



Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

Deutscher Bundestag

Innenausschuss

Ausschussdrucksache

17(4)336 A

**Peter Schaar**

Bundesbeauftragter für den Datenschutz  
und die Informationsfreiheit

POSTANSCHRIFT

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,  
Postfach 1468, 53004 Bonn

**Stellungnahme**  
**des**  
**Bundesbeauftragten für den Datenschutz**  
**und**  
**die Informationsfreiheit**

**zum**

**„Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und  
Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der  
Europäischen Union“**

**BT-Drucksache 17/5096**

**im Zusammenhang mit der öffentlichen Anhörung des Deutschen Bundestages  
– Innenausschuss –**

**am 19. September 2011**



## **1. Die „Schwedische Initiative“ im Kontext des Datenschutzes im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen**

Der Rahmenbeschluss 2006/960/JI des Rates vom 18.12.2006, die sog. „Schwedische Initiative“, ist eine Konsequenz des Grundsatzes der Verfügbarkeit, den die Regierungen der EU-Mitgliedstaaten mit der Verabschiedung des sog. Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union (ABl. C 53 vom 3.3.2005) beschlossen haben. Er besagt, dass „unionsweit ein Strafverfolgungsbeamter in einem Mitgliedstaat, der für die Erfüllung seiner Aufgaben Informationen benötigt, diese aus einem anderen Mitgliedstaat erhalten kann und dass die Strafverfolgungsbehörde in dem anderen Mitgliedstaat, die über diese Informationen verfügt, sie — unter Berücksichtigung des Erfordernisses in diesem Staat anhängiger Ermittlungen — für den erklärten Zweck bereitstellt.“ Zugespitzt heißt es: „Der bloße Umstand, dass Informationen Grenzen überschreiten, sollte nicht länger von Bedeutung sein.“ (Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. C 53 vom 3.3.2005, jeweils S. 7).

Der Erleichterung des polizeilichen Datenaustausches als Aspekt der weiteren europäischen Integration stehe ich grundsätzlich positiv gegenüber, sofern dabei die Grundrechtspositionen der Betroffenen gewährleistet bleiben. Wesentlicher Bestandteil eines Raums der Freiheit, der Sicherheit und des Rechts ist deshalb, dass in allen Mitgliedstaaten ein gleichwertiger Datenschutz auf hohem Niveau geschaffen wird. Diese Forderung entspricht auch der zentralen Verankerung des Datenschutzes durch den Vertrag von Lissabon in Art. 8 EU-Grundrechte-Charta und Art. 16 Vertrag über die Arbeitsweise der Europäischen Union. Dagegen wäre die Aufhebung der nationalen Grenzen beim polizeilichen Informationsaustausch ohne Schaffung einheitlicher hoher Datenschutzstandards in ganz Europa nicht akzeptabel. Letztere sind allerdings immer noch nicht in ausreichendem Maße verwirklicht.

Von der „Schwedischen Initiative“ erfasst sind grundsätzlich alle bei den Strafverfolgungsbehörden der Mitgliedstaaten vorhandenen Daten. Ungeachtet der Frage, inwieweit die Übermittlung von sogenannten verfügbaren Daten eine erstmalige Erhebung voraussetzen kann (vgl. dazu unter 2. a)), sollen grundsätzlich alle bereits vorhandenen Daten allen anderen Strafverfolgungsbehörden in der EU in der Weise so zugänglich gemacht werden, wie sie auch national zur Verfügung stehen.

Ohne dies explizit auszusprechen, setzt der Rahmenbeschluss dabei offensichtlich voraus, dass vergleichbare rechtstaatliche und grundrechtsschützende Gewährleistungen bei der Erhebung und Verarbeitung von Daten in allen Mitgliedstaaten bestehen. Denn zur Übermittlung der vorhandenen Daten ist jeder Mitgliedstaat grundsätzlich verpflichtet, ohne dass eine datenschutzrechtliche Überprüfung des Ersuchens des Empfängerstaats vorgenommen werden darf. Die Gründe für die Zurückhaltung von Daten sind mit Ausnahme von Art. 10 Abs. 2 des



Rahmenbeschlusses im Wesentlichen auf „eigene“ Sicherheitsinteressen begrenzt. Für den Austausch der Daten spielt es zudem grundsätzlich keine Rolle, wie die übermittelten Daten zuvor im ersuchten Staat erhoben wurden. Der ersuchende (und empfangende) Mitgliedstaat verwendet die Daten, ohne die Umstände für deren Erhebung zu kennen. Zwar ist richtig, dass durch die Voraussetzungen der justiziellen Rechtshilfe rechtstaatliche Kontrollen zu einem späteren Zeitpunkt erfolgen sollten, sofern die Daten in ein strafrechtliches Verfahren münden. Die Speicherung in polizeilichen Datenbanken wäre davon aber nicht berührt, eine Justizkontrolle fände dabei nicht statt.

All dies verdeutlicht, dass ein robustes und hohes Datenschutzniveau in der Form von verbindlichen europäischen Mindeststandards unbedingt erforderlich ist.

Zwar haben sich die Mitgliedstaaten auf den Rahmenbeschluss 2008/977/JI vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, einigen können. Dieser Rahmenbeschluss ist jedoch für den Bereich der innerstaatlichen Datenerhebung und – verarbeitung gerade nicht anwendbar. Sein Anwendungsbereich beschränkt sich vielmehr auf die weitere Verarbeitung der – z.B. auf der Grundlage der „Schwedischen Initiative“ – zwischen den EU-Mitgliedstaaten ausgetauschten personenbezogenen Daten. Aber auch insofern regelt der Datenschutz-Rahmenbeschluss vieles unzureichend bzw. lediglich dadurch, dass er auf das bestehende nationale Recht verweist. Abgesehen davon, dass er in vielen Mitgliedstaaten – darunter auch in Deutschland – noch nicht in nationales Recht umgesetzt ist, bleibt er insgesamt hinter den verfassungsrechtlichen Vorgaben zurück, die das Bundesverfassungsgericht (etwa im Hinblick auf Kernbereichsschutz, Benachrichtigungspflichten, etc) in seiner Rechtsprechung entwickelt hat.

Der Rahmenbeschluss zum Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen schafft somit nicht die zwingend notwendigen Voraussetzungen für den europäischen Datenaustausch.

Inwieweit der gegenwärtig von der Europäischen Kommission erarbeitete neue Rechtsakt für eine „säulenübergreifende“ Datenverarbeitung geeignet sein wird, ein höheres Datenschutzniveau im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu verwirklichen, ist noch offen. Damit setzt der polizeiliche Datenaustausch innerhalb der Europäischen Union nach der Umsetzung der „Schwedischen Initiative“ volles Vertrauen voraus, unterlässt es aber, eigene Regelungen und damit belastbare Bedingungen zu schaffen, die dieses Vertrauen rechtfertigen. Vielmehr werden die erforderlichen grundrechtlichen Standards jedenfalls zu einem erheblichen Teil dem nationalen Recht überlassen. Dass dabei jeweils innerstaatlich auch die Vorgaben des Europarates, insbesondere das Schutzregime der Europäischen Menschenrechtskonvention zu beachten ist, befriedigt nicht. Denn wer Regeln schafft, die einen vereinfachten Datenaustausch innerhalb der EU bezwecken, muss auch dort diffe-



renzierte Mindeststandards setzen. Diese Problematik erinnert im Übrigen an die Beratungen über eine Richtlinie zur Europäischen Ermittlungsanordnung (vgl. Beschussempfehlung und Bericht des Rechtsausschusses, BT-Drucksache 17/3234). Ähnlich wie bei der „Schwedischen Initiative“ werden auch hier die Schaffung hoher Mindeststandards und die Vereinfachung der polizeilichen Kooperation nicht im Gleichschritt vorgenommen. Dies halte ich im Ergebnis für halbherzig und unausgewogen, zumal Rahmenbeschlüsse und Richtlinien in nationales Rechts umzusetzen sind, und die beschriebenen Datenschutzdefizite durch den nationalen Gesetzgeber nicht vollständig ausgeglichen werden können.

Aus alledem folgt, dass die Herstellung eines hohen Datenschutzniveaus für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf der europäischen Eben noch nicht mit akzeptablem Ergebnis abgeschlossen ist. Die „Schwedische Initiative“ stammt noch aus der Zeit vor dem Inkrafttreten des Vertrages von Lissabon. Auf der Grundlage des Vertrages von Lissabon will die Europäische Kommission gegen Ende des Jahres konkrete Vorschläge zur Überarbeitung des gesamten EU-Rechtsrahmens inklusive der ehemaligen sog. 3. Säule vorlegen. Es bleibt abzuwarten, ob diese den aufgezeigten Anforderungen gerecht werden.

## 2. Zu den Regelungen im Einzelnen

Gerade im Hinblick auf das Fehlen eines einheitlichen Datenschutzniveaus in den europäischen Mitgliedstaaten in den Bereichen Polizei und Justiz trete ich dafür ein, die Spielräume, die der Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union bietet, zu nutzen und dessen Umsetzung ins deutsche Recht möglichst datenschutzfreundlich zu gestalten. Dies entspricht auch einer Forderung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. und 7. November 2008. Die Entschlie-ßung ist meiner Stellungnahme als Anlage 1 beigefügt.

### *a) Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln*

Die „Schwedische Initiative“ schafft keine neue Rechtsgrundlage für die Strafverfolgungsbehörden zur originären Erhebung von Daten. Sie enthält vielmehr nur Vorschriften dazu, wie der Austausch von Informationen und Erkenntnissen zwischen den Mitgliedstaaten zu erfolgen hat und in welchen Fällen eine Übermittlung von Daten, die auf der Grundlage der „Schwedischen Initiative“ ersucht werden, unterbleiben kann oder muss.



Entsprechend sollte der Gesetzentwurf zur Umsetzung der „Schwedischen Initiative“ vorsehen, dass eine Datenübermittlung unterbleibt, wenn ein Datum noch nicht erhoben ist. Dies sollte auf den ersten Blick auch unproblematisch möglich sein, weil der Rahmenbeschluss in Art. 1 Abs. 3 ausdrücklich regelt, dass eine Verpflichtung der Mitgliedstaaten, „Informationen und Erkenntnisse mit dem Ziel zu sammeln und zu speichern, sie den zuständigen Strafverfolgungsbehörden anderer Mitgliedstaaten bereitzustellen“, nicht besteht. Auch wenn es sich dabei vordergründig um einen eher technischen Ansatz handelt, ist dessen Umsetzung nicht unproblematisch. Denn in dem Rechtsakt ist gleichzeitig ein schwer auflösbares Spannungsverhältnis angelegt, weil alle Mitgliedstaaten sicherzustellen haben, dass „Informationen und Erkenntnisse“ bereit gestellt werden können und diese „Informationen und Erkenntnisse“ gem. Art. 2 Buchstabe d) Ziffer ii) nicht nur alle bei den Strafverfolgungsbehörden vorhanden, sondern auch alle „Arten von Informationen oder Angaben“ umfassen, „die bei Behörden oder privaten Stellen vorhanden und für die Strafverfolgsbehörden ohne das Ergreifen von Zwangsmaßnahmen nach Artikel 1 Absatz 5 verfügbar sind“ (sog. „verfügbare Daten“).

Vor diesem Hintergrund ist zu fragen, was unter einer Zwangsmaßnahme zu verstehen ist, wenn ein ersuchtes Datum noch bei keiner Strafverfolgungsbehörde vorhanden ist.

Die Bundesregierung schlägt im Entwurf zur Umsetzung der wenig normenklaren Vorgaben vor, die Übermittlung auszuschließen, wenn die Daten zunächst mit Zwangsmaßnahmen erhoben werden müssten (§ 92 Abs. 3 IRG-E, § 27 Abs. 2 BKAG-E, § 33 Abs. 3a BPolG-E, § 35 Abs. 2 ZFdG-E, § 11a Abs. 4 ZVerwG-E, § 6a Abs. 3 SchwArbBekG-E). Sofern die verfügbaren Daten allerdings ohne das Ergreifen von Zwangsmaßnahmen erhoben werden können, steht die Übermittlung im Ermessen der ersuchten Strafverfolgungsbehörde (§ 92 Abs. 4 IRG-E, § 27 Abs. 3 BKAG-E, § 33 Abs. 3b BPolG-E, § 35 Abs. 3 ZFdG-E, § 11a Abs. 5 ZVerwG-E, § 6a Abs. 4 SchwArbBekG-E). Zur Bestimmung des Begriffs der Zwangsmaßnahme verweist der Rahmenbeschluss auf das nationale Recht. Die Bundesregierung verzichtet in dem Entwurf allerdings auf eine Definition im Gesetzestext. Dies halte ich aus rechtstaatlichen Überlegungen für problematisch. Sofern auf eine gesetzliche Definition verzichtet wird, wäre es aus meiner Sicht vorzugswürdig, auf den missverständlichen Begriff der Zwangsmaßnahme im Gesetzentwurf gänzlich zu verzichten und durch eine enge Bestimmung dessen zu ersetzen, was im Rahmen der Schwedischen Initiative als Zwangsmaßnahme zu verstehen ist.

In der Gesetzesbegründung wird der Begriff der Zwangsmaßnahme sowohl für den präventiven als auch für den repressiven Bereich näher erläutert. Danach sind unter dem Begriff der Zwangsmaßnahme im repressiven Bereich gem. § 92 Abs. 3 IRG „Maßnahmen zu verstehen, die von der Polizei nicht im Rahmen der allgemeinen Ermittlungsbefugnis gemäß der § 163 Absatz 1, § 160 Absatz 4 Strafprozessordnung (StPO), sondern nur unter Rückgriff auf darüber hinausgehende, gesetzlich speziell geregelte Befugnisse, wie beispielsweise § 94 ff. StPO ergriffen werden können.“ (Drucksache 17/5096, S. 21). Für den präventiven Bereich



lautet die Definition folgendermaßen: „Zwangmaßnahmen in diesem Sinne im Bereich der Gefahrenabwehr sind Maßnahmen, die gegen oder ohne den Willen der betroffenen Person durchgesetzt werden und die aufgrund des damit einhergehenden wesentlichen Grundrechtseingriffs einer speziellen gesetzlichen Grundlage bedürfen, also nicht auf Generalklauseln oder vergleichbare Grundnormen (u. a. §§ 20a, 20b BKAG) gestützt werden können.“ (Drucksache 17/5096, S. 25)

Der Bundesrat hat die Definition für den präventiven Bereich in seiner Stellungnahme deutlich kritisiert. Sie greife zu kurz und sei im Ergebnis „praxisfremd und untauglich“ (Drucksache 17/5096, S. 33).

Wenngleich auch ich Zweifel habe, ob auf der Grundlage dieser Definitionen hinreichende Rechtssicherheit für die Voraussetzung von Datenübermittlungen gewährleistet werden kann, erkenne ich an, dass mit dem Rückgriff auf die Generalklausel offensichtlich der Versuch unternommen worden ist, alle Datenerhebungen auszuschließen, die aufgrund ihrer besonderen Eingriffstiefe eine spezielle Rechtsgrundlage voraussetzen. Hierbei ist zu bedenken, dass die Polizeibehörden für jede Erhebung personenbezogener Daten grundsätzlich eine Rechtsgrundlage benötigen, so dass es ein „Weniger“ zur Generalklausel nicht geben dürfte. Zudem ist der Begriff der Zwangmaßnahmen nach dem Gesetzentwurf so auszulegen, dass die Zwangmaßnahme jede staatliche Maßnahme umfasst, „die gegen oder ohne den Willen der betroffenen Personen durchgesetzt werden“ müsste. Wie es grundsätzlich auch für den repressiven Bereich auf der Grundlage der allgemeinen polizeilichen Ermittlungsklausel gem. §§ 163 Absatz 1, § 160 Absatz 4 StPO gilt, steht den Polizeibehörden damit nur ein Fragerecht ohne Verpflichtung zur Auskunftserteilung zu.

Allerdings können die Polizeibehörden auf der Grundlage der Generalklausel auch sehr sensible Daten erheben. Denn im Gegensatz zu den Bedenken des Bundesrates, die Definition greife zu kurz, kann die Datenerhebung auf der Grundlage der Generalklausel auch sehr weit gehen, etwa bei der Erhebung von Bankdaten, Telekommunikationsdaten, Gesundheitsdaten, etc. Ich erinnere insoweit an die Entscheidung des Bundesverfassungsgericht, wonach ein Ersuchen (in diesem Fall der Staatsanwaltschaft) an Kreditkartenunternehmen mit der Aufforderung zur Übermittlung der Identität von Karteninhabern, die eine bestimmte Transaktion vorgenommen haben, zulässigerweise auf die Generalklausel gestützt werden darf (BVerfG, Beschluss vom 17.2.2009 – 2 BvR 1372, 1745/07, NJW 2009, 1405 ff).

Ich rege daher an, die Gesetzesbegründung so zu ergänzen, dass bei der Ausübung des Ermessens, ob ein Datum auf der Grundlage der Generalklausel erhoben und sodann übermittelt werden soll, zwingend zu berücksichtigen ist, welche Daten zunächst erhoben werden müssten. Handelt es sich dabei um besonders sensible Daten und würde die Datenerhebung daher einen tieferen Grundrechtseingriff bedeuten, so sollte von der Erhebung grundsätzlich abgesehen werden



*b) Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden*

Im Gegensatz zu früheren Entwürfen sind in dem vorliegenden Gesetzentwurf sechs Voraussetzungen genannt, die erfüllt sein müssen, bevor ein Ersuchen bewilligt werden darf (§ 92a IRG-E, § 14a Abs. 2 BKAG-E, § 32a Abs. 2 BPolG-E, § 34a Abs. 2 ZFdG-E, § 11a Abs. 2 ZVerwG-E, § 6a Abs. 2 SchwArbBekG-E). Die jeweiligen Ziffern 1-6 der genannten Vorschriften bleiben gegenüber den Vorgaben des Art. 5 Abs. 1 bzw. Art. 5 Abs. 3 in Verbindung mit Anhang B des o. a. Rahmenbeschlusses allerdings in einer Hinsicht zurück. Im Gesetzentwurf ist darauf verzichtet worden, den Zusammenhang zwischen dem Zweck des Ersuchens und der Person, auf die sich das Ersuchen bezieht, als gesonderte Voraussetzung aufzunehmen, obwohl dies gem. Art. 5 Abs. 3 in Verbindung mit Anhang B des o. a. Rahmenbeschlusses zu den Minimalanforderungen an ein Ersuchen gehört.

Ich rege daher an, die Voraussetzungen für die Bewilligung der Ersuchen in dem Sinne zu ergänzen, dass als weitere Voraussetzung der „Zusammenhang zwischen dem Zweck, zu dem die Informationen und Erkenntnisse erbeten werden, und der Person, auf die sich diese Informationen und Erkenntnisse beziehen“ (vgl. Anhang B) hinzugefügt wird.

*c) Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen*

Die in Art. 7 Rahmenbeschluss 2006/960/JI vorgesehene sog. Spontanübermittlung wird im Gegensatz zu dem ersten Entwurf nunmehr in § 14a Abs. 3 BKAG (und entsprechend in § 32a Abs. 3 BPolG-E, § 34a Abs. 3 ZFdG-E, § 11a Abs. 3 ZVerwG-E) in präziserer Form geregelt. Dennoch fällt auf, dass die im Rahmenbeschluss genannten „konkreten Gründe“ nicht als solche Einzug in den Gesetzentwurf gefunden haben. Die „konkreten Gründe“ für die Annahme, dass die unaufgefordert übermittelten Informationen und Erkenntnisse dazu beitragen können, bestimmte Straftaten zu verhüten oder aufzuklären, sollen ins deutsche Recht so übersetzt werden, dass die Erwartung ausreicht, dass die Datenübermittlung geeignet ist, zur Verhütung bestimmter Straftaten beizutragen.

Ich rege an, eine Formulierung zu wählen, die sich enger an dem Wortlaut des Rahmenbeschlusses hält und somit die Voraussetzungen für sog. Spontanübermittlungen nicht weiter gefasst werden, als sich dies aus den Vorgaben des Rahmenbeschlusses ergibt.





*d) Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern*

Ungeachtet der unter 2a) dargestellten Problematik enthalten die in Art. 10 Rahmenbeschluss 2006/960/JI aufgeführten Verweigerungsgründe in § 27 Abs. 2 und 3 BKAG-E, § 33 Abs. 3a und 3b BPolG-E, § 35 Abs. 2 und 3 ZFdG-E, § 11a Abs. 4 und 5 ZVerwG-E, § 6a Abs. 3 und 4 SchwArbBekG-E noch weitere Spielräume für eine die Datenübermittlung weiter einschränkende Umsetzung.

Für problematisch halte ich es, dass nach dem Gesetzentwurf eine Datenübermittlung auch dann im Ermessen der ersuchten Behörde stehen soll, wenn hierdurch Leib, Leben oder Freiheit einer Person gefährdet würde. Im Hinblick auf die Hochrangigkeit der Rechtsgüter Leib und Leben sollte deren Gefährdung den zwingenden Ausschluss einer Datenübermittlung zur Folge haben.

Ebenso halte ich es für eine mit dem Rahmenbeschluss 2006/960/JI konforme Umsetzung, wenn Datenübermittlungen nicht nur abgelehnt werden können, sondern in der Regel abzulehnen sind, soweit dem Ersuchen nur Bagatellkriminalität zugrunde liegt (Art. 10 Abs. 2 Rahmenbeschluss 2006/960/JI).

*e) vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten*

Eine Datenübermittlung an eine andere ausländische Polizeibehörde hat sich nicht darin zu erschöpfen, diese polizeifachlich über eine Person zu informieren. Sie hat auch zu gewährleisten die ersuchende Behörde über solche Informationen in Kenntnis zu setzen, die dem Schutz des Betroffenen dienen, wie etwa die Zweckbindung der übermittelten Daten, eine Frist zur Aussonderungsprüfung oder zur Löschung, Kennzeichnungen, etc. Der Rahmenbeschluss zur Schwedischen Initiative enthält in Art. 8 und dort insbesondere in den Absätzen 3 und 4 einige Ansätze in diese Richtung.

Von zentraler Bedeutung für eine Übermittlung ist die Regelung zur Zweckbindung bzw. zum Genehmigungsvorbehalt gem. Art. 8 Abs. 3, wenn ein übermitteltes Datum für einen anderen Zweck als den der Übermittlung verwendet werden soll. Diese Vorschrift soll in § 27a Abs. 1 Satz 1 BKAG-E sowie in § 92b Satz 1 IRG-E, § 33a Abs. 1 Satz 1 BPolG-E, § 35a Abs. 1 Satz 1 ZFdG-E, § 11b Abs. 1 Satz 1 ZVerwG-E, § 6a Abs. 5 Satz 1 SchwArbBekG-E entsprechend umgesetzt werden. Der Rahmenbeschluss sieht eine Zweckdurchbrechung nur für den Fall vor, dass eine „unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit“ vorliegt. Gem. § 27a BKAG-E ist eine Zweckdurchbrechung bei einer „gegenwärtigen und





erheblichen Gefahr“ zulässig. Ausweislich der Gesetzesbegründung soll mit dieser leicht veränderten sprachlichen Fassung eine Anpassung an die Terminologie des deutschen Polizeirechts erfolgen (Drucksache 17/5096, S. 26). Von einer Vergleichbarkeit von einer ernsthaften und einer erheblichen Gefahr kann meines Erachtens ausgegangen werden.

Für den Bereich der Rechtshilfe in Strafsachen sieht der Gesetzesentwurf darüber hinaus vor, dass bei einer Übermittlung in einen anderen Mitgliedstaat mitzuteilen ist, dass die Verwendung der übermittelten Daten als Beweismittel grundsätzlich unzulässig ist (§ 92 Abs. 2 IRG-E). Diese Vorschrift ist nur für den repressiven Bereich vorgesehen. Meines Erachtens wäre es vorzugswürdig, diese Mitteilung bei allen Übermittlungen, also auch bei Übermittlungen auf der Grundlage von präventiven Befugnissen, vorzunehmen. Denn jedes präventiv übermittelte Datum kann auch schnell zu einem Datum werden, das im Rahmen der Strafverfolgung verwendet wird.

Im Hinblick auf die Aussonderungsprüffristen und die Löschdaten wirft der Entwurf folgendes Problem auf: Das geltende BKA-Gesetz enthält in § 14 Absatz 7 Satz 5 eine Regelung, wonach dem Empfänger der übermittelten Daten der beim BKA vorgesehene Lösungszeitpunkt mitzuteilen ist. Der § 14a BKAG-E geht dem geltenden § 14 BKAG vor. § 14a Abs. 1 Satz 2 BKAG-E erklärt ferner die für die Übermittlung im innerstaatlichen Bereich geltenden Vorschriften für anwendbar. In § 10 BKAG ist allerdings keine entsprechende Pflicht zur Mitteilung für das Aussonderungsprüfung bzw. Lösungsfrist enthalten. Als Konsequenz wäre auch bei Übermittlungen auf der Grundlage des § 14a BKAG-E keine entsprechende Mitteilung an die anderen europäischen Polizeibehörden zu machen. Dies halte ich für nicht akzeptabel. Damit würde Datenschutzes durch das Auseinanderfallen der Umsetzung der Rahmenbeschlüsse zu der „Schwedischer Initiative“ auf der einen und für den Datenschutz in der ehemaligen 3. Säule auf der anderen Seite faktisch reduziert. Denn letzterer sieht die Übermittlung von Fristen in Art. 9 Rahmenbeschluss 2008/977/JI vor.

Es sollte daher im Umsetzungsgesetz klargestellt werden, dass entsprechende Fristen und Verwendungsbeschränkungen bei Übermittlungen auf der Grundlage der Schwedischen Initiative auch mitgeteilt werden. Dies gilt grundsätzlich für alle betroffenen Rechtsgrundlagen.

Im Zusammenhang mit dem datenschutzrechtlich bedeutsamen Auskunftsrecht enthält der Rahmenbeschluss 2006/960/JI lediglich die Regelung des Art. 8 Absatz 4 Satz 5. Danach kann der empfangende Mitgliedstaat in besonderen Fällen vom übermittelnden Staat ersucht werden, Auskünfte über die Verwendung und weitere Verarbeitung der übermittelten Daten zu erteilen.

Ich habe während der Ressortberatungen erreicht, dass eine Pflicht der deutschen Stellen zur Beantwortung solcher Ersuchen durch andere Mitgliedstaaten aufgenommen worden ist (§



27a Abs. 2 BKAG-E, § 33a Abs. 2 BPolG-E, § 35a Abs. 2 ZFdG-E, § 11b ZVerwG-E). Dies entspricht auch der Verpflichtung gem. Art. 15 Rahmenbeschluss 2008/977/JI.

*f) Eine neue Vorschrift für die Datenübermittlung in Drittstaaten*

Die „Schwedische Initiative“ äußert sich zu den Voraussetzungen der Datenübermittlungen in Drittstaaten nicht. Trotzdem hat die Bundesregierung das Umsetzungsgesetz zum Anlass genommen, eine Änderung der zentralen Vorschrift für Datenübermittlungen in Drittstaaten gem. § 14 Absatz 7 Satz 7 BKAG (sowie § 33 Abs. 3 Satz 2 BPolG-E, § 34 Abs. 4 Satz 5 ZFdG-E, § 11 Abs. 2 Satz 5 ZVerwG-E) vorzuschlagen.

Die Novellierung beabsichtigt dabei eine Akzentverschiebung und eine Ergänzung.

Die geltende Fassung lautet: „Die Übermittlung unterbleibt außerdem, wenn durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, insbesondere, wenn im Empfängerland ein angemessener Datenschutzstandard nicht gewährleistet wäre.“

Für die Zukunft schlägt die Bundesregierung folgenden Wortlaut vor:

„Die Übermittlung unterbleibt außerdem, soweit, auch unter Berücksichtigung des besonderen öffentlichen Interesses an der Datenübermittlung, im Einzelfall schutzwürdige Interessen der betroffenen Person an dem Ausschluss der Übermittlung überwiegen. Zu den schutzwürdigen Interessen der betroffenen Person gehört auch das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat. Die schutzwürdigen Interessen der betroffenen Person können auch dadurch gewahrt werden, dass der Empfängerstaat oder die empfangende zwischen- oder überstaatliche Stelle im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.“

Die neue Formulierung betont den Charakter der Abwägungsentscheidung im Einzelfall. Zwar ist nicht zu bestreiten, dass die Zulässigkeit einer Datenübermittlung letztlich eine Einzelfallentscheidung ist. Der neue Vorschlag der Bundesregierung darf allerdings nicht dazu führen, die Angemessenheit des Datenschutzniveaus in den Drittstaaten in ihrer Bedeutung für die Zulässigkeit der Datenübermittlung abzumildern. Gerade vor diesem Hintergrund betrachte ich die weitere Neuerung, nach der die schutzwürdigen Interessen des Betroffenen auch dadurch gewahrt werden können, dass der Empfängerstaat den angemessenen Schutz der übermittelten Daten garantiert, mit erheblicher Skepsis. Weitere Erläuterungen zu der Garantieerklärung sucht man in der Gesetzesbegründung vergebens.

Der bloße Hinweis, dass mit dieser Novellierung eine Anpassung an den Wortlaut des IRG bezweckt ist, reicht insofern nicht aus. Deshalb und im Hinblick darauf, dass eine entspre-



chende Regelung ohne Bezug zur „Schwedischen Initiative“ ist, rege ich an, auf die vorgeschlagene Änderung zu verzichten.

*g) Die zusätzlichen Änderungen in der StPO*

Die Bundesregierung schlägt in dem Gesetzentwurf zudem vor, neben den zur Umsetzung der „Schwedischen Initiative“ erforderlichen Änderungen des deutschen Rechts zusätzliche Änderungen der Strafprozessordnung vorzunehmen, die zwar für die Umsetzung nicht zwingend erforderlich sind, aber angesichts des erhöhten „Risikos einer unzulässigen Weitergabe sensibler personenbezogener Daten, die in einem Strafverfahren gewonnen wurden“ (Gesetzesbegründung, S. 18) für erforderlich gehalten werden. Bei diesen Ergänzungen der §§ 478 Abs. 1 Satz 5 und 481 Abs. 3 StPO handelt es sich, wie die Stellungnahme des Bundesrates und die Gegenäußerung der Bundesregierung deutlich machen, um einen weiteren kritischen Punkt des Gesetzesentwurfes. Die vorgeschlagenen Ergänzungen halte ich für sinnvoll.

Nach den vorgeschlagenen Änderungen sollen die zuständigen Polizeibehörden – jeweils nur bei Zweifeln an der Zulässigkeit – vor Erteilung von Auskünften an eine andere Polizeibehörde oder bei zweckändernder (also polizeilicher) Verwendung von Daten aus Strafverfahren die Entscheidung der StA bzw. des Gerichts einholen. Die Entscheidungen darüber, ob einer Übermittlung ein Verbot entgegensteht oder ob einer polizeilichen Verwendung von Daten aus Strafverfahren eine innerstaatliche Verwendungsbeschränkung entgegensteht, liegt nach geltendem Recht allein bei der Polizeibehörde. Trotz der Unklarheiten, wann die Zulässigkeit einer Übermittlung oder Verwendung von Daten zweifelhaft ist, ist die vorgeschlagene Änderung aus meiner Sicht geeignet, um die Achtung der Betroffenenrechte durch die Einbeziehung einer Justizbehörde zu stärken.

*h) Die Änderungen in der Abgabenordnung (AO)*

Der Entwurf der Bundesregierung zur Änderung von § 117 Absatz 5 AO-E sieht vor, dass die Steuerverwaltungen der Länder und das Bundeszentralamt für Steuern (BZSt) im Rahmen der zwischenstaatlichen Amts- und Rechtshilfe gegenüber anderen EU-Staaten die betroffenen Daten durch elektronische Datenübertragung unmittelbar übermitteln können.

Dieser Regelungsentwurf geht über den durch die „Schwedische Initiative“ begründeten Umsetzungsbedarf hinaus, der sich allein auf die Vereinfachung des Austausches von Informationen zwischen Strafverfolgungsbehörden bezieht. Der Entwurf der Bundesregierung schafft



SEITE 12 VON 12 demgegenüber eine Rechtsgrundlage für einen elektronischen Austausch sämtlicher Finanzbehörden.

Auf seiner Grundlage wäre nicht nur der elektronische Austausch zwischen der strafverfolgend tätigen Steuerfahndung, sondern auch anderer Finanzbehörden (Finanzämter) sowie dem BZSt möglich. Für die Finanzbehörden konkretisieren jedoch eigene gesetzliche Regelungen die Ausgestaltung der Amtshilfe (z. B. Austausch von Informationen im Bereich direkter Steuern). Es bleibt unklar, wie das Verhältnis dieser Normen zu der vorgeschlagenen Regelung nach § 117 Absatz 5 AO-E zu definieren ist.

In materiell-rechtlicher Hinsicht bleibt der Regelungsentwurf hinter den Anforderungen der Schwedischen Initiative an den Informationsaustausch zurück. Während die Umsetzungsnorm zur Schwedischen Initiative für den Bereich der Polizei dezidierte Vorgaben (z.B. hinsichtlich der Verweigerungsgründe) enthält, werden diese für den Bereich der Finanzbehörden (einschließlich Steuerfahndung) nicht vorgeben. Gegen diese widersprüchliche Regelungssystematik bestehen Bedenken.

Die vom Bundesrat vorgeschlagenen Regelung eines neuen § 117a und 117b AO-E enthalten für die Steuerfahndung Regelungen zum Austausch von Informationen mit den Behörden anderer EU-Staaten, die den Regelungen der anderen Gesetze zur Umsetzung der „Schwedischen Initiative“ entsprechen.

Der Vorschlag des Bundesrates enthält ausschließlich Regelungen für die "mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden" und setzt damit die „Schwedische Initiative“ für die Finanzverwaltung in ausreichendem Maße um. Die Behörden der Steuerfahndung sind nach §§ 208, 404 AO nicht als Finanzbehörden, sondern in der Funktion einer Justizbehörde tätig. Mit §§ 117a bzw. 117b AO-E wird damit keine Rechtsgrundlage für den Austausch von Informationen solcher Finanzbehörden geschaffen, die dem Anwendungsbereich der Schwedischen Initiative nicht unterfallen. Insofern halte ich den Vorschlag des Bundesrates für vorzugswürdig.

**Entschließung**  
**der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder**  
**am 6. und 7. November 2008 in Bonn**

**Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur**  
**Vereinfachung des polizeilichen Datenaustausches zwischen den EU-**  
**Mitgliedstaaten geboten**

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.
- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,
- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,
- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,
- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.