GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Goethe-Universität Frankfurt am Main
Forschungsstelle für Datenschutz • Center for Data protection

Rechtswissenschaft • School of Law

Forschungsstelle für Datenschutz •
Research Center for Data Protection

Prof. Dr. Dres. h. c. Spiros Simitis

Telefon +49 (0)69 798 34230
Telefax +49 (0)69 798 34534
E-Mail a.arendt@jur.uni-frankfurt.de

www.uni-frankfurt.de

Frankfurt, den 4. Okt. 2012

Stellungnahme

zum Vorschlag der

Europäischen Kommission für eine *„Datenschutz-Grundverordnung"* vom 27. Januar 2012

für die

Anhörung des Innenausschusses des Deutschen Bundestages vom 22. Oktober 2012

Datenschutzgesetze sind seit ihren Anfängen in den siebziger Jahren des vergangenen Jahrhunderts immer unter dem Eindruck der Informationstechnologie entstanden. Nationale und supranationale Vorschriften müssen sich deshalb an ihrem jeweiligen Stand orientieren und dessen spezifischen Folgen für den Umgang mit personenbezogenen Angaben gezielt Rechnung tragen. Die von der Europäischen Kommission im Januar diesen Jahres vorgeschlagene „Datenschutz-Grundverordnung" markiert so gesehen den Wandel und strebt eine ihm angepasste Regelung. Unter genau diesem Gesichtspunkt gilt es, sich die einzelnen Regelungsvorgaben ebenso wie das Regelungskonzept anzusehen, auf das sich die nachfolgenden fünf Punkte vorwiegend beziehen.

1. Gleichviel wie die Revision des geltenden Rechts letztlich ausfallen mag, die radikale Veränderung des Regelungsprozesses sowie deren Auswirkungen sind von Anfang an zu bedenken

und dürfen keinesfalls unterschätzt werden. Die Europäische Kommission hat mit ihrer Vorlage ihren Kompetenzanspruch nicht nur bestätigt, sondern weitaus nachdrücklicher wahrgenommen. Sie hat zwar bereits mit der Datenschutzrichtlinie von 1995 nachhaltig in die Verwendung personenbezogener Angaben eingegriffen, doch der Vergleich verbietet sich. Wohl wurde damals wie heute eindringlich auf die zwingend erforderliche Harmonisierung der Verwendungsbedingungen hingewiesen, aber vor einem grundverschiedenen Hintergrund.

Die Richtlinie sollte ihrer ganzen Geschichte und Konzeption nach zuvörderst vorhandene Differenzen der gesetzlichen Anforderungen in den Mitgliedsstaaten möglichst eliminieren und gemeinsame Vorgaben angesichts der bereits existierenden Vorschriften realisieren. Die angestrebte Verordnung spiegelt dagegen in erster Linie Kommissionsvorstellungen wider, die auf der Grundlage der bisherigen nationalen und supranationalen Erfahrungen sowie einer Vielzahl bereichsspezifischer Kommissions-Vorgaben entstanden sind und von den Mitgliedsstaaten uneingeschränkt und unverändert übernommen werden müssen. Präziser ausgedrückt: Die Verordnung statuiert Grundbedingungen jeder Verarbeitung, die ebenso unionsweit wie alternativlos zu beachten sind.

Den Mitgliedsstaaten bleibt unter diesen Unständen nur eine Einfluss- und Gestaltungsmöglichkeit: Sie müssen sich intensiver denn je in den Entstehungsprozess der Datenschutzbestimmungen einschalten. Anders als bisher bietet ihnen die Einordnung in ihr eigenes Recht nicht mehr die Chance, die Kommissionsvorgaben möglichst ihren Vorstellungen anzupassen. Verordnungen dulden keine noch so verkappte Alternative. Infolgedessen ist das Vorstadium der jeweiligen Vorschriften wichtiger denn je. Gleichviel ob es um die Ankündigung oder erste Vorschläge einer Verordnung geht, beides muss mindestens genauso gründlich und kritisch analysiert und bewertet werden wie es gegenwärtig zumeist im Kontext der Umsetzung geschieht.

2. Der Wechsel von der bislang üblichen Verwendung von Richtlinien für die Regelung der Verarbeitung personenbezogener Daten zur Verordnung legt zwar den Akzent sehr viel deutlicher als zuvor auf die Erwartungen der Europäischen Kommission, bewegt sich aber durchaus im Rahmen der ihr zustehenden Regelungsmöglichkeiten. Die gezielte Monopolisierung der Entscheidung verpflichtet freilich erst recht dazu, Vorschriften zu verabschieden, die klar und verständlich formulieren, welchen Anforderungen die Verwendung personenbezogener Daten genügen muss, und dabei vor allem ein Ziel verfolgen: eine ebenso nachvollziehbare wie abschließende Regelung, die ihren Anwendungsspielraum verbindlich definiert und damit die Interpretationsmarge maximal minimiert. Genau dies ist bislang nicht erreicht. Zwei Beispiele:

Sicherlich kann man, wie schon die Datenschutz-Richtlinie von 1995 (Art. 8) und ganz in der Tradition des französischen Rechts, „besondere Kategorien der Verarbeitung" vorsehen (Art. 9), also etwa für Daten zur rassischen oder ethischen Herkunft, zu politischen Meinungen, zur

Gesundheit oder zum Sexualleben, und ihnen mit Rücksicht auf ihre „Sensitivität" einen eigenen „wesensbedingten" Status einräumen. Dann aber geht es nicht, auf die explizite Bestätigung der Notwendigkeit einer Sonderbehandlung in Art. 9 Abs. 1 der Verordnung zehn Ausnahmen folgen zu lassen und überdies in einem dritten Absatz die Kommission zu ermächtigen, in „delegierten Rechtsakten" die Modalitäten der Verarbeitung sowie die Tragweite der Ausnahmen näher zu bestimmen. Welche Bedeutung dem Sonderstatus wirklich zukommt, bleibt so gesehen nebulös. Mehr noch, die Europäische Kommission behält sich vor, Funktion und Auswirkungen einer durchaus zentralen Vorschrift zu einem Zeitpunkt festzulegen, zu dem sie bereits angenommen wurde, statt sie in die Reflexion über ihre Verabschiedung einzubringen und sich dort auch damit auseinanderzusetzen.

Das andere Beispiel: Gleichviel, ob die Verordnung die Rechtmäßigkeit der Verarbeitung (Art. 6 Nr. 5), die Information der betroffenen Personen (Art. 14 Nrn. 7 und 8), Profiling-Maßnahmen (Art. 20 Nr. 5), Auftragsverarbeiter (Art. 26 Nr. 5), die Folgenabschätzung des Datenschutzes (Art. 31 Nr. 5), Aufgaben des Datenschutzbeauftragten (Art. 37 Nr. 2) oder die Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften (Art. 43 Nr. 3) anspricht, die Verweisung auf ein Dekret kehrt in jedem Fall wieder. Der Verordnungstext vermittelt mithin nur ein höchst unvollständiges Bild seiner Anwendungsanforderungen. Genaugenommen werden lediglich die für den Anwendungsbereich signifikanten Anknüpfungspunkte markiert. Ansonsten verlässt sich die Kommission auf eine Vielzahl von Dekreten, um ihre Regelungsintentionen effektiv zu konkretisieren. Ihre Handlungsmarge mag damit nachhaltig zunehmen. Entsprechend schwieriger ist es für die Mitgliedsstaaten, sich auf eine Verordnung einzustellen, deren Reichweite sie nicht korrekt einschätzen können.

3. Schon der verkürzte Titel „Datenschutz-Grundverordnung" gibt zu erkennen, dass die vorgeschlagenen Bestimmungen Teil eines Regelungssystems sind. Sie umschreiben die Grundprinzipien, bestätigen jedoch genauso, dass es dabei nicht bleiben kann. Anders als in der Frühzeit des Datenschutzes, richtet sich der Umgang mit personenbezogenen Angaben nicht mehr nach einem einzigen, bewusst allgemein gehaltenen Gesetz. Allgemeine Datenschutzgesetze sind längst nur Vorspiel und Begleitung einer ständig zunehmenden Anzahl bereichsspezifischer Vorschriften. Genau diese Erfahrung gilt auch für die Kommission. Ebenso steht aber fest: Grundsätze und ihre bereichsspezifischen Umsetzungen können nur solange einen durchweg konsequent datenschutzkonformen Verarbeitungsverlauf gewährleisten wie sie sorgfältig abgestimmt sind sowie in eine Gesamtregelung der Verwendung personenbezogener Daten eingebracht werden.

Die „Grundverordnung" reicht folglich, für sich genommen, nicht aus. Bereits zum gegenwärtigen Zeitpunkt muss sie in eine Übersicht eingeordnet werden, die schon bestehende ebenso wie geplante bereichsspezifische Regeln im Gesamtbereich der Kommission einbezieht. Nur so lässt sich

der Stellenwert der allgemeinen Normen richtig einschätzen, können Widersprüche offengelegt und auf beiden Ebenen, der allgemeinen wie der bereichsspezifischen, korrigiert werden. Spätestens dann macht sich freilich auch die Ursache bemerkbar, die eine ebenso konsistente wie generelle Kommissionsregelung bislang verhindert: die nach wie vor divergierende Regelungskompetenz.

Kaum verwunderlich, wenn daher fast parallel zum Verordnungsentwurf einheitliche europäische Standards sowie Zertifikate für einen zumal durch eine verschärfte Haftung der Anbieter verbesserten Schutz der in Datenwolken ausgelagerten Angaben vorgeschlagen wurden. Arbeitsbeziehungen, Standardvertragsklauseln sowie die elektronische Kommunikation sind weitere Beispiele interner, von den jeweils zuständigen Generaldirektionen, wenngleich mit wechselndem Erfolg, initiierter Kommissionsdebatten über Kernfragen des Datenschutzes. Unterschiedliche Zuständigkeiten mobilisieren eben auch unterschiedliche Interessen, die nicht ohne Folgen für die Datenschutzvorschriften bleiben.

Wenn deshalb die „Grundverordnung" ihrem Anspruch, ein solides Datenschutzfundament sicherzustellen, gerecht werden soll, ist es unerlässlich, allgemeine und spezifische Vorschriften als Elemente einer, von einheitlichen Grundsätzen bestimmten Regelung anzusehen - unabhängig davon wie verschieden die Kompetenz für eine bereichsspezifische Konkretisierung genau dieser Grundsätze sein mag. Gerade in Anbetracht der „Grundverordnung" darf der Zuständigkeitswechsel nicht das Einfallstor für ein verändertes Verständnis des Datenschutzes werden.

4. So deutlich die Europäische Kommission mit ihrem Vorschlag zur „Datenschutz-Grundverordnung" einen neuen Abschnitt ihrer Regelungspolitik einleitet, so wenig lässt sich daran zweifeln, dass weit mehr als die Intention auf dem Spiel steht, fortan anders und direkter in den Umgang mit personenbezogenen Daten einzugreifen. Der Zeitpunkt des Instrumentenwechsels ist weder zufällig noch gleichgültig. Maßgeblich ist einmal mehr die Informationstechnologie. Sie zwingt dazu, die Interventionsmodalitäten zu überprüfen sowie die ihnen angemessenen Verarbeitungsvorgaben zu wählen.

Ansatz- und Orientierungspunkt ist das Internet und die von ihm gebotenen Verwendungsmöglichkeiten personenbezogener Daten. Reflexionen zum Datenschutz sind so gesehen zunächst und vor allem Überlegungen zu den Implikationen des Internet. Sie stehen freilich immer wieder ganz im Zeichen einer ebenso missverständlichen wie irreführenden Prämisse: der schlichten Gleichsetzung von Internet und Meinungsfreiheit. So anschaulich sich der Einfluss des Internet auf den Kommunikationsprozess gestaltet, so wenig darf darüber verdrängt werden, dass das Internet nicht mehr und nicht weniger als ein rein technisches Instrument ist, welches sich allerdings für sehr verschiedene Zwecke mit sehr unterschiedlichen rechtlichen

Folgen benutzen lässt. Demgegenüber ist die Meinungsfreiheit lediglich ein Kriterium, das bei den Verwendungsbedingungen der im Internet verarbeiteten Daten bedacht werden muss und sich insofern auch auf den Einsatz des Internet auswirkt. Ob freilich Einschränkungen geboten oder irrelevant sind, entscheidet sich am jeweiligen Verarbeitungskontext. Inwieweit sich also die Meinungsfreiheit Verwendungsbarrieren tatsächlich widersetzt, kann erst in dessen Kenntnis und im Hinblick auf die konkret betroffenen Daten beurteilt werden.

Am Beispiel der Meinungsfreiheit zeigt sich jedoch ebenfalls: Allgemeine, auf das Internet bezogene Vorschriften genügen nicht. Bereichsspezifische Anforderungen muss es unverändert geben. Wirtschaftliche Aktivitäten, wie der mehr und mehr auf das Internet verlagerte Verkauf einzelner Produkte oder die systematische Verarbeitung personenbezogener Daten der unterschiedlichsten Provenienz, etwa für Werbezwecke, bestätigen die Dringlichkeit einer Einbeziehung der diversen Verwendungszusammenhänge. Wie vielfältig die dabei auftauchenden Fragen sind und wie nachhaltig sich die Zugriffsabsichten auf personenbezogene Angaben ausweiten, exemplifiziert etwa die Intention von Auskunfteien, individuelle Äußerungen im Internet auch und gerade zu rein persönlichen Angelegenheiten als Informationsquelle für die Kreditfähigkeit einzelner Personen zu nutzen.

5. Die Informations- und Kommunikationstechnologie hat nicht nur die Entscheidung ausgelöst, den Umgang mit personbezogenen Daten verbindlich zu regeln. Sie begründet vielmehr genauso die Verpflichtung, sich am jeweiligen Stand dieser Technologie auszurichten, kurzum, auf ihre Entwicklung nicht nur konstant, sondern auch rechtzeitig zu reagieren. Die Verabschiedung von Datenschutzvorschriften muss unter diesen Umständen stets mit der Einsicht in ihren provisorischen Charakter einhergehen. Revisionen nach mehr als zwei Jahrzehnten, wie beim Bundesdatenschutzgesetz, oder, wie bei der EG-Datenschutzrichtlinie von 1995, nach voraussichtlich achtzehn bis neunzehn Jahren sind infolgedessen, ungeachtet kleinerer zwischendurch vorgenommener Korrekturen, offenkundig kontraproduktiv.

Wohlweislich haben vor allem skandinavische Gesetzgeber die jeweiligen Datenschutzgesetze befristet. Offenbar löst aber schon die Vorstellung, sich in einem evident konfliktreichen Bereich auf einen offenen Regelungsprozess einzulassen, Widerstände aus, die letztlich dazu führen, von einer zeitlichen Begrenzung selbst in Fällen abzusehen, in denen zuvor, wie in Schweden, die Bereitschaft dazu durchaus bestanden hatte. Seit jedoch Datenschutz, national wie supranational verfassungsrechtlich garantiert ist, kann es keine Bedenken mehr geben. Die wie immer begründete Konservierung traditioneller Verhaltensformen darf nicht maßgeblich sein. Der Gesetzgeber muss vielmehr den spezifischen Merkmalen des Regelungsgegenstandes sowie den sich daraus zwingend ergebenden Konsequenzen Rechnung tragen.

Sowohl für die geplante europäische Verordnung als auch für die Gesetze der Mitgliedsstaaten gilt deshalb: eine klare Befristung ist unumgänglich. Die jeweilige Entscheidungsinstanz ist mithin gehalten, die beschlossenen Anforderungen andauernd zu kontrollieren sowie notwendige Korrekturen zeitgerecht vorzunehmen, gleichviel ob die einzelne Regelung, wie bei der Verordnung, jedenfalls in dieser Form, erstmalig erfolgt oder, wie bei schon bestehenden Gesetzen, zur Routine zählen muss. Wer diese Verpflichtung ignoriert oder verharmlost, nimmt, national wie supranational, wirkungslose Normen in Kauf.

(Prof. Dr. Dres. h.c. S. Simitis)