DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

PRESSEMITTEILUNG

EDPS/2013/06

Brüssel, Montag 17. Juni 2013

Eine glaubwürdige EU-Cybersicherheitsstrategie muss auf Vertrauen und dem Schutz der Privatsphäre aufbauen

Cybersicherheit ist keine Entschuldigung für die **unbegrenzte** Überwachung und Analyse persönlicher Daten, so der Europäische Datenschutzbeauftragte heute aus Anlass der Veröffentlichung seiner **Stellungnahme** zur **Cybersicherheitsstrategie der Europäischen Union**. Die Strategie enthält zwar eine willkommene Bestätigung der Wichtigkeit der Datenschutzprinzipien, sie ist allerdings **unklar** bezüglich der Frage, wie diese Prinzipien in der Praxis umgesetzt werden sollen, um die Sicherheit von Personen, Unternehmen, Regierungen und anderen Organisationen zu schützen.

Peter Hustinx, EDSB, sagte hierzu: "*Es gibt keine Sicherheit ohne Privatsphäre. Deswegen bin ich erfreut, dass die EU-Strategie anerkennt, dass es nicht um Privatsphäre gegen Cybersicherheit geht, sondern dass der **Schutz der Privatsphäre** und der **Datenschutz Leitprinzipien** für die Cybersicherheit sind. Allerdings spiegeln sich die Ambitionen der Strategie nicht in der geplanten Umsetzung wider. Wir erkennen an, dass Fragen der Cybersicherheit auf internationaler Ebene durch internationale Standards und Zusammenarbeit angegangen werden müssen. Nichtsdestotrotz muss Kooperation zwischen der EU und Drittstaaten wie den USA zwingend auf einem **Fundament** aus **gegenseitigem Vertrauen** und **Respekt für die Grundrechte** aufbauen; ein Fundament, das im Moment beschädigt erscheint*."

Das allgemeine Ziel der EU-Strategie ist es, die Nutzung des Internets und aller mit ihm verbundenen Netzwerke und Informationssysteme sicherer zu machen, indem Organisation in den EU-Staaten dazu befähigt werden, Störungen und Cyber-Angriffe zu verhindern und auf sie zu reagieren. Das Ergebnis soll ein größeres Vertrauen von Personen und Organisationen in das Internet sein. Die Mitteilung der Kommission beachtet allerdings nicht genügend die Rolle des Datenschutzrechts und aktueller EU-Rechtsetzungsvorschläge, wie etwa der vorgeschlagenen Datenschutzgrundverordnung und der e-Trust-Verordnung bei der Förderung der Cybersicherheit. Sie ignoriert ebenfalls, wie wichtig es ist, den Datenschutz bereits in der Entwicklung von Systemen, die der Cybersicherheit dienen sollen, zu berücksichtigen - **eingebauter Datenschutz** -, um ein Fundament für Vertrauen zu schaffen. Die Folge ist, dass die Strategie nicht so effektiv und umfassend ist, wie die Kommission beabsichtigte.

Zwar können Maßnahmen zur Cybersicherheit die Analyse bestimmter personenbezogener Daten, wie etwa IP-Adressen, die zu einzelnen Personen zurückverfolgt werden können, mit sich bringen; Cybersicherheit kann aber auch eine **grundlegende Rolle** beim Schutz der Privatsphäre und des Datenschutzes in der Online-Umwelt spielen, vorausgesetzt, dass die Datenverarbeitung **verhältnismäßig**, **notwendig** und **rechtmäßig** ist.

Nationale Datenschutzbehörden (DSBs) spielen eine **wichtige Rolle** dabei, sicherzustellen, dass die der Verarbeitung personenbezogener Daten - auch im Internet und in Netzwerken und Informationssystemen - mit einem angemessenen Sicherheitsniveau erfolgt; sie haben ebenfalls eine Rolle in der **Bewusstseinsbildung** bezüglich der Regeln, die für Personen und Organisationen in den EU-Staaten gelten. Zusätzlichen müssen die DSB über alle neuen Verarbeitungsvorgänge, die personenbezogene Daten beinhalten sowie über Datenschutzverstöße informiert werden. Agenturen wie Europol, ENISA und

andere, die in der Mitteilung aufgeführt werden, müssen in der Erfüllung ihrer Aufgaben mit den DSB in Kontakt bleiben. Auch wenn dies in der Strategie nicht angesprochen wird, muss der Beitrag der DSB zur Cybersicherheit anerkannt werden.

Hintergrundinformationen

Am 7. Februar 2013 haben die Kommission und die Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik eine **Gemeinsame Mitteilung** an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel "**Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum**" angenommen.

Am gleichen Datum hat die Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zu **Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union** angenommen. Dieser Vorschlag wurde dem EDSB am 7. Februar 2013 zur Stellungnahme übermittelt.

Der Schutz der Privatsphäre und der Datenschutz sind Grundrechte in der EU. Nach der Datenschutzverordnung (EG) No 45/2001 ist es eine der Aufgaben des EDSB, die Europäische Kommission, das Europäische Parlament und den Rat zu Vorschlägen für neue Rechtsakte und andere Themen, die sich auf den Datenschutz auswirken, zu beraten. Zusätzlich ist die Verarbeitung personenbezogener Daten durch EU-Organe und -Einrichtungen, wenn sie spezifische Risiken für Individuen („betroffene Personen“) mit sich bringt, einer Vorabkontrolle durch den EDSB unterworfen. Wenn die vorgelegte Verarbeitung nach Ansicht des EDSB zu einem Verstoß gegen Bestimmunen der Verordnung führen könnte, legt er Verbesserungsvorschläge vor.

Personenbezogene Informationen/Daten: alle Informationen über eine bestimmte oder bestimmbare natürliche (lebende) Person, wie Namen, Geburtsdaten, Fotografien, E-Mail-Adressen und Telefonnummern. Andere Details, wie Gesundheitsdaten, für Beurteilungszwecke verwendete Daten und Verkehrsdaten bei Nutzung von Telefon, E-Mail oder Internet, werden ebenfalls als personenbezogene Daten angesehen.

Privatsphäre: das Recht einer Person, in Ruhe gelassen zu werden und Kontrolle über die Informationen über sich selbst auszuüben. Das Recht auf Privatsphäre bzw. den Schutz des Privatlebens ist in der Allgemeinen Erklärung der Menschenrechte (Artikel 12), der Europäischen Menschenrechtskonvention (Artikel 8) und der Europäischen Grundrechtecharta (Artikel 7) festgeschrieben. Die Charta enthält auch ein explizites Recht auf den Schutz personenbezogener Daten (Artikel 8).

Eingebauter Datenschutz: den Schutz der Privatsphäre und den Datenschutz bereits in das Design und die Architektur von Informations- und Kommunikationstechnologien einbauen, um die Befolgung der Privatsphären- und Datenschutzprinzipien zu vereinfachen.

Zweckbindung: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Nach Erhebung dürfen die Daten nicht weiter in einer Weise, die mit diesen Zwecken unvereinbar ist, verarbeitet werden. Dieses Prinzip dient dazu, Personen durch die Begrenzung der Verwendung ihrer Daten auf vordefinierte Zwecke zu schützen; Ausnahmen sind nur unter strengen Bedingungen und mit angemessenen Schutzmaßnahmen möglich.

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Behörde, deren Aufgabe es ist, dafür zu sorgen, dass der Schutz personenbezogener Daten und der Privatsphäre gewährleistet ist und bewährte Verfahren in den Organen und Einrichtungen der EU gefördert werden. Er erfüllt diese Aufgabe, indem er

- die Verarbeitung personenbezogener Daten durch die EU-Verwaltung überwacht,
- in Bezug auf politische Maßnahmen und Rechtsvorschriften, die sich auf den Schutz der Privatsphäre auswirken, beratend tätig ist und
- mit vergleichbaren Behörden zusammenarbeitet, um einen kohärenten Datenschutz sicherzustellen.

Die Stellungnahme (EN) ist auf der Webseite des EDSB erhältlich. Kontakt: press@edps.europa.eu

EDSB - Der europäische Hüter des Datenschutzes

www.edps.europa.eu

Folgen Sie uns auf Twitter: @EU_EDPS