17. Dezember 2015

EU-Datenschutzgrundverordnung:
Ergebnisse der Verhandlungen („Triloge“) und die 10 wichtigsten Punkte

Federführender Ausschuss des Europäischen Parlaments:
Bürgerliche Freiheiten, Justiz und Inneres (LIBE)

EP-Verhandlungsführer („Berichterstatter“):
Jan Philipp Albrecht, MdEP, Grüne / Europäische Freie Allianz

Ein besserer Datenschutz für alle in der EU – Von der Richtlinie 1995 zur Verordnung 2015

Problem: Ein Datenschutz-Flickenteppich. Bis jetzt haben die 28 Mitgliedstaaten der Europäischen Union ihre eigenen Datenschutzgesetze erlassen. Ihre Grundlage ist die Datenschutzrichtlinie von 1995. Die Grundprinzipien, niedergeschrieben in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und in Artikel 8 der EU-Grundrechtecharta, gelten. Aber unterschiedliche Gesetze und Anwendung in den Mitgliedstaaten haben zu **ungleichen Datenschutzniveaus in der EU** geführt – zum Nachteil der Bürgerinnen und Bürger wie auch der Unternehmen im Europäischen Binnenmarkt.

Lösung: Ein gleicher, hoher Datenschutzstandard für alle 500 Millionen Bürger der Europäischen Union. Die Datenschutzgrundverordnung wird **für den gesamten privaten und öffentlichen Bereich gelten**. Ausgenommen ist lediglich der Bereich der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten sowie der Strafvollstreckung. Hier wird künftig die gleichzeitig verhandelte **Richtlinie für den Datenschutz im Polizei- und Justizbereich** gelten.

Die Datenschutzgrundverordnung zielt auf **gleiche Wettbewerbsbedingungen auf der Basis hoher Datenschutzstandards**, die dem Internetzeitalter angemessen sind. Als Teil des Europäischen Digitalen Binnenmarkts wird es die Verordnung für Datenverarbeiter sowie Nutzerinnen und Nutzer leichter machen, ihre Rechte und Pflichten zu kennen und durchzusetzen. Unternehmen können sich als Sitz nicht mehr den Mitgliedstaat mit den niedrigsten Datenschutzstandards aussuchen. Die Verordnung macht europaweite Datenschutzstandards für alle auf dem europäischen Markt verbindlich – egal, ob sie über einen Sitz in der EU verfügen oder nicht. Eine strengere Durchsetzung der Regeln und neue Rechte wie das auf Datenportabilität, Prinzipien wie datenschutzkonforme Produkt- und Technikentwicklung („privacy by design“) werden das Vertrauen der Bürgerinnen und Bürger sowie der Nutzerinnen und Nutzer in den europäischen Datenschutz und den Wettbewerb im digitalen Markt stärken.

Zeitplan: Die EU-Kommission hatte ihren Gesetzesvorschlag im Januar 2012 vorgestellt. Nach der ersten Lesung im Europäischen Parlament im März 2014 und der „allgemeinen Ausrichtung“ des Rats im Juni 2015 fanden seit dem 24. Juni 2015 Verhandlungen zwischen Parlament, Rat und Kommission („Triloge“) statt, bei denen am 15. Dezember 2015 eine vorläufige Einigung erzielt wurde. Diese wurde am 17. Dezember 2015 vom federführenden Innen- und Justizausschuss des Parlaments angenommen. Sie muss von den Regierungen der EU-Mitgliedstaaten im Ausschuss der Ständigen Vertreter im Rat (Coreper) am 18. oder 21. Dezember noch bestätigt werden. Anschließend soll es die formale Annahme der Einigung auf Ministerebene und im Plenum des Europäischen Parlaments geben. Zwei Jahre nach der Veröffentlichung im EU-Amtsblatt wird die Verordnung dann in allen Mitgliedstaaten gelten.

10 wichtige Punkte

1. Rechte auf Vergessen, Datenportabilität und Zugang: Wer möchte, dass persönliche Daten gelöscht werden, muss dieses Recht auf Vergessen gegenüber Google, Facebook und Co. durchsetzen können. Der Datenverarbeiter muss die Löschanfrage auch an Dritte weiterleiten, an die er Daten weitergegeben hatte. Das Google-Spanien-Urteil des Europäischen Gerichtshofs vom Mai 2014 gründet auf der Datenschutzrichtlinie von 1995. Die Datenschutzverordnung stellt nun klar, in welchen Fällen das Recht auf Vergessen gilt. Das Recht auf Information und das öffentliche Interesse müssen mit diesem in einer Balance stehen. Hierfür schafft die Verordnung klare Regeln und Verfahren. Das Gesetz gewährleistet zudem das Recht auf Datenportabilität: Wer einen Anbieter wechseln möchte, hat das Recht, persönliche Daten mitzunehmen. Anbieter müssen die Nutzerdaten auf Anfrage auf elektronischem Weg und in einem **allgemein nutzbaren Format** kostenfrei und schnell aushändigen.

2. Informierte Einwilligung als Eckpfeiler**:** Nutzerinnen und Nutzer müssen bewusst einer Datenverarbeitung zustimmen – oder sie ablehnen können. Die Verordnung stellt nun klar, dass es keine vermutete Einwilligung geben und es nicht die Aufgabe der Nutzerinnen und Nutzer sein kann, voreingestellte Haken aus Kästchen zu entfernen. Jede Zustimmung bedarf einer klaren **zustimmenden Handlung.** Diese muss freiwillig sein, d.h. ein Vertrag darf nicht an die Verarbeitung von Daten gebunden sein, die mit der erbrachten Leistung oder dem Produkt nichts zu tun hat. Technische Standards für eine automatische Ablehnung der Datenverarbeitung, wie z.B. durch die Browsereinstellung **„Do Not Track“** für Webseiten, können nun **rechtlich verbindlich** gemacht werden**.** Das Parlament hat erfolgreich das „berechtigte Interesse“ des Datenverarbeiters, mit dem eine Datenverarbeitung auch ohne Einwilligung möglich ist, auf dasjenige beschränkt, was auf Grund der Beziehung zwischen Nutzerinnen und Nutzer auf der einen Seite und Datenverarbeiter auf der anderen Seite vernünftigerweise erwartet werden kann.

3. Informationsrechte und Transparenz: Das Parlament forderte weit mehr Auskunfts- und Informationsansprüche als die Kommission – und konnte sich durchsetzen. Nutzerinnen und Nutzer werden nun klare und präzise Auskunft darüber erhalten, wie die eigenen Daten verarbeitet werden. Datenverarbeiter müssen einfach, verständlich und kostenlos erklären, welche Daten sie in welchen Kontexten und zu welchem Zweck verarbeiten und an wen sie die Daten weitergeben. Nutzungsbedingungen müssen leicht zu verstehen sein. **EU-weit standardisierte Symbole** fassen lange und oft nur für Juristen lesbare Datenschutzerklärungen leicht verständlich und schnell erfassbar zusammen.

4. Datenweitergabe an Drittstaaten: Das Parlament bestand darauf, dass Firmen Daten nicht direkt an Behörden in Drittstaaten weitergeben dürfen. Dies ist nur erlaubt auf der Grundlage von **Rechtshilfeabkommen** oder ähnlicher, auf EU-Recht basierender Regeln. 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. Die Kommission muss nun regelmäßig über Datentransfers in Drittstaaten berichten. Nachdem der Europäische Gerichtshof im Fall Max Schrems zur Weitergabe von Facebook-Daten in die USA „Safe Harbor“ am 6. Oktober 2015 für ungültig erklärt hat, hat das Europäische Parlament weitere Absicherungen und Klärungen verlangt. Auch außerhalb der EU müssen Bürgerinnen und Bürgern, deren Daten weitergeleitet werden, gleiche Rechte zustehen, einschließlich der **Klagemöglichkeit auch im Drittstaat**. Ein Drittstaat kann nicht behaupten, dass es ein gleiches Schutzniveau für alle gibt, wenn er etwa durch **Massenüberwachung** den unverhältnismäßigen Zugriff von Behörden auf personenbezogene Daten im privaten Sektor zulässt, wie die Enthüllungen von Edward Snowden offenbarten.

5. Zukunftstaugliche Definitionen: Alle Informationen, die direkt oder indirekt einer Person zugeordnet werden können, müssen als personenbezogene Daten geschützt werden. 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 werden zu müssen – **es reicht, eine Person wiedererkennen zu können**, zum Beispiel indem sie oder er anhand von Browsermerkmalen als dieselbe Person identifiziert werden kann.

6. Harte Sanktionen: In Fällen von **Verstößen gegen die Verordnung** erwarten Unternehmen harte Sanktionen. Das Parlament setzte in den Verhandlungen eine maximale Höhe von bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens oder 20 Millionen Euro für alle anderen Datenverarbeiter durch. Diese Sanktionen sollen von Datenschutzverstößen abhalten und das Bewusstsein dafür schärfen, dass Verstöße gegen die Verordnung zugleich Verletzungen der Grundrechtecharta der Europäischen Union sind. Natürlich müssen Bußgelder immer verhältnismäßig sein. Daher drohen kleinen Unternehmen keine derart hohen Sanktionen, wenn es sich um erstmalige, versehentliche oder kleinere Verstöße handelt.

7. Privacy by Design / Privacy by Default: Datenverarbeiter müssen ihre Dienste datensparsam konzipieren und mit den datenschutzfreundlichsten Voreinstellungen anbieten. Nur solche Daten dürfen erhoben werden, die zur Erbringung des Dienstes wirklich benötigt werden. Unternehmen dürfen Dienste nicht von der Verarbeitung von Daten abhängig machen, die sie für diesen Dienst gar nicht benötigen. Das bedeutet, dass etwa eine Taschenlampen-App auf dem Smartphone nicht auf die Daten im Adressbuch zugreifen darf. Außerdem muss es möglich sein, Dienste anonym und unter Pseudonym zu nutzen.

8. Weniger Bürokratie: Neben der Reduzierung von 28 verschiedenen Standards auf ein Gesetz für den europäischen Markt sind eine ganze Reihe von Erleichterungen für Unternehmen vorgesehen, speziell für **kleinere Unternehmen.** Die Ernennung eines betrieblichen Datenschutzbeauftragten ist davon abhängig, welche und wie viele Daten verarbeitet werden und nicht davon, wie viel Personal ein Unternehmen beschäftigt. Das Parlament hat klargestellt, dass die oder der Datenschutzbeauftragte keine Vollzeitkraft sein muss und auch ein externer Dienstleister sein kann. Die Mitgliedstaaten können aber strengere Regeln für die Benennung von Datenschutzbeauftragten aufstellen.

9. Einheitliche Rechtsdurchsetzung: Ein Europäischer Datenschutzausschuss, bestehend aus den nationalen Aufsichtsbehörden, soll die einheitliche Anwendung des Datenschutzrechts sicherstellen. In Fällen von europaweiter Bedeutung kann dieser 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. Die Unabhängigkeit der Datenschutzbehörden bleibt gewahrt. Nicht die Kommission wird das letzte Wort haben, sondern der Europäische Datenschutzausschuss, der nun rechtlich verbindliche Entscheidungen für den ganzen Europäischen Markt treffen kann.

10. Ein fester Ansprechpartner für ganz Europa: Der „One-Stop Shop“-Ansatz bedeutet: Bürgerinnen und 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.