„Le Point“-Konferenz – „Das vernetzte und intelligente Zuhause“

Paris, 28. März 2013

Peter Hustinx
Europäischer Datenschutzbeauftragter

„Die Weitergabe personenbezogener Informationen und die Achtung der häuslichen Privatsphäre“

Ich freue mich sehr über die Gelegenheit, auf dieser Konferenz zu einer Frage von großer praktischer und symbolischer Bedeutung zu sprechen: Wie können wir unsere häusliche Privatsphäre in einer immer stärker vernetzten Welt schützen?

Der private Bereich unserer Wohnungen hat schon immer besonderen verfassungsmäßigen Schutz genossen und ist heute ein zentraler Aspekt des Grundrechts auf den Schutz des Privatlebens. Gegen das unerlaubte Eindringen in Privatwohnungen und das Abfangen oder Abhören privater Kommunikation gibt es aus guten Gründen besondere Garantien.

In einer Informationsgesellschaft, die auf der allgegenwärtigen Nutzung der Informations- und Kommunikationstechnologien – zu Hause wie anderswo – basiert, müssen wir uns generell um wirksamere Garantien zum Schutz personenbezogener Daten bemühen. Daher wird derzeit der Rechtsrahmen für den Datenschutz in der Europäischen Union überarbeitet.

Die Entwicklung des „intelligenten Zuhauses” könnte jedoch die vorhandenen Schutzbestimmungen weitgehend aushöhlen, wenn keine umfassenden Garantien zur Wahrung der Privatsphäre geschaffen werden. Intelligente Messsysteme mögen zwar wesentliche Vorteile mit sich bringen, erlauben aber auch die Erhebung großer Datenmengen,

mittels derer verfolgt werden kann, was die Haushaltsmitglieder in ihrer häuslichen Privatsphäre tun.

Diese Daten können für die Analyse unseres Energieverbrauchs von Nutzen sein, doch bergen sie bei Kombination mit Daten aus anderen Quellen ein hohes Risiko extensiven Data Minings.

Dies gilt umso mehr, wenn das „Internet der Dinge“ zur Realität werden sollte und alle Gegenstände, die wir derzeit zu Hause benutzen, online vernetzt wären und miteinander sowie mit externen Providern über unsere Gewohnheiten und Bedürfnisse kommunizieren würden.

Wer wird dann die Kontrolle über diese Informationen haben? Tatsächlich wir? Oder werden wir in „gläsernen Wohnungen“ leben müssen, wo vom Schutz der Privatsphäre keine Rede mehr sein kann? Wie können wir sicherstellen, dass dieser Fall *nicht* eintreten wird?

Lassen Sie mich zunächst erläutern, was aktuell unternommen wird, um wirksamere Garantien für den Schutz personenbezogener Daten zu schaffen. Unser derzeit geltender Rechtsrahmen, der die Grundlage aller nationalen Rechtsvorschriften in der EU bildet, wurde 1995 angenommen, zu einer Zeit, als das Internet noch in den Kinderschuhen steckte. Folglich bedarf er ganz klar einer Erneuerung, um vor allem einen besseren Schutz angesichts der aktuellen Herausforderungen bieten zu können.

Ein weiteres Problem ist die übermäßige Heterogenität und Komplexität der gesetzlichen Bestimmungen, da der EU-Rechtsrahmen in 27 unterschiedliche nationale Gesetze umgesetzt wurde. Eine stärkere Harmonisierung und Kohärenz in der EU würde zu einem wirksameren Schutz beitragen. Außerdem hat der Lissabon-Vertrag in allen Politikbereichen eine Grundlage für einen wirksameren und umfassenderen Schutz geschaffen.

Aus diesen Gründen unterbreitete die Europäische Kommission im Januar 2012 einen Vorschlag für eine grundlegende Reform des derzeitigen Rechtsrahmens, der nun im Europäischen Parlament und im Rat erörtert wird. Obwohl das Paket als Ganzes immer noch einige Fragen aufwirft, besteht hinsichtlich seiner Grundzüge ein breiter Konsens.

So wird, erstens, der Geltungsbereich des EU-Rechts erweitert: Dieses wird anwendbar sein, wann immer Waren oder Dienstleistungen auf dem europäischen Markt angeboten oder in der

EU ansässige Personen überwacht werden. Damit werden „gleiche Ausgangsvoraussetzungen“ geschaffen, weil Internetdienstleister und andere wichtige Akteure diesem Recht unabhängig davon unterliegen, ob sie von der EU oder von einem Drittland aus tätig werden.

Zweitens wird die Stellung betroffener Personen gestärkt, damit eine angemessene Kontrolle der Erhebung und Nutzung ihrer personenbezogenen Daten gewährleistet ist. Dies wird durch eine größere Transparenz der Datenverarbeitung, strengere Vorschriften für die Einwilligung und wirksamere Auskunfts- und Berichtigungsrechte sowie Rechte auf Löschung von Daten, einschließlich des Rechts auf Vergessen und auf Datenportabilität, erreicht.

Drittens wird die Verantwortung des für die Verarbeitung Verantwortlichen dadurch unterstrichen, dass er verpflichtet ist, die Einhaltung der Datenschutzanforderungen zu gewährleisten und nachzuweisen. Außerdem muss er zeitnahe Datenschutzfolgeabschätzungen durchführen und dafür Sorge tragen, dass alle maßgeblichen Aspekte des Schutzes der Privatsphäre bei neuen Entwicklungen von vornherein berücksichtigt werden (eingebauter Datenschutz – „Privacy by Design“).

Viertens wird die Position unabhängiger Behörden gestärkt, die mit umfassenderen und einheitlichen Befugnissen für eine wirksamere Aufsicht und Durchsetzung ausgestattet werden, einschließlich der Möglichkeit, hohe Geldbußen und andere wirksame Sanktionen zu verhängen.

Und schließlich wird die Datenschutz-Grundverordnung voraussichtlich in allen Mitgliedstaaten unmittelbar gelten und damit für mehr Harmonisierung und Einheitlichkeit in der EU sorgen. Auch werden die Aufsichtsbehörden bei Themen mit einer europäischen oder internationalen Dimension enger zusammenarbeiten.

Was aber bedeutet das alles für das „intelligente Zuhause“ und insbesondere für intelligente Messsysteme? Es besagt schlicht, dass die Privatsphäre bei der Entwicklung und Einführung derartiger Systeme eine weit größere Rolle spielen wird als bislang der Fall.

Vor rund einem Jahr nahm die Europäische Kommission eine Empfehlung zu Vorbereitungen für die Einführung intelligenter Messsysteme an. Diese Einführung ist nun, vorbehaltlich einer wirtschaftlichen Bewertung der Kosten und Nutzeffekte, bis spätestens 2020 vorgesehen.

Bei der Einführung sollten jedoch nicht nur *wirtschaftliche* Erwägungen eine Rolle spielen. Aufgrund des hohen Risikos einer die Privatsphäre verletzenden Überwachung des Verhaltens im privaten Bereich sollte jedes intelligente Messsystem auch einer Datenschutzfolgen-abschätzung unterzogen werden.

Die Artikel-29-Datenschutzgruppe wurde kürzlich zu dem vorgeschlagenen Muster für eine solche Datenschutzfolgenabschätzung, das von der Industrie festgelegt wurde, konsultiert. Die erste Reaktion der Datenschutzgruppe fiel recht kritisch aus. Sie kam zu dem Schluss, dass das vorgeschlagene Muster zu allgemein ist, keine ausreichende Anleitung beinhaltet, um eine echte Risikobewertung vornehmen zu können, und auch keine empfehlenswerten Verfahrens-weisen nennt, die speziell auf intelligente Netze anwendbar wären.

In der Stellungnahme des EDSB vom Juni 2012 wird die Notwendigkeit zusätzlicher Garantien unterstrichen, einschließlich möglicher Legislativmaßnahmen auf EU-Ebene. Diese Garantien sollten zumindest die verbindliche Anforderung an die für die Datenverarbeitung Verantwortlichen beinhalten, eine Datenschutzfolgenabschätzung durchzuführen, sowie die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten zu melden.

Außerdem haben wir empfohlen, mehr Beratung zu den Rechtsgrundlagen für die Verarbeitung von Daten und zu den Wahlmöglichkeiten für die betroffenen Personen anzubieten, wie unter anderem im Hinblick auf die Häufigkeit der Messgeräteablesung sowie die Speicherfristen.

Wir sind auch der Auffassung, dass dies eine hervorragende Gelegenheit für den verbindlichen Einsatz von Technologien zum Schutz der Privatsphäre (PET) und anderer bester verfügbarer Techniken für die Datenminimierung darstellt. Mit anderen Worten: Der „eingebaute Datenschutz“ sollte die Norm sein. Die Verbraucher sollten außerdem direkten Zugang zu ihren Energieverbrauchsdaten, ihren individuellen Profilen, den für Data Mining verwendeten Algorithmen sowie jeglichen Informationen über Fern-Ein-/Ausschaltungs-funktionalitäten haben.

Für diesen Bereich von Belang ist ganz eindeutig auch die Nutzung des Cloud Computing. Hier gilt es zu beachten: Wenn Daten „in einer Cloud“ gespeichert werden, heißt das nicht, dass sie dem Geltungsbereich des EU-Datenschutzrechts entzogen sind. Tatsächlich finden

sowohl die aktuellen als auch die künftigen Datenschutzvorschriften in der Cloud Anwendung.

Es kommt deshalb darauf an, zu klären, wer in dieser Umgebung für die Einhaltung der Datenschutzvorschriften verantwortlich ist. Es kommt hier nicht nur darauf an wer der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter ist. Wir stellen in zunehmendem Maße fest, dass sowohl die Cloud-Kunden und als auch die Anbieter von Clouddiensten Verantwortung tragen. Dies erfordert eine klare Beschreibung der jeweiligen Zuständigkeiten aller Parteien, um in der Praxis schwerwiegende Datenschutzmängel zu vermeiden.

Die Artikel-29-Datenschutzgruppe nahm im Juli 2012 eine Stellungnahme zum Cloud Computing an, in der klar dargelegt wurde, dass mithilfe wirksamer Kontrollen ein angemessener Datenschutz gewährleistet werden kann. Es bedarf lediglich verantwortungs-bewusster Beteiligter, um solche Kontrollen in der Praxis zu vereinbaren.

Dem derzeit unausgewogenen Kräfteverhältnis zwischen Cloud-Kunden und Anbietern von Cloud-Diensten könnte man meines Erachtens durch allgemeine Geschäftsbedingungen entgegensteuern, die den Datenschutzanforderungen Rechnung tragen; außerdem müssten Standards und Zertifizierungssysteme eingeführt werden, die sämtliche Datenschutzkriterien berücksichtigen. Die meisten Probleme im Bereich der internationalen Datenübermittlung könnten mittels verbindlicher unternehmensinterner Datenschutzregeln gelöst werden. Wir haben die Europäische Kommission im November 2012 dementsprechend beraten.

All dies zeigt also, dass die Privatsphäre heute tatsächlich ein brisantes Thema ist. Sowohl der Schutz der Privatsphäre als auch Sicherheitsbelange sollten angegangen werden, indem man sie von Anfang an in allen maßgeblichen Projekten berücksichtigt. Auf diese Weise lässt sich am besten ein wirksamer Schutz für die Praxis entwickeln und in den kommenden Jahren Vertrauen in die Informationsgesellschaft aufbauen.