14/DE
WP 227

GEMEINSAME ERKLÄRUNG DER IN DER ARTIKEL-29-DATENSCHUTZGRUPPE VERTRETENEN EUROPÄISCHEN DATENSCHUTZBEHÖRDEN

Angenommen am 26. November 2014

Einleitung

Unser tägliches Leben ist zunehmend durch das digitale Zeitalter geprägt. In weniger als einem Jahrzehnt wurde der berufliche, wirtschaftliche und private Lebensbereich nach und nach digitalisiert. Dies hat ein riesiges Spektrum neuer Möglichkeiten eröffnet und die Entwicklung außerordentlich innovativer Waren und Dienstleistungen ermöglicht, die auf individuelle und kollektive Bedürfnisse zugeschnitten sind. Der Grundstein dieser digitalen Welt sind personenbezogene Daten.

Die Funktionsweise des digitalen Umfelds stützt sich in hohem Maße auf komplexe Informationssysteme, die von privaten Unternehmen für ihre eigenen Zwecke eingerichtet wurden. Diese Unternehmen sammeln große Mengen personenbezogener Daten, die bisweilen gespeichert, verarbeitet und weitergegeben werden, häufig ohne ein angemessenes Maß an Kontrolle durch die Nutzer und ohne jegliche Form von wirksamer Aufsicht. Die jüngsten Enthüllungen von Edward Snowden belegen zudem, dass Behörden und Nachrichtendienste zu anderen Zwecken – vor allem unter Berufung auf die nationale Sicherheit – einen massiven Zugang zu diesen Datensystemen fordern.

Die Öffentlichkeit in der ganzen Welt ist erschüttert darüber, dass dieser Zugang routinemäßig und massiv erfolgt. Nun stellt sich die Frage, wie das mangelnde Vertrauen in (ausländische oder eigene) Regierungen sowie Nachrichten- und Sicherheitsdienste wiederhergestellt und das zugrunde liegende Problem der Kontrolle des Zugangs zu großen Mengen personenbezogener Daten behoben werden kann. Wie kann ein Rahmen eingerichtet werden, der es privaten Unternehmen und anderen einschlägigen Einrichtungen erlaubt, innovative Waren und Dienstleistungen anzubieten, die der Nachfrage der Verbraucher oder öffentlichen Bedürfnissen entsprechen, während nationale Nachrichtendienste im Rahmen des anwendbaren Rechts ihre Aufgaben wahrnehmen können, und zwar so, dass keine Überwachungsgesellschaft entsteht?

Aufgrund seiner gemeinsamen Geschichte und Kultur muss Europa sich Gehör verschaffen, um sicherzustellen, dass die Grundrechte, einschließlich des Rechts auf Privatsphäre und Datenschutz, gewahrt werden, ohne dass Innovation oder Sicherheitsbelange in unserer Gesellschaft auf der Strecke bleiben. In diesem Zusammenhang wollen die in der Artikel-29-Datenschutzgruppe vertretenen unabhängigen Datenschutzbehörden in einigen Schlüsselbotschaften ihre Vorstellungen zur Bewältigung dieser weltweiten Herausforderung darlegen.

Zu diesem Zweck hat die Artikel-29-Datenschutzgruppe auf ihrer Plenarsitzung vom 25. November 2014 die folgende Erklärung angenommen:

Europäische Werte

1. **Der Schutz personenbezogener Daten ist ein Grundrecht.** Personenbezogene Daten (einschließlich Metadaten) dürfen nicht ausschließlich als Handelsobjekt, wirtschaftlicher Vermögenswert oder gemeinsames Gut behandelt werden.

2. **Datenschutzrechte müssen gegen andere Grundrechte** wie das Recht auf Nichtdiskriminierung und auf freie Meinungsäußerung **abgewogen werden,** die in einer

demokratischen Gesellschaft gleichwertig sind. Sie müssen zudem gegen Sicherheitsbedürfnisse abgewogen werden.

3. **Technologie muss weiterhin im Dienste des Menschen stehen.** Die Tatsache, dass etwas technisch machbar ist und dass die Datenverarbeitung bisweilen nützliche Erkenntnisse liefern oder die Entwicklung neuer Dienste ermöglichen kann, bedeutet nicht zwangsläufig, dass dies gesellschaftlich akzeptable, ethisch vertretbar, angemessen oder rechtmäßig ist.

4. **Das öffentliche Vertrauen in Produkte und Dienstleistungen der digitalen Wirtschaft** hängt weitgehend davon ab, ob die Technologiebranche sich an die Datenschutzvorschriften hält. Die Einhaltung dieser Vorschriften ist ein wichtiger Wettbewerbsfaktor für die digitale Wirtschaft und gewährleistet eine nachhaltige Entwicklung zum Nutzen der Verbraucher und der Unternehmen gleichermaßen.

5. **Die Sensibilisierung der Öffentlichkeit sowie die Selbstbestimmung des Einzelnen** müssen gestärkt werden, um dazu beizutragen, die exzessive Überwachung von Einzelpersonen durch staatliche oder private Einrichtungen zu begrenzen. Wichtige Maßnahmen in diesem Zusammenhang sind die Verbesserung der digitalen Kompetenzen, einschließlich Maßnahmen zur Datenschutzaufklärung, sowie die Ermöglichung kollektiver Klagen für Einzelpersonen, um die Meldung von weit verbreiteten Verletzungen des Datenschutzes zu erleichtern.

Überwachung für Sicherheitszwecke

6. **Die geheime, massive und wahllose Überwachung** von Einzelpersonen in Europa, sei es durch staatliche oder private Einrichtungen in Europa oder anderswo, ist weder rechtmäßig, was die Verträge und Rechtsvorschriften der EU betrifft, noch ethisch vertretbar.

7. **Die uneingeschränkte massenhafte Vorratsspeicherung personenbezogener Daten für Sicherheitszwecke ist in einer demokratischen Gesellschaft nicht hinnehmbar.** Die Vorratsspeicherung von, der Zugang zu und die Nutzung von Daten durch die zuständigen nationalen Behörden sollten auf das beschränkt sein, was in einer demokratischen Gesellschaft unbedingt notwendig und verhältnismäßig ist, und wirksamen materiell- und verfahrensrechtlichen Garantien unterliegen.

8. **Die Verarbeitung personenbezogener Daten im Zusammenhang mit Überwachungstätigkeiten** darf ausschließlich im Rahmen angemessener, gesetzlich festgelegter Garantien in Übereinstimmung mit Artikel 8 der EU-Grundrechtecharta erfolgen. Derartige Garantien umfassen eine **unabhängige und wirksame Aufsicht**, an der Datenschutzbehörden im Rahmen ihrer Befugnisse effektiv beteiligt sein sollten.

9. Grundsätzlich sollte eine öffentliche Behörde in einem Nicht-EU-Land keinen uneingeschränkten **direkten Zugang zu personenbezogenen Daten haben, deren Verarbeitung dem EU-Recht unterliegt**, und zwar unabhängig von den Bedingungen dieses Zugangs und dem Standort der Daten. Kompetenzkonflikte sollten nur unter bestimmten Bedingungen gelöst werden – zum Beispiel im Zuge einer vorherigen Genehmigung durch eine Behörde in der EU oder durch ein Rechtshilfeabkommen, in denen jeweils der Zugang für ausländische Strafverfolgungsbehörden zu Daten, die aus

der EU übermittelt oder in der EU gespeichert werden, geregelt ist. Dem EU-Recht unterliegende Unternehmen müssen Ersuchen aus dem Ausland nicht unmittelbar nachkommen.

10. Keine der Bestimmungen der **europäischen Instrumente,** die **als Rahmen für internationale Datenübermittlungen** zwischen privaten Parteien eingeführt wurden, bietet eine Rechtsgrundlage für die Übermittlung von Daten an Behörden eines Drittlandes für die Zwecke der massiven und willkürlichen Überwachung (ganz gleich, ob es sich um Safe-Harbor-Regelungen, verbindliche unternehmensinterne Vorschriften oder Standardvertragsklauseln handelt).

11. Erheben staatliche oder private Parteien enorme Datenmengen, die sehr genaue Informationen über das Privatleben der Personen enthalten, deren Daten auf Vorrat gespeichert werden, sollten sie die Speicherung dieser Daten derart organisieren, dass eine unabhängige Behörde wirksam kontrollieren kann, ob die Datenschutzvorschriften eingehalten wurden. Die **Speicherung der relevanten Daten im Hoheitsgebiet der EU** kann die Ausübung dieser Kontrolle wirksam erleichtern.

Europäischer Einfluss

12. **Der Entwurf des EU-Datenschutzpakets sollte 2015 angenommen werden**. Das Paket, dass zur Vereinheitlichung des europäischen digitalen Marktes beitragen soll, muss im Einklang mit den europäischen Werten und Grundrechten ein hohes Maß an Datenschutz für Einzelpersonen sicherstellen.

13. Der Schutz personenbezogener Daten in Europa sollte nicht ganz oder teilweise durch bilaterale oder **internationale Abkommen**, auch nicht durch **Abkommen über den Handel** mit Waren oder Dienstleistungen mit Drittländern, ausgehebelt werden.

14. Die Datenschutzvorschriften der EU sind notwendig, um die politische, soziale und wirtschaftliche Lage der EU sowie alle Personen, die dem EU-Recht unterliegen, zu schützen. Ihre Grundsätze müssen **im Rahmen des Völkerrechts und des internationalen Privatrechts als international zwingende Vorschriften** gelten. Weder können ausländische Gesetze oder internationale Vereinbarungen diesen Grundsätzen vorgehen, noch können Organisationen sie durch Verträge außer Kraft setzen.

15. Die Herstellung eines ausgewogenen Verhältnisses zwischen Datenschutz, Innovation und Überwachung bedeutet **weder die Wiedereinführung von EU-Binnengrenzen noch die Abriegelung Europas** gegenüber ausländischen Partnerschaften. Es bedarf der Wahrung des hohen Schutzniveaus, das sich aus dem Erbe des europäischen Datenschutzes ableitet, zu dem unter anderem das Übereinkommen 108 des Europarats und die Datenschutzvorschriften der EU zählen.

Nächste Schritte

16. Die Datenschutzgruppe begrüßt **Stellungnahmen** aller öffentlichen oder privaten Interessenträger zu dieser Erklärung. Diese Stellungnahmen können über die eigens hierfür eingerichtete Website www.europeandatagovernance-forum.com abgegeben werden. Die Datenschutzgruppe wird diesen Stellungnahmen bei ihren Tätigkeiten im Laufe des Jahres 2015 Rechnung tragen.