34. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre

25. – 26. Oktober 2012

Punta del Este, Uruguay

Entschließung zu Cloud Computing

Cloud Computing (CC) gewinnt zunehmend an Interesse, weil es eine größere Wirtschaftlichkeit, weniger Belastung für die Umwelt, einfachere Handhabung, mehr Benutzerfreundlichkeit und viele andere Vorteile verspricht. Aufgrund folgender Tatsachen wirft die Entwicklung von CC viele wichtigen Themen auf, wie z.B. in folgender Hinsicht: Die Technologie befindet sich noch im Entwicklungsstadium, die Datenverarbeitung findet jetzt weltweit statt, und aufgrund der fehlenden Transparenz wird die Durchsetzung von Regelungen zum Schutz der Privatsphäre und der Daten sogar noch erschwert. Dadurch könnten die Risiken, die bei der Datenverarbeitung auftreten, noch erhöht werden, wie Verstöße gegen die Datensicherheit, Verstöße gegen Gesetze und Grundsätze für den Schutz der Privatsphäre und der Daten, und der Missbrauch der in der Cloud gespeicherten Daten.

Die Mitglieder der Internationalen Konferenz und andere Interessengruppen, wie zum Beispiel die International Working Group on Data Protection in Telecommunications (IWGDPT, auch bekannt als „Berlin Group“[1]), hat die mit CC verbundenen datenschutzrechtlichen Probleme untersucht.

Ohne dabei eine von einer bestimmten Gruppe vorgenommene Analyse zu unterstützen, begrüßt die Internationale Konferenz derartige Bemühungen. Um einen Beitrag für die Förderung solcher Bemühungen und zur Vermeidung der mit der Nutzung der Cloud Computing Dienste verbundenen Risiken und zur Förderung der Verantwortlichkeit und der ordnungsgemäßen Geschäftsführung zu leisten, empfiehlt die **Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre** deshalb:

- Im Vergleich mit anderen Arten der Datenverarbeitung darf Cloud Computing nicht zur Absenkung der Datenschutzstandards führen;

- die verantwortlichen Stellen sollen vor der Aufnahme von CC-Projekten die notwendigen Prüfungen der Auswirkungen und Risiken für den Datenschutz durchführen (ggf. durch vertrauenswürdige Dritte)

- Die Anbieter von Cloud-Diensten sollen angemessene Transparenz, Sicherheit, Verantwortlichkeit und Vertrauen in CC-Lösungen gewährleisten, insbesondere in Bezug auf Informationen über die Verletzung des Schutzes personenbezogener Daten und in Bezug auf Vertragsklauseln, die gegebenenfalls die Datenportabilität und Datenkontrolle durch Cloud-Nutzer unterstützen. Wenn sie als verantwortliche Stellen handeln, sollen Cloud-Diensteanbieter den Nutzern gegebenenfalls wichtige

[1] Siehe z.B. das Arbeitspapier der Gruppe „Cloud Computing – Privacy and data protection issues (Sopot Memorandum)“, Sopot (Polen), 23./24. April 2012; http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

Informationen über mögliche Auswirkungen auf den Datenschutz und über mit deren Dienste verbundene Risiken zur Verfügung stellen.

- Es sollen weitere Bemühungen im Bereich der Forschung, der Zertifizierung durch Dritte, Standardisierung, „Privacy by Design“- Technologien und anderen, damit verbundenen Systemen unternommen werden, um das gewünschte Maß an Vertrauen in CC zu erreichen. Um den Datenschutz gründlich und wirksam in Cloud Computing einzubauen, sollten schon im Anfangsstadium angemessene Maßnahmen in die Architektur von IT-Systemen und Geschäftsabläufen einbezogen werden (Privacy by Design).

- Die Gesetzgeber sollen die Angemessenheit und Interoperabilität der bestehenden Rechtsrahmen zur Erleichterung grenzüberschreitender Datenübermittlungen überprüfen, und sie sollten zusätzliche notwendige Maßnahmen zum Datenschutz im Bereich CC in Erwägung ziehen.

- Die Datenschutzbehörden sollen den verantwortlichen Stellen, Anbietern von Cloud-Diensten und Gesetzgebern weiterhin mit Informationen zu Fragen hinsichtlich des Schutzes der Privatsphäre und personenbezogener Daten zur Verfügung stehen.

Alle Interessengruppen – Anbieter, Kunden von CC und auch Regulierungsbehörden – sollten zusammenarbeiten, um ein hohes Datenschutzniveau und eine hohe IT-Sicherheit zu gewährleisten.