

25.11.05

Beschlussdes Bundesrates

Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden**KOM(2005) 475 endg.; Ratsdok. 13019/05**

Der Bundesrat hat in seiner 817. Sitzung am 25. November 2005 gemäß §§ 3 und 5 EUZBLG die folgende Stellungnahme beschlossen:

1. Der Bundesrat begrüßt das in der Vorlage zum Ausdruck gebrachte Anliegen der Kommission, das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der EU umzusetzen und den Informationsaustausch im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu verbessern.
2. Er begrüßt insbesondere die Intention des Rahmenbeschlussvorschlags, nach dem der grenzüberschreitende Austausch von strafverfolgungsrelevanten Informationen zwischen den Mitgliedstaaten - gerade bei der Terrorismusverhütung und -bekämpfung - nicht durch Unterschiede beim Datenschutz behindert und mit dem zugleich sichergestellt werden soll, dass insbesondere im Hinblick auf die Verwirklichung des Verfügbarkeitsgrundsatzes die Grundrechte und vor allem das Recht auf den Schutz der Privatsphäre sowie der Schutz personenbezogener Daten in der gesamten EU gewahrt bleiben.
3. Der Bundesrat ist allerdings der Auffassung, dass der Entwurf dem Anliegen nur teilweise gerecht wird. Bei der Schaffung einheitlicher Vorschriften für die Verarbeitung und den Schutz personenbezogener Daten ist darauf zu achten, dass

- die Angleichung der Rechtsvorschriften der Mitgliedstaaten nicht zu einer Verschärfung des Datenschutzes in diesen Ländern führt,
 - die Regelungen auf grenzüberschreitende Sachverhalte begrenzt werden und eine Ausweitung auf die innerstaatliche Datenverarbeitung - auch angesichts der insoweit äußerst zweifelhaften Zuständigkeit der EU - unterbleibt,
 - den besonderen Anforderungen und Spezifika der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ausreichend Rechnung getragen wird,
 - die rechtmäßige Tätigkeit der zuständigen Behörden, insbesondere bei der Bekämpfung des organisierten Verbrechens und des internationalen Terrorismus, in keiner Weise behindert wird,
 - keine zusätzlichen bürokratischen Einrichtungen und Anforderungen geschaffen werden und
 - ein unnötiger Personal- und Kostenaufwand in den Mitgliedstaaten vermieden wird.
4. Ferner ist der Bundesrat der Auffassung, dass der Vorschlag die finanziellen Auswirkungen der vorgesehenen Maßnahmen nicht hinreichend zum Ausdruck bringt.

Insbesondere entstehen zusätzliche Ausgaben für die Mitgliedstaaten durch

- die regelmäßige Überprüfung und Sicherstellung der sachlichen Richtigkeit der Daten (Artikel 9 Abs. 2),
- die Protokollierungen und Dokumentierung (Artikel 10),
- die sichere Übermittlung im Hinblick auf die automatisierte Datenverarbeitung (Artikel 24),
- die geplanten Schadenersatzregelungen (Artikel 28).

Der Bundesrat bittet die Bundesregierung, darauf hinzuwirken, dass die sich für die Mitgliedstaaten ergebenden Mehrbelastungen auf das unbedingt notwendige Maß beschränkt werden.

Außerdem ist darauf zu achten, dass die deutsche Sprachfassung des Rahmenbeschlusses die englische Originalfassung wortgetreu wiedergibt und dabei nach Möglichkeit identische Formulierungen aus der EG-Datenschutzrichtlinie

(Richtlinie 95/46/EG) wortgleich übernimmt.

5. Gegen die Ausgestaltung des vorgeschlagenen Rahmenbeschlusses bestehen in einigen Punkten Bedenken:
 - Der Rahmenbeschlussvorschlag legt nicht ausschließlich Bestimmungen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI EUV fest. Er betrifft - unabhängig vom Datentransfer - die Datenverarbeitung in jedem justiziellen und polizeilichen Verfahren, wie sich aus den Erwägungsgründen 3, 8 und 11, der Bestimmung über den Anwendungsbereich (Artikel 3) sowie der Systematik des Vorschlags (Kapitel I, II und IV bis VII in Abgrenzung zu Kapitel III) ergibt. Dies wird durch Artikel 1, der den Gegenstand des Rahmenbeschlusses beschreibt, indes nicht hinreichend deutlich.
 - Der Bundesrat gibt zu bedenken, dass durch das Strafverfahrensänderungsgesetz 1999 vom 2. August 2000 (BGBl. I S. 1253, 1262) die verfassungsrechtlich gebotenen, im Interesse der Rechtssicherheit und Rechtsklarheit sowie aus strafprozessual-systematischen Gründen notwendigen Rechtsgrundlagen für die Verwendung personenbezogener Informationen, die in einem Strafverfahren erhoben worden sind, sowie für die Verarbeitung und Nutzung personenbezogener Daten in Dateien geschaffen wurden. Diese Regelungen gewährleisten - ergänzt durch die jeweiligen Registergesetze nebst Errichtungsanordnungen und Rechtsverordnungen - bereits jetzt ein hohes Datenschutzniveau und zugleich eine effektive Strafverfolgung.
 - Der Bundesrat ist der Auffassung, dass die in dem Beschlussvorschlag vorgesehenen Prüf-, Dokumentations-, Protokollierungs- und Informationspflichten erheblich darüber hinausgehen und die Gefahr eines nicht mehr vertretbaren personellen Mehraufwands in sich tragen. Er bittet die Bundesregierung, im weiteren Verlauf des Verfahrens auf eine stärkere Berücksichtigung des Erwägungsgrunds 8 hinzuwirken, nach dem die rechtmäßigen Tätigkeiten der Polizei-, Zoll-, Justiz- und sonstigen zuständigen Behörden in keiner Weise behindert werden dürfen.
6. Vor diesem Hintergrund hält der Bundesrat eine grundlegende Überarbeitung des Entwurfs insbesondere in folgenden Punkten für erforderlich:

Zu Artikel 4

Die Bestimmung verlangt in ihrem Absatz 3 eine "klare Unterscheidung" zwischen den Daten bestimmter Personengruppen, wobei die Sinnhaftigkeit der Differenzierung - z. B. zwischen Zeugen und Opfern - nicht immer erkennbar ist. Im nachfolgenden Absatz wird die Verarbeitung der Daten der verschiedenen Personengruppen dann wiederum identischen Anforderungen unterstellt, was die Speicherung von Tatverdächtigen unnötig erschwert.

Der letzte Spiegelstrich des Absatzes 4 ist zudem fehlerhaft aus dem Englischen übersetzt ("the processing of the data is not excessive in relation to the offence concerned").

Zu Artikel 6

Die Regelung sieht erhebliche Erschwernisse hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten vor (z. B. Daten, aus denen ethnische Herkunft, politische Meinungen, religiöse Überzeugungen hervorgehen). Artikel 6 wird den besonderen Anforderungen und Spezifika der polizeilichen und justiziellen Zusammenarbeit in Strafsachen nicht gerecht. Die genannten Datenkategorien sind insbesondere bei der Bekämpfung des internationalen Terrorismus von Bedeutung. Vergleichbare Vorschriften auf nationaler Ebene finden daher regelmäßig auf die Datenverarbeitung für Zwecke der Gefahrenabwehr sowie zur Verfolgung von Straftaten keine Anwendung. Die in Artikel 6 Abs. 2 vorgesehenen Ausnahmen vermögen die grundsätzlichen Bedenken gegen die Regelung nicht auszuräumen.

Zu Artikel 9 insgesamt

Insbesondere die Überprüfung der Qualität von übermittelten Daten im Bereich der internationalen Zusammenarbeit nach den Kriterien des Artikels 9 erscheint weder angemessen noch praktikabel. Sofern dadurch festgelegt werden soll, dass Daten vor jeder Übermittlung bzw. Bereitstellung im automatischen Abrufverfahren auf Aktualität und Richtigkeit gesondert zu überprüfen sind, berücksichtigt dies nicht die technischen und organisatorischen Gegebenheiten der zentralen Register. Die nach nationalem Recht bestehenden Mechanismen zur Gewährleistung der Datenrichtigkeit und -aktualität erscheinen insoweit ausreichend.

Zu Artikel 9 Abs. 6

Die Vorschrift sieht vor, dass personenbezogene Daten auf Antrag der betroffenen Person gekennzeichnet werden müssen, falls ihre sachliche Richtigkeit von der betroffenen Person in Abrede gestellt wird und nicht ermittelt werden kann (Non-liquet-Fälle). Die Regelung wird den besonderen Anforderungen und Spezifika der polizeilichen und justiziellen Zusammenarbeit in Strafsachen nicht gerecht. Von den zuständigen Behörden werden, insbesondere im Bereich der vorbeugenden Bekämpfung von Straftaten, häufig bloße "Verdachtsdaten" oder sonstige weiche Daten gespeichert, deren Richtigkeit naturgemäß noch nicht bewiesen werden kann und vom Betroffenen daher regelmäßig bestritten werden wird. In vielen Fällen wäre daher die Aufgabenwahrnehmung der zuständigen Behörden nicht mehr möglich oder erheblich behindert.

Zu Artikel 9 Abs. 7 zweiter Spiegelstrich

Die Regelung sieht vor, dass personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaats übersandt wurden, gelöscht werden, falls eine nach dem innerstaatlichen Recht des anderen Mitgliedstaats vorgesehene diesbezügliche Frist abgelaufen ist und die Behörde, die die betreffenden Daten übermittelt oder zur Verfügung gestellt hat, die empfangende Behörde bei der Übermittlung oder Bereitstellung über diese Frist in Kenntnis gesetzt hat, und die personenbezogenen Daten nicht mehr für Gerichtsverfahren benötigt werden. Die Ausnahmen von der Löschungspflicht sind zu eng gefasst. Die weitere Datenverarbeitung muss auch dann möglich sein, wenn die übermittelten Daten für ein konkretes Ermittlungsverfahren oder die Abwehr von Gefahren erforderlich sind.

Zu Artikel 10 Abs. 2 und 3

Die in dieser Vorschrift vorgesehenen Protokollierungs- und Dokumentationspflichten sind als allgemeine Regelung zu weit gehend. Im nationalen Recht wird für automatisierte Abrufverfahren regelmäßig eine stichprobenartige Protokollierungspflicht als ausreichend angesehen. Ebenso ist die Dokumentationspflicht für jede nicht automatisierte Übermittlung zu weit gehend. Im innerstaatlichen Recht ist eine allgemeine gesetzliche Pflicht zur Protokollierung von Übermittlungen nicht vorgesehen.

Zu Artikel 10 Abs. 3

Die Regelung sieht eine strikte Zweckbindung der Protokolldaten für Zwecke der Datenschutzkontrolle vor. Die Regelung ist dahingehend zu ergänzen, dass

weitere Zweckänderungen zugelassen werden, z. B. in Anlehnung an § 33 Abs. 8 BPolG (Nutzung der Protokolldaten zur Verhinderung oder Verfolgung schwerwiegender Straftaten gegen Leib, Leben oder Freiheit).

Zu Artikel 12 und 13

Die deutsche Sprachfassung lässt nicht erkennen, ob die Anforderungen kumulativ oder alternativ vorliegen müssen ("wenn folgende Anforderungen erfüllt sind"). Dies beruht auf der fehlerhaften Übertragung aus dem englischen Text ("if all of the following requirements are met").

Zu Artikel 15 und 16

Die Vorschrift nimmt den seltenen Ausnahmefall, dass ein Mitgliedstaat personenbezogene Daten, die er aus einem anderen Mitgliedstaat erhalten hat, an ein Drittland oder eine internationale Einrichtung weiter übermitteln will, zum Anlass einer ausufernden Regelung, die auch Artikel 16 mit umfasst. Da die Weiterübermittlung zugleich an die Zustimmung des Mitgliedstaats gebunden wird, aus dem die Daten stammen, würde die Regelung in der Praxis leer laufen, weil das Drittland an diesen Mitgliedstaat verwiesen würde. Artikel 15 und 16 sollten deshalb gestrichen werden.

Zu Artikel 18

Die Regelung sieht vor, dass die zuständige Behörde, die die personenbezogenen Daten übersandt oder zur Verfügung gestellt hat, auf deren Antrag über die weitere Verarbeitung und deren Ergebnisse unterrichtet werden muss. Wird dem Änderungsvorschlag zu Artikel 10 Abs. 2 und 3 gefolgt, kann die Unterrichtung nur erfolgen, soweit die weitere Verarbeitung protokolliert bzw. dokumentiert ist.

Zu Kapitel IV (Artikel 19 bis 22)

Der Vorschlag des Rahmenbeschlusses befasst sich in Kapitel IV mit den Rechten der betroffenen Person. Die Regelung sieht umfangreiche Informationsrechte des Betroffenen bei der Erhebung von Daten vor. Das nationale Recht kennt derart umfangreiche Informationsrechte in der Erhebungsphase nicht. Da sich die Vorgaben nicht auf Daten beschränken, die von einem Mitgliedstaat an einen anderen übermittelt worden waren und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen im Übrigen zudem häufig dieselben Daten zu Grunde liegen, die auch auf nationaler Ebene Gegenstand der Datenverarbeitung sind, hätte eine derartige Regelung erheblichen Einfluss auf die innerstaatlichen Datenerhebungsregeln.

Informationsrechte in der Datenerhebungsphase, die über die Mitteilung der Rechtsgrundlage und eine im Einzelfall bestehende Auskunftspflicht im Falle der schriftlichen Erhebung hinausgehen, entziehen sich einer allgemeinen Regelung. Auch unter dem Gesichtspunkt der Datenqualität sind sie nur insoweit berechtigt, als sie sicherstellen sollen, dass die Datenverarbeitung mit Einwilligung der betroffenen Person auf einer wirksamen Grundlage beruht. Demgegenüber ist die Auferlegung von Hinweispflichten im Zusammenhang mit der Datenerhebung auf gesetzlicher Grundlage nicht mit einem Hinweis auf die Datenqualität zu rechtfertigen. Soweit für spezifische Arten der Datenerhebung, z. B. bei der DNA-Analyse, weitergehende Informationsrechte für erforderlich gehalten werden, ist dies gesondert für die jeweilige Einzelmaßnahme zu regeln.

Zu Artikel 21 Abs. 1 Buchstabe c und Artikel 22

In der Folge des Änderungsvorschlags zu Artikel 10 Abs. 2 und 3 kann die Mitteilung jeder Berichtigung, Löschung oder Sperrung an Dritte, an die die Daten weitergeben wurden, nur erfolgen, soweit die weitere Verarbeitung protokolliert bzw. dokumentiert ist.

Im Übrigen bestehen erhebliche Zweifel, ob die umfassende Regelung der Rechte der Betroffenen, d. h. unabhängig von einem grenzüberschreitenden Bezug, in die Zuständigkeit der EU fällt.

Zu Artikel 22

Anstatt vorzuschreiben, dass bestimmte Stellen über die Berichtigung, Sperrung oder Löschung zu unterrichten sind, wird vorgegeben, "dass automatisch eine Liste der Datenlieferanten und Empfänger dieser Daten erstellt wird". Dabei wird übersehen, dass der Rahmenbeschluss auch für die nicht automatisierte Verarbeitung in Dateien gelten soll (Artikel 3 Abs. 1). Entgegen dem Vorschlag der Kommission sollte es zudem unerheblich sein, ob eine Berichtigung auf Antrag des Betroffenen oder von Amts wegen erfolgt.

Zu Artikel 25

Die Vorschrift verlangt die Erstellung eines Verzeichnisses nach dem Vorbild der EG-Datenschutzrichtlinie (Artikel 18 und 19). Anders als in der EG-Datenschutzrichtlinie ist die Vorgabe aber nicht auf die automatisierte Datenverarbeitung beschränkt. Zweifelhaft erscheint auch, ob die Meldung an die Kontrollstelle, d.h. an die Datenschutzbehörde, gänzlich entfallen kann (vgl. Artikel 18 Abs. 2 EG-Datenschutzrichtlinie).

Der deutsche Text ist zudem missverständlich übersetzt ("ein Verzeichnis jeder vorgenommenen Verarbeitung" für "a register of any processing operation").

Zu Artikel 26

Die Vorabkontrolle, wie sie nach Artikel 20 der EG-Datenschutzrichtlinie vorgeschrieben ist, passt nicht auf die Datenverarbeitung im Anwendungsbereich des Rahmenbeschlusses. Polizei und Justiz müssen schnell und flexibel auf neue Herausforderungen reagieren. Ihre Datenverarbeitung kann deswegen nicht dem starren Verfahren einer Vorabkontrolle unterworfen werden. Absatz 1 lässt zwar Ausnahmen zu. Entscheidungskriterien müssen dabei aber die spezifischen "Risiken für die Rechte und Freiheiten der betroffenen Personen" sein. Während diese Risiken im Anwendungsbereich des Rahmenbeschlusses regelmäßig erheblich sein werden, müsste die Notwendigkeit von Eilfallentscheidungen unberücksichtigt bleiben.

Absatz 2 enthält einen Übersetzungsfehler, der die Annahme nahe legt, dass die Kontrollstelle im Gegensatz zur EG-Datenschutzrichtlinie für die Durchführung der Vorabkontrolle zwingend zuständig ist. Tatsächlich kann hier wie dort aber der behördliche Datenschutzbeauftragte mit der Maßnahme beauftragt werden. Im englischen Text heißt es nämlich: "Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority."

Zu Artikel 28

Absatz 2, der keine Parallele in der Haftungsvorschrift der EG-Datenschutzrichtlinie (Artikel 23) findet, sieht in Satz 1 eine Haftung für "unrichtige oder veraltete Daten" vor. Das Begriffspaar "unrichtig" und "veraltet" ist äußerst bedenklich, da damit auch eine Haftung für zutreffende Daten begründet würde. So wird in polizeilichen Dateien häufig vermerkt sein, dass der Betroffene zu einem bestimmten Zeitpunkt an einer bestimmten Adresse gewohnt hat. Das Datum wird nicht dadurch falsch, dass der Betroffene später verzogen ist. Würde die Polizei eine solche Information ("zuletzt wohnhaft") an eine andere Behörde übermitteln, könnte der Betroffene unter Umständen Schadensersatz geltend machen, wenn der Datenempfänger an der alten Adresse Erkundigungen über ihn eingezogen hat.

Absatz 2 sieht des Weiteren in Satz 3 vor, dass, sofern die empfangende Stelle wegen Verwendung unrichtiger oder veralteter Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder zur Verfügung gestellt wurden, Schadenersatz leistet, letztere der empfangenden Stelle den Gesamtbetrag des geleisteten Ersatzes erstattet. Es ist nicht ersichtlich, dass es für diese Regelung eine europarechtliche Grundlage gibt.

Zu Artikel 30

Ferner tragen die in Artikel 30 vorgesehenen Regelungen über die Befugnisse der unabhängigen Kontrollstellen den auch im Erwägungsgrund 17 niedergelegten Grundsätzen, wonach weder die Vorschriften für Strafverfahren noch die Unabhängigkeit der Gerichte berührt werden dürfen, nicht in ausreichendem Maße Rechnung. Der Bundesrat bittet die Bundesregierung, auf klarstellende Formulierungen hinzuwirken, die der Funktionstüchtigkeit der Strafrechtspflege Rechnung tragen.

Die in Artikel 30 des Rahmenbeschlusses vorgesehene Einrichtung von öffentlichen Stellen als Kontrollstellen, die diese Aufgabe in völliger Unabhängigkeit wahrnehmen, begegnet ebenfalls erheblichen Bedenken. Die Einrichtung der Kontrollstelle wäre als neue Aufgabe mit entsprechendem Personal- und Kostenaufwand entweder den Datenschutzbeauftragten, einer anderen öffentlichen Stelle oder einer gänzlich neu einzurichtenden Stelle zu übertragen. Die Aufgabenwahrnehmung durch eine öffentliche Stelle in völliger Unabhängigkeit hat bereits im Rahmen des derzeit anhängigen Vertragsverletzungsverfahrens Nr. 2003/4820 wegen Verstoßes gegen die Europäische Datenschutzrichtlinie zu erheblichen Problemen geführt, da bislang mit der EU keine Verständigung darüber erreicht werden konnte, dass der völligen Unabhängigkeit in der Aufgabenwahrnehmung eine - verfassungsrechtlich gebotene - Einbindung in einen hierarchischen Verwaltungsaufbau nicht entgegensteht.

Vor diesem Hintergrund ist die Regelung in Artikel 30 des Rahmenbeschlusses abzulehnen.

Zu Artikel 31 und 32

Die Regelung sieht die Einsetzung einer Gruppe auf Ebene der EU für den Schutz von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von schweren Straftaten vor.

Im Hinblick auf die auch auf europäischer Ebene bestehende Zielsetzung, den Abbau der Bürokratie voranzutreiben, ist die zwingende Notwendigkeit der oben genannten Gruppe - auch im Sinne des Subsidiaritätsgedankens - nicht erkennbar.

Zu Artikel 35

Nach Absatz 1 sollen die Mitgliedstaaten den Rahmenbeschluss bis spätestens Ende des Jahres 2006 umsetzen. Angesichts der Komplexität der Materie wäre eine Umsetzungsfrist von lediglich einem Jahr nicht einzuhalten.

Der Bundesrat bittet die Bundesregierung, sich nachhaltig für die Position des Bundesrates einzusetzen und im Rahmen der Verhandlungen auf die notwendigen Änderungen hinzuwirken. In Anbetracht der Bedeutung und des Umfangs der Regelungen sollte gegenüber der Kommission ferner eine Erläuterung zu den einzelnen Vorschriften eingefordert werden.