Axel Spies

Anmerkungen zum Positionspapier der deutschen Datenschutzbeauftragten zu Safe Harbor

ZD-Aktuell 2015, 04869

Die deutschen Datenschutzbehörden haben auf die Stellungnahme der *Art. 29-Datenschutzgruppe* (*Spies*, ZD-Aktuell 2015, 04855; *Wybitul*, ZD-Aktuell 2015, 04856) am 26.10.2015 zu den Konsequenzen der *EuGH*-Entscheidung v. 6.10.2015 in Sachen *Schrems* (ZD 2015, 549 m. Anm. *Spies*) zügig reagiert. Die 16 Punkte des neuen Positionspapiers der *Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder* dienen als weitere Grundlage für das Vorgehen der deutschen Behörden bis Ende Januar 2016. Die meisten Punkte, wie die Aufforderung an die *Kommission* und „die Datenschutzbehörden", das Datenschutzniveau (Rechtslage und Rechtspraxis) in den USA auf Herz und Nieren zu prüfen, sollten niemanden überraschen.

In dem Positionspaper finden die betroffenen Unternehmen einige Besonderheiten. Drei Punkte fallen besonders in Auge:

- **Punkt 7:** Die Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf der Grundlage von Binding Corporate Rules (BCRs) oder Datenexportverträgen erteilen. Bestehende BCRs können damit weiter genutzt werden – so weit, so gut. Was wird aber mit neuen BCRs? Die *Art. 29-Datenschutzgruppe* hat festgestellt: „During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used." Die deutschen Behörden scheinen hingegen neue BCRs mit US-Bezug nicht genehmigen zu wollen. Ob Unternehmen neue BCRs mit US-Bezug, die andere EU-Datenschutzbehörden genehmigen, dann in Deutschland nutzen werden können, ist fraglich.
- **Punkt 9:** Die Einwilligung der Betroffenen zum Transfer personenbezogener Daten kann nur „unter engen Bedingungen" eine tragfähige Grundlage sein. Der Datentransfer darf nicht „wiederholt, massenhaft oder routinemäßig erfolgen." Diese Kriterien erinnern an die Stellungnahme der französischen Datenschutzbehörde *CNIL* von 2009 zur Datenübermittlung zu Zwecken der Rechtsverfolgung (e-Discovery) in den USA. Im BDSG sind die Kriterien nicht erwähnt. Die enge Auslegung steht mit dem Leitbild eines mündigen Bürgers, der über sein Recht auf informationelle Selbstbestimmung verfügen darf, wohl kaum im Einklang. Sie führt für die Unternehmen zu massiven Umsetzungsproblemen, wenn z.B. vor jedem Datentransfer die Einwilligung konkret neu eingeholt werden muss. Nach der Formulierung des Punkts 9 zu urteilen sind auch nicht nur die Datentransfers in die USA davon betroffen. Die Beschränkungen für die deutschen Individualeinwilligungen gelten allgemein, d.h. weltweit.
- **Punkt 12**: Die *EU-Kommission* soll „zeitnah" ihre Entscheidungen zu den EU-Standardvertragsklauseln an die im *EuGH*-Urteil gemachten Vorgaben „anpassen." Das ist wohl so zu verstehen, dass eine solche Anpassung (wie immer sie aussehen soll) bis zum 31.1.2016 erfolgen muss. Wer die Genese der Standardvertragsklauseln kennt, weiß, dass eine Änderung auf EU-Ebene kompliziert und zeitraubend ist. Nationale Alleingänge oder ein „Draufsatteln" von Zusatzbedingungen für den Export sind wenig zielführend. So oder so: International tätige Unternehmen müssen ab sofort damit rechnen, die Standardklauseln in ihrer seit vielen Jahren bestehenden Form nicht mehr nutzen zu können. Dies wird massive Konsequenzen haben: Für viele Unternehmen sind die Standardklauseln nach dem *EuGH*-Urteil der einzige praktisch gangbare Weg, um Daten im Einklang mit EU-Recht exportieren zu können. Sofern die Datenimporteure in den USA unter Safe Harbor registriert waren, besteht das Zusatzrisiko, dass die Exporteure die übermittelten Daten wieder zurückholen oder löschen lassen müssten. Schwerwiegender noch: Bestehende Vertragsbeziehungen müssten im Einzelfall beendet werden (das ist zumindest die Auffassung des *LfDI für Rheinland-Pfalz* in seiner Stellungnahme (ZD-Aktuell 2015, 04870) zu Safe Harbor, ebenfalls v. 26.10.2015, dort unter Punkt 7).

Unter dem Strich betrachtet ist es zu begrüßen, dass sich die Behörden zumindest im Rahmen der 16 Punkte auf eine einheitliche Linie bis zum 31.1.2016 geeinigt haben. Ob es bis dahin zu einem großen Wurf, wie ein Safe Harbor 2.0 kommt, ist zweifelhaft – trotz einiger optimistischer Aussagen der federführenden EU-Kommissarin *Jourová*. Zurzeit baut sich in Washington ein neues Hindernis für Safe Harbor 2.0 auf, da der *US-Senat* am 27.10.2015 den Cybersecurity Information Sharing Act (CISA) verabschiedet hat. Die endgültige Abstimmung über CISA zwischen den *Kammern* des Kongresses steht noch aus, aber viele europäische Beobachter befürchten, dass CISA zu einem neuen Datenabfluss zu Gunsten der US-Behörden führt. Es ist auch keineswegs gesichert, dass bis zum 31.1.2016 der Judicial Redress Act, der gar nicht für Safe Harbor, sondern für das EU/US-Umbrella Agreement zu Gunsten der Zusammenarbeit der Strafverfolgungsbehörden gedacht war, in Kraft tritt. Viele bezweifeln, dass der Judicial Redress Act (Ziel: mehr Rechtsschutz für EU-Bürger vor US-Gerichten nach dem US Privacy Act von 1974) ausreicht, um den strengen Vorgaben des *EuGH* in voller Höhe Rechnung zu tragen.

Auch nach der Stellungnahme bleibt das Risiko bestehen, dass einige deutsche Datenschutzbehörden aus der Reihe tanzen. Der *LfDI für Rheinland-Pfalz* z.B. behauptet in der o.g. Stellungnahme (a.a.O.): „Eine Übermittlung von personenbezogenen Daten in die USA ist nur noch ausnahmsweise zulässig (§ 4c BDSG). Solche Übermittlungen bedürfen, abgesehen von den Sonderfällen des § 4c Abs. 1 BDSG, der ausdrücklichen Genehmigung des LfDI RLP. ... Er wird soweit möglich die verantwortlichen Stellen auf Alternativen zu Datenverarbeitungen in den USA hinweisen, also auf Dienstleister, die Datenverarbeitungen ausschließlich innerhalb der EU oder in Staaten mit angemessenem Datenschutzniveau vornehmen."

Ob sich konkurrierende Unternehmen solche verkaufsfördernden Maßnahmen der Behörde klaglos gefallen lassen werden, bleibt abzuwarten. Es ist durchaus möglich, dass in Zukunft die einzelnen Gerichte über diese Fragen urteilen müssen. Deren Entscheidungen werden vermutlich EU-weit divergieren. Die Gefahr einer weiteren Zersplitterung des internationalen Datenschutzes ist durchaus greifbar.

■ Vgl. auch ZD-Aktuell 2015, 04867; ZD-Aktuell 2015, 04862; *Spies*, ZD-Aktuell 2015, 04869; ZD-Aktuell 2015, 04858; ZD-Aktuell 2015, 04860; *Schröder* (Editorial), ZD 2015, 501; ZD-Aktuell 2015, 04850; *Spies*, ZD 2013, 535; *ders.*, ZD-Aktuell 2013, 03608 und *Jensen*, ZD-Aktuell 2014, 04284.

Dr. Axel Spies
ist Rechtsanwalt bei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der ZD.