17. Oktober 2013

Datenschutzgrundverordnung in 10 Punkten

Verhandlungsführer ("Berichterstatter"): Jan Philipp Albrecht MEP

Von der Richtlinie zur Verordnung

Was gilt bisher? Derzeit erlassen die 28 Mitgliedstaaten ihre eigenen Gesetze anhand der Richtlinie von 1995. Die unterschiedliche Umsetzung hat zu einem ungleichen Datenschutzniveau und einem Flickenteppich an Datenschutzregeln in der EU geführt.

Gleiche Datenschutzstandards für Alle! Ziel des Vorschlags für eine Datenschutzgrundverordnung sind hohe und dem Internetzeitalter angemessene Datenschutzstandards, die einheitlich in der ganzen EU gelten sollen. So können sich Unternehmen zukünftig als Sitz nicht mehr den Mitgliedstaat mit den niedrigsten Datenschutzstandards aussuchen ("Forum Shopping"). Doch der Reformvorschlag geht noch weiter: Künftig sollen europäische Datenschutzstandards gelten, sobald Daten von EU-BürgerInnen verarbeitet werden – egal, ob innerhalb oder außerhalb der EU.

Zentrale Forderungen:

- ***Rechte auf Löschung, Auskunft und Korrektur:*** Wer möchte, dass eigene persönliche Daten im Internet gelöscht werden, muss dieses „Recht auf Löschung“ gegenüber Google, Facebook und Co. durchsetzen können, aber auch mittels dem ersten Datenverarbeiter gegenüber Drittparteien, die die Daten von ihm erhalten haben. Wer Daten einer Person illegal veröffentlicht, muss auch dafür sorgen, dass jede Kopie davon wieder gelöscht wird. Die Fraktionen haben sich auf eine sinnvolle Balance zwischen Meinungs- und Informationsfreiheit einerseits und dem Schutz personenbezogener Daten andererseits geeinigt. Außerdem sollen Anbieter in verständlicher Sprache, kostenfrei und schnell mitteilen, welche NutzerInnendaten sie in welchen Kontexten verarbeiten und diese Daten auf Anfrage auf elektronischem Weg aushändigen.

- ***Explizite Einwilligung*:** Wenn ein Dienste-Anbieter persönliche Daten verarbeiten will, müssen sie die NutzerInnen grundsätzlich fragen, ob sie mit Verarbeitung und Weitergabe ihrer Daten einverstanden sind. Nutzungsbedingungen sollen leicht verständlich formuliert sein. Statt seitenlanger und unverständlicher allgemeiner Geschäftsbedingungen sollen standardisierte Symbole Zustimmung oder Ablehnung vereinfachen. Anbieter sollen nur dann Nutzungsprofile erstellen dürfen, wenn NutzerInnen durch die Privatsphäre-Einstellungen ihres Internetbrowsers signalisieren, dass sie das nicht verbieten. Technische Standards dafür sollen auf EU-Ebene zertifiziert werden.

- ***Informationspflicht und Transparenz:*** Die Forderung nach erweiterten Auskunfts- und Informationsansprüchen geht weit über den Vorschlag der Europäischen Kommission hinaus. So sollen NutzerInnen u.a. auch verständliche Auskunft darüber erhalten, wie die eigenen Daten verarbeitet werden oder ob der Anbieter Daten an Strafverfolgungsbehörden oder Geheimdienste weitergegeben hat.

- ***Datenweitergabe an Drittstaaten:*** Nach den Enthüllungen des Whistleblowers Edward Snowden waren die Grundlage für die Forderung, dass Google und Co. Daten nur auf der Grundlage europäischen Rechts oder darauf beruhender Rechtshilfeabkommen an Behörden in Drittstaaten weitergeben dürfen, sprich: Ohne konkrete Abkommen mit entsprechenden Staaten soll es keine Weitergabe von Daten durch Telekommunikations- und Internetunternehmen geben. Dieser Verweis war in einem ersten Kommissionsentwurf enthalten, im öffentlich vorgestellten Entwurf dann nach intensiver Lobbyarbeit und Einflussnahme der amerikanischen Regierung gestrichen. Er steht nun wieder drin.

- ***Zukunftstaugliche Definitionen:*** Alle Informationen, die direkt oder indirekt einer Person zugeordnet werden oder dafür benutzt werden können, eine Person aus einer Menge von Menschen herauszufiltern, gelten als personenbezogene Daten und müssen geschützt werden. Dies ist gerade in Zeiten von „Big Data“ wichtig, in denen mehr und mehr Datensätze zusammengeführt, kombiniert und ausgewertet werden können.

- ***Sanktionen bei Verstößen:*** Verstöße sind keine Kavaliersdelikte und Sanktionen sollen wehtun. Deshalb sollen Unternehmen hohe Strafen zahlen müssen, wenn sie gegen das neue Gesetz verstoßen. Dies kann bei großen Konzernen bis in Milliardenhöhe gehen und wird verhindern, dass Unternehmen Datenschutzverletzungen einfach einkalkulieren.

- ***Privacy by Design/Privacy by Default:*** Unternehmen müssen ihre Angebote möglichst datensparsam konzipieren und mit den datenschutzfreundlichsten Voreinstellungen anbieten. Ein starkes Prinzip der Zweckbindung bedeutet, dass nur die Daten erhoben werden, die zur Erbringung des Dienstes benötigt werden. Außerdem muss es die Möglichkeit geben, Dienste anonym und unter Pseudonym zu nutzen.

- ***Weniger Bürokratie:*** Die Ernennung eines Datenschutzbeauftragten soll vom Ausmaß der Datenverarbeitung abhängig sein, nicht von der MitarbeiterInnenzahl eines Unternehmens. Vorab-Unterrichtungen der Aufsichtsbehörden sollen zum Zweck der Bürokratiereduzierung massiv begrenzt werden, dafür wird der betriebliche Datenschutzbeauftragte nun europaweit eingeführt und ist ab einer bestimmten Schwelle verpflichtend.

- ***Einheitliche Rechtsdurchsetzung:*** Eine europäische Datenschutzaufsicht soll europäisches Datenschutzrecht effektiver durchsetzen und Entscheidungen treffen dürfen, die bisher in den Händen der nationalen Datenschutzbehörden lagen – wie es auch im EU-Wettbewerbsrecht und bei der EU-Bankenaufsicht ist. Damit ist ein „Race to the Bottom“ in Mitgliedstaaten mit schwacher Rechtsdurchsetzung in Zukunft nicht mehr möglich. Der neue EU-Datenschutzausschuss soll die nationalen Aufsichtsbehörden aber auch unterstützen können. Datenschutzbehörden brauchen mehr Personal und mehr Geld.

- ***Ein fester Ansprechpartner für ganz Europa:*** Der „one-stop-shop“-Ansatz bedeutet: BürgerInnen und Unternehmen sollen sich EU-weit nur noch an eine Datenschutzbehörde als Ansprechpartnerin wenden müssen. Für die BürgerInnen bedeutet das, dass sie ihre Beschwerden an die Datenschutzbehörde in ihrem Mitgliedstaat richten können. Unternehmen müssen ebenfalls nur noch mit der Datenschutzbehörde des Mitgliedstaats zusammenarbeiten, in dem sich der Hauptsitz des Unternehmens befindet. Bei strittigen Fragen soll der neu gegründete Europäische Datenschutzausschuss das letzte Wort haben und nicht die Europäische Kommission, so bleibt die Unabhängigkeit der Datenschutzbehörden gewahrt.

Zeitplan:

21. Oktober 2013:
Abstimmung im Innenausschuss über das Verhandlungsmandat ("Orientierungsabstimmung").

Sobald sich der Rat auf eine gemeinsame Position geeinigt hat:
Beginn der Trilog-Verhandlungen zwischen Europäischem Parlament, Rat der Europäischen Union (Ministerrat) und Europäischer Kommission. Der Europäische Rat wird am 24./25. Oktober zum Thema „Digitale Agenda“ tagen.