

EU-Datenschutzreform: Rat bestätigt Einigung mit dem Europäischen Parlament

Am 18. Dezember 2015 hat der Ausschuss der Ständigen Vertreter (ASV) die mit dem Europäischen Parlament vereinbarten Kompromisstexte zur Datenschutzreform bestätigt. Rat, Parlament und Kommission hatten die Einigung am 15. Dezember erzielt. Mit dieser Einigung wird der Forderung des Europäischen Rates entsprochen, die Verhandlungen über die Datenschutzreform bis Ende 2015 abzuschließen.

Der luxemburgische Justizminister und Präsident des Rates Félix BRAZ erklärte dazu Folgendes: "Es handelt sich um eine grundlegende Einigung mit weitreichenden Folgen. Mit dieser Reform werden nicht nur die Rechte der Bürger gestärkt, sondern auch die Vorschriften für Unternehmen an das digitale Zeitalter angepasst, während gleichzeitig der Verwaltungsaufwand verringert wird. Die Texte sind ambitioniert und zukunftsorientiert. Wir können volles Vertrauen in das Ergebnis haben."

Das Gesetzgebungspaket zur Datenschutzreform wurde 2012 von der Kommission vorgeschlagen; Ziel ist die Aktualisierung und Modernisierung der Datenschutzvorschriften. Das Paket beinhaltet zwei Rechtsakte: die Datenschutz-Grundverordnung (mit der die Richtlinie 95/46/EG ersetzt werden soll) und die Datenschutzrichtlinie im Bereich der Strafverfolgung (die den Datenschutz-Rahmenbeschluss von 2008 ersetzen soll).

Der Datenschutz bei der Verarbeitung personenbezogener Daten ist ein Grundrecht, das in der EU-Grundrechtecharta (Artikel 8) und im Vertrag über die Arbeitsweise der Europäischen Union (Artikel 16) verankert ist.

Datenschutz-Grundverordnung

Mit der Datenschutz-Grundverordnung soll das Datenschutzniveau bei der Verarbeitung personenbezogener Daten erhöht werden; gleichzeitig sollen auch durch die Verringerung des Verwaltungsaufwands mehr Geschäftsmöglichkeiten im digitalen Binnenmarkt geschaffen werden.

Besserer Datenschutz

Die Grundsätze und Regelungen für die Verarbeitung personenbezogener Daten müssen im Einklang mit den Grundrechten und Grundfreiheiten und insbesondere dem Recht auf den Schutz personenbezogener Daten stehen. Betroffene (Personen, deren Daten verarbeitet werden) erhalten durch die Stärkung der Datenschutzrechte mehr Kontrolle über ihre personenbezogenen Daten:

- Damit die für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeiten dürfen, müssen sie spezielle Vorschriften einhalten, wozu auch die notwendige Einwilligung der Betroffenen gehört;
- die Betroffenen erhalten leichteren Zugang zu ihren personenbezogenen Daten;
- es wird besser darüber informiert, was mit den Daten nach ihrer Weitergabe geschieht. So sind die Betroffenen in einer klaren und einfachen Sprache über die Datenschutzmaßnahmen zu informieren, was auch mittels standardisierter Icons erfolgen kann;
- es besteht ein Recht auf Löschung personenbezogener Daten und ein Recht auf "Vergessenwerden". So ist es Betroffenen beispielsweise möglich, die unverzügliche Entfernung personenbezogener Daten zu verlangen, die in einem sozialen Netzwerk noch während ihrer Kindheit erfasst oder veröffentlicht wurden;
- wenn ein Jugendlicher unter 16 Jahren Online-Dienste in Anspruch nehmen möchte, muss der Dienstleister sich darum bemühen zu prüfen, ob die Eltern ihre Einwilligung erteilt haben. Die Mitgliedstaaten können diese Altersgrenze herabsetzen, allerdings nicht unter das Alter von 13 Jahren;
- es besteht ein Recht auf Übertragbarkeit, so dass personenbezogene Daten leichter von einem Dienstleister, etwa einem sozialen Netzwerk, an einen anderen Dienstleister übermittelt werden können. Dies wird nicht nur die Datenschutzrechte stärken, sondern auch zu mehr Wettbewerb zwischen Dienstleistern beitragen;
- der Verarbeitung personenbezogener Daten kann aus Gründen des öffentlichen Interesses oder der berechtigten Interessen eines für die Verarbeitung Verantwortlichen rechtmäßig widersprochen werden. Unter dieses Recht fällt die Verwendung personenbezogener Daten für die Zwecke der "Profilerstellung";
- allgemeine Schutzklauseln regeln die Verarbeitung personenbezogener Daten für die Zwecke der Archivierung, sofern dies im öffentlichen Interesse liegt, sowie für die wissenschaftliche und historische Forschung oder für statistische Zwecke.

Im Hinblick auf einen leichteren Zugang zu Rechtsmitteln haben Betroffene die Möglichkeit, Entscheidungen ihrer

Datenschutzbehörde von ihrem einzelstaatlichen Gericht überprüfen zu lassen, unabhängig davon, in welchem Mitgliedstaat der für die Verarbeitung der Daten Verantwortliche seinen Sitz hat.

Mehr Geschäftsmöglichkeiten im digitalen Binnenmarkt

Mit der Verordnung wird ein unionsweit einheitlicher Rechtsrahmen sowohl für europäische als auch für außereuropäische Unternehmen geschaffen, die Online-Dienstleistungen in der EU anbieten. Damit wird eine Situation verhindert, in der widersprüchliche einzelstaatliche Datenschutzregeln den grenzüberschreitenden Datenaustausch stören könnten. Vorgesehen ist ferner eine intensivere Zusammenarbeit zwischen den Mitgliedstaaten, um sicherzustellen, dass die Datenschutzvorschriften EU-weit kohärent angewandt werden. Damit wird ein fairer Wettbewerb geschaffen und dazu beigetragen, dass Unternehmen, vor allem kleine und mittlere Unternehmen, den größtmöglichen Nutzen aus dem digitalen Binnenmarkt ziehen können.

Um Kosten zu senken und Rechtssicherheit zu schaffen, wird in bedeutenden grenzüberschreitenden Fällen, die mehrere einzelstaatliche Aufsichtsbehörden betreffen, eine einheitliche Aufsichtsentscheidung getroffen. Durch dieses Prinzip der **zentralen Anlaufstelle** wird es einem in mehreren Mitgliedstaaten tätigen Unternehmen ermöglicht, nur mit der Datenschutzbehörde in dem Mitgliedstaat zu verkehren, in dem es seinen Hauptsitz hat. Nach diesem Mechanismus gilt ferner in Streitfällen eine einheitliche Entscheidung für das gesamte Gebiet der EU.

Um die Verwaltungskosten zu senken, sieht die Verordnung einen risikobasierten Ansatz vor: Die für die Verarbeitung Verantwortlichen können Maßnahmen von dem Risiko abhängig machen, das mit den Datenverarbeitungsvorgängen verbunden ist. Verschiedene Unternehmen üben verschiedene Tätigkeiten aus, und entsprechend können auch die damit verbundenen Risiken für den Schutz der Privatsphäre variieren. Die Verordnung sieht keine einheitliche Standardlösung vor: Je höher die mit den Tätigkeiten verbundenen Risiken für die personenbezogenen Daten sind, desto strenger sind die Anforderungen.

Mehr und bessere Instrumente zur Durchsetzung der Einhaltung der Datenschutzvorschriften

Die Verordnung sieht eine Reihe von Maßnahmen für eine höhere Verantwortlichkeit und Rechenschaftspflicht der für die Verarbeitung Verantwortlichen vor, um eine umfassende Einhaltung der neuen Datenschutzvorschriften zu gewährleisten. Die Verantwortlichen müssen eine Reihe von Sicherheitsmaßnahmen anwenden; so sind etwa in bestimmten Fällen Verletzungen des Schutzes personenbezogener Daten zu melden. Um die Verordnung zukunftssicher zu machen, gelten die Grundsätze des Datenschutzes durch Technik und des Datenschutzes durch datenschutzfreundliche Voreinstellungen. Behörden und Unternehmen, die bestimmte riskante Datenverarbeitungen vornehmen, müssen einen **Datenschutzbeauftragten** benennen, der die Einhaltung der Vorschriften überwacht.

Von der Verarbeitung Betroffene sowie unter bestimmten Umständen Datenschutzorganisationen können bei einer Aufsichtsbehörde eine Beschwerde oder bei Gericht einen Rechtsbehelf einlegen, wenn die Datenschutzvorschriften nicht eingehalten werden. Für die Datenverarbeitung Verantwortliche können mit Geldstrafen von bis zu 20 Millionen Euro oder 4 % ihres gesamten Jahresumsatzes belegt werden.

Garantien für die Übermittlung personenbezogener Daten außerhalb der EU

Die Verordnung regelt die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen. Diese Übertragungen sind zulässig, sofern eine Reihe von Bedingungen und Garantien erfüllt sind, insbesondere in den Fällen, in denen die Kommission festgestellt hat, dass ein angemessenes Schutzniveau gegeben ist. Neue Angemessenheitsbeschlüsse sind mindestens alle vier Jahre zu überprüfen. Bestehende Angemessenheitsbeschlüsse und Genehmigungen bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

Die Datenschutzrichtlinie im Bereich der Strafverfolgung

Diese Richtlinie soll den Schutz personenbezogener Daten gewährleisten, die zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und zur Strafvollstreckung – wozu auch der Schutz vor und die Abwehr von Bedrohungen der öffentlichen Sicherheit gehört – verarbeitet werden.

Es ist von entscheidender Bedeutung, einen durchweg hohen Schutz der personenbezogenen Daten natürlicher Personen zu gewährleisten und dabei den Austausch personenbezogener Daten zwischen den Strafverfolgungsbehörden der einzelnen Mitgliedstaaten zu erleichtern.

Weiter reichender Geltungsbereich

Zusätzlich zur Erfassung von Tätigkeiten, die darauf abzielen, Straftaten zu verhüten, zu untersuchen, aufzudecken und zu verfolgen, wurde die neue Richtlinie auf den Schutz vor und die Abwehr von Bedrohungen der öffentlichen Sicherheit ausgeweitet.

Die neue Richtlinie würde nicht nur für die grenzüberschreitende Verarbeitung von personenbezogenen Daten gelten, sondern auch für die Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden auf rein nationaler Ebene. Der zu

ersetzende Rahmenbeschluss umfasste lediglich den grenzübergreifenden Datenaustausch.

Rechte der betroffenen Person

Die Vorschriften stellen ein Gleichgewicht her zwischen dem Recht auf Privatsphäre und der polizeilichen Notwendigkeit, nicht zu einem frühen Zeitpunkt der Untersuchung bekannt zu machen, dass Daten verarbeitet werden. In dem Text wird jedoch ausgeführt, welche Informationen der Betroffene jederzeit erhalten kann, um seine Rechte zu schützen, wenn er befürchtet, dass seine Daten verletzt worden sind.

Auch die Weitergabe personenbezogener Daten an Drittländer und internationale Organisationen wird durch die neuen Vorschriften erfasst.

Einhaltung

In der neuen Richtlinie wird festgelegt, dass ein **Datenschutzbeauftragter** zu benennen ist, der die zuständigen Behörden dabei unterstützt, die Einhaltung der Datenschutzvorschriften zu gewährleisten.

Ein weiteres Instrument zur Gewährleistung der Einhaltung ist die Folgenabschätzung. Wenn eine bestimmte Art der Verarbeitung aller Voraussicht nach ein hohes Risiko für die Rechte und Freiheiten von Personen beinhaltet, müssen die zuständigen Behörden eine Abschätzung der möglichen Folgen des Vorgangs vornehmen, insbesondere im Falle der Anwendung neuer Technologien.

Überwachung und Schadenersatz

Der Wortlaut der Richtlinie ist an den der Verordnung angepasst, um zu gewährleisten, dass generell die gleichen allgemeinen Grundsätze zur Anwendung kommen. Darüber hinaus sind die Vorschriften über die Aufsichtsbehörde weitgehend ähnlich, da die durch die Datenschutz-Grundverordnung eingerichtete Aufsichtsbehörde sich auch mit Angelegenheiten befassen kann, die unter die Richtlinie fallen. Nach der neuen Richtlinie hätten die betroffenen Personen zudem Anspruch auf Schadenersatz, wenn sie wegen einer rechtswidrigen Verarbeitung ihrer Daten einen Schaden erlitten haben.

WEITERES VORGEHEN

Am 17. Dezember hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments in einer außerordentlichen Sitzung die in den Trilogen beschlossenen Texte bestätigt. Diese Unterstützung versetzte den AStV heute in die Lage, den endgültigen Kompromisstexten von Verordnung und Richtlinie zuzustimmen. Nach der Überarbeitung durch die Rechts- und Sprachsachverständigen werden die Texte dem Rat und anschließend dem Parlament zur Annahme vorgelegt. Die Verordnung und die Richtlinie werden voraussichtlich im Frühjahr 2018 in Kraft treten.

Press office - General Secretariat of the Council of the EU

Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319

press@consilium.europa.eu - www.consilium.europa.eu/press