Zeitschrift für Datenschutz – ZD
www.zd-beck.de

Anke Zimmer-Helfrich | Chefredakteurin
RAin Katharina Joachim | Redakteurin
Karin Löscher, M.A. | Redaktionsassistentin

ZD FOKUS

Axel Spies USA und Schweiz einigen sich auf neuen Swiss-US-Privacy-Shield

ZD-Aktuell 2017, 04226

Beide Länder haben sich am 11.1.2017 auf neue Regelungen für den Datentransfer aus der Schweiz in die USA geeinigt (Swiss-US-Privacy-Shield). Dieser Schritt wurde erforderlich, weil der seit August 2016 bestehende EU-US-Privacy-Shield nicht die Schweiz abdeckt. Das Schweizer Safe Harbor war nicht direkt von dem Schrems-Urteil des *EuGH* (ZD 2015, 549 m. Anm. *Spies*) betroffen, weil die Schweiz kein EU-Mitglied ist. Gleichwohl hat die Regierung in der Schweiz mit guten Gründen darauf bestanden, nach einer Übergangszeit die Safe Harbor-Regelungen für die Schweiz (Swiss Safe Harbor) auf das Niveau des EU-US-Privacy-Shield (ZD-Aktuell 2016, 05235) anzuheben.

Der *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)* hat hierzu eine Presseerklärung veröffentlicht und führt zu diesem Punkt aus: „Mit dem Privacy Shield gelten damit für die schweizerischen Exporte von Personendaten in die USA die gleichen Standards wie für diejenigen aus der EU. Dies ist für die Rechtssicherheit im Wirtschaftsverkehr und insbesondere auch für den freien Datenaustausch zwischen der Schweiz und der EU – gerade im kommerziellen Bereich – elementar." Der *EDÖB* hatte nach der Schrems-Entscheidung in einer Mitteilung vom 28.6.2016 auf einem Swiss-US-Privacy-Shield anstelle von Swiss Safe Harbor bestanden, da Swiss Safe Harbor zur Absicherung des gleichwertigen Datenschutzniveaus in den USA ungenügend sei. Einige letzte technische Details seien noch offen. Sobald die offenen Punkte geklärt seien, würde der Swiss-US-Privacy-Shield nach 90 Tagen am 12.4.2017 in Kraft treten.

Der *Schweizer Bundesrat* und das *US Department of Commerce* werden die Einzelheiten zum Swiss-US-Privacy-Shield noch veröffentlichen. Das *US Department of Commerce* hat bereits sein Schreiben mit dem Privacy Shield Framework (Swiss-US-Privacy-Shield-Principles) und einigen Begleitschreiben ins Netz gestellt. Einer ersten Analyse zufolge scheinen die Swiss-US-Privacy-Shield-Principles und die EU-US-Privacy-Shield-Principles vom letzten Jahr in den wesentlichen Punkten wortgleich zu sein.

Für die beteiligten Parteien (alle Datenimporteure in den USA und Datenexporteure in der Schweiz) gibt es einige Dinge zu beachten. Zum Beispiel können sie nicht davon ausgehen, dass ihre Registrierungen (ihre genehmigten Privacy Statements etc.) nach dem EU-US-Privacy-Shield automatisch für die Schweiz gelten. Die Registrierungen für Datenflüsse aus der Schweiz sind getrennt zu behandeln. Nicht alle Datenflüsse aus der Schweiz können mit dem neuen Privacy Shield in die USA geleitet werden, wie schon nach EU-US Safe Harbor. Des Weiteren wird das *NTIA* die bestehenden Swiss Safe Harbor-Zertifizierungen nicht einfach zu Gunsten des Swiss-US-Privacy-Shield fortschreiben. Das bedeutet, dass die Datenimporteure sich neu unter dem Privacy Shield in den USA registrieren müssen, wenn sie ihn mittels einer Self Certification nutzen wollen. Verglichen mit Safe Harbor führt dieser Schritt zu einer Reihe von neuen internen und externen Verpflichtungen, die schon für den EU-US-Privacy-Shield relevant sind: Neue Vorschriften zur Dispute Resolution müssen beachtet und in das Privacy Shield-Statement eingearbeitet werden. Die Anforderungen an die Datenschutzerklärung (Privacy Shield-Notice) sind viel strenger als unter Safe Harbor. Wesentliche neue Anforderungen werden drittens in Bezug auf die Datenweiterleitung an Dritte (Onward Transfer) eingeführt. Insbesondere muss das unter dem Privacy Shield zertifizierte Unternehmen Verträge mit Drittanbietern abschließen, an die es Daten überträgt, wobei der Drittanbieter verpflichtet ist, dasselbe Schutzniveau wie die Privacy Shield-Principles zu gewährleisten und die Daten nur für begrenzte und spezifische Zwecke zu verarbeiten.

Die Beschwerdemöglichkeiten und die Vollstreckungs- und Haftungsverpflichtungen werden im Vergleich zu Safe Harbor durch den Swiss-US-Privacy-Shield erheblich gestärkt und an das EU-US-Privacy-Shield angeglichen: Die Betroffenen haben das Recht, Beschwerden direkt an unabhängige Streitbeilegungsgremien zu richten, sie können sich auch an die nationalen Datenschutzbehörden wenden, insb. wenn HR-Daten verarbeitet werden. Das *US-Handelsministerium* hat sich auch verpflichtet, Beschwerden über die Nichteinhaltung der Privacy Shield-

Grundsätze durch eine Organisation zu entscheiden. Die Betroffenen können als letztes Mittel ein verbindliches Schiedsverfahren durch ein „Privacy Shield-Panel" in die Wege leiten.
Die Datenimporteure und -exporteure tun gut daran, die Regelungen zum Swiss-US-Privacy-Shield mit denen des EU-US-Privacy-Shield genau zu vergleichen, bevor sie eine Entscheidung treffen. Ob es irgendwelche Übergangsfristen für Datenflüsse aus der Schweiz gibt, um die Zertifizierung des Onward Transfers unter dem EU-US-Privacy-Shield durch den Datenimporteur auf den neuesten Stand zu bringen, ist unklar. Fest steht: Die Vereinbarung mit der Schweiz füllt eine Lücke im internationalen Datenschutz. Allerdings steht zu befürchten, dass das *US-Handelsministerium* auf Grund der zusätzlichen Arbeitsbelastung noch langsamer arbeitet, um Self Certifications und Privacy Statements durchzusehen, Änderungen einzufordern und dann auf der Webseite zu veröffentlichen. Bislang sind unter dem EU-US-Privacy-Shield rd. 1.400 Unternehmen zertifiziert, die zusätzlich zu den neu hinzukommenden Datenimporteuren individuell eine Entscheidung treffen müssen, ob sie sich auch für die Schweiz unter den Swiss-US-Privacy-Shield eintragen lassen.

■ Vgl. zum EU-US-Privacy-Shield *Spies*, ZD-Aktuell 2016, 05235; ZD Aktuell 2016, 05230; ZD-Aktuell 2016,05233: *Weichert*, ZD 2016, 209; *Smagon*, ZD 2016, 55; *Schreiber/Kohm*, ZD 2016, 255 sowie *Molnár-Gábor/Kaffenberger*, ZD 2017, 18.

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

BVerwG: Klage gegen BND erfolglos

ZD-Aktuell 2017, 05432

Das *BVerwG* hat (U. v. 14.12.2016 – 6 A 9.14 und 6 A 9.15; ZD wird die Entscheidung demnächst veröffentlichen) über die Zulässigkeit von Klagen verhandelt, mit denen sich ein Rechtsanwalt und der Verein „Reporter ohne Grenzen" gegen die strategische Überwachung von E-Mail-Verkehr durch den *BND* und die Speicherung und Nutzung von Metadaten in dem System VERAS des *BND* gewandt haben.
Nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz – G10) ist der *BND* im Rahmen seiner Aufgaben berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen. Bei der strategischen Fernmeldeüberwachung werden bestimmte internationale TK-Beziehungen anhand vorher festgelegter Suchbegriffe durchsucht. Die Kl. haben die Feststellung beantragt, dass der *BND* durch die Überwachung von E-Mail-Verkehr im Rahmen der strategischen Fernmeldeüberwachung in den Jahren 2012 bzw. 2013 ihr Fernmeldegeheimnis aus Art. 10 GG verletzt hat. Das *BVerwG* hat diese Klagen als unzulässig abgewiesen und damit eine Entscheidung aus dem Jahr 2014 zu einem anderen Überwachungszeitraum im Ergebnis bestätigt.
Nach der VwGO muss sich die Feststellungsklage auf einen konkreten, gerade den jeweiligen Kl. betreffenden Sachverhalt beziehen – ein solcher war nicht feststellbar. Unter den Verkehren, die der *BND* in dem Zeitraum als nachrichtendienstlich relevant behandelt hat, befände sich kein E-Mail-Verkehr der Kl. Zwar sei dies nicht auszuschließen, lasse sich aber nicht mehr feststellen. Selbst wenn solche E-Mails erfasst worden wären, wären sie, wie alle anderen nachrichtendienstlich irrelevanten Mails, im Einklang mit den Bestimmungen des Art. 10-Gesetzes und den allgemeinen verfassungsrechtlichen Maßgaben für den Datenschutz unverzüglich und spurenlos gelöscht worden. Der *BND* war verpflichtet solche E-Mails zu löschen, weil nach dem gesetzlichen Konzept eine Benachrichtigung der Betroffenen über die Erfassung dieser E-Mail-Verkehre nicht vorgesehen ist.
Die Klagen mit dem Ziel, eine Speicherung und Nutzung von Metadaten in dem System VERAS zu unterlassen, seien noch nicht entscheidungsreif. Die in VERAS gespeicherten Metadaten nutzt der *BND* zur Erstellung von Verbindungsanalysen. Nach dem in der mündlichen Verhandlung gewonnenen Erkenntnisstand werden in VERAS auch anonymisierte Telefonie-Metadaten von Trägern des Grundrechts aus Art. 10 GG aus der strategischen Fernmeldeüberwachung nach dem Art. 10-Gesetz eingestellt. Dieses Vorgehen des *BND* bedürfe weiterer gerichtlicher Aufklärung.

■ Vgl. auch *Petri*, ZD 2013, 557; *EuGH* ZD-Aktuell 2017, 05430 und ZD-Aktuell 2016, 05301.

OVG Berlin-Brandenburg: Kein Auskunftsanspruch bei Auslandseinsätzen

ZD-Aktuell 2017, 05437

Das *OVG Berlin-Brandenburg* hat in einem Eilverfahren (B. v. 13.12.2016 – OVG 6 S 22.16; ZD wird die Entscheidung demnächst veröffentlichen) festgestellt, dass das *Auswärtige Amt* nicht verpflichtet ist, einem Pressevertreter Auskunft über den Inhalt der völker-, europa- und verfassungsrechtlichen Prüfung des sog. „Einsatzes bewaffneter deutscher Streitkräfte zur Verhütung und Unterbindung terroristischer Handlungen durch die Terrororganisation IS" sowie der Beteiligung an AWACS-Aufklärungsflügen in der Türkei zu geben.
Der *6. Senat* hat die erstinstanzliche Eilentscheidung des *VG Berlin* geändert. Der Anspruch auf Auskunftserteilung bestehe nicht, weil das Bekanntwerden der Informationen nachteilige Auswirkungen auf internationale Beziehungen haben könnte.
Ob und wie sich das Bekanntwerden von Informationen auf die Außenpolitik der *Bundesregierung* und die diplomatischen Beziehungen zu anderen Staaten auswirkt, hänge von auf die Zukunft bezogenen Beurteilungen ab, die das *Gericht* nur eingeschränkt nachprüfen kann.
Das *Auswärtige Amt* habe ausreichend dargelegt, dass die im Vorfeld des Auslandseinsatzes gegen den *IS* innerhalb der *Bundesregierung* erfolgten rechtlichen Prüfungen u.a. in Bezug auf die sog. „EU-Beistandsklausel" hoch sensibel und daher einer Auskunft nicht zugänglich sind.
Die Auskunftsverweigerung kann zudem darauf gestützt werden, dass durch das öffentliche Bekanntwerden der Auskünfte die Sicherheit der Bundesrepublik Deutschland und ihrer Bürger gefährdet werden könnte. Das gilt auch für die Informationen, die sich auf die rechtliche Prüfung beziehen, ob der AWACS-Einsatz der Zustimmung des *Bundestags* bedurfte.
Die Prüfung beinhaltet sicherheitsrelevante Betrachtungen der tatsächlichen Umstände im Einsatzgebiet und in den angrenzenden Staaten.

■ Vgl. auch *OVG Berlin-Brandenburg* ZD-Aktuell 2017, 05442; *BVerwG* ZD 2016, 500; *BVerwG* ZD 2016, 542; *OVG Berlin-Brandenburg* ZD 2013, 638 (Ls.); *BVerwG* ZD 2015, 533 sowie *BVerwG* ZD 2016, 142.