



01935/06/DE  
WP128

**Stellungnahme 10/2006**  
**zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide***  
***Interbank Financial Telecommunication (SWIFT)***

**Angenommen am 22. November 2006**

Diese Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, Generaldirektion Justiz, Freiheit und Sicherheit, B-1049 Brüssel, Belgien, Büro LX-46 01/43.

Website: [http://ec.europa.eu/justice\\_home/fsi/privacy/index\\_de.htm](http://ec.europa.eu/justice_home/fsi/privacy/index_de.htm)

## **Zusammenfassung**

Diese Stellungnahme enthält die Feststellungen der Artikel-29-Datenschutzgruppe zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide Interbank Financial Telecommunication (SWIFT)*.

In diesem Zusammenhang betont die Artikel-29-Gruppe, dass auch im Kampf gegen Terrorismus und Kriminalität die Grundrechte gewahrt bleiben müssen. Sie besteht daher auf der Achtung weltweiter Datenschutzprinzipien.

SWIFT ist ein weltweit agierender Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen. SWIFT speichert alle Überweisungsdaten für 124 Tage in zwei Rechenzentren, von denen sich eines in der EU, das andere in den USA befindet – eine Form der Datenverarbeitung, die in diesem Dokument als „Spiegelung“ bezeichnet wird. Die Zahlungsanweisungen enthalten personenbezogene Daten wie Namen des Zahlungsanweisenden oder des Zahlungsempfängers. Nach den Terrorangriffen vom September 2001 verlangte das US-Finanzministerium (UST) von SWIFT Zugang zu den in den USA gespeicherten Daten. SWIFT gab diesen Anordnungen nach, konnte aber gewisse Einschränkungen aushandeln. Aufgrund von Presseberichten Ende Juni/Anfang Juli 2006 erfuhr die Öffentlichkeit erstmals von dieser Angelegenheit.

SWIFT unterliegt als in Belgien ansässige Genossenschaft belgischem Datenschutzrecht, das die EU- Datenschutzrichtlinie 95/46/EG („die Richtlinie“) umsetzt. Die Finanzinstitute in der EU, die sich der Dienstleistungen von SWIFT bedienen, unterliegen den jeweils nationalen Datenschutzvorschriften – in Umsetzung der Richtlinie – in den Mitgliedstaaten, in denen sie angesiedelt sind.

Die Artikel-29-Gruppe kommt zu folgenden Schlussfolgerungen:

- SWIFT und die Auftrag gebenden Finanzinstitute tragen als „für die Verarbeitung Verantwortlicher“ im Sinne von Artikel 2 Buchstabe d) der Richtlinie gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten, wenn auch in unterschiedlichem Maße.
- Die Weiterverarbeitung von personenbezogenen Daten stellt angesichts der umfangreichen Anordnungen des US-Finanzministeriums (UST) einen weiteren Zweck dar, der mit der ursprünglichen kommerziellen Zweckbestimmung im Sinne von Artikel 6 Absatz 1 Buchstabe b) der Richtlinie, für die die personenbezogenen Daten erhoben wurden, nicht vereinbar ist.
- Weder SWIFT noch die Finanzinstitute in der EU haben die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informiert, wie dies gemäß Artikel 10 und Artikel 11 der Richtlinie vorgeschrieben ist, so insbesondere bezüglich der Weitergabe ihrer Daten an die Vereinigten Staaten.
- Die von SWIFT durchgeführten Kontrollmaßnahmen, so insbesondere in Bezug auf den Zugang des US-Finanzministeriums (UST) zu den Daten, ersetzen keineswegs die unabhängigen Überprüfungen, die von den gemäß Artikel 28 der Richtlinie eingerichteten Kontrollstellen hätten vorgenommen werden können.
- In Bezug auf die Übermittlung personenbezogener Daten an das Rechenzentrum in den USA kann sich SWIFT nicht auf Artikel 25 der Richtlinie berufen, um die Verarbeitung der personenbezogenen Daten zu rechtfertigen.
- Keiner der Ausnahmetatbestände nach Artikel 26 Absatz 1 der Richtlinie trifft auf die Verarbeitung von personenbezogenen Daten in den USA zu.
- SWIFT bediente sich auch nicht der nach Artikel 26 Absatz 2 der Richtlinie vorgesehenen Mechanismen, um von der belgischen Kontrollstelle für Datenschutz eine Genehmigung für die betreffende Datenverarbeitung zu erhalten.
- Die Artikel-29-Gruppe fordert SWIFT und die Finanzinstitute auf, unverzüglich Maßnahmen zu ergreifen, die die gegenwärtige unrechtmäßige Situation beenden.

- Außerdem verlangt die Artikel-29-Gruppe eine Klärung der Aufsichtsstrukturen bei SWIFT.

Die Artikel-29-Gruppe wird alle vorstehenden Punkte überwachen und einer Erfolgskontrolle unterziehen.

## INHALT

1.	HINTERGRUND .....	6
1.1.	Sachverhalt .....	6
1.2.	Fakten .....	9
1.2.1.	Datenverarbeitungstätigkeiten der SWIFT in Zahlen .....	9
1.2.2.	Kategorien der Verarbeitung personenbezogener Daten.....	10
1.2.3.	Anordnungen des US-Finanzministeriums (UST) .....	10
2.	GELTENDER RECHTLICHER RAHMEN FÜR DEN DATENSCHUTZ.....	11
2.1.	Anwendbarkeit der Richtlinie 95/46/EG .....	11
2.2.	Auf SWIFT anzuwendendes Recht .....	11
2.3.	Auf die Finanzinstitute anzuwendendes Recht .....	12
3.	ROLLE DER SWIFT UND DER FINANZINSTITUTE.....	12
3.1.	Rolle der SWIFT .....	13
3.2.	Rolle der Finanzinstitute .....	15
3.3.	Rolle der Zentralbanken .....	17
4.	BEWERTUNG DER VEREINBARKEIT MIT DEN DATENSCHUTZVORSCHRIFTEN.....	18
4.1.	Anwendung der Grundsätze in Bezug auf die Qualität der Daten und die Verhältnismäßigkeit (Artikel 6 der Richtlinie).....	18
4.1.1.	Kommerzielle Zweckbestimmung.....	19
4.1.2.	Weiterverarbeitung in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise.....	19
4.2.	Zulässigkeit der Verarbeitung von Daten (Artikel 7 der Richtlinie).....	21
4.2.1.	Verarbeitung ist erforderlich für die Erfüllung eines Vertrags (Artikel 7 Buchstabe b) der Richtlinie) .....	22
4.2.2.	Verarbeitung ist erforderlich für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt (Artikel 7 Buchstabe c) der Richtlinie).....	22
4.2.3.	Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird (Artikel 7 Buchstabe f) der Richtlinie) .....	22
4.3.	Versorgung des Betroffenen mit eindeutigen und vollständigen Informationen über das Vorhaben (Artikel 10 und 11 der Richtlinie).....	24
4.4.	Erfüllung der Meldepflichten (Artikel 18 bis 20 der Richtlinie) .....	24
4.5.	Aufsichtsmechanismen.....	24
4.6.	Grenzüberschreitender Datenfluss (Artikel 25 und 26 der Richtlinie) .....	25

4.6.1.	Angemessener Datenschutz (Artikel 25 Absatz 1 der Richtlinie).....	26
4.6.2.	Empfänger der Daten garantiert angemessene Datenschutzmaßnahmen (Artikel 26 Absatz 2 der Richtlinie).....	27
4.6.3.	Ausnahmen (Artikel 26 der Richtlinie).....	28
4.6.3.1.	<i>Die betroffene Person hat ihre Einwilligung gegeben (Artikel 26 Absatz 1 Buchstabe a) der Richtlinie).....</i>	28
4.6.3.2.	<i>Die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe b) der Richtlinie).....</i>	29
4.6.3.3.	<i>Die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder werden soll (Artikel 26 Absatz 1 Buchstabe c) der Richtlinie).....</i>	29
4.6.3.4.	<i>Die Übermittlung ist entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben (Artikel 26 Absatz 1 Buchstabe d) der Richtlinie).....</i>	29
4.6.3.5.	<i>Die Übermittlung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe e) der Richtlinie).....</i>	31
4.6.4.	Feststellungen.....	31
5.	SCHLUSSFOLGERUNGEN:.....	32
6.	SOFORTIGER HANDLUNGSBEDARF ZUR VERBESSERUNG DER GEGENWÄRTIGEN SITUATION:.....	34

## **DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -**

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995<sup>1</sup>,

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf deren Artikel 12 und 14 -

**gibt folgende Stellungnahme ab:**

### **1. HINTERGRUND**

Die unabhängigen Aufsichtsbehörden für den Datenschutz in der Europäischen Union<sup>2</sup> bewerten zurzeit die wichtige Frage der Übermittlung umfangreicher Finanzdaten von einem in der Europäischen Union ansässigen Unternehmen (SWIFT) an die US-Behörden. Die Umstände und die Einzelheiten dieser Übermittlung, insbesondere die Verarbeitung personenbezogener Daten von natürlichen Personen in Europa, erregten die Besorgnis der Datenschutzbehörden, die bei der Untersuchung des Datenflusses und bei der Analyse der Vereinbarkeit mit den europäischen Grundsätzen zum Schutz der Privatsphäre und insbesondere mit der Datenschutzrichtlinie („Richtlinie“) mit gemeinsamen Kräften vorgehen.

#### **1.1. Sachverhalt**

Ende Juni/Anfang Juli 2006 beschäftigte sich die Presseberichterstattung in den europäischen und den US-Medien mit dem Thema und stellte die Rolle und die Zuständigkeit der *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) in Bezug auf die Übermittlung von personenbezogenen Daten an das *Office of Foreign Assets Control* (OFAC, Büro zur Kontrolle ausländischen Guthabens) des US-Finanzministeriums (UST) infrage. SWIFT ist eine in Belgien ansässige Genossenschaft, die als Geldüberweisungsdienst tätig ist. Dabei wurde aufgedeckt, dass personenbezogene Daten, die im Wege des SWIFT-Netzes für internationale

---

<sup>1</sup> Amtsblatt L 281 vom 23.11.1995, S. 31, abzurufen über: [http://ec.europa.eu/justice\\_home/fsj/privacy/law/index\\_de.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm).

<sup>2</sup> Außer den in der EU zuständigen Behörden haben auch andere Datenschutzaufsichtsbehörden Untersuchungen in dieser Angelegenheit angestrengt, so in Australien, Kanada, Neuseeland, der Schweiz und Island.

Zahlungsanweisungen unter Verwendung des internationalen Bankleitzahl-Codes („BIC“) oder des „SWIFT“-Codes erhoben und verarbeitet wurden, seit Ende 2001 aufgrund von Anordnungen nach US-amerikanischem Recht zu Zwecken der Terrorismusermittlungen an das US-Finanzministerium weitergegeben worden sind.

In der Folge dieser Presseberichterstattung gab SWIFT am 23. Juni 2006 eine erste Presseerklärung<sup>3</sup> heraus. Dieser Stellungnahme zufolge ist SWIFT „eine von der Banken-Industrie betriebene genossenschaftliche Gesellschaft, die ein sicheres und standardisiertes Interbankdatennetz betreibt, an das mehr als 7.800 Bank- und Investmenthäuser weltweit angeschlossen sind“.

Die Europäische Kommission beschloss, diesen Fall genau zu verfolgen und forderte die belgischen Behörden im Juli 2006 auf, Informationen über die Umstände vorzulegen, unter denen SWIFT personenbezogene Daten verarbeitet, und ob diese dabei die belgischen Datenschutzvorschriften in Umsetzung der EU-Datenschutzrichtlinie einhält. Die Kommission überprüft bei den Mitgliedstaaten auch, ob Banken, die zur Ausführung von Zahlungsaufträgen auf SWIFT zurückgreifen, bei der Verarbeitung personenbezogener Daten im Zusammenhang mit solchen Zahlungen die jeweiligen nationalen Datenschutzvorschriften einhalten.

Mit Entschließung vom 6. Juli 2006<sup>4</sup> forderte das Europäische Parlament die Mitgliedstaaten zur Überprüfung und Sicherstellung auf, dass auf nationaler Ebene keine Gesetzeslücken vorhanden sind, und dass die Datenschutzvorschriften der Gemeinschaft auch für die Zentralbanken gelten. In dieser Entschließung brachte das Europäische Parlament auch ernsthafte Bedenken bezüglich der jeweiligen Zweckbestimmungen der Übermittlung von Daten an das US-Finanzministerium (UST) zum Ausdruck. Ebenso missbilligte es energisch „jegliche heimlichen Vorgänge auf dem Hoheitsgebiet der EU“, die die Privatsphäre von EU-Bürgern beeinträchtigen. Darüber hinaus erklärte es seine tiefe Besorgnis darüber, dass derartige Vorgänge stattfinden können, ohne dass die Bürger Europas und ihre parlamentarische Vertretung davon in Kenntnis gesetzt wurden. Schließlich forderte es die USA und ihre Geheim- und Sicherheitsdienste mit Nachdruck auf, im Geiste der guten Zusammenarbeit zu handeln und ihren Verbündeten alle Sicherheitsmaßnahmen mitzuteilen, die sie auf dem Hoheitsgebiet der EU durchführen wollen. Dabei wurde erörtert, dass es möglich ist, die Übermittlungen von Daten im Zusammenhang mit „illegalen Aktivitäten“ zu nutzen, aber auch zur Weitergabe von „Informationen über wirtschaftliche Tätigkeiten von bestimmten Einzelpersonen oder Ländern, die „Anlass zu entsprechenden Formen der Wirtschafts- und Industriespionage in großem Umfang“ geben könnten. In der Entschließung werden die Mitgliedstaaten aufgefordert, die Ergebnisse ihrer Überprüfungen der Europäischen Kommission, dem Rat und dem Europäischen Parlament mitzuteilen.

Am 27. Juli 2006 kündigte der Vorsitzende der Artikel 29-Datenschutzgruppe an, dass die europäischen Datenschutzbehörden beschlossen haben, ihre Tätigkeiten zu

---

<sup>3</sup> „Offizielle Stellungnahme von SWIFT“ zu ihren Richtlinien zur Einhaltung von Recht und Gesetz, veröffentlicht unter [http://www.swift.com/index.cfm?item\\_id=59897](http://www.swift.com/index.cfm?item_id=59897)

<sup>4</sup> Entschließung des Europäischen Parlaments zur unberechtigten Überwachung von Banküberweisungsdaten aus dem SWIFT-System durch die US-Geheimdienste (P6\_TA-PROV(2006)0317)

koordinieren. Bei ihrer darauf folgenden Sitzung am 26. und 27. September 2006 nahm die Artikel-29-Gruppe eine erste Erörterung in Vollsitzung vor.<sup>5</sup>

Am 4. Oktober 2006 wurde die Angelegenheit bei einer öffentlichen Anhörung der Ausschüsse des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres und für Wirtschaft und Währung mit dem Finanzvorstand von SWIFT und mit der Europäischen Zentralbank sowie mit anderen Teilnehmern erörtert<sup>6</sup>.

Der Europäische Datenschutzbeauftragte machte einige Vorbemerkungen zu seinen Untersuchungen über die Rolle der Europäischen Zentralbank (EZB) gemäß der Verordnung (EG) 45/2001.<sup>7</sup>

Auf nationaler Ebene haben die Datenschutzbehörden Kontakt zu ihren jeweiligen Bankenorganisationen aufgenommen.

Die Datenschutzbehörde Belgiens untersuchte die Rechtmäßigkeit der Verarbeitung der Daten durch SWIFT. Im Laufe dieser Untersuchung nahm die belgische Datenschutzbehörde direkten Kontakt zu SWIFT auf, um sowohl den Umfang als auch das Ausmaß der Überwachung und Übermittlung von Daten festzustellen. Die belgische Datenschutzbehörde stellte in ihrer Entscheidung vom 27. September 2006 fest, dass die Übermittlung von personenbezogenen Daten durch SWIFT an die SWIFT-Außenstelle in den USA gegen das belgische Gesetz vom 8. Dezember 1992 zum Schutz der Privatsphäre bei der Verarbeitung von personenbezogenen Daten verstößt<sup>8</sup>. Insbesondere fand die belgische Datenschutzbehörde heraus, dass SWIFT wesentliche Bestimmungen bezüglich der Informationspflichten, der Begrenzung der Zweckbestimmung der Verarbeitung der personenbezogenen Daten und der Übermittlung der personenbezogenen Daten an Drittländer übertreten hat. Die belgische Datenschutzbehörde traf die Feststellung, dass SWIFT „die grundlegenden europäischen Datenschutzgrundsätze intransparent, systematisch, massiv und dauerhaft verletzt hat“.

Die Artikel-29-Gruppe möchte auf der Grundlage der bei diesen Untersuchungen zusammengetragenen Informationen untersuchen, ob SWIFT die Datenschutzgrundsätze eingehalten hat, die in der Datenschutzrichtlinie enthalten sind und in allen Mitgliedstaaten durch nationale Datenschutzgesetze mit weitem Anwendungsbereich umgesetzt werden.

---

<sup>5</sup> Presseerklärungen der Artikel-29-Datenschutzgruppe: Presseerklärung der Artikel-29-Datenschutzgruppe zum Fall SWIFT vom 28.7.2006: [http://ec.europa.eu/justice\\_home/fsj/privacy/news/docs/PR\\_SWIFT\\_Affair\\_28\\_07\\_06\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf); Presseerklärung der Artikel-29-Datenschutzgruppe zum Fall SWIFT vom 27.9.2006: [http://ec.europa.eu/justice\\_home/fsj/privacy/news/docs/PR\\_Swift\\_Affair\\_26\\_09\\_06\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf).

<sup>6</sup> Der vollständige Meinungs austausch der öffentlichen Anhörung ist abrufbar unter [http://www.europarl.europa.eu/news/expert/infopress\\_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default\\_en.htm](http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default_en.htm)

<sup>7</sup> <http://www.edps.europa.eu/Press/EDPS-2006-10-EN%20swift.pdf>

<sup>8</sup> <http://www.privacycommission.be/communiqu%20E9s/AV37-2006.pdf>



SWIFT übersandte dem Vorsitzenden der Artikel-29-Datenschutzgruppe auch eine Kopie ihrer Antwortschreiben an die belgische, die spanische und die französische Datenschutzbehörde<sup>9</sup>.

## **1.2. Fakten**

### *1.2.1. Datenverarbeitungstätigkeiten der SWIFT in Zahlen*

Im Durchschnitt verarbeitet SWIFT täglich 12 Millionen Überweisungsdaten<sup>10</sup>. Der Gesamtumfang der jährlich verarbeiteten Überweisungsdaten belief sich beispielsweise im Jahr 2005 auf 2,5 Milliarden Überweisungsdaten, wovon 1,6 Milliarden für Europa und 467 Millionen für Nord-, Mittel- und Südamerika bestimmt waren. Die von SWIFT verarbeiteten Informationen betreffen die Überweisungsdaten der Finanzgeschäfte von Hunderttausenden von EU-Bürgern. Die europäischen Finanzinstitute (dieser Begriff ist nicht nur auf Banken beschränkt) nutzen den SWIFTNet-FIN-Service für die weltweite Übermittlung von Überweisungsdaten im Zusammenhang mit den jeweiligen Zahlungsanweisungen zwischen den Finanzinstituten. Diese Übermittlung erfolgt unabhängig davon, ob die Überweisungsdaten in der Europäischen Union (EU) bzw. im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland verarbeitet werden.

---

<sup>9</sup> Schreiben von SWIFT an den Vorsitzenden der Artikel-29-Datenschutzgruppe vom 31. Juli 2006.

<sup>10</sup> SWIFT-Jahresbericht 2005, abzurufen unter [http://www.swift.com/index.cfm?item\\_id=59684](http://www.swift.com/index.cfm?item_id=59684).

### 1.2.2. Kategorien der Verarbeitung personenbezogener Daten

Die über den SWIFTNet-FIN-Service übermittelten Überweisungsdaten enthalten personenbezogene Daten, wie z.B. die Namen des Zahlungsempfängers und des Zahlungsanweisenden. Die mit der Zahlung zusammenhängenden Überweisungsdaten können jedoch auch weitere Informationen enthalten, wie z.B. eine Geschäfts-/Bezugsnummer, damit der Zahlungsanweisende und der Zahlungsempfänger die jeweilige Zahlung mit ihren entsprechenden Buchungsunterlagen in Übereinstimmung bringen können. Darüber hinaus ist es bei bestimmten Arten von Überweisungsträgern möglich, nicht vorstrukturierte textliche Informationen anzufügen.

Abgesehen von ihren Verkaufsbüros in verschiedenen Ländern unterhält SWIFT zwei Rechenzentren, die in den beiden SWIFT-Außenstellen angesiedelt sind, von denen sich eine in einem EU-Mitgliedstaat und die andere in den Vereinigten Staaten befindet. In diesen Rechenzentren werden als Teil des SWIFTNet-FIN-Service alle von SWIFT verarbeiteten Überweisungsdaten für 124 Tage gespeichert und einer Form der Datenverarbeitung unterzogen, die in diesem Dokument als „Spiegelung“ bezeichnet wird, sozusagen als „Sicherungs- und Wiederherstellungsmechanismus“ für den Kunden im Falle von Streitigkeiten zwischen den Finanzinstituten oder Datenverlust. Nach dieser Zeitspanne werden die Daten gelöscht.

### 1.2.3. Anordnungen des US-Finanzministeriums (UST)

Seit den Terrorangriffen vom September 2001 erteilte das US-Finanzministerium (UST) dem SWIFT-Rechenzentrum in den Vereinigten Staaten vielfältige administrative Auflagen. Auf Anfrage erklärte SWIFT, dass sie bisher 64 Auflagen des UST erhalten und erfüllt hat.

Nach US-Recht handelt es sich bei einer administrativen Auflage um die Anordnung durch einen Regierungsbeamten einem Dritten gegenüber, durch die der Empfänger angewiesen wird, bestimmte Informationen vorzulegen.<sup>11</sup> Im vorliegenden Fall ist der Geltungsbereich der Anordnungen des US-Finanzministeriums (UST) materiell, territorial und zeitlich sehr weit gefasst und in den Auflagen und im Schriftverkehr über die Verhandlungen zwischen UST und SWIFT selbst bestimmt. Die Auflagen finden auf alle Geschäftsvorfälle Anwendung, die einen Zusammenhang mit Terrorismus aufweisen oder unter Umständen mit Terrorismus zusammenhängen können, beziehen sich auf *x* Länder und Gerichtsbarkeiten, auf *y* Daten oder auf Zeiträume „von ... bis ...“, die von einer bis zu mehreren Wochen reichen können, und gelten innerhalb und außerhalb der Vereinigten Staaten. Sie betreffen Überweisungsdaten von Interbankgeschäften innerhalb der USA, in die oder aus den USA wie auch Überweisungsdaten von außerhalb der USA, wie z.B. die Überweisungsdaten im Rahmen der EU.<sup>12</sup>

---

<sup>11</sup> Anhörung vor dem Justizausschuss des US-Senats, Unterausschuss für Terrorismusbekämpfung, technische und innere Sicherheit: „Mittel der Terrorismusbekämpfung sind: die Befugnis zur Erteilung von Anordnungen und die Inhaftierung von Terroristen bereits vor der Verurteilung durch Gerichtsverfahren“, Aussage von Rachel Brand, Principal Deputy Assistant Attorney General (etwa: Erster Stellvertretender Generalstaatsanwalt), Amt für Rechtspolitik, Justizministerium der Vereinigten Staaten, am 22. Juni 2004; [http://kyl.senate.gov/legis\\_center/subdocs/062204\\_brand.pdf](http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf)

<sup>12</sup> Vgl. Stellungnahme der belgischen Datenschutzbehörde, B.2 (nichtamtliche Übersetzung ins Englische), Fußnote 8.

SWIFT handelte eine eigene Vereinbarung mit dem US-Finanzministerium über die Modalitäten aus, wie die Auflagen zu erfüllen sind. Aufgrund dieses Verfahrens behauptet SWIFT von sich, „umfangreiche Sicherheiten und Zusicherungen hinsichtlich der Nutzung, der Vertraulichkeit, dem Ausmaß und der Kontrolle der Datensätze, die durch die Anweisung gefordert wurden“, erhalten zu haben<sup>13</sup>.

Den Feststellungen der belgischen Datenschutzbehörde zufolge wird die praktische Übermittlung der personenbezogenen Daten an das US-Finanzministerium (UST) vom SWIFT-Rechenzentrum in den USA in mehreren Schritten vollzogen. Es gibt kein unmittelbares Aussondern von individualisierten Daten, die in der SWIFT-Datenbank gespiegelt sind, sondern statt dessen die von SWIFT mit dem UST ausgehandelte Konstruktion des „Datenspeicher-Verfahrens“ („Black box“), das eine Übermittlung der Daten aus der gespiegelten SWIFT-Datenbank an einen speziellen Datenspeicher ermöglichte. Sobald die Daten in den von den USA betriebenen Datenspeicher gelangen, führt das US-Finanzministerium (UST) zielgerichtete Durchsuchungsaktionen durch.

Der belgischen Datenschutzbehörde wurden weitere Einzelheiten über die Übermittlung von personenbezogenen Daten an das US-Finanzministerium (UST) zugänglich gemacht und sind ihrer Stellungnahme zu entnehmen<sup>14</sup>.

## **2. GELTENDER RECHTLICHER RAHMEN FÜR DEN DATENSCHUTZ**

### **2.1. Anwendbarkeit der Richtlinie 95/46/EG**

Da in den Überweisungsdaten, die durch den SWIFTNet-FIN-Service übermittelt werden, personenbezogene Daten enthalten sind, ist die Artikel-29-Gruppe der Auffassung, dass die Datenschutzrichtlinie auf die Verarbeitung von personenbezogenen Daten im Wege des SWIFTNet-FIN-Service anwendbar ist.

Wie die Artikel-29-Gruppe betont, ist die Tatsache, dass die Verarbeitung von personenbezogenen Daten eine Begleitmaßnahme zu der Erbringung der eigentlichen Dienstleistung darstellt, nicht relevant für die Entscheidung darüber, ob die betreffende Organisation die Eigenschaft eines für die Verarbeitung von Daten Verantwortlichen erfüllt. Artikel 2 der Datenschutzrichtlinie enthält eine eindeutige Legaldefinition der Begriffe „Verarbeitung personenbezogener Daten“ und „personenbezogene Daten“. Fallen die von einem Rechtssubjekt durchgeführten Tätigkeiten unter diese Legaldefinitionen, so findet die Datenschutzrichtlinie Anwendung, und somit sind alle Tätigkeiten der Verarbeitung von Daten in uneingeschränkter Übereinstimmung mit dieser Richtlinie durchzuführen.

### **2.2. Auf SWIFT anzuwendendes Recht**

Nach Artikel 4 Absatz 1 Buchstabe a) der Datenschutzrichtlinie wendet jeder Mitgliedstaat die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an, „(...) die im Rahmen der Tätigkeiten einer

---

<sup>13</sup> „Offizielle Stellungnahme von SWIFT“ zu ihren Richtlinien zur Einhaltung von Recht und Gesetz, veröffentlicht unter [http://www.swift.com/index.cfm?item\\_id=59897](http://www.swift.com/index.cfm?item_id=59897).

<sup>14</sup> Siehe Fußnote 8.

Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt”.

Die Zentrale von SWIFT befindet sich in La Hulpe, Belgien. SWIFT unterhält auch zwei Rechenzentren (davon eines in Europa und das andere in den USA, die im Rahmen der Vollspiegelung tätig sind). Darüber hinaus hat SWIFT mehrere Verkaufsbüros im Vereinigten Königreich, in Frankreich, Deutschland, Italien, Spanien usw. Über die entscheidenden Fragen in Sachen Verarbeitung von personenbezogenen Daten und Übermittlung der Daten an das US-Finanzministerium (UST) wurde durch die Zentrale in Belgien entschieden.

Folglich unterliegt die Verarbeitung der personenbezogenen Daten durch SWIFT dem die europäische Datenschutzrichtlinie umsetzenden belgischem Recht, und zwar unabhängig davon, wo die Verarbeitung der betreffenden Daten stattfindet.

### **2.3. Auf die Finanzinstitute anzuwendendes Recht**

Finanzinstitute, die für ihre internationalen Zahlungsaufträge die Dienstleistungen von SWIFT nutzen, sind bezüglich der Verarbeitungsvorgänge als für die Verarbeitung Verantwortliche anzusehen, und somit ergibt sich das geltende nationale Recht aus Artikel 4 Absatz 1 Buchstabe a) der Datenschutzrichtlinie; bezüglich der Verarbeitungsvorgänge der Organe und Einrichtungen der Gemeinschaft gilt Artikel 3 der Verordnung (EG) 45/2001<sup>15</sup>. Dies bedeutet, dass bei Finanzinstituten zwar harmonisierte, aber doch verschiedene Gesetze zur Anwendung kommen.

Die Artikel-29-Gruppe betont, dass die zur Umsetzung der europäischen Datenschutzrichtlinie erlassenen nationalen Datenschutzgesetze der jeweiligen Mitgliedstaaten anzuwenden sind, da die die Finanzgeschäfte von hunderttausenden von Bürgern betreffenden personenbezogenen Daten durch in der EU niedergelassene Einrichtungen (durch die Genossenschaft SWIFT selbst wie auch durch die Finanzinstitute, die den SWIFTNet-FIN-Service nutzen) verarbeitet werden.

### **3. ROLLE VON SWIFT UND DER FINANZINSTITUTE**

Nach der Richtlinie hat der für die Verarbeitung Verantwortliche sicherzustellen, dass die Verpflichtungen bezüglich der Verarbeitung personenbezogener Daten erfüllt werden.

Fraglich ist, ob SWIFT und/oder die Finanzinstitute als „für die Verarbeitung von Daten Verantwortlicher“ oder als „Auftragsverarbeiter“ anzusehen sind.

Nach der Legaldefinition der Datenschutzrichtlinie ist 'für die Verarbeitung Verantwortlicher' „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Artikel 2 Buchstabe d));

---

<sup>15</sup> Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001, S. 1.

'Auftragsverarbeiter' ist „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet“ (Artikel 2 Buchstabe e)).

### 3.1. Rolle von SWIFT

Nach ihrer eigenen Darstellung war SWIFT stets *„ausschließlich eine Plattform zum sicheren Austausch vertraulicher Finanzdaten zwischen Finanzinstitutionen. SWIFT ist keine Bank und unterhält auch keine Konten von Kunden“*. Diese Darstellung bildete auch die Grundlage für die von einigen Datenschutzbehörden der Mitgliedstaaten vorgenommenen Bewertungen zur Genehmigung von Daten verarbeitenden Tätigkeiten ihrer jeweiligen Banken.

Die internationalen Dienstleistungsstrukturen der SWIFT und die Vertragsvereinbarungen zwischen der SWIFT und den Finanzinstituten sind ziemlich komplex. Die Artikel-29-Gruppe weist jedoch darauf hin, dass diese Art von Struktur einschließlich der Rolle des Dienstleistungserbringers, der mit anderen Wirtschaftsbeteiligten zusammenarbeitet, keinen Einzelfall darstellt. Die SWIFT-Struktur scheint ein Beispiel für ein formelles genossenschaftlich organisiertes Netz zu sein. SWIFT wurde 1973 durch eine Gruppe von europäischen Banken ins Leben gerufen, die eine neue Standardmethode zur Übermittlung von Zahlungsanweisungen an die jeweiligen Korrespondenzbanken entwickeln wollten. Zu diesem Zweck wurde eine genossenschaftliche Gesellschaft mit beschränkter Haftung nach belgischem Recht gegründet.

Die Artikel-29-Gruppe verweist auf ähnliche Fälle von genossenschaftlich organisierten Netzen, wie z.B. im Falle von „Terminated Merchant Databases“ (Datenbanken über gekündigte Händler), die von VISA und Mastercard in Zusammenarbeit mit den Finanzinstituten zur Analyse der Risiken betrieben werden, die mit der Aufnahme eines bestimmten Händlers im VISA- oder Mastercard-System verbunden sind<sup>16</sup>. Die Artikel-29-Gruppe verweist auch auf die Fälle der Verrechnungs- (Clearing-) und Saldenausgleichssysteme für Finanzgeschäfte und auf die Sitzplatzreservierungssysteme für Flugreisende, bei denen die Reisebüros und die Fluggesellschaften einerseits und die Geschäftsführer dieser Systeme (wie z.B. Galileo) andererseits unterschiedliche Verantwortlichkeiten innehaben.

Unabhängig vom bürgerlich-rechtlichen oder handelsrechtlichen Vertragsverhältnis zwischen SWIFT und den Finanzinstituten, das auch den Begriff „Unterauftragnehmer“ mit umfassen kann, ist SWIFT unter datenschutzrechtlichen Gesichtspunkten nicht einfach nur ein „Unterauftragnehmer“ oder 'Auftragsverarbeiter' im Sinne von Artikel 2 der Datenschutzrichtlinie für die normale Verarbeitung von personenbezogenen Daten zu gewöhnlichen kommerziellen Zwecken. Die Fakten zeigen, dass sich SWIFT in den letzten Jahrzehnten weiterentwickelt hat und mehr tut, als nur im Auftrag ihrer Kunden zu handeln. Selbst wenn man für einen Moment unterstellt, SWIFT habe als „Auftragsverarbeiter“ gehandelt, so hat SWIFT doch spezifische Verantwortlichkeiten übernommen, die über den Komplex der für einen Auftrag geltenden Anweisungen oder

---

<sup>16</sup> Siehe z.B. die „Leitlinien für Terminated Merchant Databases“ der Artikel-29-Datenschutzgruppe, abzurufen unter [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf).

der einem Auftragsverarbeiter obliegenden Pflichten hinausgehen und nicht mit ihrer Behauptung zu vereinbaren sind, nur ein reiner „Auftragsverarbeiter“ zu sein.<sup>17</sup> Die Geschäftsleitung von SWIFT handelt im Gefüge eines formellen genossenschaftlich organisierten Netzes, das sowohl über die Zweckbestimmungen als auch über die Mittel der Verarbeitung von personenbezogenen Daten im Rahmen des SWIFTNet-Services sowie auch darüber entscheidet, welche personenbezogenen Daten durch diesen SWIFTNet-Dienst verarbeitet werden. Die Geschäftsleitung von SWIFT entscheidet in eigener Verantwortung darüber, in welchem Umfang die mit der Verarbeitung zusammenhängenden Informationen den Finanzinstituten bereitgestellt werden. Die Geschäftsleitung von SWIFT ist in der Lage, über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten zu entscheiden, und zwar durch die Weiterentwicklung, die Vermarktung und die Veränderung von bestehenden oder neuen SWIFT-Dienstleistungen wie auch der Verarbeitung der Daten, so z.B. durch die Festlegung von für ihre Kunden verbindlichen Normen und Standards bezüglich der Form und des Inhalts von Zahlungsaufträgen, ohne dabei der Zustimmung der Finanzinstitute zu bedürfen. Auch leistet SWIFT bei der Verarbeitung personenbezogener Daten eine gewisse Wertschöpfung, so z.B. durch die Aufbewahrung und Richtigkeitsprüfung von personenbezogenen Daten und den Schutz von personenbezogenen Daten mittels hoher Sicherheitsstandards. Die Geschäftsleitung von SWIFT verfügt über die Befugnisse, bei der Verarbeitung der Daten Entscheidungen mit Gestaltungskraft zu treffen, so z.B. über die Sicherheitsstandards und die Standorte der Rechenzentren. Und schließlich besitzt die Geschäftsleitung von SWIFT uneingeschränkte Autonomie bei der Aushandlung und Kündigung der jeweiligen Dienstleistungsvereinbarungen wie auch bei der Ausarbeitung und Änderung der verschiedenen Vertragsdokumente und Geschäftspolitiken<sup>18</sup>. Die vorstehenden Merkmale fallen unter die praktischen und die rechtlichen Mittel der Verarbeitung.

In der Angelegenheit der Übermittlung von personenbezogenen Daten an das US-Finanzministerium (UST) hat SWIFT die Entscheidung getroffen, die Auflagen der USA zu erfüllen. Auch hat SWIFT die Initiative ergriffen, die Bedingungen für die Weitergabe der personenbezogenen Daten an das US-Finanzministerium (UST) in undurchsichtiger Art im Rahmen eines Verwaltungsschriftwechsels mit diesem auszuhandeln. So hat SWIFT auch bewusst entschieden, die betroffenen Finanzinstitute nicht von diesen Verhandlungen in Kenntnis zu setzen. Tatsächlich beeinträchtigten die von SWIFT erreichten und auch ausgeübten Kontrollfunktionen den Zweck und das Ausmaß der Übermittlung von Daten an das US-Finanzministerium (UST). Jedoch übersteigen diese Maßnahmen bei Weitem die normalen Funktionen eines Auftragsverarbeiters von Daten, da bei diesem zu unterstellen ist, dass er in Bezug auf die Anweisungen des für die Verarbeitung der Daten Verantwortlichen keinerlei Autonomie besitzt.

Zwar stellt sich SWIFT selbst als Auftragsverarbeiter der Daten dar, und einige Elemente könnten auch vermuten lassen, dass SWIFT bisher in bestimmten Fällen als Auftragsverarbeiter im Auftrag der Finanzinstitute tätig wurde, doch ist die Artikel-29-

---

<sup>17</sup> Der Auftragsverarbeiter von Daten muss in jedem Falle die Anforderungen der Datenschutzrichtlinie erfüllen, siehe z.B. Art. 17 Absatz 3 über Maßnahmen zur Sicherheit der Verarbeitung.

<sup>18</sup> Vgl. Ziffer 4.5.3 der allgemeinen Geschäftsbedingungen, wonach „die Zustimmung des Kunden zu einer solchen Verarbeitung vermutet wird...“.

Gruppe nach Erwägung des tatsächlichen Handlungsspielraums, über den SWIFT in den vorgenannten Situationen verfügt, der Auffassung, dass SWIFT vielmehr ein für die Verarbeitung Verantwortlicher im Sinne von Artikel 2 Buchstabe d) der Datenschutzrichtlinie ist, und zwar sowohl für die normale Verarbeitung von personenbezogenen Daten im Rahmen des SWIFTNet-Service als auch für die weitere Verarbeitung im Rahmen der Weitergabe von personenbezogenen Daten an das US-Finanzministerium (UST).

### **3.2. Rolle der Finanzinstitute**

Welche Rolle die Finanzinstitute bei der Inanspruchnahme des SWIFTNet-FIN-Service spielen, ist folgendermaßen zu bewerten: Einige Finanzinstitute waren von SWIFT nicht vollständig über das Ausmaß und die genauen Merkmale der Verarbeitung und Spiegelung der personenbezogenen Daten informiert worden, so auch nicht hinsichtlich der weiteren Übermittlung der gespiegelten personenbezogenen Daten an das US-Finanzministerium (UST). Nach der Aufdeckung dieser Fakten am und nach dem 23. Juni 2006 ist diese Situation jedoch allen Finanzinstituten bekannt, die im Rahmen von internationalen Geldüberweisungen personenbezogene Daten über den SWIFTNet-FIN-Service versenden.

Von den Finanzinstituten, die mit SWIFT arbeiten, wird vermutet und erwartet, dass sie ihren Einfluss auf die Politik der Genossenschaft in gewissem Umfang beibehalten. Einige Finanzinstitute sind im Vorstand von SWIFT vertreten; auch wurde die derzeitige Managementstruktur von SWIFT ursprünglich so ausgestaltet, dass die Banken und Finanzinstitute auch weiterhin Einfluss auf die Entscheidungsprozesse von SWIFT nehmen können. Diese Finanzinstitute sind daher so einzustufen, dass sie an der Entscheidung des Zwecks und der Mittel der Verarbeitung bei der Genossenschaft, deren Mitglieder sie sind, beteiligt sind. Auch haben sie direkten Kontakt mit den betreffenden natürlichen Personen und spielen eine wesentliche Rolle bei der Durchführung der internationalen Zahlungsaufträge ihrer Kunden.

Dabei ist jedoch stets zu berücksichtigen, dass die Finanzinstitute eigenständig sind und auf der Interbankebene ihre eigenen Ziele verfolgen können. Die Artikel-29-Gruppe hält daher fest, dass die Finanzinstitute im Rahmen des Interbankverkehrs häufig wichtige Entscheidungen über die Übermittlung personenbezogener Daten an SWIFT treffen, und dies oftmals sogar ohne ihre Kunden davon in Kenntnis zu setzen. Dies ergibt sich aus folgenden Gesichtspunkten:

- Auf der Interbankebene entscheiden die Finanzinstitutionen häufig eigenständig über die Mittel, die zur Abwicklung von Zahlungsanweisungen eingesetzt werden. Zur Übermittlung der Überweisungsdaten innerhalb des Interbanksystems können sie alternative oder konkurrierende Dienste nutzen oder entwickeln (z.B. elektronische Post, Fax, Telefon). Die auf dieser Ebene getroffene Auswahl entscheidet umfassend über die jeweiligen Merkmale des Schutzes der Privatsphäre bei den von den Finanzinstituten abgewickelten Zahlungsanweisungen. Wird ein Interbank-Service gewählt, so haben die Finanzinstitute angesichts der Vielfalt der Dienstleistungen auf der Interbankebene freie Hand, sich von anderen Elementen als der Informationssicherheit leiten zu lassen – die natürlich immer erforderlich ist – so z.B. von der jeweiligen Geschäftspolitik eines professionellen Dienstleisters in

Sachen Schutz der Privatsphäre. Die Finanzinstitute haben die Wahlmöglichkeit zwischen den strengen Maßnahmen eines bestimmten Anbieters zum Schutz der Privatsphäre und einer anderen Lösung, nämlich z.B. der Nutzung eines eigenen virtuellen Netzes als höchstmögliche Schutzgarantie für das Vertrauen ihrer Kunden und für ihre Dienstleistungen.

- Die Finanzinstitute akzeptieren und erfüllen das für den SWIFTNet-FIN-Service geltende vertragliche Rahmenwerk<sup>19</sup>. Die Vertragsunterlagen (Maßnahmen zur Wiedergewinnung und Abfrage von Daten<sup>20</sup>) und die SWIFT- Richtlinien zur Einhaltung von Recht und Gesetz weisen die Kunden von SWIFT auf den allgemeinen Grundsatz hin, dass personenbezogene Daten weitergegeben werden, wenn diese Gegenstand einer Auflage sind, die entweder gegenüber dem Kunden oder gegenüber SWIFT angeordnet wird. Der Stellungnahme der belgischen Datenschutzbehörde zufolge behauptete SWIFT, die Zahl der gegenüber Finanzinstituten angeordneten Auflagen könne sich auf Tausende oder sogar Zehntausende pro Jahr belaufen. Daher darf angezweifelt werden, dass Finanzinstitute, die auf dem internationalen Zahlungsmarkt tätig sind, den allgemeinen Grundsatz der angeordneten Auflagen nicht kennen.
- Die Finanzinstitute müssen die möglichen Auswirkungen und die Risiken für den Schutz der Privatsphäre bewerten, einschließlich der Risiken für den Schutz der Privatsphäre ihrer Kunden, die sich aus der Nutzung des SWIFTNet-FIN-Service ergeben, dessen sie sich als professionelle Dienstleister bedienen. Es ist daher wichtig, zu überprüfen, ob die Richtlinien zum Schutz der Privatsphäre des die Zahlungsanweisung erteilenden Finanzinstituts Klauseln bezüglich dieser Risiken enthalten.
- Angesichts der Tatsache, dass die Finanzinstitute bei der Erteilung von Zahlungsanweisungen im Auftrag ihrer Kunden handeln, sind diese nicht befugt, die dazu erforderlichen Daten zu anderen Zwecken als zur Zahlungsanweisung weiterzugeben. Ist einem Finanzinstitut bekannt, dass SWIFT die ihr anvertrauten Daten auch noch in anderer Weise als nur zur Zahlungsanweisung verwendet, und bedient sich dieses Finanzinstitut trotzdem auch weiterhin der Dienste von SWIFT, so ist die Frage nach der Rechtsgrundlage für derartige Überweisungen und Verwendungen zu stellen: Besteht nämlich keine besondere Vereinbarung zwischen dem Finanzinstitut und seinen Kunden, so scheint es nicht gerechtfertigt, SWIFT Bankdaten noch zu anderen Zwecken als zu der angegebenen und dem Kunden bestätigten Dienstleistung anzuvertrauen.

Folglich erfüllen die Finanzinstitute die Eigenschaft des für die Verarbeitung Verantwortlichen im Sinne des Artikels 2 Buchstabe d) der Datenschutzrichtlinie nicht nur in Bezug auf ihre eigenen Datenverarbeitungstätigkeiten, sondern sie tragen auch in

---

<sup>19</sup> Vertraglicher Bestandteil ist auch das „SWIFT-Benutzerhandbuch“, das Angaben zu den zu verwendenden standardisierten Überweisungsdaten enthält.

<sup>20</sup> Hier findet sich folgende Regelung: „Zur Vermeidung von Unklarheiten können diese Maßnahmen oder ganz allgemein die Verpflichtungen von SWIFT, das Vertrauen ihrer Kunden zu schützen, niemals so ausgelegt werden, dass SWIFT von der Wiedergewinnung und Abfrage, der Verwendung oder der Offenlegung der Zahlungsverkehrs- oder der Überweisungsdaten abgehalten werden kann, wenn diese Tätigkeiten als angemessen und notwendig anzusehen sind, um eine berechnete Auflage oder ein anderes gesetzliches Verfahren, die durch ein Gericht oder eine andere zuständige Behörde angeordnet werden, zu erfüllen“. Vgl. Stellungnahme der belgischen Datenschutzbehörde, D.2, Fußnote 8.



gewissem Umfang Verantwortung für die Datenverarbeitungstätigkeiten von SWIFT. Die Tatsache, dass sich die Managementstruktur der genossenschaftlichen Gesellschaft SWIFT anscheinend im Laufe der Zeit dahin weiterentwickelt hat, dass die Geschäftsleitung von SWIFT unabhängiger geworden ist als dies ursprünglich vorgesehen war, enthebt ihre Gründer, d.h. die Finanzinstitute nicht der Pflicht, ihre Eigenschaft als für die Verarbeitung der Daten Verantwortliche im Sinne der Datenschutzrichtlinie beizubehalten.

Aufgrund der vorstehenden Gesichtspunkte ist die Artikel-29-Gruppe der Auffassung, dass ausreichend Anhaltspunkte zur Stützung der Einschätzung vorliegen, der zufolge die genossenschaftliche Gesellschaft SWIFT und die Finanzinstitute, sofern sie vertreten sind, gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten durch den SWIFTNet-FIN-Service tragen. Gemeinsame Verantwortung bedeutet jedoch nicht unbedingt auch gleiche Verantwortung. Auch wenn SWIFT die Hauptverantwortung für die Verarbeitung personenbezogener Daten durch den SWIFTNet-FIN-Service trägt, sind die Finanzinstitute in gewissem Umfang für diese Verarbeitung der personenbezogenen Daten ihrer Kunden in diesem Dienst mitverantwortlich.

### **3.3. Rolle der Zentralbanken**

Unter Berücksichtigung der unterschiedlichen Rollen, die sie in Bezug auf SWIFT und bei der Aufsicht im Sektor der Finanzgeschäfte spielen, ist auch die Beteiligung der Zentralbanken zu untersuchen. Zunächst unterliegt SWIFT im Rahmen der Zusammenarbeit der gemeinsamen Aufsicht durch die Zentralbanken der G-10-Staaten (Gruppe der G-10)<sup>21</sup>. Diese Aufsicht konzentriert sich vorwiegend auf die Sicherstellung, dass SWIFT über effektive Kontrollen und Verfahren zur Bewältigung von Risiken für die finanzielle Stabilität und das reibungslose Funktionieren der Finanzinfrastrukturen verfügt. Darüber hinaus „überprüfen die Aufsichtsführenden auch, wie SWIFT operationelle Risiken feststellt und entschärft, und sie können auch rechtliche Risiken, die Transparenz der jeweiligen Regelungen und Verfahrensmodalitäten und die Maßnahmen zur Gewährleistung des Auskunftsrechts für die Kunden überprüfen. Auch die strategische Ausrichtung von SWIFT kann mit dem Vorstand und den Führungskräften erörtert werden“<sup>22</sup>. Das wichtigste Instrument, das die Aufsichtsbehörde für die Aufsicht über SWIFT anwenden kann, ist die Einflussnahme und Überzeugungskraft („moralischer Druck“). Die Aufsichtsführenden können Empfehlungen an SWIFT formulieren; es ist jedoch auch klar, dass diese Aufsicht über SWIFT der Genossenschaft keinerlei Bescheinigungen, Sichtvermerke oder Genehmigungen durch die Zentralbanken erteilen kann.

---

<sup>21</sup> Die Gruppe der G-10 setzt sich aus folgenden Zentralbanken zusammen: Nationalbank von Belgien, Bank von Kanada, Deutsche Bundesbank, Europäische Zentralbank, Banque de France, Banca d' Italia, Bank von Japan, De Nederlandsche Bank, Sveriges Riksbank, Schweizerische Nationalbank, Bank of England und Federal Reserve System (USA), vertreten durch die Federal Reserve Bank of New York und den Gouverneursrat des Federal Reserve System.

<sup>22</sup> Analyse der finanziellen Stabilität 2005, veröffentlicht von der Nationalbank von Belgien und abrufbar über ihre Website [www.nbb.be](http://www.nbb.be).

Die Bestimmungen über die vertrauliche Behandlung von nicht öffentlich zugänglichen Informationen sind Bestandteil der Gemeinsamen Vereinbarung zwischen SWIFT und den Zentralbanken.

Die Gruppe der G-10 wurde im Laufe des Jahres 2002 über die Übermittlung von Daten an die US-Behörden in Kenntnis gesetzt. Die Gruppe war jedoch der Auffassung, dass diese Angelegenheit nicht in den Geltungsbereich ihrer Aufsichtsrolle fällt. Außerdem legten viele Zentralbanken die Gemeinsame Vereinbarung über die Vertraulichkeit als Hinderungsgrund aus, diese Angelegenheit an die zuständigen Behörden auf nationaler und europäischer Ebene zu verweisen. Daher befasste sich die Gruppe der G-10 auch nicht mit den datenschutzrechtlichen Folgen der Datenübermittlung an die US-Behörden und informierte weder die zuständigen Behörden noch drängte sie SWIFT dazu, dies zu tun.

Darüber hinaus trug der Präsident der Europäischen Zentralbank (EZB) bei der öffentlichen Anhörung des Europäischen Parlaments vor, dass die Zentralbanken der G-10 *„das Vorgehen von SWIFT in Bezug auf die Erfüllung der angeordneten Auflagen in keiner Weise abgesegnet haben. Denn wir hätten keine derartige Einwilligung erteilen können, selbst wenn wir dies gewollt hätten, da dies außerhalb unserer Zuständigkeiten liegt. Daher blieb SWIFT für ihre Entscheidungen alleinverantwortlich“*.<sup>23</sup>

Zweitens ist hervorzuheben, dass aufgrund der begrenzten Rolle, die die Zentralbanken derzeit bei der Aufsicht über SWIFT spielen, nicht ausgeschlossen ist, dass auch eine Zentralbank unter Umständen – wie jedes andere Finanzinstitut, das den SWIFTNet-Service nutzt – als ein (gemeinsamer) für die Verarbeitung Verantwortlicher anzusehen ist, nämlich immer dann, wenn sie als Kunde von SWIFT handelt (siehe oben, Abschnitt 3.2) und sie personenbezogene Daten zu Zwecken von Interbankgeschäften verarbeitet. Unter diesem Gesichtspunkt könnte die Tatsache, dass einige Zentralbanken über die Übermittlung von Daten an die US-Behörden informiert waren, als relevant berücksichtigt werden, um ihre Verantwortung als Nutzer des SWIFT-Systems festzustellen.

#### **4. BEWERTUNG DER VEREINBARKEIT MIT DEN DATENSCHUTZVORSCHRIFTEN**

##### **4.1. Anwendung der Grundsätze in Bezug auf die Qualität der Daten und die Verhältnismäßigkeit (Artikel 6 der Datenschutzrichtlinie)**

Gemäß Artikel 6 der Richtlinie sind personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise zu verarbeiten;<sup>24</sup> sie sind für festgelegte, eindeutige und rechtmäßige Zwecke zu erheben<sup>25</sup> und nicht in einer mit diesen Zweckbestimmungen

---

<sup>23</sup> Jean-Claude Trichet: Stellungnahme des Präsidenten der EZB bei der öffentlichen Anhörung im Europäischen Parlament zur unberechtigten Überwachung von Banküberweisungsdaten aus dem SWIFT-System durch die US-Geheimdienste.

<sup>24</sup> Artikel 6 Absatz 1 Buchstabe a) der Richtlinie.

<sup>25</sup> Artikel 6 Absatz 1 Buchstabe b) der Richtlinie.

nicht zu vereinbarenden Weise weiterzuverarbeiten. Darüber hinaus müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen.<sup>26</sup> Diese letztgenannten Regeln werden zusammengefasst als „Verhältnismäßigkeitsgrundsatz“ bezeichnet. Schließlich noch sind alle angemessenen Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden.<sup>27</sup>

#### *4.1.1. Kommerzielle Zweckbestimmung*

Die personenbezogenen Daten wurden von den Finanzinstituten nur zu Zwecken der Verarbeitung der Zahlungsaufträge des Kunden und anschließend von SWIFT zu Zwecken der Durchführung des SWIFTNet-FIN-Service erhoben (kommerzieller Zweck). Als einziger festgelegter, eindeutiger und rechtmäßiger Zweck kann daher nur dieser kommerzielle Zweck für die Verarbeitung personenbezogener Daten berücksichtigt werden.

Was die Übermittlung von personenbezogenen Daten an Drittländer anbelangt, siehe weiter unten unter Abschnitt 4.6

#### *4.1.2. Weiterverarbeitung in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise*

aa) Personenbezogene Daten dürfen nicht zu Zwecken verarbeitet werden, die mit der ursprünglichen Zweckbestimmung nicht zu vereinbaren sind. Durch die Entscheidung über die Spiegelung aller Datenverarbeitungstätigkeiten in einem Rechenzentrum in den USA brachte SWIFT sich selbst in eine vorhersehbare Situation, in der sie den nach US-Recht angeordneten Auflagen unterliegt.

Im vorliegenden Falle erhielt SWIFT Auflagen, die vom US-Finanzministerium (UST) wegen der behaupteten Terrorismusermittlungen angeordnet worden waren. Dieser weitere Zweck ist ein vollkommen anderer als die ursprüngliche Zweckbestimmung und die damit verbundene Behandlung der betreffenden personenbezogenen Daten und kann unmittelbare Folgen für die Einzelpersonen haben, deren personenbezogene Daten verarbeitet werden. Dieser weitere Zweck ist nicht mit dem ursprünglichen, rein kommerziellen Zweck zu vereinbaren, für den die personenbezogenen Daten erhoben wurden.

SWIFT war dieser weitere Zweck bekannt. Die Geschäftsleitung von SWIFT billigte ihn und kooperierte. SWIFT hat auf diesen Zweck nicht hingewiesen, und zwar weder bei den Nutzern ihrer Dienstleistungen noch bei einer der Datenschutzaufsichtsbehörden.

bb) Auch wurde festgestellt, dass massive Datenübermittlungen von SWIFT an das US-Finanzministerium stattgefunden haben, ohne dass es effektiv möglich war, den individualisierten Charakter der geforderten Daten zu überprüfen. SWIFT zufolge

---

<sup>26</sup> Artikel 6 Absatz 1 Buchstabe c) der Richtlinie.

<sup>27</sup> Artikel 6 Absatz 1 Buchstabe d) der Richtlinie.

könnten potenziell alle Überweisungsdaten über das „Datenspeicher-System“ („Black box“) vom US-Finanzministerium (UST) nachgeforscht werden. Mit diesem System ist es dem US-Finanzministerium (UST) möglich, aus dem „Datenspeicher“ alle Überweisungsdaten – und die darin enthaltenen personenbezogenen Daten – abzufragen, die es für erforderlich hält.

Die Artikel-29-Gruppe weist darauf hin, dass SWIFT sogar für die Zwecke der behaupteten Terrorismusermittlungen nur spezifische und individualisierte Daten übermitteln sollte, und nur von Einzelfall zu Einzelfall und in vollständiger Übereinstimmung mit den Datenschutzgrundsätzen. Da dies nicht der Fall ist, ist die derzeit gehandhabte Praxis nicht verhältnismäßig und verletzt somit Artikel 6 Absatz 1 Buchstaben c) der Datenschutzrichtlinie.

cc) Gemäß Artikel 13 ist vorgesehen, dass „die Mitgliedstaaten Rechtsvorschriften erlassen können, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1 [Grundsatz der Zweckbeschränkung], Artikel 10, Artikel 11 Absatz 1 [Pflicht zur Information der betroffenen Person], Artikel 12 [Auskunftsrecht] und Artikel 21 [Öffentlichkeit der Verarbeitungen] beschränken, sofern eine solche Beschränkung notwendig ist für [es folgt eine Auflistung wichtiger öffentlicher Interessen] ... c) die öffentliche Sicherheit; d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten [...]; ...f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;“.

Der Europäische Gerichtshof (EuGH) hat diese Bestimmungen beleuchtet und Ausführungen zu ihrem Verständnis gemacht. In den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 („Rechnungshof“) vom 20. Mai 2003 stellte der Gerichtshof klar, dass die Übermittlung von ursprünglich für „kommerzielle“ Zwecke erhobenen Daten an Dritte, einschließlich öffentlicher Behörden, „einen Eingriff im Sinne von Artikel 8 EMRK darstellt“. Ferner müssen Ausnahmen von dem in der Datenschutzrichtlinie festgelegten Grundsatz der Zweckbeschränkung Artikel 13 dieser Richtlinie beachten, und daher müssen sie „unter dem Gesichtspunkt des Artikels 8 der Menschenrechtskonvention gerechtfertigt sein“ (Rechnungshof, C-465/00, §68 ff).

Nach der Menschenrechtskonvention ist der Eingriff in das Recht auf die Privatsphäre nur gerechtfertigt, insoweit er „gesetzlich vorgesehen ist“ und „in einer demokratischen Gesellschaft“ in einem bestimmten öffentlichen Interesse „notwendig ist“. Die Rechtsprechung in Straßburg hat wiederholt daran erinnert, dass das Gesetz, nach dem der Eingriff vorgesehen ist, „auf das zulässige Ziel der bestimmten Maßnahme abstellen und dabei mit ausreichender Klarheit die Grenzen des auf die zuständigen Behörden übertragenen Ermessens abstecken sowie bestimmen muss, wie dieses Ermessen auszuüben ist, um dem Einzelnen angemessenen Schutz gegen willkürliche Eingriffe zu bieten.“

Diese Bestimmungen können jedoch nicht zur Anwendung kommen, da SWIFT in diesen Angelegenheiten gegen belgisches Recht verstoßen hat.<sup>28</sup>

---

<sup>28</sup> Stellungnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.

dd) Die Artikel-29-Gruppe weist außerdem auf die geltenden rechtlichen Strukturen auf Regierungsebene hin. Sie betont, dass bei der Nutzung der entsprechenden Systeme der Grundsatz des Bankgeheimnisses einzuhalten ist. Sie bezieht sich diesbezüglich auf die 40+9 Empfehlungen der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ (FATF/GAFI), eines 1989 eingerichteten zwischenstaatlichen Gremiums, das nationale und internationale Fachpolitiken zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung entwickeln und fördern soll. Die Artikel-29-Gruppe verweist auch auf das System für Finanzinformationsaustausch, das von 96 Staaten zwischen den entsprechenden nationalen Zentralstellen für Geldwäscheverdacht (Egmont Secure Web, ESW) eingerichtet und vom FinCEN in den Vereinigten Staaten koordiniert wird. In diesem Rahmen können dem anfragenden Partner finanzielle Informationen in Einklang mit den nationalen Regeln des Landes erteilt werden, das die Informationen weitergibt.

Die Artikel-29-Gruppe verweist auch auf die vorhandenen Mechanismen der Zusammenarbeit, die im Rahmen der 3. Säule (polizeiliche und justizielle Zusammenarbeit) errichtet oder weiterentwickelt wurden, und insbesondere auf die am 25. Juni 2003 zwischen den USA und der EU unterzeichneten internationalen Übereinkommen<sup>29</sup> über die gegenseitige Rechtshilfe und, wenn auch etwas weiter von diesem Thema entfernt, das internationale Auslieferungsübereinkommen. Zwar sind diese Verträge noch nicht ratifiziert, doch ist ein Staat gemäß Artikel 18 der Wiener Vertragsrechtskonvention<sup>30</sup> verpflichtet, sich aller Handlungen zu enthalten, die den Vertragsgegenstand oder den Vertragszweck gefährden, wenn er diesen Vertrag bereits unterzeichnet oder die Ratifizierungsinstrumente ausgetauscht und nicht mitgeteilt hat, dass er keine Vertragspartei werden möchte.

Durch die Entscheidung über die Spiegelung aller Datenverarbeitungstätigkeiten in einem Rechenzentrum in den USA brachte sich SWIFT im Ergebnis selbst in eine vorhersehbare Situation, in der sie den nach US-Recht angeordneten Auflagen unterliegt, und in der die Verarbeitung von personenbezogenen Daten derart organisiert wurde, dass eine Umgehung der bereits bestehenden Strukturen und internationalen Übereinkommen vorzuliegen scheint.

Insgesamt gesehen ist die Artikel-29-Gruppe der Auffassung, dass die Grundsätze der Zweckbeschränkung und der Vereinbarkeit, der Verhältnismäßigkeit und der Erforderlichkeit der Verarbeitung personenbezogener Daten nicht eingehalten sind.

#### **4.2. Zulässigkeit der Verarbeitung von Daten (Artikel 7 der Richtlinie)**

Um als rechtmäßig zu gelten, muss die Verarbeitung personenbezogener Daten zulässig sein und einem der in Artikel 7 der Richtlinie aufgeführten Gründe genügen.

---

<sup>29</sup> „Auslieferungsübereinkommen zwischen der EU und den USA“ und „Übereinkommen über die gegenseitige Rechtshilfe zwischen der EU und den USA“.  
[http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l\\_181/l\\_18120030719en00270033.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf) und [http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l\\_181/l\\_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20European%20union%22](http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20European%20union%22)

<sup>30</sup> Wiener Vertragsrechtskonvention vom 23. Mai 1969. Die Vereinigten Staaten haben diese Konvention unterzeichnet.

*4.2.1. Die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags (Artikel 7 Buchstabe b) der Richtlinie)*

SWIFT verarbeitet die in den Überweisungsdaten enthaltenen personenbezogenen Daten im Rahmen des SWIFTNet-Fin-Services nur zur Durchführung der Zahlungsaufträge, mit der die Finanzinstitute SWIFT betraut haben.

Selbst wenn man in diesem Zusammenhang der Auffassung ist, dass die Verarbeitung zu diesem kommerziellen Zweck notwendig ist, um den Vertrag zwischen SWIFT und den betreffenden Finanzinstituten zu erfüllen, so ist jedoch die Art der Ausführung, nämlich die Spiegelung der personenbezogenen Daten im Rechenzentrum in den USA, bereits aus anderen Gründen, die weiter unten unter Ziffer 4.6. erörtert werden, nicht akzeptabel.

*4.2.2. Die Verarbeitung ist erforderlich für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt (Artikel 7 Buchstabe c) der Richtlinie)*

Die Verarbeitung und die Spiegelung könnten erforderlich gewesen sein, um eine rechtliche Verpflichtung zu erfüllen, der der für die Verarbeitung Verantwortliche unterliegt.

SWIFT hat mit seiner Zentrale in Belgien für diese spezielle Verarbeitung formell keine Rechtsgrundlage nach belgischem oder europäischem Recht herangezogen. Die Artikel-29-Gruppe hält ferner fest, dass nach belgischem oder europäischem Recht keine rechtliche Verpflichtung zu dieser speziellen Datenverarbeitung besteht. Ferner hat die Artikel-29-Gruppe bereits in ihrer „SOX-Stellungnahme“<sup>31</sup> dargelegt, dass „eine Verpflichtung aufgrund eines ausländischen Statuts oder einer ausländischen Verordnung (...) möglicherweise nicht als rechtliche Verpflichtung gilt, die die Datenverarbeitung in der EU legitimieren würde. Jede andere Interpretation würde es ausländischen Vorschriften leicht machen, die EU-Vorschriften gemäß der Richtlinie 95/46/EG zu umgehen“. Die Artikel-29-Gruppe ist der Auffassung, dass diese Schlussfolgerung auch für den vorliegenden Fall gilt.

Artikel 7 Buchstabe c) der Datenschutzrichtlinie kann daher in diesem Falle nicht zur Rechtfertigung der Verarbeitung und der Spiegelung der Daten herangezogen werden.

*4.2.3. Die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird (Artikel 7 Buchstabe f) der Richtlinie)*

Gemäß Artikel 7 Buchstabe f) der Richtlinie könnte die Verarbeitung und die Spiegelung zur Verwirklichung des berechtigten Interesses erforderlich sein, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird,

---

<sup>31</sup> Stellungnahme 1/2006 zur Anwendung von EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption sowie Banken- und Finanzkriminalität.

denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt ist, überwiegen.

Fraglich ist, ob Artikel 7 Buchstabe f) der Richtlinie herangezogen werden kann, um die Verarbeitung und die Spiegelung zu rechtfertigen, mit den Folge nämlich, dass die Maßnahmen der Verarbeitung im Rechenzentrum in den USA den Auflagen nach US-Recht unterliegen.

Es ist nicht in Abrede zu stellen, dass SWIFT ein berechtigtes Interesse an der Erfüllung der Auflagen nach US-Recht hat. Hätte SWIFT diesen Anordnungen nicht Folge geleistet, so hätte sie sich dem Risiko von Sanktionen nach US-Recht gegen sie ausgesetzt. Andererseits ist es auch wichtig, ein „ordentliches Gleichgewicht“ zu finden und zu halten, nämlich zwischen den Risiken für SWIFT, von den USA mit Sanktionen wegen etwaiger Nichterfüllung der Auflagen belegt zu werden, und dem Schutz der Rechte des Einzelnen.

Artikel 7 Buchstabe f) der Richtlinie verlangt, dass ein Gleichgewicht hergestellt wird zwischen dem berechtigten Interesse, das durch die Verarbeitung der personenbezogenen Daten verwirklicht wird, und den Grundrechten der betroffenen Person. Bei der Prüfung des Gleichgewichts der Interessen sind die Fragen der Verhältnismäßigkeit, der Subsidiarität, der Schwere der behaupteten Rechtsverletzungen, die mitgeteilt werden können, und die Folgen für die betroffenen Personen zu berücksichtigen. Im Zusammenhang mit der Prüfung des Gleichgewichts der Interessen sind auch angemessene rechtliche Garantien zu gewährleisten. So bestimmt insbesondere Artikel 14 der Richtlinie, dass die betroffene Person das Recht hat, jederzeit aus überwiegenden, schützwürdigen Gründen dagegen Widerspruch einlegen können, dass sie betreffende Daten verarbeitet werden, wenn die Verarbeitung der Daten auf Artikel 7 Buchstabe f) beruht.

SWIFT führte die Verarbeitung und die Spiegelung ihrer Daten „intransparent, systematisch, massiv und dauerhaft“<sup>32</sup> durch, ohne zum Zeitpunkt der Verarbeitung der Daten den weiteren und nicht zu vereinbarenden Zweck spezifiziert und ohne die Nutzer ihrer Dienste auf diesen Zweck hingewiesen zu haben. Diese weitere Verarbeitung und Spiegelung für einen nicht zu vereinbarenden Zweck könnte weit reichende Auswirkungen auf jeden Einzelnen haben.

Die Artikel-29-Gruppe ist daher der Auffassung, dass das Interesse oder die Grundrechte und Grundfreiheiten von vielen betroffenen Personen die Interessen von SWIFT, nicht mit US-Sanktionen wegen etwaiger Nichterfüllung der Auflagen belegt zu werden, überwiegen.

---

<sup>32</sup> Stellungnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.

#### **4.3. Versorgung des Betroffenen mit eindeutigen und vollständigen Informationen über das Vorhaben (Artikel 10 und 11 der Richtlinie)**

Gemäß Artikel 10 und Artikel 11 der Richtlinie ist der für die Verarbeitung Verantwortliche verpflichtet, betroffene Personen über die Tatsache, die Zweckbestimmung und die Funktionsweise seiner Datenverarbeitung, über die Empfänger der personenbezogenen Daten und über das Bestehen von Auskunfts-, Berichtigungs- und Löschungsrechten für den Betroffenen zu informieren. Alle Kunden von Finanzinstituten haben ungeachtet ihrer Nationalität oder ihres Wohnsitzlandes das Recht, zu wissen, was mit ihren „vertraulichen“ Daten passiert.

Die Artikel-29-Gruppe stellt fest, dass diese Informationen in Bezug auf die Verarbeitung und die Spiegelung der Daten im Rechenzentrum in den USA weder durch SWIFT noch durch die betreffenden Finanzinstitute erteilt wurden.

Aufgrund von Artikel 13 der Richtlinie können die EU-Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte nach dieser Richtlinie in gewissem Umfang beschränken. Eine solche Beschränkung muss eine notwendige Maßnahme sein, um z.B. die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen von Einzelfall zu Einzelfall zu gewährleisten, und dies nur, wenn dieser Eingriff unter dem Gesichtspunkt des Artikels 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist. Eine derart lange und umfassende Maßnahme ohne jegliche Information der Betroffenen kann jedoch nicht in Einklang mit Artikel 13 stehen.

#### **4.4. Erfüllung der Meldepflichten (Artikel 18 bis 20 der Richtlinie)**

Die für die Verarbeitung Verantwortlichen müssen die Anforderungen der Artikel 18 bis 20 der Datenschutzrichtlinie bezüglich der Meldung ihrer Datenverarbeitungstätigkeiten an die nationalen Datenschutzbehörden bzw. der Vorabkontrolle durch diese erfüllen.

In den Mitgliedstaaten, in denen ein solches Verfahren vorgesehen ist, unterliegen die Verarbeitungen unter Umständen insofern einer Vorabkontrolle durch die nationale Datenschutzbehörde, als diese Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können. Die Bewertung, ob solche Verarbeitungen unter das Erfordernis der Vorabkontrolle falle, hängt von den nationalen Rechtsvorschriften und von der Praxis der nationalen Datenschutzbehörden ab.

Die Artikel-29-Gruppe hält fest, dass SWIFT der belgischen Datenschutzbehörde zwar einige Verarbeitungsarten gemeldet hat<sup>33</sup>, nicht aber die Verarbeitung und die Spiegelung im Rechenzentrum in den USA, die der Durchführung von internationalen Zahlungsaufträgen diene, und auch nicht den weiteren Zweck mitgeteilt hat.

#### **4.5. Aufsichtsmechanismen**

Die Einrichtung von Datenschutzaufsichtsbehörden in den EU-Mitgliedstaaten, die ihre Aufgaben völlig unabhängig wahrnehmen, stellt eine wesentliche Komponente für den

---

<sup>33</sup> Stellungnahme der belgischen Datenschutzbehörde, vgl. Fußnote 8.



Schutz des Bürgers bei der Verarbeitung personenbezogener Daten dar. Dieser Grundsatz der völligen Unabhängigkeit der Kontrollstelle ist in Artikel 28 der Richtlinie festgelegt.

Aufgrund der mangelnden Informationen durch SWIFT, die Finanzinstitute und die Aufsichtsführenden in der nationalen Datenkontrollstelle konnten die vorhandenen Datenschutz-Kontrollmechanismen der Richtlinie nicht effektiv angewandt werden. Die Artikel-29-Gruppe bedauert, dass keine formelle oder informelle Vorabkonsultation der SWIFT oder der Finanzinstitute mit den Datenschutzbehörden in Bezug auf die Verarbeitung und Spiegelung von personenbezogenen Daten im Rechenzentrum in den USA stattgefunden hat.

Die Überprüfungen durch die nationalen Behörden ergaben, dass die Kontrollmaßnahmen, die SWIFT zur Übermittlung der SWIFT-Daten an das US-Finanzministerium (UST) durchführte, hauptsächlich aus den Kontrollen einer privaten Wirtschaftsprüfungsgesellschaft bestanden sowie aus der Überprüfung durch SWIFT-Angestellte („Innenrevisoren“), die aber aus Sicherheitsgründen keine Einzelheiten über die internen Feststellungen berichten durften. SWIFT gab ferner an, von einem hochrangigen Ausschuss aus Vertretern der G-10-Zentralbanken beaufsichtigt zu werden und dieses Aufsichtsgremium in der Angelegenheit der US-Anweisungen informiert zu haben.

Zwar können die von SWIFT durchgeführten Kontrollmaßnahmen zur einer erhöhten Sicherheit der Datenverarbeitung beitragen, doch besteht die Artikel-29-Gruppe mit Nachdruck auf der Tatsache, dass keine anderweitigen Mechanismen, die von den für die Verarbeitung Verantwortlichen bereitgestellt werden, die Kontrolle der Datenverarbeitung durch eine öffentliche und unabhängige Kontrollstelle gemäß den Anforderungen nach Artikel 28 der Richtlinie ersetzen können. Jedenfalls erklärte sich die von den G-10-Zentralbanken eingesetzte Aufsichtsgruppe für unzuständig, Fragen im Zusammenhang mit dem Schutz von personenbezogenen Daten zu untersuchen.

Die Artikel-29-Gruppe missbilligt im Ergebnis die Tatsache, dass die vorhandenen Mechanismen für eine unabhängige Kontrolle durch die öffentlichen Kontrollstellen für die Verarbeitung von personenbezogenen Daten bei den durch den SWIFTNet FIN-Service verarbeiteten personenbezogenen Daten umgangen worden sind.

#### **4.6. Grenzüberschreitender Datenfluss (Artikel 25 und 26 der Richtlinie)**

Artikel 25 und 26 der Richtlinie finden Anwendung, wenn personenbezogene Daten in ein Drittland übermittelt werden. Jegliche Übermittlung von Daten, die im Hoheitsgebiet der EU erhoben wurden und außerhalb des EU-Territoriums verwendet werden sollen, muss nach der Richtlinie einer Bewertung der Angemessenheit des Schutzniveaus unterzogen werden. Darüber hinaus können die Bestimmungen der Richtlinie, die sich auf die Übermittlung von personenbezogenen Daten an Drittländer beziehen, nicht getrennt von den übrigen Bestimmungen der Richtlinie angewandt werden. Wie in Artikel 25 Absatz 1 ausdrücklich bestimmt ist, gelten diese Bestimmungen „vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften“. Dies bedeutet, dass ungeachtet der

Bestimmungen, auf sich die Übermittlung von Daten an ein Drittland stützt, auch noch die anderen einschlägigen Bestimmungen der Richtlinie einzuhalten sind<sup>34</sup>.

Die normale Funktionsweise des SWIFTNet-FIN Services umfasst aufgrund der Standorte der SWIFT-Rechenzentren auch einen ständigen und massiven grenzüberschreitenden Datenfluss. Die Rechenzentren von SWIFT sind keine eigenständigen Rechtssubjekte, sondern Außenstellen (*“succursales”*) der genossenschaftlichen Gesellschaft nach belgischem Recht. Die Übertragungsschaltung und Zwischenspeicherkapazität der beiden Rechenzentren von SWIFT in Europa und in den USA funktioniert folgendermaßen: Die Überweisungsdaten werden in den Rechenzentren automatisch entschlüsselt, um die Informationen in nur wenigen tausendstel Sekunden zwischenzuspeichern. Dieser „Zwischenspeicherungsprozess“ dient der Zulässigkeitsprüfung (Kontrolle auf Richtigkeit oder auf Eintragungen von Buchstaben/Zahlen in den obligatorischen Mitteilungsfeldern) der Informationen (z.B. der Sicherstellung, dass das richtige Währungskürzel für die Geldüberweisung eingetragen ist, z.B. “EUR”) auf der Grundlage von standardisierten Inhalten. Während dieses Prozesses werden die Informationen aus Sicherheitsgründen (Sicherungskopie) auch für 124 Tage in beiden Rechenzentren abgespeichert und stellen dann perfekte „Spiegelbilder“ dar. Damit wird sichergestellt, dass die Datenspeicherung parallel erfolgt und die Daten identisch sind.

Damit SWIFT personenbezogene Daten rechtmäßig in den USA verarbeiten und spiegeln kann, müssen zunächst diese Daten aus der EU dorthin übermittelt werden, und zwar gemäß belgischem Recht, das in Umsetzung der Datenschutzrichtlinie erlassen wurde, und insbesondere in Übereinstimmung mit den Artikeln 25 und 26 über die Übermittlung personenbezogener Daten in Drittländer. Die Datenübermittlungen von SWIFT in die Vereinigten Staaten sind daher unter Berücksichtigung von zweierlei Gesichtspunkten zu betrachten: Erstens unter dem Gesichtspunkt der wirtschaftlichen Verarbeitung und Spiegelung der personenbezogenen Daten durch SWIFT Belgien im Wege der Übermittlung an ihr Rechenzentrum in den USA und zweitens unter dem Gesichtspunkt der Verarbeitung dieser Daten für einen weiteren Zweck im Wege der mit SWIFT vereinbarten Nutzung durch das US-Finanzministerium (UST).

#### *4.6.1. Angemessener Datenschutz (Artikel 25 Absatz 1 der Richtlinie)*

Gemäß Artikel 25 Absatz 2 der Richtlinie wird die Angemessenheit des Schutzniveaus, das ein Drittland bietet, „unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Landesregeln und Sicherheitsmaßnahmen berücksichtigt.“

Unter Berücksichtigung der vorstehenden Kriterien und in Anwendung der in der Arbeitsunterlage WP12<sup>35</sup> festgelegten Grundsätze ist die Artikel-29-Gruppe der

---

<sup>34</sup> Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114.

Auffassung, dass in den USA derzeit nur die “Safe Harbour“-Nichtbeanstandungsregelung ein angemessenes Schutzniveau für Datenübermittlungen aus der EU an die US-Organisationen bietet, die dieser Regelung beigetreten sind. Finanzielle Dienstleistungen werden von ihr jedoch nicht erfasst<sup>36</sup>.

Daher konnte sich SWIFT als belgisches Rechtssubjekt für die Verarbeitung und Spiegelung in seinem Rechenzentrum in den USA nicht auf Artikel 25 der Richtlinie stützen.

#### 4.6.2. Der Empfänger der Daten garantiert angemessene Datenschutzmaßnahmen (Artikel 26 Absatz 2 der Richtlinie)

Gemäß Artikel 26 Absatz 2 der Richtlinie kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch dann genehmigen, wenn der für die Verarbeitung der Daten Verantwortliche „ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet“. Nach dem letzten Halbsatz von Artikel 26 Absatz 2 „können sich diese Garantien insbesondere aus entsprechenden Vertragsklauseln ergeben“. Zur Erleichterung der Verwendung von Vertragsklauseln hat die Europäische Kommission drei Entscheidungen hinsichtlich Standardvertragsklauseln veröffentlicht, wovon zwei die Übermittlung von einem für die Verarbeitung von Daten Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen regeln, während die dritte die Übermittlung von einem für die Verarbeitung von Daten Verantwortlichen an einen Auftragsverarbeiter betrifft<sup>37</sup>. Abgesehen von der Möglichkeit, Vertragsklauseln zu benutzen, um so ausreichende Garantien zu bieten, hat die Artikel-29-Gruppe seit 2003 zusätzlich an der Möglichkeit gearbeitet, dass multinationale Unternehmensgruppen „verbindliche unternehmensinterne Vorschriften“ für dieselben Zwecke verwenden können<sup>38</sup>.

---

<sup>35</sup> „Übermittlung personenbezogener Daten an Drittländer : Anwendung von Artikeln 25 und 26 der EU-Datenschutzrichtlinie“, von der Art. 29-Gruppe angenommen am 24. Juli 1998; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/1998/wp12\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf).

<sup>36</sup> vgl. [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)

<sup>37</sup> In Bezug auf die Übermittlung von einem für die Verarbeitung Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen veröffentlichte die Kommission den ersten Satz Standardvertragsklauseln am 15. Juni 2001; in der Folge ergänzte sie diese Entscheidung, um einen neuen Satz alternativer Klauseln anzufügen (mit Entscheidung vom 27. Dezember 2004). In Bezug auf die Übermittlung von einem für die Verarbeitung Verantwortlichen an einen Auftragsverarbeiter veröffentlichte die Kommission einen Satz Standardvertragsklauseln am 27. Dezember 2001. Alle diese Klauseln sind auf folgender Website abzurufen: [http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm).

<sup>38</sup> Vgl. Arbeitsdokument WP 74, „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“, von der Artikel-29-Gruppe angenommen am 3. Juni 2003 mit weiteren ergänzenden Dokumenten WP107 und WP108.

Im vorliegenden Fall hat SWIFT jedoch für die Verarbeitung und Spiegelung in seinem Rechenzentrum in den USA keinen Gebrauch von diesen Möglichkeiten gemacht.<sup>39</sup>

#### 4.6.3. Ausnahmen (Artikel 26 der Richtlinie)

Nach Artikel 26 Absatz 1 der Richtlinie können Übermittlungen von personenbezogenen Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, vorgenommen werden, wenn eine der folgenden unter Buchstaben a) bis f) aufgeführten Voraussetzungen erfüllt ist. Wie die Artikel-29-Gruppe bereits in ihrem oben erwähnten Arbeitsdokument WP12<sup>40</sup> ausgeführt hat, ist Artikel 26 Absatz 1 zwangsläufig eng auszulegen.

In dieser Hinsicht möchte die Artikel-29-Gruppe betonen, dass diese Logik dieselbe ist wie die des Zusatzprotokolls zur Konvention 108 des Europarates. Im Bericht über dieses Protokoll wird festgestellt, dass „es im Ermessen der Vertragsparteien steht, Ausnahmen vom Grundsatz des angemessenen Schutzniveaus festzulegen. Die entsprechenden innerstaatlichen Rechtsvorschriften müssen jedoch den dem europäischen Recht innewohnenden Grundsatz beachten, dass Ausnahmeklauseln eng auszulegen sind, damit die Ausnahme nicht zur Regel wird“.<sup>41</sup>

Im vorliegenden Falle sind die folgenden Ausnahmen möglich:

##### 4.6.3.1. Die betroffene Person hat ihre Einwilligung gegeben (Artikel 26 Absatz 1 Buchstabe a) der Richtlinie)

Damit man sich rechtswirksam auf diese Ausnahme berufen kann, muss die betroffene Person ohne jeden Zweifel ihre Einwilligung zu der betreffenden Übermittlung gegeben haben. Wie bereits im Arbeitsdokument WP 12 der Artikel-29-Gruppe ausgeführt, muss diese Einwilligung, wie auch immer die Umstände sind, unter denen sie gegeben wird, gemäß der Legaldefinition des Artikels 2 Buchstabe h) der Richtlinie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben sein und den Willen des Betroffenen zu Ausdruck bringen.<sup>42</sup> Die betroffene Person muss darüber informiert sein, dass es sich bei der betreffenden Übermittlung um ein Drittland ohne angemessenes Schutzniveau oder um ein Drittland handelt, in dem keine ausreichenden Garantien geboten werden, und kann aufgrund dessen entscheiden, ob er das damit verbundene Risiko eingehen will oder nicht.

---

<sup>39</sup> Sollte SWIFT jedoch Gebrauch von diesen Möglichkeiten machen, so möchte die Artikel-29-Gruppe in Erinnerung rufen, dass die Ausnahmen vom geltenden Datenschutzrecht für alle künftigen Datenübermittlungen in jedem Falle nicht über die in einer demokratischen Gesellschaft notwendigen Beschränkungen hinausgehen dürfen.

<sup>40</sup> Vgl. oben, Fußnote 35.

<sup>41</sup> Vgl. Bericht über das Zusatzprotokoll zur Konvention 108 über Kontrollbehörden und grenzüberschreitende Datenströme, Artikel 2 Absatz 2 Buchstabe a); dieses Dokument ist abzurufen unter

<http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm>

<sup>42</sup> Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114.

SWIFT hat keine ‚Einwilligung ohne jeden Zweifel‘ von den Personen erhalten, die von der Verarbeitung und Spiegelung im Rechenzentrum in den USA betroffen sind, und kann sich daher nicht auf Artikel 26 Absatz 1 Buchstabe a) der Richtlinie berufen.

*4.6.3.2. Die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe b) der Richtlinie)*

Diese Ausnahme bedeutet, dass die übermittelten Daten auch tatsächlich zu Zwecken der Erfüllung dieses Vertrags oder dieser vorvertraglichen Maßnahmen erforderlich sein müssen. Daher vertritt die Artikel-29-Gruppe die Rechtsauffassung, dass diese Bedingung nicht auf die Datenübermittlungen von SWIFT an ihr Rechenzentrum in den USA anwendbar ist, da SWIFT keine direkten Vertragsbeziehungen mit den betroffenen Personen unterhält. Ebenso wenig ist diese Ausnahme auf die Übermittlung von zusätzlichen Informationen, die nicht zu Übertragungszwecken benötigt werden, oder auf eine Übermittlung, die einem anderen Zweck als der Erfüllung des Vertrags dient, anwendbar. Ganz allgemein gesagt gestatten es die Ausnahmen nach Artikel 26 Absatz 1 Buchstaben b) bis e) nur, dass die Daten, die zu Übermittlungszwecken erforderlich sind, auf der Grundlage der individuellen Ausnahme übermittelt werden dürfen; für Zusatzdaten ist auf andere Mittel zurückzugreifen, um den Beweis der Angemessenheit zu erbringen.

*4.6.3.3. Die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder werden soll (Artikel 26 Absatz 1 Buchstabe c) der Richtlinie)*

Wie dies schon bei der Ausnahme nach Artikel 26 Absatz 1 Buchstabe b) der Fall war, kann bei einer Übermittlung von Daten in ein Drittland, das keinen angemessenen Schutz gewährleistet, auch nicht davon ausgegangen werden, dass sie unter den Ausnahmetatbestand von Artikel 26 Absatz 1 Buchstabe c) fällt, es sein denn sie gilt als tatsächlich „zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll“, und sie besteht die entsprechende „Erforderlichkeitsprüfung“. Dabei ist nachzuweisen, dass ein enger und substantieller Zusammenhang zwischen dem Interesse der betroffenen Person und dem Vertragszweck besteht.<sup>43</sup>

Die Artikel-29-Gruppe ist der Auffassung, dass auch diese Voraussetzung nicht auf die Datenübermittlungen von SWIFT an sein Rechenzentrum in den USA anwendbar ist.

*4.6.3.4. Die Übermittlung ist entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder*

---

<sup>43</sup> Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114

*gesetzlich vorgeschrieben (Artikel 26 Absatz 1 Buchstabe d) der Richtlinie)*

SWIFT legte dar, die Spiegelung der Datenverarbeitung an ihre Rechenzentren gelte als wichtiger Baustein im globalen Finanzsystem, diese Spiegelung der Datenverarbeitung sei von den Aufsichtsführenden (G-10 Zentralbanken) aus Sicherheits- und Verlässlichkeitsgründen vorgeschlagen worden und die Infrastruktur von SWIFT werde als für das globale Finanzgewerbe wesentlich angesehen. SWIFT behauptet, dieser Grund rechtfertige die Übermittlung auf der Rechtsgrundlage von Artikel 26 Absatz 1 Buchstabe d) der Richtlinie.

Die Artikel-29-Gruppe kann dieser Auslegung nicht folgen. Selbst wenn erwiesen wäre, dass die internationale Spiegelung der Verarbeitung (auf einem anderen als dem europäischen Kontinent) im Sinne von Artikel 26 Absatz 1 Buchstabe d) der Richtlinie „für die Wahrung eines wichtigen öffentlichen Interesses erforderlich oder gesetzlich vorgeschrieben ist“, so ist es immer möglich, die Spiegelung einer solchen Verarbeitung in einem Land außerhalb der EU oder des EWR, das ein angemessenes Schutzniveau bereitstellt, vorzunehmen. Die Artikel-29-Gruppe bezieht sich dabei auf Länder wie z.B. Argentinien<sup>44</sup> oder Kanada<sup>45</sup>, die nach den Entscheidungen der Europäischen Kommission den Anforderungen der Richtlinie genügen. Die „Spiegelung“ in einem Nicht-EU-Land ohne ein angemessenes Datenschutzniveau war und ist nicht erforderlich und auch nicht im Rahmen von Artikel 26 Absatz 1 Buchstabe d) zu rechtfertigen.

Darüber hinaus wurden personenbezogene Daten, die im Rahmen des SWIFT-Netzes für internationale Geldüberweisungen unter Nutzung des BIC- oder des SWIFT-Codes erhoben und verarbeitet und in den USA gespiegelt worden waren, seit Ende 2001 aufgrund von Anordnungen nach US-Recht dem US-Finanzministerium (UST) bereitgestellt.

Die vollkommene Rückverfolgbarkeit von Geldüberweisungen kann ein besonders wichtiges und wertvolles Instrument bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Geldwäsche und Terrorismusfinanzierung sein und war Gegenstand einer Regelung nach EU-Recht<sup>46</sup>.

Die Artikel-29-Gruppe erkennt an, dass demokratische Gesellschaften die Terrorismusbekämpfung im Interesse der staatlichen Sicherheit als legitimes Ziel verfolgen, und dass zu diesem berechtigten Zweck Maßnahmen ergriffen werden können, die mit dem fundamentalen Recht auf Schutz der personenbezogenen Daten im Widerstreit stehen. Sie erinnert daran, dass sie sich diesen Aufgaben uneingeschränkt verpflichtet fühlt, aber auch der Ansicht ist, dass die internationalen Instrumente sehr wohl ein angemessenes rechtliches Rahmenwerk liefern, auf der Grundlage dessen eine internationale Zusammenarbeit möglich ist. Zu diesem Zweck sollten nach Auffassung

---

<sup>44</sup> Entscheidung der Kommission C(2003) 1731 vom 30. Juni 2003; ABl. L 168 vom 5.7.2003.

<sup>45</sup> Entscheidung der Kommission 2002/2/EG vom 20.12.2001 über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet; ABl. L 2/13 vom 4.1.2002.

<sup>46</sup> Z.B. Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, verabschiedet am 8. November 2006, noch nicht veröffentlicht; ursprünglich Vorschlag der Kommission, KOM (2005) 343.

der Artikel 29-Gruppe die bereits vorhandenen Möglichkeiten, die durch die aktuellen Formen der internationalen Zusammenarbeit geboten werden, und die im Hinblick auf die Terrorismusbekämpfung und die Terrorismuserforschung entstanden sind, noch mehr ausgeschöpft und zugleich das erforderliche Maß an Grundrechtsschutz sichergestellt werden.

Die Artikel-29-Gruppe stellt aber nichtsdestoweniger fest, dass Artikel 26 Absatz 1 Buchstabe d) der Richtlinie auch nicht greift, da die Übermittlung nicht für die Wahrung eines wichtigen öffentlichen Interesses eines EU- Mitgliedstaates (Belgien) erforderlich oder gesetzlich vorgeschrieben ist. Bei diesem Punkt der Richtlinie hatten die Verfasser ganz klare Vorstellungen, dass in diesem Zusammenhang nur wichtige öffentliche Interessen darunter fallen, die von der nationalen Gesetzgebung, die auf die in der EU niedergelassenen für die Verarbeitung von Daten Verantwortlichen Anwendung findet, auch als solche bezeichnet sind. Jede andere Auslegung würde es einer ausländischen Behörde leicht machen, das in der Richtlinie festgelegte Erfordernis eines angemessenen Schutzes im Empfängerland zu umgehen.

*4.6.3.5. Die Übermittlung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich (Artikel 26 Absatz 1 Buchstabe e) der Richtlinie)*

Diese Ausnahme trifft auf Übermittlungen zu, die mit dem individuellen Interesse der betroffenen Person zusammenhängen müssen, und, wenn es sich um Gesundheitsdaten handelt, so muss die Übermittlung für eine wichtige Diagnose erforderlich sein. Demzufolge könnte dieser Ausnahmetatbestand nicht herangezogen werden, um die Übermittlung von personenbezogenen medizinischen Daten zu Zwecken wie etwa allgemeinen medizinischen Forschungsarbeiten zu rechtfertigen.<sup>47</sup>

SWIFT hat nicht behauptet, dass die Übermittlung zur Wahrung lebenswichtiger Interessen der von der Verarbeitung und Spiegelung im Rechenzentrum in den USA betroffenen Personen erforderlich ist. Die Artikel-29-Gruppe ist auch der Auffassung, dass diese Ausnahme hier in jedem Fall irrelevant ist. Artikel 26 Absatz 1 Buchstabe e) der Richtlinie kann also auch nicht herangezogen werden.

*4.6.4. Feststellungen*

SWIFT hätte aufgrund von Artikel 26 Absatz 2 der Richtlinie eine rechtmäßige Übermittlung von personenbezogenen Daten an ihr Rechenzentrum in den USA vornehmen können. Jedoch hat sich SWIFT dazu entschieden, die personenbezogenen Daten zu übermitteln, ohne die rechtlichen Anforderungen nach belgischem Recht zu erfüllen, denen derartige internationale Datentransfers unterliegen.

SWIFT kann keine der anderen Ausnahmen von Artikel 26 der Richtlinie für sich geltend machen.

---

<sup>47</sup> Artikel-29-Gruppe: Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995. WP 114; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf).

Was die Verarbeitung und die Spiegelung in den USA anbelangt, so ist selbst die kommerzielle Verarbeitung und Spiegelung nicht rechtmäßig erfolgt. Die kontinuierliche Verarbeitung und Spiegelung bleibt angesichts ihres überdies nicht zu vereinbarenden Zwecks und ihres großen Ausmaßes nicht in den Grenzen dessen, was in einer demokratischen Gesellschaft erforderlich ist, und hindert SWIFT des Weiteren an der Übermittlung von personenbezogenen Daten in die USA.

## 5. SCHLUSSFOLGERUNGEN:

Aufgrund dessen ist die Artikel-29-Gruppe folgender Auffassung:

- 5.1. Die EU-Datenschutzrichtlinie 95/46/EG ist auf den Austausch von personenbezogenen Daten durch den SWIFTNet FIN Service anwendbar;
- 5.2. SWIFT und die Finanzinstitute tragen nach den Vorgaben der Richtlinie gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten durch den SWIFTNet FIN Service. Auch wenn SWIFT dabei die Hauptverantwortung trägt, sind die Finanzinstitute in gewissem Umfang für diese Verarbeitung der personenbezogenen Daten ihrer Kunden mitverantwortlich.
- 5.3. SWIFT und die Finanzinstitute in der EU haben die Vorgaben der Richtlinie nicht beachtet:
  - 5.3.1. *SWIFT*: Hinsichtlich der Verarbeitung und der Spiegelung personenbezogener Daten im Rahmen des SWIFTNet FIN Services muss SWIFT seinen Verpflichtungen nach der Richtlinie als der für die Verarbeitung verantwortlichen Stelle nachkommen; dies betrifft insbesondere die Informationspflichten, die Meldepflicht und die Verpflichtung zur Wahrung eines angemessenen Schutzniveaus bei internationalen Datentransfers;
  - 5.3.2. *Finanzinstitute*: Die Finanzinstitute in der EU müssen als die für die Verarbeitung von personenbezogenen Daten verantwortlichen Stellen ihrer rechtlichen Verpflichtung nachkommen und sicherstellen, dass SWIFT vollständig die rechtlichen Anforderungen, insbesondere auch des Datenschutzrechts, erfüllt, um den Schutz ihrer Kunden zu gewährleisten. Die Finanzinstitute müssen sich auch über die unterschiedlichen Zahlungssysteme, deren technische und rechtliche Ausgestaltung und die damit verbundenen Risiken informieren. Soweit Finanzinstitute sich nicht (hinreichend) bemüht haben, sich diese Kenntnisse zu beschaffen, haben sie wesentliche rechtliche Risiken hinsichtlich ihrer grundlegenden Sorgfaltspflichten gegenüber ihrer Kunden in Kauf genommen. Die Artikel-29-Gruppe hält es für unabdingbar, dass die Finanzinstitute als professionelle Dienstleister ihre Kunden in Übereinstimmung mit den Transparenzforderungen der Richtlinie hinreichend unterrichten, insbesondere über die Inanspruchnahme von Dienstleistern wie z.B. den SWIFTNet FIN Service, die umfangreiche Übermittlungen in Länder ohne adäquates Datenschutzniveau nach der Richtlinie



durchführen, oder wenn solche Übermittlungen besondere Bedenken oder Risiken aus Datenschutzsicht hervorrufen.

- 5.4. Die Artikel-29-Gruppe vertritt zudem die Auffassung, dass der Mangel an Transparenz sowie an angemessenen und effektiven Kontrollmechanismen beim gesamten Prozess der Übermittlung von personenbezogenen Daten in die USA und weiter an das US-Finanzministerium eine schwere Verletzung der Richtlinie darstellt. Darüber hinaus sind auch die Garantien für die Datenübermittlung in ein Drittland, wie sie die Richtlinie vorsieht, und die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit nicht beachtet worden.

Bezüglich der Übermittlung von personenbezogenen Daten an UST ist die Artikel-29-Gruppe der Ansicht, dass der intransparente, systematische, massive und dauerhafte Transfer von personenbezogenen Daten von SWIFT an UST in einer heimlichen, intransparenten und systematischen Art über Jahre hinweg ohne geltende Rechtsgrundlage und ohne die Möglichkeit einer unabhängigen Überprüfung durch öffentliche Aufsichtsbehörden eine Verletzung europäischer Datenschutzgrundsätze darstellt und nicht in Übereinstimmung mit belgischem und europäischem Recht steht. Für den Kampf gegen den Terrorismus gibt es bereits einen internationalen Rechtsrahmen. Die dort bestehenden Möglichkeiten sollten konsequent unter Sicherstellung des erforderlichen Schutzes der Grundrechte genutzt werden.

- 5.5. Die Artikel-29-Gruppe erinnert noch einmal<sup>48</sup> an die Verpflichtung der demokratischen Gesellschaften, die Grundrechte und Grundfreiheiten des Einzelnen zu achten. Der Schutz der personenbezogenen Daten des Einzelnen ist Teil dieser Grundrechte und Grundfreiheiten<sup>49</sup>. Die Datenschutzrichtlinien 95/46/EG und 2002/58/EG der Gemeinschaft bilden einen Teil dieser Verpflichtung<sup>50</sup>. Beide Richtlinien zielen auf die Achtung der Grundrechte und Grundfreiheiten und insbesondere auf das Recht auf Privatsphäre einschließlich des Schutzes von personenbezogenen Daten ab. Sie zielen auch auf die Achtung der Rechte, die durch Art. 8 der Europäischen Menschenrechtskonvention (EMRK) und durch Art. 8 der Europäischen Charta der Grundrechte geschützt werden. In all diesen Rechtsinstrumenten sind Ausnahmen für die Verbrechensbekämpfung unter klar definierten Bedingungen vorgesehen.

---

<sup>48</sup> Artikel-29-Datenschutzgruppe: Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus, abrufbar unter; [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2001\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm).

<sup>49</sup> Siehe insbesondere Art. 8 der Charta der Grundrechte der Europäischen Union wie auch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in den Rechtssachen "Aman" vom 16. Februar 2000 und "Rotaru" vom 4. Mai 2000.

<sup>50</sup> Siehe die Erwägungsgründe 1, 2, 10 und 11 der Richtlinie 95/46/EG.

## **6. SOFORTIGER HANDLUNGSBEDARF ZUR VERBESSERUNG DER GEGENWÄRTIGEN SITUATION:**

**Daher fordert die Artikel-29-Gruppe folgende sofortige Maßnahmen zur Verbesserung der derzeitigen Situation:**

- 6.1. **Beendigung der Rechtsverletzungen:** SWIFT und die Finanzinstitute müssen ihren rechtlichen Verpflichtungen nach nationalem und europäischem Recht nachkommen. Dies beinhaltet Maßnahmen, die sicherstellen, dass alle Datenübermittlungen in Übereinstimmung mit geltendem Recht erfolgen. Im Falle der Nichtbeachtung müssen die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen mit Sanktionen zur Rechtsdurchsetzung durch die zuständigen Aufsichtsbehörden nach den Vorgaben der Richtlinie und jeweiligem nationalem Recht rechnen.
- 6.2. **Rückkehr zur rechtmäßigen Datenverarbeitung:** Die Artikel-29-Gruppe fordert SWIFT und die Finanzinstitute dazu auf, unverzüglich Maßnahmen zu ergreifen, die die gegenwärtige unrechtmäßige Situation beenden und nur noch internationale Datenüberweisungen durchzuführen, die in vollständiger Übereinstimmung mit dem Datenschutzrecht stehen. Die Artikel-29-Gruppe begrüßt, dass einige Aufsichtsbehörden die Finanzinstitute bereits dazu drängen, unverzüglich eine Lösung zu suchen.
- 6.3. **Handlungsbedarf gegenüber SWIFT:** SWIFT als für die Datenverarbeitung verantwortliche Stelle muss hinsichtlich aller seiner Daten verarbeitenden Tätigkeiten die erforderlichen Maßnahmen ergreifen, zu denen sie das belgische Datenschutzgesetz in Umsetzung der Richtlinie verpflichtet.
- 6.4. **Handlungsbedarf gegenüber den Zentralbanken:** Die jetzige Situation bedarf einer Klärung der Aufsichtsstrukturen bei SWIFT. Die Artikel-29-Gruppe empfiehlt deshalb angemessene Lösungen. Dazu gehört insbesondere, dass die Umsetzung von datenschutzrechtlichen Regelungen klar unter diese Aufsichtspflicht fällt, unbeschadet der Befugnisse der nationalen Datenschutzaufsichtsbehörden. Auch gehört dazu sicherzustellen, dass die zuständigen Behörden, wenn notwendig, vorschriftsmäßig und rechtzeitig unterrichtet werden. Die Artikel-29-Gruppe vertritt die Ansicht, dass die Nichtbefolgung von Datenschutzgesetzen das Vertrauen der Kunden in ihre Banken erschüttern kann und dies auch die finanzielle Stabilität von Zahlungssystemen zu beeinträchtigen vermag (Vertrauensrisiko). Rechtliche Hindernisse, wie die Verpflichtung zur Einhaltung des Berufsgeheimnisses durch die Aufsichtsgremien, die als Argumente dazu benutzt werden könnten, die effektive Kontrolle der unabhängigen Aufsichtsbehörden einzuschränken, können im Falle einer möglichen Verletzung von verfassungsmäßigen Rechten oder Menschenrechten nicht angeführt werden.
- 6.5. **Handlungsbedarf gegenüber den Finanzinstituten:** Alle Finanzinstitute in der EU, einschließlich der Zentralbanken, die die Dienstleistungen des SWIFTNet Fin Service benutzen, haben gemäß Artikeln 10 und 11 der Richtlinie 95/46/EG sicherzustellen, dass sie ihre Kunden angemessen

darüber unterrichten, wie deren Daten verarbeitet werden und welche Rechte die Betroffenen haben. Sie haben sie auch darüber zu informieren, dass die US-Behörden Zugriff auf die Daten haben können. Die Datenschutzaufsichtsbehörden werden diese Informationspflicht durchsetzen, um sicherzustellen, dass sie europaweit von allen Finanzinstituten eingehalten werden. Sie werden auch bei der Abfassung einheitlicher Informationstexte zusammenarbeiten. Die Artikel-29-Gruppe erinnert in diesem Zusammenhang an ihre Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten<sup>51</sup>. Es scheint auch angemessen, dass die Finanzinstitute und Zentralbanken technische Alternativen zu den derzeitigen Verfahren in Erwägung ziehen, um einen Zahlungstransfer zu gewährleisten, der im Einklang mit den Grundsätzen der Richtlinie steht.

### **Die Artikel-29-Gruppe hebt Folgendes hervor:**

- 6.6. **Wahrung unserer Grundwerte im Kampf gegen das Verbrechen:** Die Artikel-29-Gruppe erinnert daran, dass jede im Kampf gegen Verbrechen und Terrorismus getroffene Maßnahme nicht die Standards hinsichtlich des Schutzes von Grundrechten beeinträchtigen soll und darf, die unsere demokratischen Gesellschaften auszeichnen. Im Kampf gegen den Terrorismus ist es unabdingbar, dass die Grundwerte geschützt werden, die die Basis unserer demokratischen Gesellschaft bilden und bei denen es sich genau um die Werte handelt, die Terroristen zu zerstören suchen.
- 6.7. **Globale Datenschutzgrundsätze:** Die Artikel-29-Gruppe erachtet es als wesentlich, dass die Grundsätze zum Schutz personenbezogener Daten einschließlich der Kontrolle durch unabhängige Aufsichtsbehörden auch im Rahmen eines weltweiten Austauschs von Informationen vollständige Beachtung finden.

**Die Artikel-29-Gruppe wird alle vorstehenden Punkte überwachen und einer Erfolgskontrolle unterziehen.**

Brüssel, den 22. November 2006

*Für die Datenschutzgruppe*  
Der Vorsitzende  
Peter Schar

---

<sup>51</sup> Artikel-29-Datenschutzgruppe: „Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten“ vom 25. November 2004, WP 100;  
[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp100\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf).