ARTIKEL-29-DATENSCHUTZGRUPPE

1470/14/DE
WP 222

Erklärung zu den Ergebnissen der letzten Tagung des Rates „Justiz und Inneres“ (JI)

Angenommen am 17. September 2014

Hintergrund

Während der letzten Tagung des Rates „Justiz und Inneres“ (JI) vom 5. und 6. Juni hat der Rat der EU eine allgemeine Ausrichtung zu spezifischen Aspekten des Entwurfs einer Datenschutzverordnung erzielt.

Diese Ausrichtung umfasst die folgenden Aspekte:

- die Bestimmungen über den räumlichen Anwendungsbereich, Artikel 3 Absatz 2,

- die Definitionen der Begriffe „verbindliche unternehmensinterne Datenschutzvorschriften“ und „internationale Organisationen“ (Artikel 4 Absätze 17 und 21) und

- die Bestimmungen über die Übermittlung personenbezogener Daten an Drittstaaten oder internationale Organisationen (Kapitel V).

Die nach Artikel 29 eingesetzte Datenschutzgruppe (im Folgenden die „Gruppe“) begrüßt diese Einigung, da sie eine wichtige Etappe in Richtung eines umfassenden EU-Rahmens für Datenschutz darstellt. Die Gruppe möchte die Bedeutung einer Reihe von Optionen zur Ermöglichung von Datenübermittlungen betonen. Sie ist jedoch nach wie vor besorgt über die Auswirkungen auf die Ressourcen der Datenschutzbehörden, falls der Prozess betreffend die neuen Instrumente für die Übermittlung nicht ausreichend gefördert oder ermöglicht wird. Vor dem Hintergrund der bevorstehenden Verhandlungen möchte die Gruppe ihre Ansichten über diese allgemeine Ausrichtung äußern.

1. Räumlicher Anwendungsbereich

Dem Kompromisstext zufolge findet die Verordnung Anwendung auf einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung

a) dazu dient, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist, oder

b) der Beobachtung ihres Verhaltens dient, soweit ihr Verhalten in der Europäischen Union erfolgt.

Darüber hinaus enthält Erwägungsgrund 20 zusätzliche Spezifikationen, um zu bestimmen, ob ein für die Verarbeitung Verantwortlicher betroffenen Personen in der Union Waren oder Dienstleistungen anbietet. So soll beispielsweise geprüft werden, ob der für die Verarbeitung Verantwortliche offensichtlich beabsichtigt, mit in einem oder mehreren Mitgliedstaaten der Union ansässigen Personen Geschäfte zu machen (z. B. Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist).

Die Gruppe begrüßt diese Bestimmungen, da sie nicht nur den räumlichen Anwendungsbereich festlegen, sondern auch die Notwendigkeit unterstreichen, die Anwendung der EU-Vorschriften auf nicht in der Union niedergelassene für die Verarbeitung Verantwortliche, die personenbezogene Daten von betroffenen Personen in der Union verarbeiten, weitestgehend

sicherzustellen. Der Wortlaut spiegelt auch die in einer früheren Stellungnahme (WP191/Stellungnahme 01/2012) geäußerten Ansichten der Gruppe wider.

Die Gruppe möchte allerdings darauf hinweisen, dass gemäß dem Vorschlag des Europäischen Parlaments auch nicht in der Union niedergelassene Auftragsverarbeiter (Artikel 3 Absatz 1) erfasst sein sollten, wenn die Verarbeitung auf Unionsbürger abzielt.

2. Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (Kapitel V)

Anwendung verbindlicher unternehmensinterner Datenschutzvorschriften (BCR)

Gemäß Artikel 43 Absatz 1 Buchstabe a gelten die BCR für „alle Mitglieder" der Unternehmensgruppe. Die Gruppe empfiehlt den Wortlaut durch „alle betreffenden Mitglieder" zu ersetzen, da nicht alle Unternehmen innerhalb der Unternehmensgruppe Daten übermitteln oder es auch sein kann, dass die BCR nicht für alle Unternehmen innerhalb der Unternehmensgruppe gelten sollen.

Einführung neuer Instrumente als Rahmen für Übermittlungen

Laut Kompromisstext (Artikel 42 Absatz 2) dürfen personenbezogene Daten an ein Drittland übermittelt werden, sofern der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien wie BCR, Standarddatenschutzklauseln usw. vorgesehen hat. Diese Garantien können auch genehmigte Verhaltensregeln, genehmigte Zertifizierungsmechanismen sowie rechtsverbindliche und durchsetzbare Instrumente zwischen den staatlichen Behörden und Stellen umfassen.

Die genehmigten Verhaltensregeln bzw. die genehmigten Zertifizierungsmechanismen sollten seitens des nicht in der Union ansässigen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters eingegangene verbindliche und durchsetzbare Verpflichtungen enthalten, damit der Schutz personenbezogener Daten, die aus der EU stammen, gewährleistet ist.

Zudem gibt es eine Zweiteilung zwischen geeigneten Garantien, die keiner besonderen Genehmigung einer Aufsichtsbehörde bedürfen (BCR, Standarddatenschutzklauseln, rechtsverbindliche und durchsetzbare Instrumente zwischen den staatlichen Behörden und Stellen, genehmigte Verhaltensregeln und genehmigte Zertifizierungsmechanismen), sowie geeigneten Garantien, die einer Genehmigung durch die zuständige Aufsichtsbehörde bedürfen (insbesondere Vertragsklauseln, die nicht auf vereinbarten Standardvertragsklauseln beruhen, und Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen).

1) Bemerkungen im Hinblick auf die Möglichkeit, Übermittlungen durch rechtsverbindliche und durchsetzbare Instrumente zwischen den staatlichen Behörden oder Stellen einen rechtlichen Rahmen zu geben

Die Gruppe begrüßt diese Bestimmung, da sie nicht nur die üblichen Garantien, auf die aller Wahrscheinlichkeit nach der private Sektor zurückgreift (z. B. BCR, Standarddatenschutzklauseln), und Ausnahmeregelungen für die Datenübertragung im

öffentlichen Sektor vorsieht, sondern auch die Möglichkeit, Übermittlungen zwischen staatlichen Behörden oder Stellen zu regeln.

In einigen Fällen ist jedoch die Notwendigkeit zu rechtfertigen, sich auf Regelungen zu stützen, die darauf abzielen, rechtlich und faktisch so verbindlich wie möglich zu sein, ohne förmlich diese Verbindlichkeit aufzuweisen.

2) Bemerkungen im Hinblick auf die Möglichkeit, Übermittlungen durch genehmigte Verhaltensregeln oder genehmigte Zertifizierungsmechanismen einen rechtlichen Rahmen zu geben

Die Gruppe begrüßt, dass genehmigte Verhaltensregeln oder genehmigte Zertifizierungsmechanismen rechtsverbindliche und durchsetzbare Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in dem Drittland enthalten. Heute sind verbindliche Instrumente für die Regelung internationaler Datenübermittlungen erforderlich. Mit dem Vorhandensein von Angemessenheitsbeschlüssen, der Verfügbarkeit von Standard- und Ad-hoc-Vertragslösungen und der neuen Kodifizierung verbindlicher unternehmensinterner Datenschutzvorschriften lässt sich nur noch schwer begründen, warum die Datenübermittlung im privaten Sektor auf der Grundlage unverbindlicher Instrumente erfolgen soll. Es würde dem gemeinsamen Besitzstand zuwiderlaufen, geeignete Garantien in Betracht zu ziehen, die nicht in einem rechtsverbindlichen Instrument vorgesehen sind.

Außerdem sollte die Möglichkeit, genehmigte Zertifizierungsmechanismen oder genehmigte Verhaltensregeln als rechtlichen Rahmen für Datenübermittlungen einzuführen, unbedingt im Einklang mit den Artikeln 38 und 39 des Verordnungsentwurfs stehen und gesetzlich festgelegt werden.

Wie bereits in einer früheren Stellungnahme dargelegt, befürwortet die Gruppe die Förderung der Zertifizierung, fordert jedoch die Aufnahme einer besseren Definition und Beschreibung der Elemente des Zertifizierungsverfahrens.

Die Gruppe ist der Auffassung, dass die Zertifizierung ein angemessenes Instrument ist, um die Einhaltung der Vorschriften sicherzustellen und zu garantieren, dass die internen Grundsätze und Verfahren zum Schutz der Privatsphäre umgesetzt werden und effizient und zuverlässig sind.

Nach Auffassung der Gruppe sollte der Anwendungsbereich der Zertifizierungsmechanismen für die internationale Datenübermittlung spezifiziert werden, um die Wechselwirkungen mit anderen bestehenden Instrumenten wie BCR und Vertragsklauseln klarzustellen.

Die Gruppe möchte überdies nochmals betonen, dass jegliches Zertifizierungssystem die Aufsichtsfunktion und die Unabhängigkeit der Datenschutzbehörden nicht beeinträchtigen darf. Folgende Situation ist zu vermeiden: Im Falle eines Verstoßes seitens des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters hat die Aufsichtsbehörde vor Erwägung sonstiger Maßnahmen zunächst nachzuweisen, dass dieser Verstoß auf eine Abweichung von dem zertifizierten Modell zurückzuführen ist. Dies würde in vielen Fällen die Durchsetzung sehr erschweren, wenn nicht sogar unmöglich machen.

Anstelle der Zertifizierung einzelner Unternehmen würde die Gruppe einen Mechanismus vorziehen, für den die Aufsichtsbehörden und/oder der Europäische Datenschutzausschuss (EDPB) Leitlinien bereitstellen, indem Anforderungen und Garantien festgelegt werden, denen Zertifikationssysteme genügen müssen. In der Folge sollten die Aufsichtsbehörden oder der EDPB eng in den Prozess der Akkreditierung der Zertifizierungsstellen eingebunden sein.

Darüber hinaus sollten die Kriterien für die Akkreditierung der Zertifizierungsstelle spezifiziert werden; diese könnten sich an bestehenden Anforderungen in anderen Sektoren wie Umweltschutz, Sicherheit, Landwirtschaft und Gesundheitswesen oder an internationalen Normen (ISO/IEC 17011) orientieren. Zu den Kriterien können gehören:

- Berufliche Kompetenz: Die Zertifizierungsstelle verfügt über eine ausreichende Zahl kompetenter Mitarbeiter (intern, extern, befristet oder unbefristet, in Vollzeit oder Teilzeit), die über die Ausbildung, Schulung, Fachkenntnisse, Fähigkeiten und Erfahrung verfügen, die zur Wahrnehmung der Aufgaben erforderlich sind.

- Unparteilichkeit: Die Zertifizierungsstelle besitzt eine Organisationsstruktur, die die Objektivität und Unparteilichkeit ihrer Tätigkeiten garantiert.

- Interessenkonflikt: Die Zertifizierungsstelle muss frei von tatsächlichen oder potenziellen Interessenkonflikten sein.

- Vertraulichkeit: Die Zertifizierungsstelle trifft geeignete Vorkehrungen, um die vertrauliche Behandlung der erhaltenen Informationen sicherzustellen.

- Haftung und Finanzierung: Die Zertifizierungsstelle muss aus ihren Tätigkeiten entstehende Haftungsansprüche decken und über ausreichende finanzielle Mittel verfügen.

Wenn die Zertifizierungsstelle Antragsteller ungerechtfertigt zertifiziert, sollten Verwaltungsgeldstrafen über die Stelle verhängt und ihr die Zertifizierung entzogen werden.

Damit eine echte Kohärenz und ein einheitliches hohes Schutzniveau bei allen umgesetzten Instrumenten gewährleistet ist, ist es von entscheidender Bedeutung, dass die gleichen Interessenträger Voraussetzungen für die Datenübermittlung (für BCR, Vertragsklauseln, Verhaltensregeln und Zertifizierungsmechanismen) festlegen. Darüber hinaus sollten die Aufsichtsbehörden und der EDPB eindeutig an der Entwicklung der von den Zertifizierungsstellen zu verwendenden Referenzgrundlage mitwirken. Im Zuge der Entwicklung einer solchen Referenzgrundlage könnten auch externe Interessenträger konsultiert werden.

In jedem Fall muss unabhängig von den verwendeten Instrumenten (BCR, Standardvertragsklauseln, Safe-Harbour-Regelung usw.) das gleiche Schutzniveau gewährleistet werden, um Inkohärenzen und Verstöße im Hinblick auf das Schutzniveau außerhalb der EU zu vermeiden.

Möglichkeit, bei wichtigen Gründen des öffentlichen Interesses die Datenübermittlung zu beschränken

Der Text sieht ausdrücklich die Möglichkeit vor, aus wichtigen Gründen des öffentlichen Interesses die Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer zu beschränken (Artikel 44 Absatz 5a). Entsprechende nationale Maßnahmen der Mitgliedstaaten sind der Europäischen Kommission mitzuteilen.

Angesichts der Enthüllungen zu Überwachungsprogrammen von Behörden der nationalen Sicherheit begrüßt die Gruppe diese Bestimmung.

Allerdings könnte der Verweis auf das öffentliche Interesse weit ausgelegt werden (wird beispielsweise der Begriff der nationalen Sicherheit abgedeckt?). Ferner scheint diese Bestimmung keinen ausreichenden tatsächlichen und wirksamen Schutz der europäischen Bürger sicherzustellen. Sie muss daher präzisiert werden. Die in dem neuen Artikel 43a des Europäischen Parlaments vorgesehenen Bestimmungen könnten diesbezüglich nützlich sein.

In dem vorgeschlagenen Artikel 43a hat das Europäische Parlament die Verpflichtung eingeführt, natürliche Personen zu informieren, wenn ein für die Verarbeitung Verantwortlicher einer öffentlichen Behörde eines Drittlandes in den letzten 12 Monaten Zugang zu ihren Daten gewährt hat. Zudem ist die Verpflichtung vorgesehen, vor der Datenübermittlung die Genehmigung der Aufsichtsbehörde einzuholen. Transparenz in Bezug auf diese Verfahren wird das Vertrauen erheblich stärken.

Wie den Bemerkungen der Gruppe anlässlich der Abstimmung im LIBE-Ausschuss am 21. Oktober 2013 zu entnehmen (diese wurden am 11.12.2013 veröffentlicht), wurde es als äußerst wichtig angesehen, dass parallel zu diesem Vorschlag ein internationales Abkommen – insbesondere zwischen der EU und den USA – geschlossen wird, damit ein tragfähiger und solider Schutzrahmen entsteht. Daher sollte die für den Antrag einer Behörde eines Drittlandes auf Zugang zu personenbezogenen Daten zuständige Aufsichtsbehörde die für den Antrag zuständige nationale Behörde in der EU und nicht die Datenschutzbehörde sein.

Beibehaltene Ausnahmeregelung in Bezug auf die berechtigten Interessen des für die Verarbeitung Verantwortlichen

Ungeachtet der Datenübermittlungen auf der Grundlage eines Angemessenheitsbeschlusses der Kommission oder geeigneter Garantien (BCR, Vertragsklauseln, Verhaltensregeln usw.), die für den öffentlichen und den privaten Sektor gelten, können Übermittlungen auch auf der Grundlage der in Artikel 44 aufgeführten Ausnahmen erfolgen. Gemäß der Ausnahme nach Artikel 44 Absatz 1 Buchstabe h sind Datenübermittlungen auf der Grundlage der berechtigten Interessen des für die Verarbeitung Verantwortlichen zulässig, sofern

- die Übermittlung nicht in großem Maßstab oder häufig erfolgt,

- die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen und

- der für die Verarbeitung Verantwortliche geeignete Garantien vorgesehen hat, wie in Erwägungsgrund 88 näher erläutert.

Gruppe begrüßt diese Bestimmung, da sie ihrem bereits früher geäußerten Standpunkt (Stellungnahme 1/2012 und Erklärung vom 27. Februar 2013), dem zufolge eine derartige Ausnahme nur ausnahmsweise für Übermittlungen gelten darf, die nicht groß angelegt, nicht regelmäßig und nicht systematisch sind.

Die Gruppe weist erneut darauf hin, dass die Rechtsverbindlichkeit eines der wichtigsten Erfordernisse für internationale Übermittlungsinstrumente im Zusammenhang mit der Gewährleistung geeigneter Garantien für die betroffenen Personen ist. Darüber hinaus sollte die Selbsteinschätzung für Übermittlungen an Drittländer in Abweichung von geeigneten Garantien sehr beschränkt sein.

In diesem Zusammenhang wird in Erwägungsgrund 87 die Verringerung und/oder Beseitigung des Dopings im Sport als ein gewichtiger Grund des öffentlichen Interesses erwähnt. Die Gruppe stellt die Möglichkeit, dem Kampf gegen Doping im Sport einen derartigen Stellenwert einzuräumen, in Frage, zumal sie eine internationale Datenübermittlung an ein Drittland ohne weitere Garantien erlaubt. Da die fraglichen Daten sehr sensibler Art sein können, ist die Gruppe der Auffassung, dass die Übermittlung solcher Daten weiterhin den für alle internationalen Übermittlungen geltenden gemeinsamen Grundsätzen unterliegen sollte.