Prof. Dr. jur. Hartmut Aden

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Hochschule für Wirtschaft und Recht/Berlin School of Economics and Law
Fachbereich Polizei und Sicherheitsmanagement
Professur für Öffentliches Recht und Europarecht
Alt-Friedrichsfelde 60
10315 Berlin
Tel. 030 30877-2868 (d.) oder 030 473705-51 Fax -52
E-Mail: Hartmut.Aden@hwr-berlin.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)585 E

Stellungnahme

zum Vorschlag der Europäischen Kommission

für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012)10 endg.,

und zu anderen hierauf bezogenen Dokumenten,

vorgelegt zur Anhörung des Innenausschusses des Deutschen Bundestages in Berlin am 22. Oktober 2012

Aufgrund der knapp bemessenen Vorbereitungszeit beschränkt sich diese Stellungnahme auf wenige ausgewählte Aspekte der von der Europäischen Kommission vorgelegten Entwürfe und Papiere. Im Mittelpunkt stehen Schwachstellen des Richtlinienentwurfs, für die ich dem Deutschen Bundestag empfehle, im Hinblick auf die weiteren Beratungen des Entwurfs im Europäischen Parlament und im Rat Stellung zu nehmen.

A) Grundsatzfragen

Der Datenaustausch zwischen Strafverfolgungsbehörden und insbesondere zwischen Polizeibehörden in der Europäischen Union und darüber hinaus hat sich seit den 1990er Jahren sehr dynamisch entwickelt.[1] Ursächlich hierfür sind die schnelle Entwicklung der Informationstechnologie und die parallele Institutionalisierung zahlreicher Kooperations- und Koordinationsforen für Polizei und Strafjustiz in Europa und darüber hinaus. Den institutionellen Rahmen hierfür bilden zentralisierte Datenbanken wie u. a. das Schengener Informationssystem,

[1] Der Kommissionsvorschlag knüpft hieran an, vgl. KOM(2012)10 endg., Begründungserwägung Nr. 3.

die Europol-Datenbanken sowie bi- und multilaterale Kooperationsstrukturen, in denen Informationen ausgetauscht werden.

Die Bemühungen der Europäischen Kommission um die Schaffung eines verbesserten Rechtsrahmens für den Datenschutz sind vor diesem Hintergrund grundsätzlich positiv zu bewerten. Neben sinnvollen Vorschlägen enthält der vorliegende Richtlinienentwurf aber auch einige gravierende Schwachstellen. **Ich empfehle dem Deutschen Bundestag, hierzu Stellung zu beziehen und für die weiteren Beratungen im Rat und im Europäischen Parlament Nachbesserungen einzufordern.**

Die öffentliche Diskussion hat sich in den zurückliegenden Monaten weitgehend auf den parallel von der Europäischen Kommission vorgelegten Entwurf für eine Datenschutz-Grundverordnung konzentriert. Der Richtlinienentwurf für den Strafverfolgungsbereich wurde dagegen vergleichsweise wenig thematisiert und problematisiert. Es wäre bedauerlich, wenn die Richtlinie aufgrund des weniger großen öffentlichen Interesses an dieser Thematik in einer Fassung verabschiedet würde, die hinter den Möglichkeiten eines modernen Datenschutzes auf hohem Niveau zurückbleibt.

I. Harmonisierungskonzept: *Race to the top* statt *Race to the bottom* sichern

Dem Richtlinienentwurf liegt kein klares Harmonisierungskonzept zugrunde. Richtig betont Begründungserwägung Nr. 7 das Ziel, „einen durchweg hohen Schutz der personenbezogenen Daten natürlicher Personen zu gewährleisten“.[2] Zugleich soll eine Harmonisierung der Datenschutzstandards den Datenaustausch zwischen den zuständigen Behörden der Mitgliedstaaten erleichtern. Dem liegt offenbar die Überlegung zugrunde, dass die Bereitschaft von Strafverfolgungsbehörden, Informationen an Behörden anderer Mitgliedstaaten weiterzugeben, steigen könnte, wenn die übermittelnde Behörde sich darauf verlassen kann, dass die empfangende Behörde Datenschutzstandards einhalten wird.

Diese Hypothese ist allenfalls in Teilen zutreffend. Wenn die Kooperation zwischen Strafverfolgungsbehörden in der EU trotz des umfangreichen institutionellen und rechtlichen Instrumentariums noch nicht überall reibungslos funktioniert, ist dies insbesondere eine Vertrauens-

frage. Nicht alle Strafverfolgungsbehörden in der EU bieten uneingeschränkte Gewähr dafür, dass sie gleichermaßen hohe professionelle Standards einhalten. In einigen EU-Staaten ist Korruption weiterhin verbreitete Praxis. Wenn Strafverfolgungsbehörden, die professionellen Standards nicht voll gerecht werden, keine oder weniger Information erhalten, so sind Datenschutzbegründungen hierfür allenfalls eine vordergründige Höflichkeitsgeste. Oft werden vermeintliche Datenschutzgründe „vorgeschoben", um eine aus anderen Gründen nicht gewollte Kooperation zu verweigern.

In Art. 1 Abs. 2 des Richtlinienentwurfs sind die Zielsetzungen, die Begründungserwägung Nr. 7 skizziert, unzulänglich umgesetzt worden. Hier fehlt die Festlegung auf einen *hohen* Schutzstandard.[3]

Die Zielformulierung in Art. 1 Abs. 2 (b), der zufolge die Richtlinie sicherstellen soll, „dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten wird", ist zumindest missverständlich. Im Kern geht es darum, dass alle Mitgliedstaaten ein so hohes Datenschutzniveau garantieren müssen, dass ein schlechter Datenschutzstandard in einem Mitgliedstaat keinen Anlass mehr geben muss, seinen Behörden den Zugang zu Informationen zu verweigern. Dies sollte in den Zielsetzungen auch klar formuliert werden.

Zur Gewährleistung eines hohen Datenschutzniveaus sollte die Zielformulierung außerdem klarstellen, dass es sich um eine *Mindestharmonisierung* handelt, von der die Mitgliedstaaten zugunsten eines höheren Schutzniveaus abweichen können. Eine solche Klarstellung wäre auf einem Feld, auf dem europäische und mitgliedstaatliche Regelungen ineinandergreifen, auch im Hinblick auf das Subsidiaritätsprinzip angemessen. Für den Umweltschutz ist die Abweichungsmöglichkeit zugunsten eines höheren Schutzstandards bereits im Primärrecht verankert (Art. 193 AEUV). Art. 16 AEUV enthält eine solche generelle Abweichungsklausel für den Datenschutz nicht, so dass diese in den sekundärrechtlichen Vorschriften zu verankern ist. Nur so kann gewährleistet werden, dass ein Regulierungswettbewerb für ein hohes Datenschutzniveau entsteht (*Race to the top*). Denn typischerweise kommt es im Regulierungswett-

[2] Ähnlich auch die begleitende Mitteilung der Europäischen Kommission, Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012)9 endgültig, Abschnitt 4.

[3] Kritisch hierzu auch Peter Hustinx/European Data Protection Supervisor, 2012, Opinion […] on the data protection reform package, Brüssel, 7. März 2012, Rn. 310.

bewerb zwischen den Mitgliedstaaten dadurch zu Innovationen, dass in einzelnen Mitgliedstaaten neue Ideen entwickelt und erprobt und sodann Vorbild für die EU-weite Regulierung werden. Die Richtlinie könnte hier an die Formulierung des Art. 1 Abs. 5 des Datenschutz-Rahmenbeschlusses 2008/977/JI anknüpfen.

Problematisch ist im Hinblick auf das Harmonisierungskonzept auch der Titel des Entwurfs. Dieser erwähnt nicht nur den Datenschutz, sondern auch den „freien Datenverkehr". Diese Konzeption ist für die Strafverfolgung verfehlt. Hier werden in vielen Fällen „sensible" personenbezogene Daten verarbeitet, die besonders schutzbedürftig sind, z. B. Informationen über verdächtige Personen. Es kann nicht darum gehen, für solche Informationen einen „freien Datenverkehr" zu eröffnen. Die Zielsetzung muss vielmehr so präzisiert werden, dass ein in allen EU-Mitgliedstaaten gleichermaßen hohes Datenschutzniveau erreicht werden soll. Ein solches überall hohes Datenschutzniveau könnte es den Strafverfolgungsbehörden erleichtern, Informationen auszutauschen, ohne dass in dem empfangenden Mitgliedstaat Verstöße gegen Datenschutzprinzipien zu befürchten sind.

Empfehlung A 1: *Ich empfehle dem Deutschen Bundestag,*

- *sich für die Präzisierung der Zielsetzungen der Richtlinie einzusetzen. Anzustreben ist ein „hohes" Datenschutzniveau. Die Formulierung der Zielsetzung sollte so geändert werden, dass sie keinen Gegensatz zwischen Datenschutz und effektiver Strafverfolgung suggeriert.*
- *die Streichung der Begriffe „sowie zum freien Datenverkehr" aus dem Titel zu verlangen.*

II. Polizeiliche Gefahrenabwehr vollständig von der Richtlinie erfasst?

Der Titel des Richtlinienentwurfs könnte zu dem Schluss führen, dass die Gefahrenabwehr im Sinne der Terminologie des deutschen Polizeirechts nur insoweit erfasst sein soll, als es um die Verhütung von Straftaten geht. Einzelne Bestimmungen des Entwurfs lassen indes darauf schließen, dass auch andere Tätigkeiten von Gefahrenabwehrbehörden erfasst sein sollen, z. B. wenn Art. 7 (d) die „Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit" als einen von mehreren rechtmäßigen Verarbeitungszwecken nennt. Wenn der

Anwendungsbereich sich hierauf erstrecken soll, sollte dies bei den Formulierungen zu den Zielen (Art. 1) und zum Anwendungsbereich (Art. 2) der Richtlinie klargestellt werden.

Empfehlung A 2: *Ich empfehle dem Deutschen Bundestag, darauf hinzuwirken, dass der Anwendungsbereich der Richtlinie für Tätigkeiten, die nach der deutschen Terminologie der Gefahrenabwehr zugerechnet werden, klarer gefasst wird.*

III. Datenschutz auch als Qualitätssicherung für die transnationale Polizeiarbeit verstehen

Der Richtlinienentwurf enthält diverse Elemente, die nicht nur dem Schutz personenbezogener Daten, sondern auch der Qualitätssicherung der transnationalen Strafverfolgung dienen. So fördern z. B. die Bestimmungen zur Datensicherheit (Art. 27 des Entwurfs) auch das Ziel, einen korrekten, vollständigen und nicht manipulierten Informationsbestand für die behördliche Arbeit zu gewährleisten. Fehler in den Datenbeständen oder unbefugte Informationsweitergabe an Dritte können leicht zu erheblichem Mehraufwand führen oder den Zweck der behördlichen Maßnahme sogar vereiteln.

Empfehlung A 3: *Ich empfehle dem Deutschen Bundestag, sich dafür einzusetzen, dass die Notwendigkeit eines hohen Standards an Datenschutz und Datensicherheit für eine effektive Tätigkeit der Strafverfolgungsbehörden klarer formuliert wird.*

IV. Rolle der Europäischen Kommission überdenken und „hohes“ statt „angemessenes“ Datenschutzniveau für Übermittlungen an Drittstaaten fordern

Die Europäische Kommission als Entwurfsverfasser hat sich in dem Richtlinienentwurf einige neue Aufgaben zugeschrieben. So erklärt Art. 34 des Entwurfs die Bestimmung des Grundverordnungs-Entwurfs auch hier für anwendbar, nach der die Kommission über ein „angemessenes“ Datenschutzniveau in Drittstaaten entscheidet. Diese inhaltlich weitreichende Entscheidungskompetenz sollte nicht bei der Kommission liegen. Eine breitere Entscheidungsbasis unter Einbeziehung zumindest des Europäisches Parlaments, der mitgliedstaatlichen Datenschutzbehörden und des Rates erschiene hier im Interesse der Qualitätssicherung und eines demokratisch abgesicherten Entscheidungsverfahrens erforderlich. Die in Art 49 Abs. 1 (d)

vorgesehene Möglichkeit einer Stellungnahme des nach der Grundverordnung einzusetzenden Europäischen Datenschutzausschusses erscheint nicht ausreichend.

Bedenklich ist auch die Anknüpfung an ein „angemessenes" Datenschutzniveau bei der Übermittlung von Daten an Drittstaaten und internationale Organisationen. Insbesondere für die Übermittlung „sensibler" Daten an Stellen außerhalb der EU sollte grundsätzlich ein „hohes" Datenschutzniveau Voraussetzung sein. Denkbar wäre hierfür ein transparentes Bewertungsverfahren, bei dem Drittstaaten und internationale Organisationen bezüglich ihres Datenschutzniveaus verschiedenen Qualitätsstufen zugeordnet werden können (z. B. „schwach", „niedrig", „angemessen", „hoch", „sehr hoch").

Eine solche differenzierte Klassifizierung wäre m. E. auch für die EU-Mitgliedstaaten denkbar und sinnvoll. Denn die implizite Annahme des Entwurfs, dass mit einer solchen Richtlinie automatisch ein überall gleichermaßen hohes Datenschutzniveau erreicht werden kann, dürfte zumindest mittelfristig eine Illusion bleiben.

Empfehlung A 4: *Ich empfehle dem Deutschen Bundestag, sich dafür einzusetzen, dass die Europäische Kommission weitreichende Entscheidungen wie die über die Angemessenheit des Datenschutzniveaus von Drittstaaten und internationalen Organisationen nicht allein treffen kann. Voraussetzung für die Übermittlung „sensibler" Daten sollte ein „hohes" oder „sehr hohes" Datenschutzniveau bei den empfangenden Stellen sein.*

B) Ausgewählte Schwachstellen des Entwurfs und Verbesserungspotentiale

Neben der Präzisierung des Harmonisierungszwecks (s.o., A I), des Anwendungsbereichs (s. o., A III) und der Rolle der Europäischen Kommission (s. o., A IV) sollte der Entwurf im Rahmen der Beratungen unter weiteren Aspekten nachgebessert werden. Hier können nur ausgewählte Schwachstellen aufgegriffen werden. Ergänzend sei auf die Stellungnahme des Europäischen Datenschutzbeauftragten Peter Hustinx vom 7. März 2012 verwiesen, die eine Reihe weiterer Änderungs-, Präzisierungs- und Ergänzungsvorschläge enthält.[4]

[4] Hustinx/Europäischer Datenschutzbeauftragter 2012, a. a. O., Rn. 305 ff.

I. Präzisere Regelungen zur Datenübermittlung erforderlich

Der Richtlinienentwurf definiert die Datenübermittlung sinnvoll als eine Form von „Verarbeitung“ (Art. 3 Nr. 3). Spezifische Regelungen für die Übermittlung enthält Kapitel V (Art. 33 ff.) des Entwurfs für die Zusammenarbeit mit Nicht-EU-Staaten und internationalen Organisationen. Erforderlich wären aber auch klare Regelungen für die Datenübermittlung zwischen Strafverfolgungsbehörden innerhalb der Europäischen Union. Hierfür sollten Mindeststandards zu folgenden Fragen definiert werden:

- Übermittlungen dürfen nur für klar definierte Zwecke erfolgen. Wenn diese mit dem ursprünglichen Erhebungszweck ausnahmsweise nicht identisch sind, bedarf diese Zweckänderung klarer gesetzlicher Grundlagen.
- Für die Datenübermittlung innerhalb wie außerhalb der EU reicht es nicht, Pflichten für die übermittelnde Stelle zu formulieren (so in unzulänglicher Form Art. 37 des Entwurfs). Auch für den Empfänger müssen klare Pflichten gelten.
- Besondere rechtliche Vorschriften sollten die *Zweckbindung auch nach einer Übermittlung sichern*, damit die empfangende Stelle die Daten nicht für unzulässige andere Zwecke verwendet oder an Dritte weiterleitet. Dies ist u. a. auch deshalb relevant, weil Polizei und Nachrichtendienste in vielen EU-Staaten institutionell nicht klar getrennt sind. Die Weiterleitung von Informationen aus der Strafverfolgung an die Nachrichtendienste muss die absolute Ausnahme bleiben, was durch hohe inhaltliche Anforderungen zu sichern ist.
- Für die Datensicherheit, den Datenschutz und für die Qualitätssicherung der polizeilichen Datenbestände ist es m. E. unerlässlich, dass bei übermittelten Daten jederzeit nachvollziehbar bleibt, aus welcher Quelle sie stammen. Dies erfordert eine entsprechende Kennzeichnung der betreffenden Datensätze. Nur so können z. B. Fehler korrigiert und neue Erkenntnisse nachträglich zur Aktualisierung eines Datensatzes genutzt werden. Übermittelte Daten sollten von der übermittelnden und von der empfangenden Stelle nach einheitlichen Standards so *gekennzeichnet* werden, dass die Herkunft und die Zweckbestimmung für beide Seiten jederzeit erkennbar bleibt. Hier sollte auch klargestellt werden, dass die empfangende Stelle die übermittelnde und damit verantwortliche Stelle zu informieren hat, wenn Fehler in den übermittelten Daten vermutet oder gefunden werden oder neue Erkenntnisse eine Aktualisierung des Datensatzes erforderlich machen.

Die Art. 9 bis 12 des Datenschutz-Rahmenbeschlusses 2008/977/JI enthalten hierfür (verbesserungsbedürftige) Regelungsansätze, die in weiterentwickelter Form in die Richtlinie übernommen werden sollten.

Empfehlung B 1: *Ich empfehle dem Deutschen Bundestag, sich dafür einzusetzen, dass in die Richtlinie klare Regelungen für die Übermittlung von Daten auch innerhalb der EU aufgenommen werden, damit ein hohes Datenschutzniveau und eine hohe Datenqualität gesichert werden, insbesondere durch Mindeststandards für Empfängerpflichten und Präzisierungen zur Zweckbindung und zur Kennzeichnung übermittelter Daten.*

II. Unzulängliche Regelungen für die Datenübermittlung an Drittstaaten und internationale Organisationen streichen bzw. nachbessern

Die Regelungen zur Datenübermittlung an Drittstaaten und internationale Organisationen sind nicht nur wegen der (zu) starken Rolle problematisch, die sich die Europäische Kommission hier zugedacht hat. Auch inhaltlich sind diese Regelungen verbesserungsbedürftig. Die Bewertungskriterien für ein hohes Datenschutzniveau sollten präzisiert werden (hierzu auch oben, A IV).

Besonders problematisch ist die Ausnahmeklausel in Art. 36 des Entwurfs, die eine Übermittlung sogar ohne Feststellung eines angemessenen Datenschutzniveaus beim Empfänger zulässt. Insbesondere die unter Art. 36 b) und c) aufgeführten Varianten sind so weit gefasst, dass ein negatives Votum der Kommission bezüglich des Datenschutzniveaus beim Empfänger praktisch belanglos würde, da die Datenübermittlung aufgrund der Ausnahmeklausel dennoch erfolgen könnte.[5]

Empfehlung B 2: *Ich empfehle dem Deutschen Bundestag, sich dafür einzusetzen, dass die Ausnahmeklausel in Art. 36 des Richtlinienentwurfs gestrichen, zumindest aber wesentlich enger und präziser formuliert wird.*

[5] Kritisch hierzu auch M. Bäcker/G. Hornung, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa. Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht, in: ZD 2012, S. 147-152 (151).

III. Rechtsfolgen für die Bildung unterschiedlicher Betroffenenkategorien definieren

Art. 5 des Richtlinienentwurfs schreibt den Mitgliedstaaten vor, zwischen verschiedenen Kategorien von betroffenen Personen zu unterscheiden, die von verurteilten Straftätern und Tatverdächtigen bis zu Opfern und möglichen Zeugen reichen. Diese Differenzierung ist sinnvoll und in Vorschriften des deutschen Strafprozess- und Polizeirechts Standard. Die Richtlinie enthält indes keine näheren Ausführungen dazu, welche Konsequenzen die Zuordnung zu einer dieser Kategorien haben soll. Hier sollten Mindeststandards formuliert werden, die deutlich machen, dass die Zuordnung zu diesen Kategorien zu unterschiedlichen Verarbeitungsregeln führt – mit stärkeren Restriktionen u. a. für die Datenspeicherung und -übermittlung, wenn Zeugen, Opfer oder unbeteiligte Dritte betroffen sind. Der Europäische Datenschutzbeauftragte hat zudem die sinnvolle Forderung erhoben, dass die Kategorisierung für die Mitgliedstaaten bindend sein sollte. Die einleitende Formulierung „so weit wie möglich“ sollte daher gestrichen werden.[6]

Empfehlung B 3: *Ich empfehle dem Deutschen Bundestag, sich dafür einzusetzen, dass die Vorschrift über die Bildung unterschiedlicher Personenkategorien durch Mindestanforderungen an die Rechtsfolgen der Kategorisierung ergänzt wird.*

C) Gesamtfazit

Diese Stellungnahme enthält insbesondere Hinweise auf Schwachstellen des vorliegenden Richtlinienentwurfs, die der Nachbesserung bedürfen. Nur wenn es gelingt, die Qualität des Entwurfs wesentlich zu verbessern, kann eine solche Richtlinie zu einem hohen Datenschutzniveau bei den Strafverfolgungsbehörden in der EU und bei ihrer Zusammenarbeit beitragen.

gez. Prof. Dr. Hartmut Aden

[6] Hustinx/Europäischer Datenschutzbeauftragter 2012, a. a. O., Rn. 352 f.