Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

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

An den
Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn Wolfgang Bosbach, MdB

nur per E-Mail

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL Ref7@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 27.03.2012

nachrichtlich:

Vorsitzenden des Rechtsausschusses
Herrn Siegfried Kauder, MdB

Vorsitzenden des Ausschusses
für die Angelegenheiten der Europäischen Union
Herrn Gunther Krichbaum, MdB

Vorsitzenden des Ausschusses für Wirtschaft und Technologie
Herrn Ernst Hinsken, MdB

Vorsitzenden des Ausschusses
für Ernährung, Landwirtschaft und Verbraucherschutz
Herrn Hans-Michael Goldmann, MdB

Vorsitzende des Ausschusses für Kultur und Medien
Frau Monika Grütters, MdB

BETREFF **70. Sitzung des Innenausschusses am 28. März 2012, TOP 6a und 6b**

Sehr geehrter Herr Bosbach,

im Hinblick auf den Ablauf der Subsidiaritätsfrist für die Kommissionsentwürfe einer EU-Grundverordnung zum Datenschutz und einer Richtlinie zur Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden (TOP 6a und 6b der 70. Sit-

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

zung des Innenausschusses) wäre ich Ihnen für die Einbeziehung der folgenden Anmerkungen in die Beratungen des Innenausschusses dankbar.

Seit vielen Jahren wird die Modernisierung des Datenschutzrechts sowohl auf nationaler als auch auf europäischer Ebene gefordert. Entsprechende Bemühungen zur Modernisierung des deutschen Datenschutzrechts sind bislang erfolglos geblieben. Deshalb sehe ich es als große Chance für den Datenschutz, dass die EU-Kommission mit dem vorgelegten Datenschutzpaket (bestehend aus einer Datenschutzgrundverordnung für den Binnenmarkt und einer Richtlinie für Polizei und Justiz) endlich die Weichen für ein modernes Datenschutzrecht stellen will.

Eine von einer ausreichenden Zahl von Parlamenten der Mitgliedstaaten unterstützte Subsidiaritätsrüge hätte zur Folge, dass das europäische Gesetzgebungsverfahren nur fortgesetzt werden kann, wenn EP und Rat diese Rüge zurückgewiesen haben. Sollte der entsprechende Schwellenwert für die Subsidiaritätsrüge erreicht werden, wäre damit zumindest eine erhebliche Verzögerung verbunden. Allerdings geht von dem Antrag der Subsidiaritätsrüge auch bei Verfehlen des Schwellenwerts eine nachhaltige negative Botschaft gegenüber den europäischen Institutionen aus, die aus meiner Sicht vermieden werden sollte, zumal – wie ich im Folgenden aufzeigen werde – aus meiner Sicht die Argumente für das Vorliegen einer Verletzung des Prinzips der Subsidiarität nicht durchschlagen.

Ich halte es für dringend erforderlich, dass Deutschland in den weiteren Beratungen auf eine Verbesserung der vorgeschlagenen Regelungen hinwirkt und plädiere deshalb für einen konstruktiven und proaktiven Ansatz, der die Kommission in ihrem Anliegen unterstützt und zugleich für Verbesserungen im Sinne eines effektiven und modernen Datenschutzrechts eintritt. Die von dem Antrag ausgehende fundamental ablehnende Signalwirkung würde eine derartige konstruktive Linie praktisch unmöglich machen.

Im Mittelpunkt sollte deshalb stehen, das Vorhaben der Kommission konstruktiv zu begleiten und dabei die ohne Zweifel bestehenden Defizite und Schwächen der Vorschläge zu beheben. Eine detaillierte Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder werde ich Ihnen nach deren Realisierung zeitnah zusenden.

1. Datenschutzgrundverordnung

Der Vorschlag der Datenschutzgrundverordnung ist auf Art. 16 AEUV gestützt, der neuen durch den Vertrag von Lissabon eingeführten Rechtsgrundlage für den Erlass von Datenschutzvorschriften. Die Kommission vertritt die Auffassung, dass die Union

den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten regeln kann, wenn die Verarbeitung im Rahmen der Ausübung von Tätigkeiten erfolgt, die in den Anwendungsbereich des Unionsrechts fallen. Vorschriften für den freien Verkehr personenbezogener Daten – auch solche, die von den Mitgliedstaaten oder von nicht-öffentlichen Stellen verarbeitet werden – können auf dieser Grundlage erlassen werden. Insofern tritt die Datenschutzgrundverordnung an die Stelle der bisherigen Datenschutzrichtlinie 1995/46.

Soweit sich die Subsidiaritätsbedenken auf das Regelungsinstrument einer Verordnung an Stelle einer Richtlinie beziehen, ist folgendes zu anzumerken:
Die Verordnung ist nur dann als unverhältnismäßig anzusehen, wenn sich das mit dem Rechtsakt verfolgte Ziel auch mit einem weniger intensiv in die Souveränität der Mitgliedstaaten eingreifenden Instrument erreichen ließe.

Zwar teile ich die Auffassung, dass aus datenschutzrechtlicher Sicht eine Richtlinie den Vorteil hätte, dass über den europäischen Mindeststandard hinausgehende nationale Datenschutzregelungen getroffen werden könnten. Durch die Verordnung werden auch Fragen aufgeworfen wie beispielsweise die, nach der Weitergeltung der aufgrund der Bundesverfassungsgerichtsentscheidung zum Volkszählungsgesetz (BVerfGE 1/65) entstandenen zahlreichen bereichsspezifischen Regelungen zum Datenschutz in deutschen Gesetzen. Zudem stellt sich die Frage nach der Reichweite einer Verordnung, wenn z. B. Art. 6 Abs.1 Nr. f in Verbindung mit Art. 6 Abs. 5 des Verordnungsentwurfs der Kommission erlaubt, „berechtigte Interessen“ für bestimmte Verarbeitungszwecke zu definieren und dabei eine Änderung des materiellen Anwendungsbereichs der Verordnung ermöglichen könnte.

Diese Fragen sind unzweifelhaft im weiteren Rechtsetzungsverfahren zu bereinigen. Dennoch halte ich die gegen die Verordnung gerichteten Subsidiaritätsbedenken nicht für durchschlagend. Denn auch für eine Verordnung sprechen wichtige Argumente. Mit ihrer unmittelbaren Anwendbarkeit nach Art. 288 AEUV trägt sie zur Rechtsvereinheitlichung bei und erhöht die Rechtssicherheit durch die Einführung harmonisierter Kernbestimmungen und durch einen besseren Grundrechtsschutz. Auf diese Weise sorgt sie gleichzeitig für einen besser funktionierenden Binnenmarkt.

Nach dem Subsidiaritätsprinzip (Art. 5 Absatz 3 EUV) wird die Union nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind.
In ihrer Subsidiaritätsanalyse führt die Kommission aus, dass aus folgenden Gründen Maßnahmen auf EU-Ebene notwendig sind:

- Das Recht auf Schutz personenbezogener Daten, das in Art. 8 der Grundrechtecharta verankert ist, verlangt ein unionsweit einheitliches Datenschutzniveau. Ohne gemeinsame EU-Vorschriften bestünde die Gefahr, dass der Datenschutz in den Mitgliedstaaten nicht in gleichem Maße gewährleistet ist, was den grenzüberschreitenden Verkehr personenbezogener Daten zwischen Mitgliedstaaten mit unterschiedlichen Datenschutzanforderungen behindern würde.
- Der Transfer personenbezogener Daten sowohl in andere EU-Staaten als auch in Drittstaaten nimmt rasant zu. Die praktischen Schwierigkeiten bei der Durchsetzung der Datenschutzvorschriften und die hierzu notwendige Zusammenarbeit zwischen den Mitgliedstaaten und ihren Behörden erfordern eine Organisation auf EU-Ebene, um die einheitliche Anwendung des Unionsrechts zu gewährleisten. Die EU ist auch die geeignete Ebene, um sicherzustellen, dass alle Betroffenen bei der Übermittlung personenbezogener Daten in Drittländer effektiv in gleichem Maße geschützt sind.
- Die Mitgliedstaaten können die derzeitigen Probleme – vor allem die durch die Uneinheitlichkeit der nationalen Vorschriften bedingten Probleme – nicht allein überwinden. Es besteht daher ein besonderer Bedarf an einer harmonisierten, kohärenten Regelung, die einen reibungslosen Transfer personenbezogener Daten innerhalb der EU ermöglicht und gleichzeitig EU-weit allen Betroffenen einen wirksamen Datenschutz garantiert.
- Wegen Art und Umfang der Probleme, die nicht auf einen oder mehrere Mitgliedstaaten beschränkt sind, werden die vorgeschlagenen Legislativmaßnahmen der EU eine größere Wirkung entfalten als vergleichbare Maßnahmen auf Ebene der Mitgliedstaaten.

Nach dem Verhältnismäßigkeitsprinzip muss jedes Handeln zielgerichtet sein und darf nicht über das hinausgehen, was für die Erreichung der angestrebten Ziele notwendig ist. An diesem Grundsatz hat sich die Kommission bei Ausarbeitung dieses Vorschlags von der Feststellung und Analyse der möglichen Optionen bis hin zu ihren Formulierung orientiert.

Die referierten Feststellungen der KOM betreffend die Einhaltung des Subsidiaritätsprinzips sind zwar recht pauschal, treffen aber im Grundsatz zu. Kritisch zu sehen ist die Verlagerung zahlreicher Kompetenzen auf die EU-Ebene im Wege der Delegation und Komitologie (Ermächtigung zum Erlass sekundärer Rechtsakte) sowie die KOM-Befugnisse in Bezug auf einzelbehördliche Maßnahmen im Konsistenzverfahren, insb. gem. Art. 60, 62 (1) a), (2) der Grundverordnung.

2. Datenschutz-Richtlinie für Polizei und Justiz

Die Kommission beruft sich auch hinsichtlich der JI- Richtlinie auf Art. 16 AEUV – der neuen durch den Vertrag von Lissabon eingeführten Rechtsgrundlage für den Erlass von Datenschutzvorschriften, die auch für die polizeiliche und justizielle Zusammenarbeit in Strafsachen gelte. Zudem weist die Kommission darauf hin, dass der Schutz personenbezogener Daten in Art. 8 der EU-Grundrechtecharta als Grundrecht ausgestaltet ist. Die Kompetenz zur Rechtsetzung beschränke sich zudem nicht auf die übermittelten Daten, sondern umfasse auch die innerstaatliche Datenverarbeitung. Nach meiner Auffassung sprechen gute Gründe dafür, auch in diesem Bereich eine Rechtsetzungskompetenz für die Union anzunehmen.

Im Hinblick auf die besondere Grundrechtsrelevanz der Datenverarbeitung durch Polizei und Justiz sehe ich es als besonders bedeutsam an, dass hier keine Abstriche an den durch nationales Recht (insbesondere die Rechtsprechung des Bundesverfassungsgerichts, etwa zum informationellen Selbstbestimmungsrecht, zum unantastbaren Kernbereich privater Lebensgestaltung und zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) bestehenden Vorgaben vorgenommen werden. Vor diesem Hintergrund halte ich das vorgesehene Regelungsinstrument einer Richtlinie für diesen Bereich für geeignet. Allerdings muss bei der Ausformulierung der Vorschriften gewährleistet werden, dass hier – anders als beim nicht-öffentlichen Bereich – keine volle Harmonisierung im Sinne einer "Deckelung" der grundrechtssichernden Maßnahmen stattfindet.

Ich halte eine Richtlinie für den Datenschutz in der polizeilichen und justiziellen Datenverarbeitung auch für erforderlich. Der gegenwärtige Rechtszustand ist unbefriedigend, denn die bisherige allgemeine Datenschutzrichtlinie ist - wie auch die vorgesehene Datenschutzgrundverordnung – für den JI-Bereich nicht anwendbar. Der Rahmenbeschluss für die ehemalige dritte Säule (2008/977/JI vom 27. November 2008; ABl. L 350 vom 30.12.2008, S. 60) umfasst nicht die innerstaatliche Datenverarbeitung. Die Bundesregierung hatte sich mit der von ihr befürworteten Erstreckung der Datenschutzvorgaben auf die innerstaatliche Datenverarbeitung seinerzeit nicht im Rat durchsetzen können.

Auch wenn die Richtlinie im Grundsatz als geeignetes Instrument für die Schaffung eines EU-weit möglichst hohen, gemeinsamen Mindeststandards für die Datenverarbeitung von Polizei und Justiz erscheint, ist doch zu konzedieren, dass der Richtlinienentwurf in wichtigen Punkten unzureichend ist und sogar deutlich hinter dem durch die Verordnung angestrebten Schutzniveau zurückbleibt.

So halte ich es für erforderlich, den Schutz unverdächtiger Bürger – etwa vor Vorratsdatenspeicherung – ausdrücklich zu regeln. Dies gilt insbesondere im Hinblick auf spezifische Garantien zum Schutze von Personen, deren Daten als Opfer, Zeuge oder sonstige Person gespeichert werden dürfen. Ebenso fehlen Bestimmungen zu Löschungs- und Aussonderungsprüffristen und für den innereuropäischen Datenaustausch. Insbesondere muss sichergestellt werden, dass nationale Verwendungsbeschränkungen – etwa für Daten aus TKÜ-Maßnahmen – oder Löschungsfristen auch von den anderen Mitgliedstaaten zu beachten sind. Schließlich sollte ein europaweit einheitlicher Mindeststandard für das Auskunftsrecht der Betroffenen und für dessen Einschränkungen gelten.

Kritisch sehe ich auch, dass europäische Institutionen – etwa Europol und Eurojust – gänzlich von dem Geltungsbereich des Richtlinienentwurfs ausgenommen werden. Es liegt in der Logik des von der Union seit langem verfolgten Ziels der Schaffung eines gemeinsamen Raums der Sicherheit, des Rechts und der Freiheit, auch die europäischen Institutionen in den geplanten Rechtsrahmen einzubeziehen.

Mit freundlichen Grüßen