Anlage zum Schreiben des Herrn Ministers an GRC- und ITA-Vorsitz

Vorschlag für eine Roadmap zur Beschleunigung der Verhandlungen über die EU-Datenschutzreform

1. Rechtsform und höhere Datenschutzstandards im öffentlichen Bereich

Über die Frage der Rechtsnatur der Datenschutz-Grundverordnung besteht bislang im Rat keine Einigkeit. Zentrales Anliegen einer Reihe von Mitgliedstaaten ist es, das spezifische und zum Teil über das Schutzniveau der Datenschutz-Grundverordnung hinaus gehende Datenschutzrecht für die Verwaltungen der Mitgliedstaaten zu erhalten. Ebenso soll die Möglichkeit erhalten bleiben, höhere Schutzstandards gegenüber spezifischen Gefährdungen durch bestimmte Behörden, Dateien und öffentliche Register schaffen zu können. Für Deutschland ist dies ein sehr wichtiges Anliegen.

In diesem Zusammenhang wurde die Frage diskutiert, ob nicht eine Richtlinie für den Bereich der Verwaltung die geeignetere Rechtsform wäre. Die bisher vorgesehenen Öffnungsklauseln haben offenbar noch nicht für eine hinreichende Einigung sorgen können.

Um in diesem Punkt substantiell voranzukommen und Klarheit in Bezug auf die vielen sich im Zusammenhang mit dem öffentlichen Bereich stellenden Fragen zu schaffen, schlage ich als weitergehenden Kompromiss eine Öffnungsklausel in Art. 1 oder Art. 2 der Datenschutz-Grundverordnung vor, die es den Mitgliedstaaten im öffentlichen Bereich erlauben würde, bei Bedarf über die Bestimmungen der Datenschutz-Grundverordnung hinauszugehen und strengere nationale Datenschutzbestimmungen zu erlassen (etwa bei den Betroffenenrechten, Maßnahmen der Datensicherheit oder bei Protokollierungen). Die gleiche Problematik stellt sich aus Sicht Deutschlands in Bezug auf den Beschäftigtendatenschutz. Die Formulierung für eine solche Öffnungsklausel könnte lauten:

> *„Diese Verordnung hindert die Mitgliedstaaten nicht, in ihrem Recht ein höheres Schutzniveau bei der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen in Ausübung ihrer hoheitlichen Befugnisse sowie im Bereich des Beschäftigtendatenschutzes vorzusehen.“*

2. Konkretisierung der Voraussetzungen der Einwilligung

Die Einwilligung in die Datenverarbeitung ist eines der zentralen Elemente des Datenschutzrechts. Ziel der Einwilligung ist es, dass der Betroffene selbstbestimmt ent-

scheiden kann, welche Informationen sie über sich preisgeben möchten. Wir möchten die Einwilligung als Rechtsgrundlage für eine Datenverarbeitung und als besondere Ausprägung des Rechts auf Privatheit weiter stärken. Eine Einwilligung sollte ausdrücklich, freiwillig und nach vorheriger Information über wesentliche Punkte der Datenverarbeitung erfolgen, damit sie nicht bloße Legitimationsfiktion ist. Nötig ist eine Konkretisierung dieser Voraussetzungen der Einwilligung für bestimmte Situationen, damit durch die Einwilligung Verantwortung nicht in unfairer Weise auf den Betroffenen verlagert wird. Zweifel an der Freiwilligkeit bestehen z.B. bei einem erheblichen Ungleichgewicht zwischen Betroffenem und datenverarbeitender Stelle oder wenn der Betroffene auf eine Leistung der datenverarbeitenden Stelle angewiesen ist.

3. „One Stop Shop“

Die Beratungen der JI-Räte im Oktober und Dezember 2013 sowie zuletzt am 6. Juni 2014 haben die Bedeutung eines sogenannten „One Stop Shops“ im Interesse der Unternehmen betont, gleichzeitig jedoch deutlich gemacht, dass die Bürgernähe der Datenschutzaufsicht gewährleistet sein muss. Der Juristische Dienst des Rates hat in seinem Gutachten vom 19. Dezember 2013 die Auffassung vertreten, dass ein „One Stop Shop“-Modell, das Zuständigkeiten und Befugnisse bei einer einzigen Aufsichtsbehörde konzentriert, und damit zur Folge hat, dass sich ein Betroffener regelmäßig an die Aufsichtsbehörde und das Gericht eines anderen Mitgliedstaats wenden muss, nicht mit den Grundrechten der Europäischen Union vereinbar ist. Deutschland hat aus diesem Grunde ein alternatives „One Stop Shop“-Verfahren vorgeschlagen, das die lokalen Aufsichtsbehörden stärkt und die notwendige Bürgernähe sicherstellt. Die Beratungen des JI-Rates am 6. Juni 2014 haben gezeigt, dass der deutsche Vorschlag eine gute Basis ist, um den Bedenken des Juristischen Dienstes Rechnung zu tragen. Auch angesichts der deutlichen Unterstützung aus dem Kreis der Mitgliedstaaten, insbesondere Frankreichs, möchte ich noch einmal für diesen Vorschlag werben und gleichzeitig deutlich machen, dass Deutschland nur eine Lösung mittragen könnte, die die grundrechtlichen Argumente des Juristischen Dienstes des Rates beachtet.

4. Drittstaatenübermittlungen

Das Kapitel über Drittstaatenübermittlungen ist in einer global vernetzten Welt in mehrfacher Hinsicht von herausragender Bedeutung. Ich freue mich, dass wir hierzu im JI-Rat am 6. Juni 2014 wichtige Fortschritte erzielen konnten. Drei Punkte müssen indessen bei den weiteren Verhandlungen rasch geklärt werden:

- Erstens müssen die Regelungen einen effektiven Schutz der Betroffenen bieten. Dies gilt insbesondere für die Datenherausgabe von Unternehmen an Behörden in Drittstaaten. Deutschland hat deshalb einen Vorschlag für einen Art. 42a eingebracht, der mir nach dem gegenwärtigen Beratungsstand des Kapitels V aus deutscher Sicht unverzichtbar erscheint. Mit einer Protokollnotiz haben wir dieses Anliegen im Rat noch einmal in Erinnerung gerufen.

- Zweitens brauchen wir in der Verordnung selbst einen stabilen Rechtsrahmen für Instrumente wie Safe Harbor. Der Handlungsbedarf bei Safe Harbor wurde bereits durch die Evaluierung der Kommission aufgezeigt. Die Empfehlungen der Kommission zur Verbesserung von Safe Harbor (Verbesserung von Transparenz, Rechtsschutz und Durchsetzung) sollten rasch umgesetzt werden und eine „Safe Harbor"-Regelung auf dieser verbesserten Basis als Grundlage für Vereinbarungen von Unternehmen in entsprechenden Drittstaaten in der Verordnung verankert werden.

- Drittens dürfen die Regelungen zu Drittstaatenübermittlungen nicht dazu führen, dass Internetveröffentlichungen praktisch unmöglich gemacht werden. Der Europäische Gerichtshof hatte in seiner „Lindqvist"-Entscheidung unter anderem die Frage zu beantworten, ob die Regelungen zu Drittstaatenübermittlungen auf Internetveröffentlichungen anwendbar sind. Da die Homepage von Frau Lindqvist, auf der sie vor allem Informationen für ihre Konfirmandenschüler zur Verfügung stellte, praktisch aus jedem Land der Welt abgerufen werden kann, hätte eine Anwendung der Drittstaatenregelungen dazu geführt, dass Internetveröffentlichungen regelmäßig zu unzulässigen Transfers in Drittstaaten auch ohne angemessenes Datenschutzniveau führen und damit zu untersagen wären. Diese Konsequenz hat der Europäische Gerichtshof im Kern mit der Begründung abgelehnt, dass dies nicht gewollt sein könne. Auch der Gesetzgeber der Datenschutzrichtlinie 95/46 habe dies nicht gewollt. Entsprechende Internetsachverhalte habe er seinerzeit noch nicht vor Augen haben können. Aufgrund der Struktur des Internets, nach der eingestellte Daten weltweit abrufbar sind, würde die Sonderregel für Drittstaatenübermittlungen sonst zu einer allgemeinen Regel für die Datenübermittlung im Internet. Dies könne zu einer erheblichen, wenn nicht gar umfassenden Einschränkung von Internetveröffentlichungen führen, was auch eine massive Einschränkung der Meinungsfreiheit zur Folge hätte. Bei der Beurteilung, ob eine Drittstaatenübermittlung vorliegt, stellt sich schon die Frage nach dem Anknüpfungspunkt. Stellt man auf den Standort des E-Mail-Providers ab, bedeutet dies, dass E-Mail-Provider, die keine Niederlassung in einem Mitgliedstaat ha-

ben, nur unter den zusätzlichen Voraussetzungen der Drittstaatenregelungen genutzt werden dürfen.

5. Big Data und Profiling

Wir sollten darüber hinaus die Internettauglichkeit der Regelungen der Datenschutz-Grundverordnung in Bezug auf Cloud Computing, soziale Netzwerke, Wearables oder Internet der Dinge noch weiter verbessern. Hinter dem Stichwort Big Data verbergen sich Datenverarbeitungen, die enorme gesellschaftliche Chancen (z.B. in den Bereichen Gesundheit, Bildung und Umweltschutz) bieten. Ein wichtiger Anwendungsfall von Big Data ist die Erstellung von personenbezogenen Profilen. Profile werden aber nicht nur über Big Data-Anwendungen erstellt, sondern auch durch die Auswertung von Daten, die ein einzelner Diensteanbieter über seine Nutzer sammelt. Große Datenmengen erlauben es, z.B. personenbezogene Profile und individuelle „Scorewerte“ zu erstellen und Wahrscheinlichkeitsaussagen über das Verhalten einer Person zu treffen. Profilbildungen werden mittlerweile auch mit nicht personenbezogenen Daten und mit von den Betroffenen selbst veröffentlichten personenbezogenen Daten vorgenommen. Informationspflichten und Einwilligungserfordernisse können diese Gefahren mindern. Sie stoßen jedoch an Grenzen, wenn die Information der Betroffenen erst deren Identifizierung verlangt, wodurch ein zusätzliches Datenschutzproblem entsteht. Auch wegen der Masse der Daten und der Vielzahl der Betroffenen werden deshalb weltweit in Wissenschaft und Praxis Ideen für zusätzliche Schutzmechanismen entwickelt. Ich trete daher dafür ein bewährte Instrumente wie die Einwilligung zu stärken und erforderlichenfalls zusätzliche Schutzmechanismen vorzusehen. Darüber hinaus müssen den Betroffenen effektive Auskunftsansprüche zur Verfügung stehen, um Entscheidungen, die - wie etwa eine Bewertung der Kreditwürdigkeit - auf Profilen beruhen, nachvollziehen zu können.

6. Meinungs- und Informationsfreiheit

Im Hinblick auf das Urteil des Europäischen Gerichtshofs in der Rechtssache Google ./. Spanien (Az. C-131/12) sollten wir uns bei einem der kommenden Räte der Frage zuwenden, ob und gegebenenfalls welche Konsequenzen aus diesem Urteil für den Schutz der Privatsphäre unter Berücksichtigung auch der Auswirkungen auf die Meinungs-, Presse- und Informationsfreiheit zu ziehen sind. In der öffentlichen Diskussion geht es dabei vor allem um die Frage, wie sachgerechte Entscheidungen der Suchmaschinenbetreiber sichergestellt werden können, bei denen nicht nur der Schutz der Privatsphäre gesichert, sondern auch der Meinungsfreiheit angemessen Rechnung getragen werden kann. Im Raum stehen Forderungen nach unabhängigen

Schiedsstellen, zu deren Einrichtung und Verfahren sehr unterschiedliche Lösungen denkbar sind.