EUROPÄISCHE KOMMISSION

Brüssel, den 13.7.2011
KOM(2011) 429 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung

1. EINLEITUNG

Als der Rat dem Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus („TFTP-Abkommen“)[1] zustimmte, forderte er die Kommission gleichzeitig auf, dem Europäischen Parlament und dem Rat spätestens ein Jahr nach dem (am 1. August 2010 erfolgten) Inkrafttreten des Abkommens „einen rechtlichen und technischen Rahmen für die Extraktion der Daten auf dem Gebiet der EU“ vorzulegen[2]. Das Europäische Parlament hat wiederholt gefordert, auf lange Sicht eine dauerhafte, rechtlich fundierte europäische Lösung für die Extraktion der angeforderten Daten auf europäischem Boden einzuführen[3]. In der Mitteilung „EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa“ ist bereits festgehalten, dass die Kommission 2011 ein EU-Konzept für die Extraktion und Auswertung von in der EU gespeicherten Finanztransaktionsdaten entwickeln wird.[4] Angesichts der erwiesenen Wirksamkeit des TFTP-Abkommens mit den USA wird erwartet, dass ein europäisches System entscheidend dazu beitragen kann, den Zugang von Terroristen zu Ausrüstung und Finanzierung zu unterbinden sowie ihre Transaktionen nachzuverfolgen. Artikel 11 des TFTP-Abkommens sieht vor, dass die Kommission während der Laufzeit des Abkommens eine Studie über die mögliche Einführung eines vergleichbaren EU-Systems durchführt, das eine gezieltere Datenübermittlung erlaubt. Diese Mitteilung ist der erste Teil der Reaktion der Kommission auf diesen Artikel und die Forderung des Rates. In ihr werden die Maßnahmen beschrieben, die die Kommission zur Entwicklung des geforderten „rechtlichen und technischen Rahmens“ ergriffen hat, und Möglichkeiten aufgezeigt, wie dieses Ziel erreicht werden könnte. Im derzeitigen Stadium wird noch keine Option bevorzugt. Daher werden alle zu berücksichtigenden Aspekte der in Betracht kommenden Optionen vorgestellt. Angesichts der politischen Bedeutung dieses Themas und seiner rechtlichen wie technischen Komplexität möchte die Kommission den Rat und das Europäische Parlament über den Stand der Überlegungen informieren und eine Diskussion ins Leben rufen. Die Kommission hält es für sinnvoll, zunächst eine vertiefende Debatte durchzuführen und dann auf der Grundlage einer Folgenabschätzung konkrete Vorschläge vorzulegen.

---

1 ABl. L 195 vom 27.7.2010, S. 5.

2 Beschluss des Rates vom 13. Juli 2010 über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (ABl. L 195 vom 27.7.2010, S. 3).

3 Siehe beispielsweise die Entschließung P7_TA(2010)0143 und die Begründung für die Empfehlung A7-0224/2010.

4 KOM(2010) 673 endg. vom 22.11.2010. Siehe Maßnahme 2 unter Ziel 2, S. 8.

Mit dieser Mitteilung soll in keiner Weise dem geplanten Vorschlag der Kommission vorgegriffen werden. Letzterer wird den genannten Diskussionen Rechnung tragen und die Ergebnisse einer Folgenabschätzung berücksichtigen, die sich auf eine Studie gründen wird, die die Kommission im zweiten Halbjahr 2010 in Auftrag gegeben hat. Wegen der Auswirkungen eines Legislativvorschlags auf die Grundrechte und insbesondere auf das Recht auf den Schutz personenbezogener Daten wird bei der Folgenabschätzung besonders auf die Notwendigkeit und die Angemessenheit etwaiger von der Kommission vorgeschlagener Maßnahmen geachtet werden. Dabei wird die Kommission den Leitlinien folgen, die in ihrer Mitteilung über die Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union[5] enthalten sind.

In der Folgenabschätzung werden zudem die erforderlichen technischen Hintergrundinformationen gegeben und alle in Frage kommenden Optionen ausführlich analysiert werden. Die betreffenden Aspekte sind bereits mit zahlreichen Beteiligten wie den Mitgliedstaaten, Datenschutzbehörden, Europol und dem benannten Anbieter von Zahlungsverkehrsdiensten erörtert worden. Die Endergebnisse der genannten Studie werden allerdings erst Ende dieses Jahres vorliegen. Um die Folgenabschätzung zu unterstützen, hat die Kommission drei Sachverständigentreffen mit den genannten Beteiligten veranstaltet, an denen auch die für die Durchführung des Programms zum Aufspüren der Terrorismusfinanzierung (TFTP) zuständigen US-Behörden teilgenommen haben. Die nachfolgend vorgestellten Optionen gründen sich auf die ersten Zwischenergebnisse der Studie und die Diskussionsergebnisse der Sachverständigentreffen.

2. ZIELE EINES EU-SYSTEMS ZUM AUFSPÜREN DER TERRORISMUSFINANZIERUNG

In Bezug auf die Schaffung eines EU-eigenen Systems zum Aufspüren der Terrorismusfinanzierung gelten zwei Hauptanforderungen:

- Das System muss einen wirksamen Beitrag zur Bekämpfung des Terrorismus und seiner Finanzierung innerhalb der Europäischen Union leisten, und

- es muss zur Begrenzung der in Drittstaaten übermittelten Menge personenbezogener Daten beitragen. Daher sollte das System eine nach den Grundsätzen und Bestimmungen des EU-Datenschutzrechts erfolgende Verarbeitung der für seinen Betrieb benötigten Daten im Hoheitsgebiet der EU ermöglichen.

In den Vereinigten Staaten hat das TFTP nachweislich einen erhöhten Nutzen für die Bekämpfung des Terrorismus und seiner Finanzierung bewirkt, wovon nicht nur die US-Behörden, sondern auch die Behörden der EU-Mitgliedstaaten sowie von Drittländern profitiert haben. Bei der unlängst durchgeführten Überprüfung des TFTP-Abkommens[6] hat sich gezeigt, dass seit der Einführung des TFTP in den Vereinigten Staaten über 2 500 Berichte an Behörden von Drittländern weitergeleitet wurden, die meisten davon (1 700) an EU-Länder. Die Effizienz des TFTP und sein Nutzen für die Bekämpfung des Terrorismus und seiner Finanzierung wurden auch aus den beiden Berichten von Richter Bruguière deutlich, den die Europäische Kommission im Jahr 2008 mit der Überprüfung des Programms beauftragt hatte. Bei den im Rahmen des TFTP zusammengetragenen Informationen, die an

[5] KOM(2010) 573 endg. vom 19.10.2010.
[6] SEK (2011) 438 endg. vom 30.3.2011.

EU-Behörden weitergeleitet wurden, handelte es sich unter anderem um wichtige konkrete Hinweise auf eine Reihe (versuchter) schwerer Terroranschläge wie die Anschläge von Madrid und London, die geplanten Flüssigsprengstoffanschläge auf Transatlantikflüge von 2006 oder den Anschlagsversuch von 2007 auf US-Interessen in Deutschland. Das Überprüfungsteam der EU gelangte zu dem Schluss, dass ihm überzeugende Hinweise auf den Nutzen des TFTP für die Bekämpfung des Terrorismus und seiner Finanzierung vorgelegt worden waren. Angesichts dieser Erkenntnisse besteht begründeter Anlass zu der Erwartung, dass auch ein EU-weites System zum Aufspüren der Terrorismusfinanzierung von großem Nutzen für die Anstrengungen der EU und ihrer Mitgliedstaaten zur Bekämpfung des Terrorismus und seiner Finanzierung wäre.

Obschon die Wirksamkeit des TFTP für die Bekämpfung des Terrorismus und seiner Finanzierung außer Frage steht, sind schwere Bedenken wegen der Auswirkungen des Programms auf die Grundrechte des Einzelnen geäußert worden. Diese Bedenken richten sich vor allem dagegen, dass im Zuge der Umsetzung des TFTP-Abkommens große Mengen personenbezogener Daten an US-Behörden übermittelt werden, von denen sich die große Mehrheit auf unbescholtene Bürger bezieht, die mit dem Terrorismus und seiner Finanzierung nichts zu tun haben. Die Daten werden dabei (nach Maßgabe bestimmter Datenkategorien) *en masse* übermittelt, nicht jedoch auf individueller Grundlage (d.h. nicht aufgrund von sich auf eine oder mehrere Einzelpersonen beziehenden Anfragen). Grund hierfür ist, dass der Anbieter von Zahlungsverkehrsdiensten, der die Daten bereitstellt, nicht über die technischen Möglichkeiten für eine Übermittlung einzelpersonenbezogener Daten verfügt. Zudem müsste der Anbieter von Zahlungsverkehrsdiensten für eine einzelpersonenbezogene Datenübermittlung eine spezielle Such- und Analysefunktion einführen, die für seine Geschäftsabläufe nicht erforderlich ist und erhebliche Ressourcen in Anspruch nehmen würde. Auch würden einzelpersonenbezogene Anfragen dem Anbieter von Zahlungsverkehrsdiensten zur Kenntnis bringen, gegen welche konkreten Personen im Zusammenhang mit Untersuchungen über terroristische Vereinigungen und ihre finanziellen Beziehungen ermittelt wird, was der Effizienz derartiger Untersuchungen abträglich sein könnte.

Damit bei dieser *En-masse*-Übermittlung keine Daten missbräuchlich verwendet werden, wurden umfangreiche Sicherheitsvorkehrungen getroffen. So dürfen die übermittelten Datenmengen beispielsweise nur zu den Zwecken der Bekämpfung des Terrorismus und seiner Finanzierung durchsucht und verwendet werden. Die unlängst durchgeführte Überprüfung des TFTP-Abkommens hat ergeben, dass diese Sicherheitsvorkehrungen wie im Abkommen vorgesehen umgesetzt werden.

Ferner ist argumentiert worden, dass die Übermittlung solch großer Mengen personenbezogener Daten an einen Drittstaat einen ungerechtfertigten Eingriff in die Grundrechte der betreffenden Bürger darstellt und dass dabei jeweils die Notwendigkeit und die Verhältnismäßigkeit dieses Eingriffs berücksichtigt werden sollten. Deshalb hat der Rat die Kommission aufgefordert, Vorschläge zur Einführung eines „Rahmens für die Extraktion der Daten auf dem Gebiet der EU“ vorzulegen, damit vor allem sichergestellt wird, dass die Daten nach Maßgabe der Bestimmungen und Grundsätze des EU-Datenschutzrechts und in Übereinstimmung mit der Charta der Grundrechte der Europäischen Union verarbeiten werden. Die behördliche Erhebung und Verarbeitung von Finanzdaten berührt das in Artikel 16 AEUV und Artikel 8 der Charta verankerte Recht auf den Schutz personenbezogener Daten.

Gemäß Artikel 52 Absatz 1 der Charta dürfen Einschränkungen dieser Grundrechte nur vorgenommen werden, wenn sie gesetzlich vorgesehen sind – mit der nötigen Präzision und Qualität, um Vorhersehbarkeit zu gewährleisten – und den Wesensgehalt dieser Rechte und Freiheiten achten. Der Grundsatz der Notwendigkeit und Verhältnismäßigkeit muss gewahrt werden, um einem von der Europäischen Union anerkannten Zielsetzung zu entsprechen. Diese Grundsätze sind mithin nicht nur bei der Entscheidung über eine etwaige Einführung eines EU-weiten Systems zum Aufspüren der Terrorismusfinanzierung, sondern auch bei der Prüfung der für die Umsetzung eines solchen Systems in Frage kommenden Optionen zu berücksichtigen. Diese Grundsätze berühren gleichermaßen jedwede Entscheidung über Fragen wie den Anwendungsbereich eines solchen Systems, die Vorhaltezeiten oder die Rechte des Einzelnen auf Datenzugang, -löschung usw. Diese Aspekte werden in dieser Mitteilung nicht ausführlich behandelt. Sie müssen in der Folgenabschätzung umfassend analysiert werden.

Die Einrichtung eines Systems für die Extraktion der Daten auf dem Gebiet der EU hätte natürlich Auswirkungen auf das geltende TFTP-Abkommen. Diesbezüglich wird in Artikel 11 Absatz 3 des Abkommens darauf hingewiesen, dass sich die Rahmenbedingungen des Abkommens durch die Einführung eines EU-weiten Systems grundlegend ändern könnten und dass sich die Parteien einander im Hinblick auf die Notwendigkeit einer entsprechenden Anpassung des Abkommens konsultieren sollten, falls die Europäische Union beschließt, ein solches System einzuführen. Daher hätten alle Optionen auch Folgen für die künftige Umsetzung und eine entsprechende Anpassung des geltenden TFTP-Abkommens.

3. DIE HAUPTFUNKTIONEN EINES EU-SYSTEMS ZUM AUFSPÜREN DER TERRORISMUSFINANZIERUNG

Eines der ersten Ergebnisse der oben genannten Diskussion mit den Beteiligten war, dass eine große Mehrheit der Beteiligten der Auffassung ist, dass bei der Einrichtung eines EU-Systems zum Aufspüren der Terrorismusfinanzierung vor allem auf die Sicherheit der EU-Bürger geachtet werden sollte. Ihrer Auffassung nach sollte das System nicht nur dazu dienen, den US-Behörden sachdienliche Informationen zu übermitteln: Auch die Behörden der Mitgliedstaaten haben großes Interesse an den Ergebnissen, die ein solches System liefern kann. Dies bedeutet auch, dass sich beim TFTP zwar Anregungen für den Aufbau eines solchen Systems holen ließen, ein gleichwertiges EU-weites System aber nicht unbedingt dieselben Merkmale wie das TFTP aufweisen müsste. Zudem müsste bei der Einführung eines EU-weiten Systems den Besonderheiten der Verwaltungs- und der Strafrechtsbestimmungen der EU einschließlich der Einhaltung der bereits angesprochenen Grundrechte Rechnung getragen werden.

Jedes zum Aufspüren der Terrorismusfinanzierung gedachte System müsste in Übereinstimmung mit den oben genannten Hauptzielen folgende Kernfunktionen aufweisen:

- Erstellung und Übermittlung (rechtsgültiger) Anfragen an den oder die benannten Anbieter von Zahlungsverkehrsdiensten zwecks Übermittlung der betreffenden Rohdaten an den oder die Empfangsberechtigten. Dies schließt die Bestimmung der anzufordernden Nachrichtenkategorien und der Häufigkeit der Übermittlung dieser Nachrichten sowie die Aufrechterhaltung des diesbezüglichen Kontakts mit den Anbietern ein;

- Überwachung und Genehmigung von sich auf derartige Rohdaten beziehenden Anfragen an den oder die benannten Anbieter einschließlich Überprüfung der Frage, ob bei der

Erstellung der sich auf die Rohdaten beziehenden Anfrage den geltenden Einschränkungen Rechnung getragen wurde;

- Entgegennahme und Speicherung (Verarbeitung) der von dem oder den benannten Anbieter(n) übermittelten Rohdaten einschließlich Implementierung eines geeigneten Systems für die physische und die elektronische Datensicherheit;

- Durchführung der konkreten Suchvorgänge unter den übermittelten Daten in Übereinstimmung mit dem geltenden Rechtsrahmen und auf Grundlage entsprechender Anfragen von Behörden der Mitgliedstaaten, der Vereinigten Staaten oder anderen Drittländern (auf der Grundlage klar definierter Bedingungen und Schutzklauseln) oder auf Eigeninitiative der mit der Verarbeitung der Daten befassten Behörde(n);

- Überwachung und Genehmigung der Suchvorgänge unter den übermittelten Daten;

- Analyse der Suchergebnisse durch Abgleich mit anderen vorliegenden Informationen oder Erkenntnissen;

- Weiterleitung der Suchergebnisse (ohne weitere Analyse) oder der Analyseergebnisse an die Empfangsberechtigten;

- Einführung einer geeigneten Datenschutzregelung, in der insbesondere die geltenden Vorhaltezeiten, die Protokollierungspflichten sowie die Behandlung von Anträgen auf Datenzugang, -berichtigung und -löschung geregelt werden.

Diese Kernfunktionen müssten je nach Option in entsprechenden Rechtsakten der EU, der Mitgliedstaaten oder auf beiden Ebenen festgelegt werden.

4. BEI DER OPTIONSPRÜFUNG ZU BERÜCKSICHTIGENDE GRUNDSÄTZE

Außer von den Überlegungen über die oben genannten Kernfunktionen hängt die Wahl der am besten geeigneten Option zu einem großen Teil davon ab, wie die verschiedenen Optionen bestimmten Grundsätzen gerecht werden. Letztere werden zurzeit im Rahmen der Folgenabschätzung geprüft und nachfolgend näher beschrieben.

4.1. Wirksamkeit

Die erwartete Wirksamkeit der verschiedenen Optionen im Hinblick auf das angestrebte Kernziel, die Bekämpfung des Terrorismus und seiner Finanzierung, ist ein zentrales Kriterium. Unter diesem Aspekt sind solche Optionen vorzuziehen, die die Möglichkeiten für einen Datenaustausch und eine Datenanalyse auf internationaler Ebene erhöhen, denn dadurch erhöhen sich die Wirksamkeit und der Gesamtnutzen. Insbesondere die Auswahl der Organisation(en), die mit der Datenanalyse sowie der Übermittlung der Analyseergebnisse an die entsprechenden Behörden betraut wird/werden, wird eine bedeutende Auswirkung auf die Gesamtwirksamkeit des Systems sowie auf die übermittelte Datenmenge haben. Ungeachtet dessen sollten die Mitgliedstaaten in Übereinstimmung mit den derzeitigen Praktiken weiterhin allein entscheiden, ob ihre Informationen oder Erkenntnisse anderen Behörden mitgeteilt werden dürfen.

4.2. Datenschutz

Austausch und Analyse von Informationen und Erkenntnissen sind auf länderübergreifender Ebene nur möglich, wenn sie von einem robusten und gut entwickelten Datenschutzrahmen begleitet werden. Die Wirksamkeit eines solchen Rahmens hängt nicht nur von den geltenden Rechtsvorschriften ab, die betroffenen Personen die Ausübung ihrer Rechte – wie zum Beispiel Inanspruchnahme eines Rechtsbehelfs – ermöglichen, sondern auch von der Verfügbarkeit unabhängiger und erfahrener Datenschutzbeauftragter und –prüfbehörden. Einige Behörden, die für eine Mitwirkung beim Aufbau eines EU-Systems zum Aufspüren der Terrorismusfinanzierung in Frage kommen, verfügen bereits über derartige Strukturen, andere müssten diese erst noch schaffen. Daher gilt es die datenschutzrechtlichen Auswirkungen der einzelnen Optionen sorgfältig nach Maßgabe der in Abschnitt 2 genannten Grundsätze für die Wahrung der Grundrechte zu prüfen.

4.3. Datensicherheit

Robuste Datenschutzbestimmungen müssen mit modernsten Infrastrukturen und Technologien für die Datensicherheit kombiniert werden. Aus Gründen der Datensicherheit ist es angebracht, die Zahl der Standorte, an denen die übermittelten Daten verarbeitet werden dürfen, zu begrenzen und auch die externen Zugriffsmöglichkeiten auf die Daten einzuschränken. Sicherste Lösung wäre eine Speicherung an nur einem Standort und ohne externen Zugriff. Von den Organisationen, die beim Aufbau eines EU-Systems zum Aufspüren der Terrorismusfinanzierung mitwirken könnten, verfügen zwar die meisten bereits über geeignete Technologien für eine sichere Datenverarbeitung, aber zurzeit können noch nicht alle von ihnen Daten verarbeiten, die höher als „EU - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft sind.

4.4. Datenspeicherung

Die Speicherung der Daten könnte entweder auf nationaler Ebene oder auf EU-Ebene erfolgen. Auf EU-Ebene könnten die von dem oder den benannten Anbieter(n) übermittelten Daten in den Räumlichkeiten von Europol oder einer anderen EU-Einrichtung wie der gegenwärtig im Aufbau befindlichen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht[7] gespeichert werden. Da die Datenspeicherung untrennbar mit Fragen des Datenschutzes und der Datensicherheit verbunden ist, sollte die Entscheidung, welche Organisation für die Datenspeicherung verantwortlich sein soll, stark von den Regeln dieser Organisationen für Fragen des Datenschutzes und der Datensicherheit abhängig gemacht werden.

4.5. Rückgriff auf bestehende Strukturen und Instrumente

Bei sämtlichen Optionen sollte möglichst auf bestehende Strukturen zurückgegriffen werden. So würden die Kosten begrenzt, und die gesammelten Erfahrungen wie auch die vorhandenen Infrastrukturen könnten genutzt werden. Damit die bestehenden Instrumente genutzt werden können, ist es jedoch erforderlich, dass die neuen Aufgaben, die einer bestehenden Organisation übertragen werden, von deren Mandat abgedeckt werden. Europol, Eurojust oder nationale Justizbehörden beispielsweise könnten dafür in Frage kommen, die Überprüfung

[7] KOM (2010) 93 endg. vom 19.3.2010.

und Genehmigung der Datenanfragen an den oder die benannten Anbieter von Zahlungsverkehrsdiensten durchzuführen.

4.6. Zusammenarbeit zwischen den zuständigen Behörden

Die nachfolgend beschriebenen Optionen sehen in unterschiedlichem Umfang eine Zusammenarbeit und einen Informations- und Erkenntnisaustausch zwischen nationalen Behörden sowie zwischen nationalen und EU-Behörden vor. Die einzelnen Mitgliedstaaten haben unterschiedliche Methoden für die Zusammenarbeit ihrer nationalen Behörden bei der Terrorismusbekämpfung eingeführt, und bei jedem Vorgehen auf EU-Ebene wäre den Einschränkungen Rechnung zu tragen, die sich aus den Vorrechten ergeben, die die Mitgliedstaaten gemäß Artikel 72 AEUV bei der Wahrnehmung ihrer Zuständigkeiten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit genießen. Jedes EU-eigene System zum Aufspüren der Terrorismusfinanzierung müsste den Mitgliedstaaten folglich ein hohes Maß an Kontrolle in Bezug auf die von ihnen für den Austausch über das System zur Verfügung gestellten Informationen und Erkenntnisse zugestehen. Einige der nachfolgend genannten Organisationen haben verschiedene Ansätze zur Lösung dieser Frage entwickelt, von denen einige unmittelbar auf das vorgeschlagene EU-System angewendet werden könnten.

4.7. Erster Überblick über die möglichen finanziellen Auswirkungen der verschiedenen Optionen

Die Gesamtkosten der Einrichtung eines EU-weiten Systems zum Aufspüren der Terrorismusfinanzierung und ihre Verteilung auf die EU- und die nationale Ebene würden weitgehend von der gewählten politischen Option abhängen. Sie würden sich in jedem Fall zusammensetzen aus den

- Kosten für die sichere Übermittlung und Speicherung der Daten, die die benannten Anbieter bereitstellen;
- Kosten für die Entwicklung und Pflege der erforderlichen Software für die Suchvorgänge und die Anzeige der Suchergebnisse;
- Kosten für die Übermittlung der Suchergebnisse und Analysen an Empfangsberechtigte;
- Kosten für das Personal, das die Suchvorgänge und die Analysen durchführt und die Ergebnisse weiterleitet;
- Kosten für das Personal, das die Überwachung und die Kontrollen vornimmt;
- Kosten für das Personal, das für den Datenschutz und die Wahrung der Bürgerrechte zuständig ist.

Derzeit liegen zwar noch keine ausführlichen Kostenschätzungen vor, aber ersten Berechnungen zufolge dürften allein für das EU-Konzept und die verschiedenen nachfolgend erörterten hybriden Optionen Einrichtungskosten von 33-47 Mio. EUR zuzüglich jährlicher Betriebskosten von 7-11 Mio. EUR anfallen. Die verschiedenen Optionen werden nachfolgend in Abschnitt 6 beschrieben. Am teuersten wäre Option 3 mit Einrichtungskosten von 43 Mio. EUR für die EU und 3,7 Mio. EUR für die Mitgliedstaaten zusammen und jährlichen Betriebskosten von 4,2 Mio. EUR für die EU und 6,8 Mio. EUR für die

Mitgliedstaaten zusammen. Am billigsten wäre Option 2 mit Einrichtungskosten von 33 Mio. EUR für die EU und jährlichen Betriebskosten von 3,5 Mio. EUR für die EU bzw. 3,3 Mio. EUR für die Mitgliedstaaten zusammen. Bei Option 1 würden sich die Einrichtungskosten auf 40,5 Mio. EUR für die EU belaufen, hinzu kämen jährliche Betriebskosten von 4 Mio. EUR für die EU und 5 Mio. EUR für die Mitgliedstaaten zusammen. Diese Kosten wären natürlich geringer, wenn auf Personal bestehender Organisationen oder auf bereits vorhandene Infrastrukturen sowie Hard- und Software zurückgegriffen werden könnte. Die Kosten für die Einrichtung und den Betrieb eines rein nationalen Systems wären erheblich höher (390 Mio. EUR für die Einrichtung und 37 Mio. EUR für den jährlichen Betrieb), da alle Mitgliedstaaten eigene Hochsicherheitsdatenverarbeitungssysteme einrichten und entsprechendes Betriebspersonal beschäftigen müssten.

Diese Beträge sind vorläufig und müssen im Lichte der Ergebnisse der Folgenabschätzung weiter analysiert und aufgeschlüsselt werden.

5. ZU BERÜCKSICHTIGENDE ASPEKTE

Unabhängig davon, welche Option für die Errichtung und den Betrieb eines EU-weiten Systems zum Aufspüren der Terrorismusfinanzierung letztendlich ausgewählt wird, gilt es einer Reihe von Aspekten Rechnung zu tragen, die mit dem Anwendungsbereich eines solchen Systems zu tun haben. Diese werden nachfolgend erörtert.

5.1. Soll das EU-System auf die Bekämpfung des Terrorismus und seiner Finanzierung begrenzt werden oder auch gegen andere Kriminalitätsformen eingesetzt werden?

Zahlungsverkehrsdaten sind nicht nur für die Bekämpfung des Terrorismus und seiner Finanzierung nützlich. Es bestehen nur geringe Zweifel, dass sie auch ein wertvolles Mittel zur Bekämpfung anderer Formen der Schwerkriminalität und insbesondere der organisierten Kriminalität und der Geldwäsche darstellen würden. Die im Zusammenhang mit dem TFTP-Abkommen angestellten Überlegungen über die Verhältnismäßigkeit des Vorgehens haben gleichwohl zu einer genauestens eingehaltenen Begrenzung der Datennutzung auf die Zwecke der Bekämpfung des Terrorismus und seiner Finanzierung geführt. Die bisherigen Vorgespräche haben ergeben, dass weitgehend Einigkeit darüber besteht, dass diese Überlegungen über die Verhältnismäßigkeit des Vorgehens dafür sprechen, in Übereinstimmung mit den in Abschnitt 2 dargelegten allgemeinen Überlegungen zum Thema Wahrung der Grundrechte für ein EU-weites System dieser Art den gleichen begrenzten Anwendungsbereich vorzusehen.

5.2. Soll auf mehr als nur einen Anbieter internationaler Zahlungsverkehrsdienste zurückgegriffen werden?

Das geltende TFTP-Abkommen sieht vor, dass Daten von nur einem Anbieter internationaler Zahlungsverkehrsdienste angefordert werden. Dabei handelt es sich eindeutig um den weltweit wichtigsten Anbieter dieser Art, aber auf dem Markt sind auch noch andere Anbieter tätig. Der Wunsch nach mehr Effizienz und nach gleichen Voraussetzungen für alle Marktbeteiligten würde dafür sprechen, ein System zu schaffen, das für alle Anbieter internationaler Zahlungsverkehrsdienste gilt. In jedem Fall gilt es bei der Wahl der geeigneten

Option die Verwaltungslast zu berücksichtigen, die Anbietern derartiger Zahlungsverkehrsdienste entstehen würde.

5.3. Sollen neben internationalen auch nationale Zahlungsverkehrsdaten berücksichtigt werden?

Das geltende TFTP-Abkommen sieht vor, dass nur Daten von Anbietern internationaler Zahlungsverkehrsdienste angefordert werden, d.h. von Zahlungsverkehrsdiensten für internationale Transaktionen (u.a. zwischen Mitgliedstaaten der EU, aber mit Ausnahme von Zahlungsverkehrsdaten im Zusammenhang mit dem Einheitlichen Euro-Zahlungsverkehrsraum (SEPA)). Mit Blick auf ein EU-weites System zum Aufspüren der Terrorismusfinanzierung gilt es aber auch in Betracht zu ziehen, ob auch Zahlungsverkehrsdienstleistungen zwischen Mitgliedstaaten berücksichtigt werden sollten oder ob eine Begrenzung auf den internationalen Austausch von Zahlungsverkehrsdienstleistungen gelten sollte. Rein nationale Zahlungsverkehrsdienste, auf die ja nur für nationale Finanztransaktionen zurückgegriffen wird, sind derzeit vom Anwendungsbereich des TFTP-Abkommens ausgeschlossen. Ein Rückgriff auf nationale Zahlungsverkehrsdienste könnte aber für die Bekämpfung von Terrorismus und anderen Straftaten interessant sein. Dennoch hat sich ungeachtet der Frage, ob ein solcher Rückgriff auf EU-Ebene geregelt werden sollte, in den bisherigen Vorgesprächen herauskristallisiert, dass ein solcher Datenzugriff weitgehend als unangemessen betrachtet wird und daher vom Anwendungsbereich eines EU-weiten Systems ausgeschlossen werden sollte.

5.4. Welche Arten von Zahlungsverkehrsdaten sollen erfasst werden?

Im internationalen Bankensystem werden viele verschiedene Arten von Zahlungsverkehrsdaten verwendet. Das geltende TFTP-Abkommen ist auf eine bestimmte Art dieser Daten beschränkt. Ein Zugang zu anderen Arten von Zahlungsverkehrsdaten könnte für die Bekämpfung des Terrorismus und seiner Finanzierung sowie möglicherweise auch von sonstigen Straftaten interessant sein. Dennoch sprechen auch hier der Proportionalitätsgrundsatz und das vorrangige Ziel der Wahrung der Grundrechte der Bürger dafür, das Spektrum der durch das System erfassten Zahlungsverkehrsdaten zu begrenzen. Nähere Einzelheiten dieses technischen Aspekts werden in der Folgenabschätzung behandelt werden.

6. OPTIONEN FÜR EIN EU-SYSTEM ZUM AUFSPÜREN DER TERRORISMUSFINANZIERUNG

Die nachfolgend aufgeführten Optionen werden von der Kommission zurzeit im Rahmen der laufenden Folgenabschätzung geprüft. Sie stellen weder darauf ab, von vornherein bestimmte Einschränkungen vorzugeben, noch greifen sie in irgend einer Weise den Ergebnissen der Folgenabschätzung oder einer auf ihrer Grundlage getroffenen Entscheidung der Kommmission vor.

Eine Möglichkeit, die bei der Ausarbeitung neuer Initiativen und der sie begleitenden Folgenabschätzungen stets in Betracht gezogen wird, besteht darin, alles beim Alten zu belassen, was in diesem Falle hieße, am geltenden TFTP-Abkommen festzuhalten und keinen Vorschlag zur Einführung eines EU-Systems zum Aufspüren der Terrorismusfinanzierung vorzulegen. Diese Option würde jedoch nicht der in Abschnitt 1 angesprochenen, an die Kommission gerichteten Forderung des Rates und des Europäischen Parlaments gerecht,

einen „rechtlichen und technischen Rahmen für die Extraktion der Daten auf dem Gebiet der EU" vorzulegen. Außerdem würde so weder ein Beitrag zur Begrenzung der an Drittländer übermittelten Menge personenbezogener Daten geleistet noch dafür Sorge getragen, dass die Daten im Hoheitsgebiet der EU und nach Maßgabe der Grundsätze und Vorschriften des Datenschutzrechts der EU verarbeitet werden. Alle anderen, nachfolgend im Detail erörterten Optionen sehen hingegen mögliche Wege zur Schaffung eines EU-Systems zum Aufspüren der Terrorismusfinanzierung vor.

Theoretisch könnten sämtliche in Abschnitt 3 genannten Kernfunktionen eines EU-weiten Systems zum Aufspüren der Terrorismusfinanzierung entweder auf EU-Ebene oder aber auf nationaler Ebene implementiert werden. Auch könnten die einzelnen Funktionen einer oder mehreren verschiedenen Organisationen nach Maßgabe ihrer bestehenden Verantwortlichkeiten übertragen werden, oder es könnten neue Organisationen geschaffen werden, die diese Funktionen wahrnehmen. Dabei könnte es sich entweder um EU-Organisationen oder aber um nationale Organisationen handeln. Theoretisch wäre also sowohl ein rein EU-weites Vorgehen möglich, bei dem sämtliche Kernfunktionen ausschließlich an EU-Organisationen übertragen würden, als auch ein rein nationaler Ansatz, bei dem sämtliche Funktionen auf nationaler Ebene implementiert würden. Generell gilt, dass die für ein zentrales, dezentrales oder hybrides System in Frage kommenden Optionen nicht unbedingt die gleichen sein müssen wie bei anderen Initiativen, die eine Datenverarbeitung zum Zwecke der Bekämpfung des Terrorismus und der organisierten Kriminalität beinhalten: Jede Initiative in diesem Bereich sollte nach Maßgabe ihrer eigenen, ganz speziellen Vorzüge beurteilt werden.

Sowohl die rein zentralen als auch die rein nationalen Ansätze sind mit großen Nachteilen behaftet. Beispielsweise wäre es der Effizienz eines ausschließlich EU-weiten Vorgehens zweifelsohne sehr abträglich, dass keine Verbindungen zu Strafverfolgungsbehörden und Nachrichtendiensten bestehen würden und auch nicht auf bewährte Praktiken der Mitgliedstaaten zurückgegriffen werden könnte. Ohne Mitwirkung der zuständigen nationalen Behörden wäre es nahezu unmöglich, genau zu ermitteln, welche Datenkategorien von dem oder den benannten Anbieter(n) angefordert werden sollten. Auch wäre der Nutzen des Systems eingeschränkt, wenn Datenbankabfragen nur auf der Grundlage der auf EU-Ebene verfügbaren Informationen möglich wären, denn nach dem derzeitigen Stand der EU-Integration sind derartige Informationen überwiegend nur auf nationaler Ebene verfügbar. Zudem ist es unwahrscheinlich, dass die Mitgliedstaaten einem rein EU-weiten Vorgehen zustimmen würden, da dies keinen Nutzen für ihre eigenen Anstrengungen zur Bekämpfung des Terrorismus und seiner Finanzierung bringen würde. Bei den bisherigen Vorgesprächen haben die Mitgliedstaaten zudem zu verstehen gegeben, dass diese Option aus rechtlichen und operativen Gründen politisch nur schwer zu akzeptieren wäre.

Das genaue Gegenteil, ein rein nationales Vorgehen, würde das Risiko einer nicht einheitlichen Umsetzung in den einzelnen Mitgliedstaaten in sich bergen. Zudem wäre die Gefahr, dass es zu Verstößen gegen die Datensicherheit kommt, größer, weil die betreffenden Daten ja in 27facher Form und Menge bereitgestellt werden müssten. Auch wären Schwierigkeiten bei der Umsetzung eines harmonisierten Datenschutzrahmens und eines harmonisierten Konzepts zur Festlegung (und Kontrolle) anderer erforderlicher Einschränkungen (wie die Begrenzung auf den Terrorismus und seine Finanzierung) vorprogrammiert. Bei einem rein nationalen Vorgehen wäre zudem unklar, welcher Mitgliedstaat für die Abwicklung der Suchanfragen aus Drittländern zuständig wäre, und der zusätzliche Nutzen, den die Suchergebnisanalyse auf EU-Ebene bewirken kann, wäre nicht gegeben. Letztendlich wäre diese Option, wie bereits erwähnt, auch mit beträchtlich höheren

Kosten verbunden, da sämtliche Mitgliedstaaten eigene Hochsicherheitsdatenverarbeitungssysteme einrichten und entsprechendes Betriebspersonal beschäftigen müssten.

Bei den Vorarbeiten mit den Beteiligten kristallisierte sich folglich schnell heraus, dass diese beiden Extremlösungen keine Unterstützung finden würden und dass Einigkeit darin besteht, dass eine Hybridlösung, bei der die verschiedenen Funktionen auf verschiedene Organisationen auf EU-Ebene und auf nationaler Ebene aufgeteilt werden, im Hinblick auf die Verwirklichung der beiden Hauptziele vermutlich die besten Ergebnisse ermöglichen würde. Dieser Konsens erleichtert zwar die Suche nach der am besten geeigneten Option, aber auch der Hybridansatz bringt eine große Zahl zu klärender Fragen mit sich. Die drei in Betracht kommenden Hybridlösungen, die sich bei den laufenden Vorarbeiten als die plausibelsten Optionen herausgestellt haben, werden in den nachfolgenden Abschnitten im Detail erläutert und im Anhang in tabellarischer Form vorgestellt.

6.1. Option 1: Einrichtung einer mit Koordinierungs- und Analyseaufgaben befassten zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung

Diese Option sieht die Einrichtung einer zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung und eine überwiegende Umsetzung der Aufgaben und Funktionen auf EU-Ebene vor. So würden Anfragen nach Rohdaten an den oder die benannten Anbieter, die Überprüfung dieser Anfragen, die Bearbeitung und Durchführung von Suchvorgängen, die Verarbeitung der Suchergebnisse und die Weiterleitung von Berichten an die Suchanfragesteller allesamt auf EU-Ebene erfolgen. Die Erstellung der Anfragen an den oder die benannten Anbieter könnte gleichwohl in Absprache mit den zuständigen Behörden der Mitgliedstaaten erfolgen, und die Mitgliedstaaten könnten auf Wunsch eigene Analysten zwecks Mitwirkung an den Suchvorgängen zur zentralen EU-Stelle abstellen. Im Unterschied zur gänzlich zentralen Option könnten die Mitgliedstaaten (wie bei der derzeitigen Zusammenarbeit mit dem TFTP der Fall) darum ersuchen, dass bestimmte Suchvorgänge in ihrem Namen oder von ihren eigenen Analysten durchgeführt werden.

Die Mitgliedstaaten müssten Informationen mit der zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung austauschen und, bevor eine Suche eingeleitet werden könnte, zur Begründung der Suchanfrage die betreffende Verbindung zum Terrorismus „nachweisen“ bzw. ihre Anfragen vorab von den zuständigen nationalen Behörden genehmigen lassen. Bei diesen nationalen „Behörden“ könnte es sich beispielsweise um mit der Terrorismusbekämpfung befasste Staatsanwälte oder Untersuchungsrichter handeln. Falls diese eine bestimmte Suche unter den bereitgestellten Daten genehmigen würden, könnte die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung sodann den betreffenden Suchvorgang ohne weitere Überprüfung durchführen. In diesem Fall müssten der zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung auch keine weiteren Informationen mitgeteilt werden. Die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung würde die Suchergebnisse und ihre Analyse anschließend zurückübermitteln und könnte auch von sich aus Informationen übermitteln. Die Vereinigten Staaten und andere Drittländer müssten derartige Suchvorgänge nach einem ähnlichen Verfahren beantragen.

Die Überwachung der Einhaltung der Sicherheits- und Kontrollvorschriften würde ebenfalls zentral erfolgen, nach Möglichkeit im Wege der Beaufsichtigung durch externe Beteiligte wie Vertreter des oder der Anbieter und ernannte unabhängige Aufseher. Datenschutz, -integrität und -sicherheit würden ebenfalls auf zentraler Ebene sichergestellt.

Hauptschnittstellen des Systems könnten Europol und Eurojust sein. In diesem Fall müssten die von ihnen zu erfüllenden Aufgaben mit ihrem im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) festgelegten Auftrag stehen. Auch müsste zunächst ermittelt werden, in wie weit die geltenden Rechtsakte zur Festlegung ihrer Arbeitsweise geändert werden müssten. Falls Europol zur zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung bestimmt würde, müsste Europol sich auch mit Anträgen von betroffenen Personen auf Datenzugang, -berichtigung oder -sperrung nach Maßgabe seines geltenden Rechtsrahmens und der einschlägigen Datenschutzvorschriften befassen. Die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung würde ihre Funktion in Übereinstimmung mit dem geltenden Rechtsrahmen erfüllen, und Beschwerden und Einsprüche würden ebenfalls nach Maßgabe der geltenden Rechtsvorschriften abgewickelt. Auf einzelstaatlicher Ebene hätten die nationalen Strafverfolgungsbehörden die Aufgabe, die Suchanfragen zu überprüfen und gegebenenfalls zu genehmigen. Auch könnte in Erwägung gezogen werden, neue nationale Stellen zu schaffen, doch diese Entscheidung sollte entsprechend dem Subsidiaritätsgrundsatz am besten den Mitgliedstaaten überlassen werden.[8]

6.2. Option 2: Einrichtung einer nur zur Datenextraktion befugten zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung

Wie bei Option 1 würde auch bei dieser Option eine zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung eingerichtet, die die Aufgabe hätte, Anfragen nach Rohdaten an den oder die benannten Anbieter zu richten, die Anfragen zu überprüfen, Suchvorgänge durchzuführen und Suchanfragen zu bearbeiten. Bei Option 2 wäre die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung jedoch nicht befugt, die Suchergebnisse zu analysieren und sie mit anderen vorliegenden Informationen und Erkenntnissen zu vergleichen, wenn die betreffenden Suchvorgänge auf Antrag von Behörden der Mitgliedstaaten durchgeführt werden, d.h. die Rolle der zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung wäre in diesem Fall darauf beschränkt, die Suchergebnisse zu ermitteln und sie in anschaulicher Form zu übermitteln.

Wie bei Option 1 würden Anfragen nach Rohdaten an den oder die benannten Anbieter in enger Absprache mit den Mitgliedstaaten erfolgen, wobei letztere der zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung ihre spezifischen Anforderungen mitteilen könnten und die zentrale EU-Stelle diese sodann prüfen und die Anfragen entsprechend formulieren würde.

Die Mitgliedstaaten könnten um in ihrem Namen durchzuführende Suchvorgänge ersuchen. Dabei würde jeweils auf nationaler Ebene überprüft, in wie weit die Anfrage begründet ist und eine Verbindung zum Terrorismus besteht. Die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung würde sodann die genehmigten Suchvorgänge durchführen und sämtliche Ergebnisse in anschaulicher Form an die Mitgliedstaaten zurückübermitteln. Somit würden ausschließlich Behörden der Mitgliedstaaten die Suchergebnisse analysieren, wobei diese jederzeit von sich aus Informationen übermitteln könnten.

Bei Suchanfragen im Namen der EU-Organe, der Vereinigten Staaten und anderer Drittländer hätte die zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung die Aufgabe, die betreffenden Suchvorgänge durchzuführen und die Ergebnisse im Namen der EU-Organe, der

[8] Zu diesem Zeitpunkt sind die Folgen für den Haushalt der EU-Agenturen, die eine Rolle bei der Umsetzung des Systems spielen könnten, noch nicht bekannt.

Vereinigten Staaten und anderer Drittländer zu analysieren. Sie könnte auf dieser Grundlage jederzeit von sich aus Informationen übermitteln.

Wie bei den vorgenannten Optionen würde die Einhaltung der Sicherheits- und Kontrollvorschriften zentral überwacht, nach Möglichkeit im Wege der Beaufsichtigung durch externe Beteiligte wie Vertreter des oder der Anbieter und ernannte unabhängige Aufseher. Datenschutz, -integrität und -sicherheit würden ebenfalls auf zentraler Ebene sichergestellt.

Ebenfalls wie bei den vorgenannten Optionen könnten Europol und Eurojust die Hauptschnittstellen des Systems sein. Auf innerstaatlicher Ebene wären vor allem die nationalen Strafverfolgungsbehörden und die Nachrichtendienste beteiligt. Ebenso stünde den Mitgliedstaaten entsprechend dem Subsidiaritätsgrundsatz frei, neue nationale Stellen einzurichten. Europol und/oder die nationalen Stellen würden unter Mitwirkung der nationalen Datenschutzbehörden und der gemeinsamen Kontrollinstanz von Europol alle Anträge von EU-Bürgern auf Datenzugang, -berichtigung oder -sperrung bearbeiten. Beschwerden und Einsprüche würden nach Maßgabe der geltenden Rechtsvorschriften auf nationaler oder auf EU-Ebene abgewickelt.[9]

6.3. Option 3: Einrichtung einer mit Koordinierungsaufgaben befassten EU-Behörde auf der Grundlage der zentralen Meldestellen (FIU-Plattform)

Diese Option sieht die Einrichtung einer von den zentralen Meldestellen der Mitgliedstaaten gebildeten erweiterten FIU-Plattform vor. Diese ad-hoc-Behörde würde jeweils die Anforderungen der einzelnen zentralen Meldestellen ermitteln, diese zu einer spezifischen Anfrage nach Rohdaten bündeln und die Anfrage, die zudem auf zentraler Ebene zu überprüfen und zu genehmigen wäre, sodann an den oder die benannten Anbieter richten.

Jede zentrale Meldestelle hätte die Aufgabe, im Namen des betreffenden Mitgliedstaats Suchvorgänge durchzuführen, die Suchergebnisse zu verarbeiten, Analysen vorzunehmen und Berichte an die zuständigen Stellen zu schicken. Dabei würde jeweils auf nationaler Ebene oder auf EU-Ebene überprüft, in wie weit die Suchanfrage begründet ist und eine Verbindung zum Terrorismus besteht. Die zentralen Meldestellen wäre zudem für die unaufgeforderte Informationsübermittlung zuständig.

Die erweiterte FIU-Plattform wäre befugt, im Namen der EU-Organe sowie von Drittländern, mit denen die EU entsprechende Abkommen schließt, Suchvorgänge durchzuführen und die Ergebnisse zu analysieren. Sie könnte zudem von sich aus Informationen übermitteln.

Die Überwachung der Einhaltung der Sicherheits- und Kontrollvorschriften würde zentral erfolgen, nach Möglichkeit im Wege der Beaufsichtigung durch externe Beteiligte wie Vertreter des oder der Anbieter und ernannte unabhängige Aufseher. Datenschutz, -integrität und -sicherheit würden ebenfalls auf zentraler Ebene sichergestellt.

Der erweiterten FIU-Plattform würde eine förmliche Rechtspersönlichkeit verliehen, und ihr würden zudem klar festgelegte Aufgaben und Zuständigkeiten übertragen. Hauptakteure auf einzelstaatlicher Ebene wären die zentralen Meldestellen sowie die nationalen Strafverfolgungsbehörden und Nachrichtendienste.

---

[9] Siehe Fußnote 8.

Die Behörde auf EU-Ebene würde auch sämtliche Anträge von EU-Bürgern auf Datenzugang, -berichtigung oder -sperrung bearbeiten. Beschwerden und Einsprüche würden nach Maßgabe der geltenden Rechtsvorschriften auf nationaler oder auf EU-Ebene abgewickelt.

7. FAZIT

Auf der Grundlage der bisherigen Vorarbeiten der Kommission werden in dieser Mitteilung – ohne den Ergebnissen der Folgenabschätzung vorgreifen zu wollen – mögliche Optionen für die Einführung eines „rechtlichen und technischen Rahmens für die Extraktion der Daten auf dem Gebiet der EU“ im Zusammenhang mit einem System zum Aufspüren der Terrorismusfinanzierung vorgestellt. Dabei wird deutlich, dass es wichtige Entscheidungen (vor allem im Hinblick auf die Wahrung der Grundrechte) zu treffen gilt und im weiteren Verlauf der Vorarbeiten noch zahlreiche technische, organisatorische und finanzielle Fragen genauer geklärt werden müssen. Angesichts dieser wichtigen Aufgaben ist die Kommission der Auffassung, dass für die weiteren Vorarbeiten und für die Diskussionen mit dem Rat und dem Europäischen Parlament genügend Zeit eingeräumt werden sollte.

*** * ***

Anhang: tabellarische Übersicht über die hybriden Optionen

	Option 1: Einrichtung einer mit Koordinierungs- und Analyseaufgaben befassten zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung	Option 2: Einrichtung einer nur zur Daten-extraktion befugten zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung	Option 3: Einrichtung einer mit Koordinierungsaufgaben befassten EU-Behörde auf der Grundlage der zentralen Meldestellen (FIU-Plattform)
Erstellung und Einreichung von Rohdatenanfragen	zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung in Absprache mit den Mitgliedstaaten	zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung in Absprache mit den Mitgliedstaaten	erweiterte FIU-Plattform
Überwachung und Genehmigung der Rohdatenanfragen	Eurojust oder eine sonstige bestehende Einrichtung	Eurojust oder eine sonstige bestehende Einrichtung	Eurojust oder eine sonstige bestehende Einrichtung
Entgegennahme und Speicherung der Rohdaten und Gewährleistung der Datensicherheit	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur
Durchführung von Suchvorgängen unter den Rohdaten	zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung, von den Mitgliedstaaten abgestellte Analysten oder beides	zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung	zentrale Meldestellen, erweiterte FIU-Plattform
Überwachung und Genehmigung der Suchvorgänge	unabhängige Beaufsichtigung, nach Möglichkeit durch nationale Behörden	unabhängige Beaufsichtigung durch nationale Behörden	unabhängige Beaufsichtigung
Analyse der Suchergebnisse	zentrale EU-Stelle zum Aufspüren der Terrorismusfinanzierung, von den Mitgliedstaaten abgestellte Analysten oder beides	Bei nationalen Suchanfragen wären die nationalen Behörden zuständig, bei Suchanfragen der EU oder von Drittländern die Analysten der zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung	erweiterte FIU-Plattform, zentrale Meldestellen der Mitgliedstaaten

Übermittlung der Suchergebnisse	Europol-Analysten oder von den Mitgliedstaaten abgestellte Analysten	Bei nationalen Suchanfragen wären die nationalen Behörden zuständig, bei Suchanfragen der EU oder von Drittländern die Analysten der zentralen EU-Stelle zum Aufspüren der Terrorismusfinanzierung	FIU-Plattform, zentrale Meldestellen der Mitgliedstaaten
Umsetzung einer geeigneten Datenschutzregelung	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur	Europol oder eine sonstige EU-Einrichtung wie die IT-Agentur