11. Juni 2015

EU-Datenschutzgrundverordnung: Stand der Dinge – 10 wichtige Punkte

Federführender EP-Ausschuss: Bürgerliche Freiheiten, Justiz und Inneres (LIBE), EP-Verhandlungsführer ("Berichterstatter"): Jan Philipp Albrecht, Grüne/EFA

Von der Richtlinie 1995 zur Verordnung 2015

Problem: Ein Datenschutz-Flickenteppich. Derzeit erlassen die 28 Mitgliedstaaten ihre eigenen Gesetze, Grundlage ist die Datenschutzrichtlinie von 1995. Die Grundprinzipien, vom deutschen Bundesverfassungsgericht zusammengefasst als "informationelle Selbstbestimmung", gelten noch immer, aber unterschiedliche Gesetze und Anwendung in den Mitgliedstaaten haben zu ungleichen Datenschutzniveaus in der EU geführt. Darüber hinaus können Nutzer ihre Rechte nur begrenzt durchsetzen.

Lösung: Ein gleicher hoher Datenschutzstandard für Alle. Ziel des Vorschlags für eine neue Datenschutzgrundverordnung im Internetzeitalter sind hohe Datenschutzstandards, die einheitlich in der ganzen EU gelten sollen. Eine einheitliche Verordnung wird als Teil des europäischen digitalen Binnenmarkts unmittelbar europaweit Gesetz. Nutzer und Datenverarbeiter haben dann europaweit dieselben Rechte und Pflichten. Unternehmen können sich als Sitz nicht mehr den Mitgliedstaat mit den niedrigsten Datenschutzstandards aussuchen. Darüber hinaus gilt europäisches Datenschutzrecht für alle auf dem europäischen Markt – gleich, ob von innerhalb oder außerhalb der EU. Strengere Durchsetzung und Prinzipien wie datenschutzkonforme Produkt- und Technikentwicklung("privacy by design") werden das Vertrauen der Bürger und Nutzer in den europäischen Datenschutz stärken.

Stand der Dinge: Trilog beginnt im Juni. Die EU-Kommission hat ihren Gesetzesvorschlag im Januar 2012 vorgestellt. Im Europäischen Parlament wurden auch durch intensive Lobbyarbeit 3.999 Änderungsanträge eingereicht. Das Europäische Parlament nahm im März 2014 nahezu einstimmig in erster Lesung seine Version des Entwurfs an. Die Mitgliedstaaten im Rat der Innen- und Justizminister waren lange festgefahren, aber seit Sommer 2014 bewegen sie sich auf eine gemeinsame Position zu. Die Ratsposition soll am 15. Juni durch die Justizminister (für Deutschland ist das Innenministerium federführend) verabschiedet werden.
Parlament, Rat und Kommission wollen die "Trilog"-Verhandlungen über das endgültige Gesetz schon noch vor der Sommerpause am 24. Juni 2015 beginnen und bis Ende 2015 abschließen. Nach zwei Jahren Übergangszeit wird die Verordnung dann in allen EU-Mitgliedstaaten gelten.

10 wichtige Punkte

Recht auf Löschung, Auskunft und Korrektur: Wer möchte, dass persönliche Daten gelöscht werden, muss dieses „Recht auf Löschung“ gegenüber Google, Facebook und Co. durchsetzen können. Der Datenverarbeiter muss die Anfrage auf Löschung auch an Dritte weiterleiten, an die er die Daten weitergegeben hatte. Außerdem sollen Anbieter kostenfrei und schnell die Nutzerdaten auf Anfrage auf elektronischem Weg aushändigen.
Das teilweise umstrittene „Recht auf Vergessenwerden“ ist vom Europäischen Parlament begrenzt worden: Nur wer Daten einer Person rechtswidrig veröffentlicht, muss auch dafür sorgen, dass jede Kopie davon wieder gelöscht wird. Die Verordnung fordert einen sinnvollen Ausgleich zwischen Meinungs- und Informationsfreiheit einerseits und dem Schutz personenbezogener Daten andererseits.
Während das Parlament davon ausgeht, dass das im Google-Spanien-Urteil des Europäischen Gerichtshofs vom Mai 2014 konstatierte „Recht auf Nicht-Auflistung“ bereits im Text enthalten ist, da es auf dem bereits seit der Richtlinie von 1995 bestehenden Recht auf Löschung basiert, ist dies im Rat immer noch umstritten.

***Informierte Einwilligung als Eckpfeiler*:** Nutzer müssen darüber informiert werden, was mit ihren Daten passiert. Sie müssen grundsätzlich bewusst einer Datenverarbeitung zustimmen - oder sie ablehnen können. Während das Parlament auf der „expliziten“ Einwilligung“ besteht, wie von der Kommission vorgeschlagen, will der Rat die sehr viel schwammigere Formulierung „eindeutig“, die Datenverarbeitern die Hintertür offenhalten würde, die Zustimmung doch nicht einzuholen. Technische Standards für eine Ablehnung der Datenverarbeitung, z.B. „Do Not Track“ für Webseiten, können auf EU-Ebene zertifiziert werden und damit allgemeine Gütigkeit erlangen. Das Parlament hat das „berechtigte Interesse“ des Datenverarbeiters, mit dem eine Datenverarbeitung auch ohne Einwilligung möglich ist, darauf beschränkt, was auf Grund der Beziehung zwischen Nutzer und Datenverarbeiter vernünftigerweise erwartet werden kann. Die Mitgliedstaaten dagegen wollen, dass eine Datenverarbeitung lediglich auf Basis des „berechtigten Interesses“ des Verarbeiters erlaubt sein soll – und zwar zu ganz anderen Zwecken, als ursprünglich verabredet. Das würde die Idee des Datenschutzes grundsätzlich in Frage stellen und wäre auch im Widerspruch zur Charta der Grundrechte der EU.

Informationsrechte und Transparenz: Das Parlament fordert weit mehr Auskunfts- und Informationsansprüche als die Kommission. So sollen Nutzer laut Parlament u.a. verständliche Auskunft darüber erhalten, wie die eigenen Daten verarbeitet werden oder ob der Anbieter Daten an Strafverfolgungsbehörden oder Geheimdienste weitergegeben hat. Datenverarbeiter werden einfach, verständlich und kostenlos erklären müssen, welche Daten sie in welchen Kontexten verarbeiten. Nutzungsbedingungen müssen leicht zu verstehen sein. Standardisierte Symbole sollen laut Parlament lange und nur für Juristen lesbare Datenschutzerklärungen ersetzen. Der Rat hat dies nicht vorgesehen, scheint aber für die Idee offen zu sein.

Datenweitergabe an Drittstaaten: Das Parlament besteht darauf, dass Firmen Daten nicht direkt an Behörden in Drittstaaten weitergeben dürfen. Dies ist nur erlaubt auf der Grundlage europäischen Rechts und darauf beruhender Rechtshilfeabkommen. Dieser Schutzschild gegen den ausländischen Zugriff auf europäische Daten war bereits in einem ersten Kommissionsentwurf enthalten, aber nach intensiver Einflussnahme der amerikanischen Regierung gestrichen worden. Das Parlament hat ihn nach den Snowden-Enthüllungen wieder hineingeschrieben. Im Text der Mitgliedstaaten steht dieser Ansatz zwar nicht, sie scheinen aber offen dafür zu sein. Das Parlament fordert außerdem regelmäßige Berichte der Kommission zu Datentransfers in Drittstaaten.

Zukunftstaugliche Definitionen: Alle Informationen, die direkt oder indirekt einer Person zugeordnet werden können, sind als personenbezogene Daten geschützt. Dies ist gerade in Zeiten von „Big Data“ wichtig. Das Parlament hat auch klargestellt, dass Daten nicht unbedingt auf die bürgerliche Identität einer Person schließen lassen müssen, um geschützt zu sein – es reicht, eine Person wiedererkennen zu können.

Starke Sanktionen: Verstöße sind keine Kavaliersdelikte und Sanktionen sollen wehtun. Die Kommission hat Bußgelder bis zu zwei Prozent des weltweiten Jahresumsatzes vorgeschlagen, die Mitgliedstaaten wollen dabei bleiben. Das Parlament will dies auf bis zu fünf Prozent des Jahresumsatzes des Unternehmens oder 100 Millionen Euro erhöhen. Dies wird sicherstellen, dass Unternehmen Datenschutzverletzungen nicht einfach einkalkulieren. Natürlich müssen Bußgelder immer verhältnismäßig sein, daher müssen kleine Unternehmen keine Angst vor hohen Strafen haben, wenn es sich nur um kleinere Verstöße handelt.

Privacy by Design/Privacy by Default: Datenverarbeiter müssen ihre Dienste datensparsam konzipieren und mit den datenschutzfreundlichsten Voreinstellungen anbieten. Ein starkes Prinzip der Datensparsamkeit bedeutet, dass nur die Daten erhoben werden, die zur Erbringung des Dienstes wirklich benötigt werden. Der Rat möchte eine deutlich schwammigere Formulierung. Außerdem muss es laut Parlament die Möglichkeit geben, Dienste anonym und unter Pseudonym zu nutzen. Das Parlament hat ausdrücklich ein Kopplungsverbot vorgesehen, das verhindern soll, das Nutzer Dienste nur nutzen können, wenn sie dem Anbieter Daten zur Verfügung stellen, die mit dem eigentlichen Dienst nichts zu tun haben.

Weniger Bürokratie: Nach Ansicht des Parlaments soll die Ernennung eines betrieblichen Datenschutzbeauftragten davon abhängig sein, welche Daten verarbeitet werden und wie viele und nicht davon, wie viele Mitarbeiter ein Unternehmen beschäftigt. Vorab-Meldungen an die Aufsichtsbehörden sollen hingegen zum Zweck des Bürokratieabbaus massiv begrenzt werden. Der Rat will diese Entscheidung den Mitgliedstaaten überlassen. Das Parlament hingegen hat klargestellt, dass der oder die Datenschutzbeauftragte keine Vollzeitkraft sein muss und auch ein externer Dienstleister sein kann. Das Parlament hat auch die Dokumentationspflichten für die Datenverarbeiter auf ein Minimum beschränkt, während der Rat hier noch viele Anforderungen stellt.

Einheitliche Rechtsdurchsetzung: Ein europäischer Datenschutzausschuss, bestehend aus den nationalen Aufsichtsbehörden, soll die einheitliche Anwendung des Datenschutzrechts sicherstellen und kann dazu in Fällen von europaweiter Bedeutung auch bindende Entscheidungen treffen – ähnlich wie im Wettbewerbsrecht und bei der Bankenaufsicht. Damit ist ein „Race to the Bottom“ in Mitgliedstaaten mit schwacher Rechtsdurchsetzung in Zukunft nicht mehr möglich. Parlament und Rat sind sich grundsätzlich über diesen Ansatz einig und wollen nicht der Kommission das letzte Wort überlassen – so bleibt die Unabhängigkeit der Datenschutzbehörden gewahrt. Das Parlament drängt darauf, dass die Datenschutzbehörden mehr Ressourcen und mehr Personal bekommen. Der Rat will, dass sie Datenverarbeitern bei Verstößen konkrete Auflagen machen können.

Ein fester Ansprechpartner für ganz Europa: Der „One-Stop Shop“-Ansatz bedeutet: Bürger müssen sich in der gesamten EU nur noch an eine Datenschutzbehörde wenden. Betroffene können ihre Beschwerden an die Datenschutzbehörde in ihrem Mitgliedstaat richten, egal wo der Datenmissbrauch passiert ist. Unternehmen müssen ebenfalls nur noch mit der Datenschutzbehörde des Mitgliedstaats zusammenarbeiten, in dem sich der Hauptsitz des Unternehmens befindet.