BUNDESKANZLERAMT ÖSTERREICH

WERNER FAYMANN
BUNDESKANZLER

An die
Präsidentin des Nationalrats
Mag[a] Barbara PRAMMER
Parlament
1017 Wien

XXIV. GP.-NR
9146 /AB
14. Nov. 2011

GZ: BKA-353.110/0151-I/4/2011

zu 9255 /J

Wien, am 14. November 2011

Sehr geehrte Frau Präsidentin!

Die Abgeordneten zum Nationalrat Zanger, Kolleginnen und Kollegen haben am 14. September 2011 unter der **Nr. 9255/J** an mich eine schriftliche parlamentarische Anfrage betreffend Datenschutzprobleme in der Microsoft-Cloud gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu den Fragen 1 bis 4:

- *Warum stehen die Heimatschutzgesetze der USA in Bezug auf den Austausch sensibler Kundendaten über dem Datenschutzabkommen USA – EU?*
- *Warum müssen gerade Daten europäischer Kunden, die in der Cloud gesammelt werden, offengelegt werden?*
- *Wo setzt der Schutzbereich des Datenschutzabkommens zwischen den USA und der EU an, wenn nicht bei sensiblen Kundendaten?*
- *Wie kann Ihr Ministerium garantieren, dass Kundendaten von US-Unternehmen mit der gebotenen Sorgfalt behandelt werden?*

Die Datenschutz-Richtlinie 95/46/EG verbietet es grundsätzlich, personenbezogene Daten aus Mitgliedstaaten der EU in Staaten zu übermitteln, die über kein dem Unionsrecht vergleichbares Datenschutzniveau verfügen. Die Europäische Kommission kann mittels eines festgelegten Verfahrens feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet und somit ein Datentransfer erlaubt ist. Diesfalls ergibt sich innerstaatlich, dass der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutzniveau keiner Genehmigungspflicht durch die Datenschutzkommission unterliegt.

Im Zusammenhang mit den USA wurde ein besonderes Verfahren entwickelt. US-Unternehmen können dem sogenannten „Safe Harbor" beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums (Federal Trade Commission – FTC) eintragen lassen. Damit verpflichten sich die Unternehmen öffentlich und unmissverständlich, die „Safe Harbor Principles" („Grundsätze des Sicheren Hafens") und die dazugehörenden – verbindlichen – „Frequently Asked Questions" (FAQ) einzuhalten. Laut Entscheidung der Kommission vom 26. Juli 2000 verfügen die in den USA tätigen, dem „Safe Harbor" beigetretenen Unternehmen über ein angemessenes Datenschutzniveau. Diese Liste ist online zugänglich (http://export.gov/safeharbor/).

Neben den oben dargestellten Möglichkeiten können auch völkerrechtliche Verträge zwischen den USA und – je nach kompetenzrechtlicher Zuständigkeit – der EU und/oder den einzelnen Mitgliedstaaten eine Grundlage für zulässige Datenübermittlungen bilden (siehe zum Beispiel das EU/US Abkommen zum Austausch von Flugpassagierdaten oder das sogenannte „SWIFT-Abkommen" bzw. auf bilateraler Ebene das Abkommen zwischen den USA und Österreich über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten sowie daran anknüpfende Amts- und Rechtshilfeabkommen).

Der US-behördliche Zugriff auf Daten in den USA – auch auf jene in Unternehmen, die dem „Safe Harbor" beigetreten sind – richtet sich nach US-amerikanischem Recht, dessen Auslegung nicht in die Zuständigkeit des Bundeskanzleramtes fällt. Letztlich können aber die in einem zivilrechtlichen Verhältnis grundgelegten Datenschutzgrundsätze in Form der „Safe Harbor Principles" einem auf US-gesetzlicher Ebene ausgestalteten Zugriffsrecht nicht entgegen gehalten werden.

Um feststellen zu können, auf welcher Rechtsgrundlage Behörden auf Daten zugreifen (bzw. welches Recht überhaupt anwendbar ist) und welche Behörden oder Gerichte im Fall einer Rechtsverletzung zuständig sind, bedarf es jeweils einer Prüfung im Einzelfall.

Zu den Fragen 5 bis 9:

- *Welche Maßnahmen hat Ihr Ministerium bislang gesetzt, um dem Missbrauch von Kundendaten zwischen den USA und der EU entgegen zu wirken?*
- *Welche Maßnahmen wird Ihr Ministerium in Zukunft setzen, um dem Missbrauch von Kundendaten zwischen den USA und der EU entgegen zu wirken?*

- *Ist von Seite Ihres Ministeriums geplant, auf EU-Ebene verstärkt für den Schutz von personenbezogenen Daten einzutreten?*
- *Wenn ja, welche Schritte sind konkret geplant?*
- *Wenn nein, warum werden keine weiteren Schritte geplant?*

Die in Geltung stehenden Datenschutzinstrumente sehen zahlreiche Betroffenenrechte vor, die dem Rechtsschutz dienen und Datenmissbrauch unterbinden sollen. Dies ist – wie schon ausgeführt – von den zuständigen Stellen einzelfallbezogen zu prüfen.

Die Vertreter des Bundeskanzleramts setzen sich auf EU-Ebene in den entsprechenden Gremien laufend für eine Stärkung des Datenschutzes ein. In diesem Zusammenhang verweise ich etwa auf die Verhandlungen für ein Datenschutzabkommen zwischen den USA und der EU im Bereich der polizeilichen und justiziellen Zusammenarbeit.

Die Europäische Kommission arbeitet derzeit an einem Entwurf für einen neuen Rechtsrahmen für den Datenschutz auf unionsrechtlicher Ebene, um die datenschutzrechtlichen Instrumente an die neuen technologischen Entwicklungen und die Anforderungen der Globalisierung anzupassen und den Datenschutz im Einklang mit dem Vertrag von Lissabon und der Grundrechtecharta in Bezug auf das gesamte Handeln der EU zu gewährleisten. Das Bundeskanzleramt hat zur entsprechenden Mitteilung der Europäischen Kommission sowie zu den diesbezüglichen Schlussfolgerungen des Rates die österreichische Position koordiniert und wird in der nachfolgenden Diskussion des Entwurfs auf unionsrechtlicher Ebene datenschutzrechtliche Anliegen vertreten. Ein Fokus wird dabei auch auf den neuen technologischen Entwicklungen liegen.

Zu den Fragen 10 bis 12:

- *Wird der gegenwärtige Schutz personenbezogener Daten in einer Cloud von Ihrem Ministerium als ausreichend betrachtet?*
- *Wenn ja, warum?*
- *Wenn nein, was ist konkret angedacht, um das zu ändern?*

Mangels spezifischer Vorschriften für Cloud Computing kann sich die Anwendung bestehender datenschutzrechtlicher Instrumente in der Praxis schwierig gestalten. Eine Lösung kann nur unionsweit (bzw. weltweit) gefunden werden.

Im neuen Rechtsrahmen für den Datenschutz auf Unionsebene werden auch Regelungen zu Cloud Computing (bzw. die dahinterstehenden datenschutzrechtlichen Fragestel-

lungen) Berücksichtigung finden. Auch das Europäische Parlament fordert in diesem Zusammenhang eine Klärung der Zuständigkeiten der für die Datenverarbeitung Verantwortlichen sowie der Datenverarbeiter und der Datenbankanbieter, um die entsprechenden rechtlichen Verantwortlichkeiten besser zuweisen und dafür sorgen zu können, dass die Betroffenen wissen, wo ihre Daten gespeichert werden, wer Zugang zu ihren Daten hat, wer über die Verwendung der personenbezogenen Daten beschließt und welche Art von Backup- und Recovery-Prozessen vorhanden sind.

Das Bundeskanzleramt wird sich auf Unionsebene an der Diskussion dieser Problematik nach entsprechender innerstaatlicher Koordination lösungsorientiert beteiligen.

Mit freundlichen Grüßen