierte Unternehmen oder Behörden. Bei Geschäften oder Geschäftsbeziehungen hingegen, die gemäß Risikobewertung durch das Office of the Chief Compliance Officer (**OCCO**) und den Grundsätzen der EU-Richtlinien über AML-CFT[2] mit hohem Risiko behaftetet sind, ist eine intensivere Due-Diligence-Prüfung erforderlich. In derartigen Fällen können zusätzliche Informationen angefordert werden. Dies gilt beispielsweise, wenn es um politisch exponierte Personen (PEP), Wohltätigkeitsorganisationen, Vorgänge mit hohem Compliance-Risiko usw. geht.

Die Ergebnisse dieses Prozesses fließen in die Compliance-Kontrolle bei neuen Projekten ein und können die Ablehnung von Gegenparteien oder zusätzliche Compliance-Anforderungen in den zu unterzeichnenden Verträgen zur Folge haben. Die Verarbeitung läuft an, wenn ein EIB-Beamter die Aufnahme geschäftlicher Beziehungen zu einer neuen Gegenpartei in Erwägung zieht.

Nach Aufnahme einer Geschäftsbeziehung läuft die Überwachung der Gegenparteien weiter, um die Frage beantworten können, ob die Erstbewertung überprüft werden muss („kontinuierliche Überwachung der Beziehung zur Gegenpartei").

Für die Verarbeitung Verantwortlicher ist die Europäische Investitionsbank mit dem bereits genannten OCCO als Kontaktstelle.

Betroffene Personen sind Personen, die unmittelbar oder mittelbar Eigentümer[3] juristischer Personen sind, mit denen die EIB im Rahmen der Finanzierung von Projekten Geschäftsbeziehungen unterhält oder aufzunehmen beabsichtigt, sowie Personen, die in diesen juristischen Personen geschäftsführend tätig sind („Counterparty Key Persons"). Dabei handelt es sich um Personen in Schlüsselpositionen (z. B. Präsident, Vorstandsvorsitzender) und Mitglieder von Lenkungsorganen (Vorstand, Verwaltungsausschuss, Aufsichtsrat, Gemeinderat oder Gleichwertiges) der Gegenpartei.

[1] [...]
[2] [...]
[3] Dieser Begriff sollte als deckungsgleich mit der Definition des „wirtschaftlichen Eigentümers" in Artikel 3 Absatz 6 der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (ABl. L 309 vom 25.11.2005, S. 15) betrachtet werden.

Ist eine Person aus den genannten Kategorien zufälligerweise eine PEP, gilt dies als Anzeichen für erhöhtes Risiko. PEP sind in Artikel 3 Absatz 8 der Richtlinie 2005/60/EG definiert als[4] „*natürliche Personen, die wichtige öffentliche Ämter ausüben oder ausgeübt haben, und deren unmittelbare Familienmitglieder oder ihnen bekanntermaßen nahe stehende Personen*". Nähere Erläuterungen hierzu finden sich in Artikel 2 der Richtlinie 2006/70/EG der Kommission.[5] Gemäß diesem Artikel bezieht sich der Ausdruck „Personen, die wichtige öffentliche Ämter ausüben oder ausgeübt haben" (ohne zeitliche Begrenzung) auf Staatschefs, Regierungschefs, Minister, stellvertretende Minister und Staatssekretäre, Parlamentsmitglieder, Mitglieder von obersten Gerichten, Verfassungsgerichten oder sonstigen hochrangigen Institutionen der Justiz, gegen deren Entscheidungen, von außergewöhnlichen Umständen abgesehen, kein Rechtsmittel eingelegt werden kann, Mitglieder der Rechnungshöfe oder der Vorstände von Zentralbanken, Botschafter, Geschäftsträger und hochrangige Offiziere der Streitkräfte sowie Mitglieder der Verwaltungs-, Leitungs- oder Aufsichtsorgane staatlicher Unternehmen. „*Familienmitglieder*" sind definiert als Eltern, Ehepartner (oder Gleichgestellte), Kinder und deren Partner. „*Nahe stehende Personen*" sind definiert als jede natürliche Person, die mit einer PEP gemeinsame wirtschaftliche Eigentümerin von Rechtspersonen und Rechtsvereinbarungen ist oder wirtschaftliche Eigentümerin einer Rechtsperson oder Rechtsvereinbarung ist, die tatsächlich zum Nutzen einer PEP errichtet wurde. Mit diesen Bestimmungen sollen auch gleichwertige Situationen auf EU- oder internationaler Ebene erfasst werden.

Gemäß Meldung werden im „Counterparty Acceptance Process" folgende **Datenkategorien** erhoben:

- Identifizierungsdaten;
- Daten im Zusammenhang mit Straftaten, Untersuchungen, strafrechtlichen Ermittlungen und öffentlichen Strafregistern;
- Geschäftsbeziehungen.

Diese Daten werden teilweise unmittelbar bei den betroffenen Personen erhoben, stammen teilweise aber auch aus anderen Quellen wie Zeitungen, Spezialdatenbanken des privaten Sektors und Websites. Die beiden letztgenannten Quellen können neue Berichte über (mutmaßlich) gesetzwidriges Verhalten beinhalten.

Im Folgenden eine detaillierte **Beschreibung der Verarbeitung**: Im Verlauf des **Counterparty Acceptance Process** erhobene Daten werden von dem das betreffende EIB-Geschäft betreuenden Sachbearbeiter verwendet, um [die Gegenpartei zu Compliance-Zwecken zu beurteilen]. [Sachbearbeiter befassen sich mit Aspekten wie] der Identität und dem Hintergrund der Gegenpartei und des betreffenden Geschäfts. Unter anderem [wird geprüft,] ob die Gegenpartei oder Schlüsselpersonen der Gegenpartei gesetzwidriger oder schädlicher/rufschädigender Aktivitäten oder zweifelhafter Praktiken beschuldigt wurden[6], ob ihr Vermögen aus ungesetzlichen Tätigkeiten stammen könnte, oder ob sie ein unangemessenes Geschäftsgebaren an den Tag legen.

[Des Weiteren ist der Frage nachzugehen,] ob ihr Name auf einschlägigen Sanktionslisten steht, ob die zuständigen Behörden gegen sie straf- oder verwaltungsrechtliche Ermittlungen eingeleitet haben, ob sie vorbestraft sind oder strafrechtlich verurteilt wurden, ob Sanktionen gegen sie verhängt oder große Zivilverfahren gegen sie anhängig sind, oder ob sie andere Bedenken bezüglich ihrer Integrität aufwerfen, die dem Ansehen der EIB abträglich sein könnten. Diese [Beurteilung] soll bei der Bewertung des Risikos von Geldwäsche,

[4] Oben zitiert.
[5] ABl. L 214 vom 4.8.2006, S. 29.
[6] [...]

Terrorismusfinanzierung und anderer Compliance-Risiken gemäß der Integritätscharta der EIB[7] und dem Papier über Compliance und die Compliance-Funktion in Banken[8] des Baseler Ausschusses für Bankenaufsicht helfen.

Wird eine dieser Fragen mit „Ja“ beantwortet, ist das OCCO anzuhören. Das OCCO gibt dann eine Stellungnahme zu dem durch die Gegenpartei entstehenden Risiko ab, die in den Bericht an das Direktorium einfließt oder parallel dazu vorgelegt wird, bevor dieses die Geschäftsbeziehung billigt. Diese Berichte können Empfehlungen enthalten, beispielsweise betreffend die Aufnahme von Integritätsklauseln in den Vertrag, denen zufolge die Gegenpartei verpflichtet ist, mit Sanktionen belegte und/oder strafrechtlich verurteilte Führungskräfte oder Mitarbeiter zu entlassen, oder die Verpflichtung, über die Ergebnisse von Untersuchungen und die Einhaltung von Vorschriften einschlägiger Behörden Bericht zu erstatten.

Bei manchen Gegenparteien[9] kann eine vereinfachte Prüfung (Simplified Due Diligence („SDD“)) durchgeführt werden, sofern keine konkreten Bedenken bezüglich ihrer Integrität bestehen. In diesem Fall gelten weniger strenge Dokumentationsanforderungen.[10] Geschäfte, die als mit einem höheren Risiko behaftet eingestuft werden, werden einer Enhanced Due Diligence („EDD“) unterzogen. Eine solche Einstufung kann beispielsweise vorgenommen werden, wenn PEP beteiligt sind. Das bedeutet, dass das OCCO neben den bereits erwähnten Kontrollen die Durchführung zusätzlicher Kontrollen empfiehlt. So kann unter anderem verlangt werden, dass Counterparty Key Persons Identitätsdokumente vorlegen, dass der wirtschaftliche Eigentümer und/oder die PEP die Herkunft ihres Vermögens mit Unterlagen belegen, und dass der wirtschaftliche Eigentümer und/oder die PEP einen Lebenslauf oder eine Interessenerklärung vorlegen.

Nach Herstellung einer Geschäftsbeziehung können Gegenparteien **kontinuierlich überwacht** werden. Hierbei werden durch regelmäßige Überprüfungen die im Verlauf des Counterparty Acceptance Process erhobenen Daten auf den neuesten Stand gebracht. Solche Überprüfungen werden vor der ersten Zahlung, vor weiteren Zahlungen, wenn die letzte Zahlung mehr als ein Jahr zurückliegt, und danach im Allgemeinen einmal pro Jahr vorgenommen. Außerdem halten die EIB-Beamten, die den Kontakt zu den Gegenparteien halten, Ausschau nach diese betreffenden möglichen Problemen oder Gerüchten oder bestimmten Warnzeichen. Abgesehen von der Frage, ob bestimmte Vorgänge aus dem üblichen Muster herausfallen, oder ob es vor kurzem Änderungen bei den Eigentumsverhältnissen gegeben hat, wird auch der Frage nachgegangen, ob Gegenparteien (oder Personen, die öffentlich mit ihnen in Verbindung gebracht werden) einen fragwürdigen Hintergrund haben, oder ob es neue Berichte über sie gibt, denen zufolge sie möglicherweise gegen straf- oder zivilrechtliche Bestimmungen oder andere Vorschriften verstoßen haben. Bei Vorliegen solcher Warnhinweise wird das OCCO informiert. Sind PEP beteiligt, wird jährlich[11] überprüft, ob ihnen weitere öffentliche Ämter übertragen wurden, die Bedenken bezüglich ihrer Integrität hervorrufen könnten, und ob gegen sie wegen gesetzwidriger Aktivitäten strafrechtliche Ermittlungen oder Untersuchungen durchgeführt wurden. Auch Schlüsselpersonen von Gegenparteien werden darauf überwacht, ob sie politisch exponierte

[7] Abrufbar unter:http://www.eib.org/attachments/general/occo_charter_en.pdf.
[8] Abrufbar unter:http://www.bis.org/publ/bcbs113.pdf.
[9] Kredit- oder Finanzinstitute in der Best Practice Area [], notierte Unternehmen, deren Wertpapiere zum Handel auf einem regulierten Markt in der Best Practice Area zugelassen sind, Behörden oder andere Gegenparteien, die die technischen Kriterien in Artikel 40 Absatz 1 Buchstabe b der Richtlinie 2005/60/EG erfüllen.
[10] Dies bezieht sich im Wesentlichen auf die Dokumentationsanforderungen für juristische Personen.
[11] Oder häufiger, sofern das OCCO dies empfiehlt.

Personen geworden sind oder, falls sie bereits politisch exponierte Personen sind, ob sie bei der Gegenpartei eine andere Aufgabe übernommen haben.

Daten, die im Verlauf des Counterparty Acceptance Process und bei der kontinuierlichen Überwachung von Gegenparteien erhoben werden, können an die Mitglieder der leitenden Organe der EIB, interne Dienststellen der EIB, Organe und Einrichtungen der EU (insbesondere OLAF) und nationale zentrale Meldestellen für Geldwäsche (FIU) **übermittelt** werden. Übermittlungen an externe Stellen erfolgen entweder auf Ersuchen des Empfängers oder auf Initiative der EIB an nationale FIU, falls Verdacht auf Geldwäsche oder Terrorismusfinanzierung besteht. Übermittlungen an Drittländer sind nicht vorgesehen.

Betroffene Personen werden über die Verarbeitung in einem Abschnitt auf unterschiedliche Weise **informiert**. Das Verfahren für Integrität und AML-CFT besagt, dass *„der Bank* [in diesem Zusammenhang] *eingereichte personenbezogene Daten im Einklang mit der Verordnung (EG) Nr. 45/2001 verarbeitet werden"* und dass sie *„unter der Aufsicht des Chef-Compliance Officer der EIB-Gruppe (GCCO) verarbeitet und nur für die AML-CFT-Zwecke der EIB verwendet werden"*. Gemäß dem Verfahren haben betroffene Personen das Recht auf *„Auskunft über diese Daten und deren Berichtigung und Sperrung"* und können sie *„ihre Rechte jederzeit ausüben, indem sie sich an das OCCO und/oder den Europäischen Datenschutzbeauftragten wenden"*. Das Verfahren enthält ferner eine allgemeine Beschreibung der Schritte, die die EIB im Verlauf des Counterparty Acceptance Process unternimmt. Lauf Meldung bearbeitet der für die Verarbeitung Verantwortliche Anträge auf Löschung und Sperrung innerhalb von 30 Arbeitstagen. Das Verfahren für Integrität und AML-CFT ist auf der EIB-Website öffentlich zugänglich. Finanzverträge werden eine Klausel über die Anwendbarkeit der Verordnung enthalten[12]. Die EIB hat ferner angekündigt, einen „Ad hoc-Hinweis" über die Einhaltung der Verordnung (EG) Nr. 45/2001 zu veröffentlichen.

Die Daten werden zehn Jahre nach Beendigung der Geschäftsbeziehung **aufbewahrt**. Eine Weiterverarbeitung für wissenschaftliche oder statistische Zwecke ist nicht vorgesehen.

Die Daten werden elektronisch in einem beschränkten Bereich der EIB-Server im Einklang mit allgemeinen **Sicherheitsvorschriften** der EIB (z. B. Verhaltenskodex für Mitarbeiter, IT-Standards und Passwortvorschriften) gespeichert. Die Papierfassungen werden in verschlossenen Schränken des OCCO aufbewahrt, zu denen nur eigens befugte Mitarbeiter des OCCO Zugang haben.

3. RECHTLICHE ANALYSE

3.1. Vorabkontrolle

Die gemeldeten Verarbeitungsvorgänge sind eine Verarbeitung personenbezogener Daten (*„alle Informationen über eine bestimmte oder eine bestimmbare natürliche Person"* – 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.

[12] Die Klausel lautet folgendermaßen: „Die Verarbeitung personenbezogener Daten durch die Bank erfolgt im Einklang mit den geltenden Rechtsvorschriften der Europäischen Union über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und den freien Datenverkehr".

In Artikel 27 Absatz 1 der Verordnung ist festgelegt, dass „*Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können*“ vom EDSB vorab kontrolliert werden. Artikel 27 Absatz 2 der Verordnung enthält eine Liste der Verarbeitungen, die solche Risiken beinhalten können. 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.

Wie bereits in Kapitel 2 beschrieben, können Daten über Verdächtigungen bzw. Straftaten verarbeitet werden (Artikel 27 Buchstabe a). Ziel des Counterparty Acceptance Process ist es, die Persönlichkeit der betroffenen Personen und hier vor allem ihr Verhalten im Hinblick darauf zu bewerten (Artikel 27 Buchstabe b), ob sie ein Risiko bezüglich AML-CFT oder Integrität/Ansehen darstellen. Es lässt sich auch nicht ausschließen, dass bei den Überprüfungen durch EIB-Beamte vor Abschluss eines Vertrags eine Verknüpfung von personenbezogenen Daten hergestellt wird, die ursprünglich zu unterschiedlichen Zwecken verarbeitet wurden (Artikel 27 Buchstabe c). Schließlich kann die Verarbeitung durchaus zum Ausschluss natürlicher Personen von einem Recht, einer Leistung oder einem Vertrag führen (Artikel 27 Buchstabe d). Aus allen diesen Gründen ist die Verarbeitung einer Vorabkontrolle zu unterziehen.

Eine Vorabkontrolle gemäß Artikel 27 der Verordnung sollte grundsätzlich vor Aufnahme der Verarbeitung durchgeführt werden. Im Schriftwechsel mit dem EDSB wurde klargestellt, dass das gemeldete Verfahren *„der Reorganisation, Vervollständigung und Modernisierung der teilweise schon zuvor bestehenden Compliance-Aktivitäten der EIB, ihrer Straffung und der Steigerung ihrer Effizienz dient“*. Es wurde ferner unterstrichen, dass dies dem EDSB bereits in einer früheren Meldung im Jahr 2007 dargelegt worden war. Unabhängig davon, ob die EIB diese Verarbeitung bereits gemeldet hatte oder nicht, bleibt die Tatsache, dass die gemeldete Verarbeitung bei der EIB schon vor der Meldung bestand, wenn auch in einer anderen, weniger strukturierten Form. Die hier vorgenommene Vorabkontrolle ist also keine echte Vorabkontrolle, sondern eher eine Ex-post-Vorabkontrolle. Der EDSB bedauert sehr, dass in diesem Fall die Meldung bei ihm nicht rechtzeitig, also vor Aufnahme der Verarbeitung, eingereicht wurde. Sämtliche im Zusammenhang mit dieser Stellungnahme ausgesprochenen Empfehlungen sind dessen ungeachtet von dem für die Verarbeitung Verantwortlichen ordnungsgemäß umzusetzen.

Die Meldung des DSB ging am 3. April 2012 ein. Weitere Fragen wurden am 13. April, 26. Juni, 6. August und 8. Oktober 2012 übermittelt; die Antworten gingen am 23. Mai, 30. Juli, 1. Oktober und 5. Dezember 2012 ein. Der Entwurf der Stellungnahme wurde dem DSB am 6. Dezember 2012 zur Kommentierung vorgelegt; seine Bemerkungen gingen beim EDSB am 15. Januar 2013 ein. Nach diesen Antworten wurde für den 4. Februar 2013 eine Sitzung anberaumt. Gemäß Artikel 27 Absatz 4 der Verordnung hat der EDSB seine Stellungnahme innerhalb von zwei Monaten abzugeben. Der Fall wurde für insgesamt 248 Tage ausgesetzt. Unter Berücksichtigung aller Aussetzungszeiträume muss die Stellungnahme daher spätestens am 11. Februar 2013 angenommen werden.

3.2. Rechtmäßigkeit der Verarbeitung

Gemäß der Meldung beruht die Rechtmäßigkeit der Verordnung auf Artikel 5 Buchstabe a und b der Verordnung. Gemäß Artikel 5 Buchstabe a 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.[13] Im Hinblick auf Artikel 5 Buchstabe b ist zu prüfen, ob der für die Verarbeitung Verantwortliche einer rechtlichen Verpflichtung zur Erhebung und Verarbeitung von Daten unterliegt, die ihm keinen Ermessensspielraum lässt.[14] Das Erfordernis einer rechtlichen Verpflichtung gemäß Artikel 5 Buchstabe b ist offenkundig stärker als das Erfordernis einer Rechtsgrundlage gemäß Artikel 5 Buchstabe a, da normalerweise eine konkrete Verpflichtung gefordert wird, die dem für die Verarbeitung Verantwortlichen keine andere Wahl lässt, als die Daten zu verarbeiten.

3.2.1. Artikel 5 Buchstabe a

3.2.1.2. Von der EIB angeführte Rechtsgrundlagen

In der Meldung führte der für die Verarbeitung Verantwortliche eine Reihe möglicher Rechtsgrundlagen an, ohne jedoch darauf einzugehen, welche die Rechtmäßigkeit gemäß Artikel 5 Buchstabe a oder b belegt. Es handelt sich hierbei um Artikel 67 Absatz 3, Artikel 75, Artikel 215 und Artikel 325 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), das Protokoll Nr. 5 zum Vertrag (Satzung der EIB), insbesondere dessen Artikel 16 und Artikel 18 Absatz 1, die Richtlinien 2005/60/EG und 2006/70/EG sowie die *„im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU angenommenen Beschlüsse und Verordnungen des Rates“*. Wie nachstehend erörtert, sind mehrere dieser Bestimmungen keine angemessene Rechtsgrundlage für die gemeldete Verarbeitung.

Artikel 67 Absatz 3 AEUV ist eine allgemeine Bestimmung über den Raum der Freiheit, der Sicherheit und des Rechts, der zufolge die Union *„darauf hinwirkt,* [...] *Kriminalität zu verhüten und zu bekämpfen“*. Diese Bestimmung ist zu allgemein gehalten, als dass sie unmittelbar als Rechtsgrundlage für die Verarbeitungen durch die EIB gemäß Artikel 5 Buchstabe a herangezogen werden könnte. So würden beispielsweise betroffene Personen nicht erfassen können, in welchem Umfang personenbezogene Daten über sie erhoben und weiter verarbeitet werden könnten. Darüber hinaus wird bei den gemeldeten Verarbeitungsvorgängen auch das durch betroffene Personen entstehende „Reputationsrisiko“ bewertet, das an einen „Straftatbestand“ nicht heranreicht.

Artikel 325 Absatz 1 AEUV besagt: *„Die Union und die Mitgliedstaaten bekämpfen Betrügereien und sonstige gegen die finanziellen Interessen der Union gerichtete rechtwidrige Handlungen mit Maßnahmen nach diesem Artikel, [...]“*. Im weiteren Verlauf des Artikels werden die Aufgaben der Kommission und der Mitgliedstaaten aufgeführt und die Mitgesetzgeber der Union ermächtigt, die zu diesem Zweck erforderlichen Maßnahmen zu ergreifen. Abgesehen von der allgemeinen Bestimmung in Absatz 1 findet sich kein Hinweis

[13] 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“.

[14] Gemäß Artikel 5 Buchstabe b muss die „Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich sein, der der für die Verarbeitung Verantwortliche unterliegt“.

auf konkrete Maßnahmen. Wie schon bei Artikel 67 Absatz 3 AEUV gilt auch hier, dass die Bestimmung zu allgemein gefasst ist, als dass sie allein unmittelbar als Rechtsgrundlage für die Verarbeitungen durch die EIB im Bereich AML-CFT-gemäß Artikel 5 Buchstabe a herangezogen werden könnte.

Der für die Verarbeitung Verantwortliche bezieht sich ferner auf Artikel 75 und Artikel 215 AEUV. Diese beiden Bestimmungen ermächtigen die Union dazu, Rechtsvorschriften über das Einfrieren von finanziellen Vermögenswerten zu erlassen, erlauben aber selber nicht das Einfrieren finanzieller Vermögenswerte oder verlangen auch nicht, dass bei Kunden überprüft wird, ob sie auf einer Sanktionsliste stehen. Die Verarbeitungen durch die EIB können sich daher nicht unmittelbar auf diese Bestimmungen des Vertrags stützen. Die auf der Grundlage dieser Bestimmungen angenommenen Verordnungen und Beschlüsse können andererseits durchaus die Rechtsgrundlage für einen Teil der gemeldeten Verarbeitungen bilden, nämlich für die Kontrollen der EIB, mit denen überprüft werden soll, ob die Gegenpartei auf einer relevanten Sanktionsliste steht.[15] Sie decken jedoch nicht die anderen Teile der Verarbeitung im Zusammenhang mit AML-CFT und Reputationsrisiken ab. Ein Verweis auf eine solche Bestimmung kann also nicht als ausreichende Rechtfertigung der Verarbeitung insgesamt gelten, sondern nur eines Teils.

Mit Blick auf umfassendere europäische Rechtsvorschriften im Bereich AML-CFT nennt der für die Verarbeitung Verantwortliche in der Meldung die Richtlinien 2005/60/EG und 2006/70/EG als mögliche Rechtsgrundlagen. In diesen Richtlinien wird der rechtliche Rahmen zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung abgesteckt („AML-CFT-Richtlinien"). Wie alle Richtlinien sind sie an die Mitgliedstaaten gerichtet und daher auf die EIB nicht unmittelbar anwendbar. Richtlinien sind generell nicht unmittelbar anwendbar, da sie in den Mitgliedstaaten in einzelstaatliches Recht umgesetzt werden müssen. Der EDSB schließt daher aus, dass die AML-CFT-Richtlinien *unmittelbar* eine Rechtsgrundlage für die hier zu prüfenden Verarbeitungen sein können.

Zusammenfassend kann festgehalten werden, dass die von dem für die Verarbeitung Verantwortlichen in der Meldung erwähnten Rechtsgrundlagen für den Zweck von Artikel 5 Buchstabe a der Verordnung kaum geeignet sein dürften. Nachstehend geht der EDSB auf die möglichen Rechtsgrundlagen ein, die die Verarbeitung legitimieren könnten.

3.2.1.3. Mögliche Rechtsgrundlagen

Nach Auffassung des EDSB muss die Rechtsgrundlage für den Zweck von Artikel 5 Buchstabe a in Rechtsvorschriften gesucht werden, die auf die EIB unmittelbar angewandt werden, wie beispielsweise der Satzung und den von EIB-Organen auf der Grundlage dieser Satzung angenommenen Vorschriften. So heißt es insbesondere in Artikel 18 Absatz 1 der

[15] Insgesamt sind rund 20 Verordnungen in Kraft, die sich auf Artikel 215 AEUV oder andere, ältere Rechtsgrundlagen stützen, und die restriktive Maßnahmen einschließlich des Einfrierens finanzieller Vermögenwerte regeln. Die Bestimmungen dieser Verordnungen weichen zwar leicht voneinander ab, doch enthalten alle auf diesen Artikeln fußenden Rechtsakte Bestimmungen, die sich weitgehend an Artikel 2 der Verordnung (EG) Nr. 881/2002 anlehnen, der besagt: „Alle Gelder und wirtschaftlichen Ressourcen, die einer [...] natürlichen oder juristischen Person, Gruppe oder Organisation gehören oder in deren Eigentum stehen oder von ihr verwahrt werden, werden eingefroren". Weiter heißt es dort, dass den aufgeführten Personen oder Organisationen „weder direkt noch indirekt Gelder oder wirtschaftlichen Ressourcen zur Verfügung gestellt werden oder ihnen zugutekommen dürfen". Werden solchen Personen oder Organisationen dessen ungeachtet Gelder zur Verfügung gestellt, werden gegen die hierfür Verantwortlichen Sanktionen wie beispielsweise Geldbußen verhängt, es sei denn „sie wussten nicht und hatten keinen Grund zu der Annahme", dass sie mit ihrem Handeln gegen diese Bestimmungen verstoßen (Artikel 2 Absatz 4 der Verordnung (EG) Nr. 881/2002).

Satzung der EIB, dass die EIB *„auf die wirtschaftlich zweckmäßigste Verwendung ihrer Mittel im Interesse der Union achtet“*. Dieser Grundsatz bedeutet für die EIB, dass sie unter anderem zu gewährleisten hat, dass ihre Ressourcen nicht für Geldwäsche oder Terrorismusfinanzierung verwendet werden. Auch die Verwendung von Mitteln für Gegenparteien, die ein Risiko für Integrität oder Ansehen darstellen, widerspräche dem Ziel der wirtschaftlich zweckmäßigsten Verwendung der Mittel im Interesse der Union. Derartige Geschäfte würden sich nachteilig auf das Ansehen der EIB als einer öffentlichen Einrichtung auswirken, die EU-Gelder verwaltet, und würden das Ansehen der Bank selbst beschädigen.

Artikel 12 der EIB-Satzung beauftragt den Prüfungsausschuss damit, zu prüfen, *„ob die Tätigkeit der Bank mit den bewährtesten Praktiken im Bankwesen im Einklang steht“*. Überprüfungen im Bereich AML-CFT (also CDD) gehören zweifelsohne zu den bewährtesten Praktiken im Bankwesen in Europa und darüber hinaus, wie es auch in den Empfehlungen der FATF[16] in diesem Bereich eingeräumt wird. In gewisser Weise lassen sich Maßnahmen zur Vermeidung von Geschäftsbeziehungen mit Gegenparteien, die Risiken für Integrität und Ansehen darstellen, auch als anerkannte Bankenpraxis betrachten.[17] Den Integritäts-/Reputationsrisiken kommt für öffentliche internationale Finanzinstitutionen wie die EIB noch größere Bedeutung als für nationale Geschäftsbanken zu. Besondere Aufmerksamkeit ist daher erforderlich, um zu vermeiden, dass das Ansehen der EIB durch Geschäfte mit unseriösen Personen gefährdet wird.

Die vorstehend genannten Bestimmungen können zwar grundsätzlich als Rechtsgrundlage herangezogen werden, doch sind sie nach Auffassung des EDSB zu allgemein und unbestimmt formuliert, als dass sie allein eine hinreichende Grundlage für die hier zu prüfende Verarbeitung ergeben. Mit anderen Worten: Die in Artikel 12 und Artikel 18 Absatz 1 der EIB-Satzung formulierten allgemeinen Verpflichtungen müssen umgesetzt und konkretisiert werden. So sollte die EIB unbedingt genau angeben und definieren, was für die Zwecke der AML-CFT-Verarbeitung als „bewährteste Praktiken im Bankenwesen“ (Artikel 12) anzusehen ist.

In diesem Zusammenhang nimmt der EDSB die Arbeiten der EIB zur Kenntnis, mit denen ein Rahmen für die Bestimmung bewährtester Praktiken im Bankenwesen für den Zweck von Artikel 12 der Satzung abgesteckt werden soll. So enthält insbesondere die vom Verwaltungsrat angenommene Integritätscharta der EIB den Grundsatz, dass die EIB-Gruppe ihre Aufgaben *„in Einklang mit den allgemein anerkannten Standards der finanziellen und administrativen „Good Practice“ erfüllt [...]“*. Weiter heißt es dort, dass das OCCO dazu beiträgt, *„sicherzustellen, dass die EIB-Gruppe die anwendbaren Gesetze, Vorschriften, Regeln und allgemein anerkannten branchenüblichen Praktiken und Standards einhält [...]“*. Und weiter: *„Dies betrifft Vorbeugung gegen Geldwäsche und Korruption sowie gegen die Verwendung von Mitteln zu terroristischen Zwecken [...]“*.

Außerdem erklärte der Verwaltungsrat der EIB, dass die EIB *„freiwillig die geltenden Bestimmungen der wichtigsten EU-Richtlinien und die entsprechenden für den Bankensektor*

[16] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations.

[17] Siehe z. B. Baseler Ausschuss für Bankenaufsicht, „Compliance and the compliance function in banks“, April 2005: „Der Ausdruck „Compliance-Risiko“ wird in diesem Papier definiert als das Risiko straf- oder verwaltungsrechtlicher Sanktionen, erheblicher finanzieller Verluste oder eines Reputationsverlustes, die/den eine Bank als Folge der Nichteinhaltung von Gesetzen, Verordnungen, Vorschriften, entsprechenden Standards von Selbstregulierungsorganisationen und für ihre Banktätigkeit geltenden Verhaltenskodizes erleiden kann“ (Hervorhebung durch uns), siehe S. 7.

verbindlichen Standards anwendet" (Hervorhebung durch uns)[18]; damit dürften im Wesentlichen die AML-CFT-Richtlinien und die FATF-Empfehlungen gemeint sein. Zu diesem Zweck nahmen Verwaltungsrat und Direktorium einen Rahmen für die Einhaltung bewährtester Praktiken im Bankenwesen („Rahmen") an, der sich auf die oben genannten Richtlinien und mehrere andere Texte stützt. Auf Beschluss des Prüfungsausschusses haben sich bewährte Praktiken bei der EIB *„auf die darin niedergelegten Grundsätze zu stützen"*. Weiterhin hat der Prüfungsausschuss ein Dokument vorgelegt, in dem das von EIB-Beamten bei der Durchführung von AML-CFT-Kontrollen einzuhaltende Verfahren beschrieben ist („Verfahren"). Ergänzt wird das Verfahren durch [...] nähere Einzelheiten zu diesen Kontrollen. Der Rahmen stützt sich in der Hauptsache auf das Verfahren für Integrität und AML-CFT sowie die entsprechenden [dazugehörenden Dokumente]. Der Rahmen wurde anschließend dem Rat der Gouverneure gemeldet.

Grundsätzlich dürften die gemeldeten Verarbeitungen für die Wahrnehmung solcher Aufgaben erforderlich sein. Ohne Überprüfung der Identität und des Hintergrunds des Kunden vor Aufnahme einer Geschäftsbeziehung mit ihm und ohne kontinuierliche Überwachung wäre die EIB nicht in der Lage, Fälle aufzudecken und zu vermeiden, in denen ihre Mittel zur Geldwäsche oder Terrorismusfinanzierung verwendet würden oder die Gegenpartei Reputationsrisiken für die EIB bedeuten würde. Es sollte jedoch bedacht werden, dass Erforderlichkeit ein relatives Kriterium ist, und der für die Verarbeitung Verantwortliche 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.

In Anbetracht dessen vertritt der EDSB die Ansicht, dass die Bestimmungen der EIB-Satzung und der dazu gehörenden Durchführungsbestimmungen (also Integritätscharta, Rahmen, Verfahren und [dazugehörende Dokumente]) grundsätzlich eine ausreichende Rechtsgrundlage für die Zwecke von Artikel 5 Buchstabe a der Verordnung bieten. Diese Dokumente sind jedoch nicht alle öffentlich zugänglich, sondern lediglich die Integritätscharta und das Verfahren. Darüber hinaus sind die Informationen in den öffentlich zugänglichen Dokumenten (Charta und Verfahren) nicht umfassend. Der Klarheit und Transparenz halber empfiehlt der EDSB, in das Verfahren einige Zusatzangaben zur Art der bei natürlichen Personen vorgenommenen Kontrollen aufzunehmen, wie sie in den einschlägigen Richtlinien und/oder [dazugehörenden Dokumenten] festgelegt sind (siehe beispielsweise die Informationen über Counterparty Key Persons, EDD und SDD, PEP usw.). Dem EDSB ist das Argument bekannt, demzufolge zu viele Einzelheiten in den veröffentlichten Dokumenten Versuche zur Umgehung der AML-CFT-Maßnahmen erleichtern könnten. Im Interesse der Rechtssicherheit sollten das Geschäftsgebaren der EIB jedoch transparenter gemacht werden. Bezüglich des Detailgrads bieten die 40 Empfehlungen der FATF mit ihren Auslegungsvermerken[19] einen Standard dafür, was offengelegt werden kann, ohne die Wirksamkeit von AML-CFT-Maßnahmen zu gefährden.

3.2.2. Artikel 5 Buchstabe b

Im Hinblick auf die Anwendbarkeit von Artikel 5 Buchstabe b ist zu prüfen, ob der für die Verarbeitung Verantwortliche einer rechtlichen Verpflichtung zur Erhebung und Verarbeitung von Daten unterliegt, die ihm keinen Ermessensspielraum lässt. Aus den teilweise bereits

[18] Stellungnahme des Direktoriums zu den Berichten des Prüfungsausschusses für das Jahr 2010, S. 1 (Anlage zum Bericht des Prüfungsausschusses an den Rat der Gouverneure über das Geschäftsjahr 2010).

[19] http://www.fatf-gafi.org/documents/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

genannten Gründen ist der EDSB der Auffassung, dass die von der EIB angeführten Bestimmungen für den Zweck von Artikel 5 Buchstabe b nicht in Betracht kommen.

Artikel 67 Absatz 3 AEUV besagt zwar, dass die Union darauf hin wirkt, Kriminalität zu verhüten und zu bekämpfen, enthält jedoch keinerlei konkrete Verpflichtung für die EIB, eine AML-CFT-Regelung zu schaffen. Gleiches gilt für Artikel 325 AEUV, der lediglich den allgemeinen Grundsatz enthält, dass die Union und die Mitgliedstaaten Betrügereien und sonstige gegen die finanziellen Interessen der Union gerichtete rechtswidrige Handlungen mit von der Kommission und den Mitgliedstaaten ergriffenen Maßnahmen bekämpfen. Aus den vorstehend in Abschnitt 3.2.1 dargelegten Gründen sind Artikel 75 und Artikel 215 AEUV für die EIB nicht unmittelbar maßgeblich. Gleiches gilt für die AML-CFT-Richtlinien, weil sie auf die EIB keine Anwendung finden.

Artikel 12 und Artikel 18 Absatz 1 der Satzung verpflichten die EIB ganz allgemein dazu, i) ihre Mittel wirtschaftlich am zweckmäßigsten im Interesse der Union zu verwenden und ii) mit den bewährtesten Praktiken im Bankwesen im Einklang zu stehen. Wie bereits unterstrichen, ist im Hinblick auf die Anwendbarkeit von Artikel 5 Buchstabe b zu prüfen, ob der für die Verarbeitung Verantwortliche einer rechtlichen Verpflichtung zur Erhebung und Verarbeitung von Daten unterliegt, die ihm keinen Ermessensspielraum lässt. Die konkreten Verarbeitungsvorgänge müssen unmittelbar auf den Vertrag oder einen auf seiner Grundlage erlassenen Rechtsakt zurückgehen. Die vorstehend genannten Bestimmungen enthalten keine konkrete Verpflichtung zur Verarbeitung für AML-CFT-Zwecke. Der EDSB ist daher nicht davon überzeugt, dass im vorliegenden Fall Artikel 5 Buchstabe b anzuwenden ist.

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. Auch wenn die Verarbeitung besonderer Datenkategorien nicht das Hauptziel der Verarbeitung ist, kann nicht ausgeschlossen werden, dass derartige Daten verarbeitet werden. Bei den zur Bekämpfung der Terrorismusfinanzierung durchgeführten Überprüfungen 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 Mitarbeiter der EIB 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. Dieser Grundsatz könnte als allgemeine Bestimmung in die AML-CFT-Erläuterungen eingehen.

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". Laut Meldung können Daten über Verdächtigungen oder Straftaten als Teil des Counterparty Acceptance Process und der anschließenden Überwachung der Gegenpartei verarbeitet werden. Der AML-CFT-Rahmen erwähnt augenscheinlich nicht, dass die EIB Daten über Straftaten gemäß Artikel 10 Absatz 5 erhebt und verarbeitet.

Der EDSB empfiehlt der EIB daher, eine eigene Rechtsgrundlage zu schaffen (einen Beschluss auf der angemessenen Verwaltungsebene), der die EIB dazu ermächtigt, Daten im Einklang mit Artikel 10 Absatz 5 in Anwendung der einschlägigen Bestimmungen des Vertrags oder der Satzung zu verarbeiten. Die Verarbeitung besonderer Datenkategorien sollte auf jeden Fall auf das zur Einhaltung der gesetzlichen Verpflichtungen bezüglich AML-CFT erforderliche Maß beschränkt werden. Zur Gewährleistung von Notwendigkeit, Verhältnismäßigkeit und Datenqualität sollten diesbezüglich angemessene Garantien vorgesehen werden (siehe hierzu auch nachstehenden Abschnitt 3.4).

3.4. 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).

Bezüglich der Kriterien der Erheblichkeit und Zweckentsprechung sollte die Verarbeitung auf die Datenkategorien beschränkt sein, bei denen eine direkte Verbindung zur Gewährleistung der Einhaltung der anwendbaren Bankengesetze gegeben ist. Das bedeutet vor allem, dass Ausdrücke wie „*straf- oder verwaltungsrechtliche Ermittlung*", „*Vorstrafen, strafrechtliche Verurteilungen oder große Zivilverfahren*" usw. insofern als Verweis auf solche Daten zu deuten sind, als sie sich auf die Befolgung der AML-CFT-Verpflichtungen beziehen. Bei einigen Fragestellungen wird außerdem die Verbindung mit AML-CFT-Zwecken nicht immer deutlich. Dies gilt beispielsweise für Behauptungen wie „*zweifelhafte Praktiken*" oder „*sonstige Integritätsrisiken*". Der EDSB empfiehlt der EIB, bei jeder einzelnen Frage der Frage nachzugehen, ob eine Verbindung zu AML-CFT-Zwecken besteht, und diese Verbindungen dem EDSB zu erläutern und zu begründen. Fragen, bei denen eine solche Verbindung nicht besteht, müssen gestrichen werden. Außerdem sollten Bestimmungen über bestimmte Überprüfungen ausgewogen und im Einklang mit dem Grundsatz der Verhältnismäßigkeit und anderen Datenschutzanforderungen ausgelegt werden.

Bei einigen Datenkategorien kann davon ausgegangen werden, dass sie von guter Qualität sind; dazu gehören Identifizierungsdaten, die von den betroffenen Personen selbst stammen, oder Auszüge aus öffentlichen Strafregistern. Bei anderen Datenkategorien, wie angeblichen rechtswidrigen oder unehrenhaften Aktivitäten, die sich unter Umständen auf Presseberichte stützen, lässt sich dies nicht so leicht sagen. Hier hat die EIB mit geeigneten Maßnahmen für ein hohes Maß an sachlicher Richtigkeit zu sorgen. Zu solchen Maßnahmen könnte beispielsweise der Verzicht auf die Nutzung unzuverlässiger Presseberichte gehören, oder der Abgleich von Informationen aus Presseberichten mit zuverlässigen unabhängigen Quellen, oder auch die Möglichkeit für betroffene Personen, ihre Sache zu vertreten. Die EIB sollte mit Verfahren gewährleisten, dass Daten bei Bedarf auf den neuesten Stand gebracht werden und dass Behauptungen, die sich als unbegründet erweisen, so bald wie möglich gelöscht werden.

Besonders zu achten ist auf die Vermeidung von Verwechslungen aufgrund von Namensgleichheit.

Der EDSB schlägt der EIB ferner vor, mit wirksamen Maßnahmen ein hohes Maß an Datenqualität zu gewährleisten. Diese Maßnahmen sollten z. B. folgende wichtige Bereiche abdecken[20]:

- Sachbearbeiter, die die CDD durchführen, sollten darin geschult werden, sie im Einklang mit den Datenschutzanforderungen durchzuführen;
- Ermittlung guter und schlechter AML-CFT-Praktiken, insbesondere im Hinblick auf KYC, CDD-Praktiken, das Ausfüllen von Fragebögen, Berichterstattung und kontinuierliche Überwachung;
- Vermeiden des Einsatzes von Profiling-Techniken;
- Aufnahme („Listing") von Verfahren und Mechanismen für erneute Bewertungen und regelmäßige Überprüfung und deren Streichung („Delisting");
- Grundsatz der Gewährleistung der Genauigkeit öffentlicher Quellen;
- Beschreibung, ob und wie die Organisation zwischen Faktendaten, Meinungsdaten, Intelligence-Daten und den für verschiedene Kategorien betroffener Personen erhobenen Daten unterscheidet;
- strikte und klare Anwendung des Grundsatzes der Zweckbindung, insbesondere bei Übermittlungen.

Der EDSB empfiehlt der EIB, wie weiter oben ausgeführt wirksame Maßnahmen auszuarbeiten und umzusetzen, die ein hohes Maß an Datenqualität gewährleisten.

3.5. Datenaufbewahrung/Datenspeicherung

Personenbezogene Daten dürfen nur so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht (Artikel 4 Absatz 1 Buchstabe e).

Wie im Abschnitt „Sachverhalt" dieser Stellungnahme dargestellt, werden die Daten zehn Jahre aufbewahrt. Eine Weiterverarbeitung für wissenschaftliche oder statistische Zwecke ist nicht vorgesehen.

Auch wenn die Richtlinie 2005/60/EG nicht unmittelbar anwendbar ist, geben doch die darin und in den einzelstaatlichen Rechtsvorschriften zu ihrer Umsetzung genannten Aufbewahrungsfristen eine gewisse Orientierungshilfe bezüglich angemessener Aufbewahrungsfristen. Gemäß Artikel 30 dieser Richtlinie sind solche Daten *„mindestens fünf Jahre*" aufzubewahren. In den allermeisten Mitgliedstaaten gilt eine Aufbewahrungsfrist von fünf Jahren.[21] Dem EDSB gegenüber konnte nicht eindeutig belegt werden, warum die EIB eine deutlich längere Aufbewahrungsfrist benötigt, wenn sich in der Praxis in den allermeisten Fällen eine Aufbewahrungsfrist von fünf Jahren als ausreichend erwiesen hat. Der für die Verarbeitung Verantwortliche äußerte allerdings Bedenken dahingehend, dass eine Aufbewahrungsfrist von fünf Jahren in Fällen nicht ausreichen würde, in denen auch nach Ablauf dieser Frist Unterlagen angefordert werden können, beispielsweise in

[20] Siehe in diesem Zusammenhang die Stellungnahme Nr. 14/2011 der Artikel-29-Datenschutzgruppe zu Datenschutzfragen in Bezug auf die Verhütung von Geldwäsche und Terrorismusfinanzierung, S. 15-16.

[21] 25 von 27 Mitgliedstaaten haben sich für eine Aufbewahrungsfrist von fünf Jahren entschieden; lediglich Spanien und Slowenien wählten eine Frist von sechs Jahren. Siehe Arbeitsunterlage der Kommissionsdienststellen: Compliance with the anti-money laundering directive by cross-border banking groups at group level, SEC (2009) 939 final (Einhaltung der Richtlinie über die Bekämpfung der Geldwäsche durch grenzüberschreitende Bankengruppen auf Gruppenebene, SEK (2009) 939 final), S. 50f.

Gerichtsprozessen, insbesondere in Drittländern. Die EIB führt ferner aus, dass sie bisher im Bereich AML-CFT nur über geringe Erfahrungen verfügt und daher nicht beurteilen kann, ob eine Aufbewahrungsfrist von zehn Jahren ausreicht oder übertrieben ist. Die Erfahrung wird also zeigen, ob diese Frist geändert werden muss. In Anbetracht dieser Argumente schlägt der EDSB der EIB vor, nach den ersten zehn Jahren praktischer Erfahrungen im Bereich AML-CFT erneut zu prüfen, ob eine Aufbewahrungsfrist von zehn Jahren erforderlich ist. Gestützt auf die Ergebnisse einer solchen Prüfung sollte die EIB nachweisen können, dass eine so viel längere Aufbewahrungsfrist tatsächlich erforderlich ist.

3.6. Datenübermittlung

Übermittlungen an Empfänger, die der Verordnung unterworfen sind, sind in Artikel 7 der Verordnung geregelt; Übermittlungen an Empfänger, die nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG unterliegen, sind in Artikel 8 der Verordnung geregelt, wohingegen Übermittlungen an Empfänger, die solchen Rechtsvorschriften nicht unterworfen sind, im Einklang mit den Vorschriften in Artikel 9 der Verordnung zu erfolgen haben.

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 EIB 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. Nach Angaben der EIB erfolgen Übermittlungen an andere Organe und Einrichtungen der EU in der Hauptsache an OLAF, aber auch an den Rechnungshof. 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 FIU von Mitgliedstaaten unterliegen je nach Umsetzung der Richtlinie 95/46/EG in dem betreffenden Mitgliedstaat entweder Artikel 8 oder Artikel 9 der Verordnung: Vom Anwendungsbereich der Richtlinie sind zwar Strafverfolgungsaktivitäten ausgenommen, doch haben sich viele Mitgliedstaaten für eine horizontale Umsetzung der Richtlinie mit einem Gesetz für alle Sektoren entschieden. In diesen Mitgliedstaaten fallen Übermittlungen an ihre nationalen FIU unter Artikel 8. 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.*“

Nach Auffassung des EDSB sollte diese Bestimmung dahingehend ausgelegt werden, dass, wenn die Daten nicht auf Ersuchen des Empfängers übermittelt werden, der Übermittelnde zu überprüfen hat, ob die Übermittlung wirklich erforderlich ist. Wenn also die EIB personenbezogene Daten an Untersuchungsstellen in einem Mitgliedstaat übermittelt, sollte sie zuvor überprüfen, ob diese Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich sind. Diese Bestimmung deckt Übermittlungen an zentrale Meldestellen ab, wenn gemäß dem in Artikel 22 der Richtlinie 2005/60/EG festgelegten Grundsatz berechtigter Grund zu der Annahme besteht, dass Geldwäsche oder Terrorismusfinanzierung vorliegt. Die konkrete Notwendigkeit ist jedoch in jedem Einzelfall zu prüfen.

Für Mitgliedstaaten, die solche Tätigkeiten aus dem Anwendungsbereich ihrer Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG ausgenommen haben, gilt Artikel 9. Gemäß Artikel 9 Absatz 1 sind solche Übermittlungen zulässig, wenn im Empfängerland ein angemessenes Schutzniveau gewährleistet ist. Da es sich bei diesen Empfängern sowohl um EU-Mitgliedstaaten als auch um Unterzeichner des Übereinkommens Nr. 108 des Europarates[22], handelt, kann hier grundsätzlich von einem angemessenen Schutzniveau ausgegangen werden. Außerdem könnte in bestimmten Fällen die Ausnahmeregelung von Artikel 9 Absatz 6 Buchstabe d (*für die Wahrung eines wichtigen öffentlichen Interesses* [...] *erforderlich)* herangezogen werden. Die Ausnahme ist jedoch restriktiv auszulegen und ihre Anwendung in jedem Einzelfall zu prüfen.

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

3.7. 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. Gemäß Artikel 20 sind Einschränkungen möglich. Die EIB erwähnt in ihrer Meldung, dass diese Rechte gemäß Artikel 20 Absatz 1 Buchstabe a, b und c der Verordnung unter Umständen eingeschränkt werden können.

Nach Angaben der EIB dürfte Artikel 20 Absatz 1 Buchstabe (Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten) vermutlich am häufigsten als Grund für die Auskunftsverweigerung angeführt werden. 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 auch ausgeübt werden können.

Auf jeden Fall ist von der EIB Artikel 20 Absatz 3 zu berücksichtigen und einzuhalten: *„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.“* Bezüglich der Informationspflicht ist diese Bestimmung gemeinsam mit Artikel 11, 12 und 20 der Verordnung auszulegen (siehe nachstehenden Abschnitt 2.2.9).

Zu berücksichtigen ist ferner Artikel 20 Absatz 4: *„Wird eine Einschränkung nach Absatz 1 angewandt, um der betroffenen Person den Zugang zu verweigern, unterrichtet der Europäische Datenschutzbeauftragte bei Prüfung der Beschwerde die betroffene Person nur darüber, ob die Daten richtig verarbeitet wurden und, falls dies nicht der Fall ist, ob alle erforderlichen Berichtigungen vorgenommen wurden“*. Dann ist das indirekte Auskunftsrecht zu gewähren. Diese Bestimmung wird beispielsweise in den Fällen eine Rolle spielen, in denen die betroffene Person über den Prozess in Kenntnis gesetzt wurde oder davon erfahren hat, das Recht auf Auskunft aber noch gemäß Artikel 20 eingeschränkt ist.

Artikel 20 Absatz 5 besagt: *„Die Unterrichtung nach den Absätzen 3 und 4 kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt*“. Es kann für die EIB erforderlich sein, zum Schutz der Untersuchung die Unterrichtung im

[22] Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, ETS Nr. 108.

Einklang mit dieser Bestimmung aufzuschieben. Über eine solche Aufschiebung ist jedoch fallweise zu entscheiden.

Artikel 14 der Verordnung gewährt der betroffenen Person das Recht, unrichtige oder unvollständige Daten zu berichtigen. Da es sich meist um sensible Fälle handelt, kommt diesem Recht eine zentrale Bedeutung zu, um die Qualität der verwendeten Daten zu gewährleisten, was im vorliegenden Fall mit dem Recht auf Verteidigung verknüpft ist. Jede in Artikel 20 der Verordnung vorgesehene Einschränkung ist im Lichte der vorstehenden Ausführungen zum Recht auf Auskunft anzuwenden.

3.8. Informationspflicht gegenüber der betroffenen Person

Die betroffene Person muss zumindest nachstehende Informationen erhalten (siehe Artikel 11 und 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 auf Anrufung des EDSB
- bei Daten, die bei der betroffenen Person erhoben werden, Hinweis auf den freiwilligen oder obligatorischen Charakter der Antworten sowie auf mögliche Konsequenzen einer Nichtbeantwortung
- bei Daten, die nicht bei der betroffenen Person erhoben werden, Angabe des Ursprungs der Daten, allerdings nicht dann, wenn der für die Verarbeitung Verantwortliche diese Informationen zur Wahrung des Berufsgeheimnisses nicht offenlegen darf.

Die EIB stellt die Vorschriften und Verfahren für AML-CFT (also das Verfahren für Integrität und AML-CFT) auf ihre Website und nimmt einen Hinweis auf die Anwendbarkeit der Verordnung (EG) Nr. 45/2001 in ihre Finanzierungsverträge auf. Zwar kann dieser Hinweis das Bewusstsein für die anzuwendenden Datenschutzvorschriften schärfen, doch reicht er allein nicht aus, zumal er betroffene Personen erst zu spät erreicht, nachdem nämlich die Verarbeitung bereits angelaufen ist.

Bezüglich der Mittel für die Unterrichtung ist der EDSB der Auffassung, dass die Veröffentlichung des Verfahrens auf der Website allein nicht ausreicht, um zu gewährleisten, dass betroffene Personen die Informationen tatsächlich erhalten. Denn vermutlich lesen nicht alle 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. Der EDSB empfiehlt insbesondere, der Gegenpartei diese Informationen bei der ersten einschlägigen Gelegenheit zu geben (also nach der Herstellung des ersten Kontakts, der das Verfahren auslöst), mit der Bitte, sie an die betreffende(n) bestimmte(n) oder bestimmbare(n) Person(en) (beispielsweise innerhalb der Organisation) weiterzugeben.

Zum Inhalt des Verfahrens merkt der EDSB an, dass das Verfahren für Integrität und AML-CFT in seiner jetzigen Form betroffene Personen nicht über Empfänger (Empfängerkategorien) von Daten informiert, keine eindeutige Rechtsgrundlage für die

Verarbeitung nennt und keine vollständige Liste von Datenkategorien enthält. Es enthält ferner weder Informationen über mögliche Konsequenzen einer Auskunftsverweigerung (wenn die Daten direkt bei der betroffenen Person erhoben werden) noch über die Quellen, aus denen bei anderen erhobene Daten stammen.

Der Hinweis auf die Ausübung der Rechte betroffener Personen „*durch Kontaktaufnahme mit dem OCCO und/oder dem Europäischen Datenschutzbeauftragten*" sollte durch einen Satz ersetzt werden, der etwa lauten könnte: „Betroffene Personen können ihre Rechte ausüben, indem sie den für die Verarbeitung Verantwortlichen ansprechen; sie haben das Recht, sich jederzeit an den Europäischen Datenschutzbeauftragten zu wenden"; damit würde der Unterschied zwischen den Rollen dieser beiden Personen deutlicher. Es sollten auch die Kontaktdaten des für die Verarbeitung Verantwortlichen hinzugefügt werden. Alle in diesem Abschnitt aufgezählten Mängel sind zu beseitigen.

3.9. 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*".

Der EDSB erinnert die EIB daran, dass alle Expertensysteme nur als Informations- und Warnelement zur Unterstützung des Entscheidungsprozesses des Direktoriums eingesetzt werden sollten und eine nach menschlicher Analyse ergehende endgültige Entscheidung nicht ersetzen können.

3.10 Sicherheitsmaßnahmen

Nach sorgfältiger Analyse der bestehenden Sicherheitsmaßnahmen ist der EDSB zu der Auffassung gelangt, dass diese Maßnahmen im Lichte von Artikel 22 der Verordnung (EG) Nr. 45/2001 angemessen sind.

4. SCHLUSSFOLGERUNG

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

- gewährleisten, dass die zuständigen Sachbearbeiter auf die Vorschriften betreffend besondere Datenkategorien in Artikel 10 der Verordnung hingewiesen werden und keine besonderen Datenkategorien verarbeiten, sofern nicht eine der in Artikel 10 Absatz 2 oder 4 vorgesehenen Ausnahmen greift. Dies könnte in Form einer allgemeinen Bestimmung in den AML-CFT-[Dokumenten] geschehen;
- in das Verfahren einige Zusatzangaben zur Art der bei natürlichen Personen vorgenommenen Kontrollen aufnehmen, wie sie in den einschlägigen EU-Richtlinien

und/oder [dazugehörenden Dokumenten] festgelegt sind (siehe beispielsweise die Informationen über Counterparty Key Persons, EDD und SDD, PEP usw.);

- mit einem Beschluss auf der angemessenen Verwaltungsebene eine Rechtsgrundlage schaffen, der zufolge die EIB befugt ist, Daten gemäß Artikel 10 Absatz 5 zu verarbeiten. Die Verarbeitung besonderer Datenkategorien sollte auf jeden Fall auf das zur Einhaltung der gesetzlichen Verpflichtungen bezüglich AML-CFT erforderliche Maß beschränkt werden;
- bei jeder einzelnen Frage bewerten, [...] ob eine klare, unmittelbare Verbindung zu AML-CFT-Zwecken besteht, diese Verbindungen dem EDSB erläutern und begründen und Fragen [vermeiden], die keine solche Verbindung aufweisen;
- wie in Abschnitt 3.4 erörtert, wirksame Maßnahmen ausarbeiten und umsetzen, mit denen ein hohes Maß an Datenqualität gewährleistet wird;
- nach zehnjähriger praktischer Erfahrung im Bereich AML-CFT die Notwendigkeit der Aufbewahrungsfrist von zehn Jahren bewerten und dem EDSB über diese Notwendigkeit Bericht erstatten;
- das Recht auf Auskunft und Berichtigung nur fallweise und nur so lange wie erforderlich einschränken; mit angemessenen Verfahren dafür sorgen, dass diese Rechte tatsächlich ausgeübt werden können;
- den Hinweis auf die Ausübung der Rechte betroffener Personen „*durch Kontaktaufnahme mit dem OCCO und/oder dem Europäischen Datenschutzbeauftragten*“ durch einen Satz ersetzen, der etwa lauten könnte: „Betroffene Personen können ihre Rechte ausüben, indem sie den für die Verarbeitung Verantwortlichen ansprechen; sie haben das Recht, sich jederzeit an den Europäischen Datenschutzbeauftragten zu wenden“;
- wie in Abschnitt 3.8 dargestellt, die derzeitigen Mängel in den Informationen für betroffene Personen beseitigen;
- betroffenen Personen in einer eigenen Datenschutzerklärung Informationen geben, die auf die Website der EIB gestellt wird und neuen Gegenparteien am Beginn des Counterparty Acceptance Process mit der Bitte vorgelegt wird, sie an die betreffende(n) bestimmte(n) oder bestimmbare(n) Person(en) (beispielsweise innerhalb der Organisation) weiterzugeben.

Brüssel, den 7. Februar 2013

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter