Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Bericht zum ersten Swiss-US Privacy Shield Review (2018)

I. Überblick

Die regelmässige, jährliche Überprüfung der Funktionsweise des Swiss-US Privacy Shield ist im Swiss-US Privacy Shield Framework vorgesehen (Joint Review Mechanism). Nach Inkraftsetzung der Privacy Shield Absprache am 17. April 2017 fand am 20. Oktober 2018 der erste Joint Review der Schweizer Delegation und der US Regierung in Brüssel statt.

Mittlerweile haben sich 2'883 US Unternehmen dem Swiss-US Privacy Shield Programm angeschlossen, darunter Facebook, Inc., Microsoft Corporation mit 27 Tochtergesellschaften (covered entities) und Google LLC (Stand Februar 2019).

Hinsichtlich des kommerziellen Teils des Swiss-US Privacy Shield ist anzumerken, dass beim EDÖB im Berichtsjahr zwei Fälle betreffend «false claims» (Unternehmen, die sich fälschlicherweise als Privacy Shield zertifiziert ausgeben) durch Betroffene eingereicht wurden, welche beide in Zusammenarbeit mit dem DoC gelöst werden konnten (vgl. auch Ziff. 1.4).

Ferner sind ca. zehn berechtigte Beschwerden gegen zertifizierte Unternehmen bei privaten, unabhängigen Stellen für die alternative Streitbeilegung (ADR) eingereicht worden. Beschwerden betreffend zertifizierte Unternehmen, die den EDÖB als unabhängige Beschwerdestelle gewählt haben, oder Beschwerden in Bezug auf beschäftigungsrelevante Daten von Arbeitnehmern (zwingende Aufsicht durch EDÖB) sind keine eingegangen.

Auch betreffend den behördlichen Zugriff auf Personendaten (Ombudspersonmechanismus) ist bisher kein Fall beim EDÖB eingegangen.

Es liegt somit der Schluss nahe, dass die vom Swiss-US Privacy Shield zur Verfügung gestellten Rechtsinstrumente bislang wenig genutzt worden sein dürften. Zu beachten ist dabei allerdings, dass der Swiss-US Privacy Shield erst seit April 2017 in Kraft ist. Ferner gilt es zu bedenken, dass vor einer allfälligen ADR zuerst das zertifizierte Unternehmen selbst angegangen werden sollte. Es ist deshalb davon auszugehen, dass eine quantitativ schwer abschätzbare Anzahl von Verletzungen bereits auf diesem Weg beseitigt werden konnte.

Die Schweiz war am ersten Review durch das SECO (Lead) und den EDÖB (aufsichtsbehördliche Optik) vertreten. Auf der US Seite nahmen Vertreter des Departments of Commerce (DoC) teil.

Das Treffen erfolgte im Nachgang des 2. Joint Reviews des EU-US Privacy Shields, an dem die Schweizer Delegation mit Beobachterstatus anwesend war, jedoch keine Fragen stellen durfte. Am EU-US Joint Review 2018 nahmen seitens der USA Vertreter folgender Behörden teil:

- DoC,
- Department of State (DoS),
- Federal Trade Commission (FTC),
- Departement of Transportation (DoT),

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

- Office of the Director of National Intelligence (ODNI),
- Department of Justice (DoJ),
- Privacy and Civil Liberites Oversight Board (PCLOB, unabhängige Stelle zur Überwachung des Schutzes der Privatspähre und den bürgerlichen Freiheiten),
- vorübergehende amtierende (acting) Ombudsperson (und Mitarbeiter),
- Inspector General für Intelligence Community

Für die EU nahmen Vertreter der nachfolgenden Gremien teil:

- EU-Kommission
- Mitglieder des Europäischer Datenschutzausschuss (EDSA/engl. EDPB)

Die Ausgangslage und der Wortlaut des Swiss und des EU Privacy Shields sind praktisch identisch. Ein Grossteil der Themen wurde denn auch ausschliesslich anlässlich des EU-US Reviews behandelt. Es sind dies z.B. der behördliche Zugriff auf Personendaten und verschiedene Aspekte des kommerziellen Teils des Abkommens (z.B. Definition von HR Daten, Tätigkeitsbereich der FTC/des DoT).

Die Funktion des EDÖB entspricht grösstenteils derjenigen des EDSA (bis 25. Mai 2018: Artikel 29 Arbeitsgruppe [WP29]).

Die wichtigsten Erkenntnisse des EDSA resultieren aus vorgängigem schriftlichem Austausch mit den USA sowie der Diskussion anlässlich des zweiten EU-US Joint Reviews. Sie können vielfach analog für das Swiss–US Privacy Shield übernommen werden. Angesichts der Tatsache, dass die Schweiz und die EU ihre Rechtsordnungen mit Blick auf den Datenschutz gegenseitig als gleichwertig anerkennen, bejaht die Schweiz die Angemessenheit des Datenschutzniveaus des Swiss-US Privacy Shield, soweit die EU die Adäquanz des EU-US Privacy Shield als erfüllt beurteilt.

Auf Stufe der EU haben sowohl die Kommission als auch der EDSA je einen eigenen Bericht im Rahmen der beiden bisherigen Joint Reviews (2017 und 2018) verfasst.[1]

Zum Zwecke des koordinierten Ablaufs und der Vor- und Nachbereitung der Überprüfung spricht sich der EDÖB mit den Datenschutzbehörden der EU ab. Folglich überschneidet sich der nachfolgende Bericht zu grossen Teilen mit dem Bericht des EDSA.

Spezifisch für das Swiss-US Privacy Shield ist anzumerken, dass im Rahmen dieses ersten Joint Reviews der persönliche Kontakt zum DoC hergestellt wurde. Ferner konnte das Verfahren der Ernennung der fünf offiziell ernannten, in der Schweiz wohnhaften Schiedsrichter des Swiss–US Privacy Shields, welche die Liste der EU ergänzen, vor dem ersten Swiss-US Review finalisiert werden. Die Namen der fünf zusätzlichen Schiedsrichter wurden auf der International Centre for Dispute Resolution der American Arbitration Association (ICDR/AAA) vor den durch die EU ernannten aufgelistet. Somit ist der Schiedsrichtermechanismus für das Swiss–US Privacy Shield vollständig operativ.[2]

Zudem wurden am ersten Swiss-US Privacy Shield Review zum einen die Einrichtung und Inbetriebnahme der im Swiss-US Privacy Shield Framework vereinbarten Elemente, zum anderen deren Funktionsweise und deren Entwicklung diskutiert. Dabei konnte die Schweiz davon profitieren, dass die EU und die USA bereits 2017 einen ersten Review zum EU-US Privacy Shield (in Kraft seit 12.7.2016) durchgeführt haben. Verschiedene Empfehlungen der EU im Rahmen ihres Reviews 2017 wurden durch

[1] https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

[2] vgl. hierzu auch die Website des EDÖB samt Leitfaden:
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

die US Behörden auch für das Swiss-US Privacy Shield umgesetzt. In Bezug auf die kommerziellen Aspekte ist das DoC unter anderem der Forderung der EU Kommission nachgekommen, aktiver nach Unternehmen zu suchen, die sich fälschlicherweise als Privacy Shield zertifiziert ausgeben. Zudem überprüft es zertifizierte Unternehmen regelmässiger als zu Beginn, um mögliche Schwachstellen bei der Einhaltung der Principles zu identifizieren.

Bezüglich des behördlichen Zugriffs auf Personendaten durch US Behörden haben die Vertreter des EDSA im Rahmen des EU-US Review 2018 hervorgehoben, dass die US Behörden seit dem EU-US Review 2017 erfreulicherweise hilfreiche Dokumente zum besseren Verständnis der Datenerhebungen veröffentlicht haben. Auch die Diskussion anlässlich des zweiten EU-US Reviews trug zum besseren Verständnis der Überwachungsprogramme und zur Erhöhung der Transparenz bei (beispielsweise Entscheidungen betreffend Foreign Intelligence Surveillance Court [FISA Court]).

Aus aufsichtsbehördlicher Sicht sind insbesondere folgende Ausführungen relevant:

II. Datenschutzrechtliche Prüfung

1. Kommerzielle Aspekte

1.1. Informationen und Anleitungen für US Unternehmen

Das Verständnis von Datenschutz in der Schweiz/Europa unterscheidet sich grundlegend von jenem in den USA. Um unterschiedliche Auslegungen der im Privacy Shield festgelegten Grundsätze (Principles), möglichst zu verhindern, müssen diese klar und eindeutig sein. Beim Selbst-Zertifizerungsverfahren nehmen die meisten US Unternehmen ein Selbst-Assessment vor und lassen die Compliance-Überprüfung nicht durch externe Dienste vornehmen. Die zu befolgenden Regelungen sind komplex. Insbesondere die Regeln zur Weitergabe von Daten durch zertifizierte Unternehmen an Dritte (Onward Transfer) scheinen Unternehmen vor grosse Herausforderungen zu stellen. Der EDÖB hat im Verlauf des Jahres 2018 diesbezügliche Anfragen infolge verschiedener Unklarheiten von Schweizer Unternehmen, welche Daten in die USA transferieren, erhalten. Die EU hatte im Rahmen ihres ersten Reviews im Jahr 2017 gefordert, dass den Unternehmen klare Anleitungen und verständliche Informationen zur Verfügung gestellt werden. Dieser Forderung ist das DoC nachgekommen und hat nun FAQ betreffend „Accountability for Onward Transfer Principle“ auf seiner Website publiziert.[3] Weitere Anleitungen werden erwartet.

1.2. Klare und einfach zugängliche Informationen für Schweizer Betroffene

Aufgrund der Vielschichtigkeit des Privacy Shield Frameworks kann es sich für Schweizer Betroffene (und Betroffene in der EU) schwierig gestalten, ihre Rechte geltend zu machen. Klare, verständliche und leicht zugängliche Informationen sind daher notwendig. Das DoC hat auf seiner Privacy Shield Website nun unter der Sektion „EU and Swiss Individuals“ Informationen für Betroffene und eine Übersicht des Programms aufgeschaltet.[4] [5]

Weitere Informationen zu den Rechten von Schweizer Betroffenen finden sich auf der Website des EDÖB.[6]

---

[3] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs
https://www.privacyshield.gov/article?id=Processing-FAQs

[4] https://www.privacyshield.gov/Individuals-in-Europe

[5] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq

[6] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

1.3. Selbstzertifizierung und Rezertifizierung

Da US Unternehmen sich mittels einer Selbstzertifizierung dem Privacy Shield Programm anschliessen, und wie erwähnt nur wenige das Compliance Assessment über externe Firmen vornehmen lassen, ist es wichtig, dass die Erfüllung der datenschutzrechtlichen Grundsätze bei der Zertifizierung und Rezertifizierung durch das DoC überprüft wird. Diesbezüglich wurden seit Inkraftsetzung des Privacy Shields durch die US Behörden Verbesserungen vorgenommen. Das DoC überprüft nun sowohl bei der Erst- als auch bei der Rezertifizierung folgende Punkte:

1. Registrierung mit einem Independent Recourse Mechanism (IRM) Unternehmen
2. Entrichtung des Beitrags betr. Annex I Arbitral Fund Contribution
3. Einhaltung des Privacy Shield “Supplemental Principle 6“ (Zugang)
4. Vollständigkeit und Konsistenz der “Certification Information”
5. Datenschutzerklärung (Vorhandensein der 13 Elemente, die den Privacy Shield verlangt, wird auch in den Privacy Policies der Unternehmen überprüft)

Bei Bedarf verlangt das DoC von den Unternehmen, die über Links abrufbaren Informationen zu präzisieren. Zudem überprüft das DoC die Anmeldungen auf Widersprüchlichkeiten zwischen den Angaben in den Privacy Policies der Unternehmen und der Privacy Shield Liste (z.B. Angaben zur Zertifizierung für HR/non HR Data).

Gemäss Angaben des DoC am EU-US Review wurden mehrere Unternehmen aufgrund dieser Überprüfungen wegen Nichterfüllung der Prinzipien tatsächlich abgelehnt.

Eine beachtliche Verbesserung ist das vom DoC neu eingeführte Verbot für US Unternehmen, in ihren Privacy Policies auf das Privacy Shield Programm zu verweisen, bevor die Überprüfung der Selbstzertifizierung durch das DoC abgeschlossen und der Name des Unternehmens auf der Privacy Shield Liste veröffentlich worden ist. Frühzeitige Verweise auf die Privacy Shield Mitgliedschaft müssen von der Website entfernt werden. So können Widersprüchlichkeiten zwischen Angaben in Privacy Policies und tatsächlichem Stand der Erstzertifizierungen vermieden werden.

Diskutiert wurde am zweiten EU-US Review auch die Rezertifizierung. Es ist verschiedentlich vorgekommen, dass das Gültigkeitsdatum der Erstzertifizierung vor dem Abschluss des Rezertifizierungsverfahrens abgelaufen war und die betreffenden Unternehmen einige Zeit ohne gültige Zertifizierung auf der Liste figurierten. Der EDÖB geht mit dem EDSA einig, dass für die Individuen in dieser zeitlichen Lücke zwar kein Nachteil entsteht, solange ein US Unternehmen sich öffentlich zur jederzeitigen Einhaltung der Principles verpflichtet. Nichtsdestotrotz wäre es wünschenswert, Unsicherheiten darüber, ob ein US sich dem Programm lückenlos verpflichtet, komplett auszuschliessen.

1.4. Aufsicht und Überwachung der Einhaltung der Principles durch das DoC

Seit dem ersten EU-US Review hat das DoC die Überwachung der Einhaltung der Privacy Shield Grundsätze durch US Unternehmen erheblich verbessert, wovon auch das Schweizer Abkommen profitiert. Das DoC wird auch im Rahmen des Swiss-US Privacy Shields wie folgt von Amtes wegen tätig:

- Vierteljährlich ermittelt es betreffend "false claims" (Unternehmen, die sich fälschlicherweise als Privacy Shield zertifiziert ausgeben).

Beim EDÖB sind bisher zwei Fälle von „false claims“ eingegangen, welche beide in Zusammenarbeit mit dem DoC gelöst werden konnten.

- Den als „nicht compliant“ identifizierten Unternehmen lässt das DoC ein Schreiben zukommen mit Androhung der Übermittlung an die FTC/DoT bei weiterbestehender Nichteinhaltung der Anforderungen resp. der Nichtvornahme der Löschung vom Privacy Shield Programm. Unternehmen können innert 30 Tagen antworten. Das DoC führt eine Liste der Unternehmen welche nicht auf das Schreiben reagieren.

- Ferner führt das DoC stichprobenartige Web Searches durch.

- Das DoC hat bei 100 Unternehmen (inklusive EU-US Privacy Shield) Stichproben nach dem Zufallsprinzip vorgenommen. Im Fokus standen der Zugang zu den Privacy Policies, die Reaktionsbereitschaft der Unternehmen und die Verfügbarkeit des IRM.

- Eine Person ist zuständig, die Medien nach Stichworten zu durchsuchen, um mögliche Verletzungen des Privacy Shield Frameworks zu ermitteln.

- Das DoC überprüft Unternehmen regelmässig auf «defekte/tote Links» (broken links) zur Privacy Policy auf der Privacy Shield Liste.

Der EDSA begrüsste im Rahmen des zweiten EU-US Reviews diese neuen Überwachungsmassnahmen zwar, bemängelte jedoch, dass diese Kontrollen sich auf Formalitäten beschränken. Materielle Überprüfungen seien aber zentral. Wichtig sei die Überprüfung aller Principles, insbesondere jene der Onward Transfers. Das DoC habe bisher zum Beispiel noch keine Kopien von Privacy Provisions von Verträgen zwischen US Organisationen und ihren Auftragnehmern (Agents) verlangt. Da aber Onward Transfers auch in Drittstaaten ohne adäquaten Datenschutz vorgenommen werden können, müsse die Verantwortlichkeit klar geregelt sein. Nach Ansicht des DoC hingegen beinhaltet der Privacy Shield keine Überprüfungen auf solch hohem Detaillierungsgrad.

Anlässlich des ersten Swiss–US Reviews machte das DoC gegenüber dem EDÖB deutlich, dass nach seiner Ansicht das Privacy Shield Abkommen mit einem Gesetz zu vergleichen sei, welches zwar für die zertifizierten Unternehmen verbindlich sei, die Betroffenen aber zur Durchsetzung ihres Rechts grundsätzlich (auch) selber aktiv werden müssen. Entsprechend nimmt das DoC in der Regel auf Hinweis von aussen hin Abklärungen bei US Unternehmen vor.

Der EDÖB teilt die Meinung des EDSA. Er erachtet ex officio Überwachungen durch US Behörden als angezeigt, weil es sich für Betroffene aufgrund der Komplexität der (nicht immer offensichtlichen) Datenbearbeitungen schwierig gestaltet, ihre Rechte überhaupt geltend zu machen.

1.5. Aufsicht und Überwachung der Einhaltung der Principles durch die FTC

Der EDÖB hatte anlässlich seines ersten Joint Reviews keine Möglichkeit, direkten Kontakt mit Vertretern der FTC aufzunehmen, da diese ausschliesslich am EU-US Review teilnahmen, an dem die Schweiz Beobachter war (vgl. Ziff. I) und keine Fragen stellen durfte. Jedoch gelten die dort gemachten Ausführungen analog auch für das Swiss-US Privacy Shield Abkommen.

Die FTC hat seit dem letztjährigen EU–US Review ihre Aktivitäten betreffend Aufsicht und Durchsetzung der Privacy Shield Principles verstärkt.

Mittlerweile sind gemäss Angaben der FTC insgesamt 40 Anwälte fast ausschliesslich für den Bereich «Privacy» zuständig. Diese werden zusätzlich, unter anderem durch technische Experten, unterstützt.

Es wurden von der FTC einige neue Fälle der Nichteinhaltung von Privacy Shield Grundsätzen erfasst, es entzieht sich jedoch der Kenntnis des EDÖB, ob diese Organisationen (auch) dem Swiss-US Privacy Shield angeschlossen waren.

Versuchsweise hat die FTC Civil Investigative Demands (CIDs) verschickt, um die Einhaltung der Privacy Shield Prinzipien zu kontrollieren. Details zu den Zielobjekten und Inhalten der Formulare gab die FTC aber nicht preis. Grundsätzlich hat die FTC einen grossen Spielraum in ihrer Überprüfungstätigkeit. Ein konkreter Verdacht ist nicht notwendig.

Der EDÖB schliesst sich der Meinung des EDSA an, dass es zwar erfreulich ist, dass die FTC vermehrt auch von Amtes wegen tätig wird. Da die FTC aber keine Details bekanntgegeben hat, ist eine Beurteilung der konkreten Fälle und der Tätigkeiten der FTC nicht möglich. Eine Einschätzung, bis zu welchem Grad sie tatsächlich die Einhaltung der Prinzipien überprüft, kann deshalb nicht vorgenommen werden.

1.6. Independent Recourse Mechanisms

Für eine Harmonisierung und zur besseren Übersichtlichkeit der jährlichen Berichte der Firmen, die IRM Dienstleistungen anbieten, hat das DoC Richtlinien herausgegeben. Diese zeigen auch mögliche Interessenkonflikte von Firmen auf, die sowohl ex officio compliance als auch IRM Dienstleistungen an dieselben US Unternehmen anbieten. Die IRM Firmen sind angehalten, in ihren jährlichen Berichten zu beschreiben, wie sie solche Interessenkonflikte vermeiden oder zu lösen gedenken.

1.7 Personaldaten

Beim Begriff „Personaldaten“ (HR Daten) gibt es eine Diskrepanz zwischen der Interpretation der US Behörden und jener der Schweizer resp. EU Vertretern. Die unterschiedliche Auslegung wurde bereits beim ersten EU–US Review 2017 diskutiert und im anschliessenden Bericht der WP29 eingehend erörtert. Gemäss dem DoC sollen nur solche Daten von Angestellten unter die Definition HR Daten fallen, welche innerhalb desselben Unternehmens in die USA transferiert werden. Personaldaten eines Schweizer (oder EU) Unternehmens, welche hingegen an einen Privacy Shield zertifizierten Auftragsnehmer in den USA transferiert werden, gelten nach dieser Auffassung nicht als HR Daten, sondern als Konsumentendaten. Folglich profitieren letztere nicht vom erhöhten/zusätzlichen Schutz, welches das Privacy Shield Framework für HR Daten vorsieht (zum Beispiel die obligatorische Unterstellung unter den EDÖB, welcher verbindliche Empfehlungen an die US Unternehmen abgeben kann).

Der EDÖB teilt die Meinung der WP29 (und des EDSA), dass HR Daten jegliche Personendaten umfassen sollen, die in der EU resp. der Schweiz im Rahmen eines Arbeitsverhältnisses bearbeitet werden, unabhängig davon, ob sie durch den Arbeitgeber oder einen Auftragsbearbeiter bearbeitet werden. HR Daten sollen nur dann ohne Weiteres an US Unternehmen transferiert werden dürfen, wenn deren Privacy Shield Zertifizierung auch HR Daten umfasst. Der EDÖB ist der Ansicht, dass sämtliche in der Schweiz erhobenen Angestelltendaten eines besonderen Schutzes bedürfen: Aufgrund des Subordinationsverhältnisses bei der Datenerhebung steht es den Arbeitnehmern nicht gänzlich frei, ihre Personendaten preiszugeben. Daher ist es wichtig, dass sie bei der weiteren Bearbeitung dem vorgesehenen erhöhten Schutz unterstehen (z.B. ausdrückliche Einwilligung Opt-in statt Opt-out bei der Bearbeitung zu Marketingzwecken).

Die Uneinigkeiten betreffend diese Auslegungen konnten durch die EU und die US Behörden bisher nicht bereinigt werden. Nachdem beim letzten EU-US Review die Definition von HR Daten diskutiert wurde, lag der Fokus beim diesjährigen Review auf den Konsequenzen der unterschiedlichen Interpretationen. Die Vertreter der EU äusserten insbesondere Bedenken, weil die im Privacy Shield Abkommen zugesicherten restriktiveren Regeln zum Schutz von Arbeitnehmern nicht durchgesetzt werden können. Der EDÖB erklärte dem DoC anlässlich des Schweizer Reviews, dass er sich der Auffassung des EDSA vollumfänglich anschliesst.

2. Behördliche Zugriffe auf Personendaten/nationale Sicherheit

Die für die nationale Sicherheit zuständigen US Vertreter waren einzig am EU-US Review anwesend, an welchem der EDÖB als Beobachter anwesend war. Angesichts der Tatsache, dass die EU und die Schweiz gegenseitig einen angemessenen Datenschutz gewährleisten, kann sich der EDÖB hinsichtlich der behördlichen Zugriffen den Ausführungen zu den Analysen des EDSA anschliessen. Es wird daher auf den Bericht des EDSA vom 22. Januar 2019 sowie der WP29 vom 28. November 2017[7] verwiesen.

2.1. Datenerhebung unter Section 702 Foreign Intelligence Surveillance Act (FISA) und Executive Order (EO) 12 333

Der EDSA verlangt insbesondere unabhängige Überprüfungen dass Datenerhebungen nach Section 702 FISA nicht willkürlich erfolgen und keine Massenerhebungen stattfinden. Er hält an den Ausführungen im Bericht der WP29 vom 28. November 2017 fest, insbesondere dass in Bezug auf die Verhältnismässigkeit im Generellen und die Erforderlichkeit im Speziellen unabhängige Einschätzungen über die Definition des Begriffs „target" und über das „tasking of Selectors" (z.B. Telefon, E-Mailadresse etc.) vorzunehmen seien. Der EDSA bedauert, dass mit der Re-Autorisierung der Section 702 FISA Ende 2017 keine zusätzlichen Schutzmassnahmen für EU (resp. Schweizer) Betroffene, z.B. gemäss der PPD-28, implementiert wurden. In der PPD-28 wird u.a. bestimmt, dass ein Datenzugriff so zweckgebunden und zielgerichtet wie möglich zu erfolgen hat. Ferner schreibt sie unter anderem gewisse Garantien für die personenbezogenen Informationen aller Privatpersonen unabhängig von ihrer Nationalität oder ihres Wohnorts vor. Datenerhebungen sollen gemäss PPD-28 „as tailored and as feasible as possible" sein. Die Nutzung von Personendaten, die durch Massenüberwachung beschafft wurden, wird auf sechs Zwecke beschränkt.

Bezüglich Überwachungen, bei denen (gestützt auf die EO 12 333) Personendaten ausserhalb der USA erhoben werden, verweist der EDSA auf die Ausführungen der WP29 im Rahmen des ersten EU-US Review. Für die Gewährleistung eines angemessenen Datenschutzniveaus eines Drittstaates muss gemäss EDSA nicht nur die Datenbearbeitung innerhalb dieses Staates angemessen sein, sondern auch die Regelungen, die dem Drittstaat erlauben, ausserhalb seines Territoriums Daten zu bearbeiten, insofern EU (resp. Schweizer) Personendaten betroffen sind.

Demgegenüber sind die US Behörden der Ansicht, dass Datenbearbeitungen gestützt auf die EO 12 333ausserhalb des Anwendungsbereichs des Privacy Shield liegen, weil gestützt auf die EO 12 333 keine Daten **innerhalb der USA** bearbeitet werden dürfen. Aufgrund der nach wie vor bestehenden Unklarheit und der Unvorhersehbarkeit der Anwendung der EO 12 333 verweist der EDSA auf den letztjährigen Bericht der WP29. Die von den US Behörden bestätigte (grundsätzliche) Anwendung der PPD-28 begrüsste der EDSA.
Jedoch kommt er nach der Analyse der seitens der US Behörden zur Verfügung gestellten Informationen zur PPD-28 zum Schluss, dass weder der Bericht des PCLOB zur PPD-28 noch der zweite EU-US Review neue Informationen zur Auslegung des PPD-28 Textes gebracht hat. Insbesondere erwähnt er unter anderem Unklarheiten bei der Interpretation der oben erwähnten sechs Zwecke. Zudem wäre ein detaillierter follow-up Bericht über die Anwendung der PPD-28 bei den verschiedenen Überwachungsprogrammen zu begrüssen. Es ist zudem wünschenswert, dass der PCLOB in seinem fertigzustellenden Bericht zur EO 12 333 u.a. über deren konkrete Anwendbarkeit sowie über die Notwendigkeit und Verhältnismässigkeit der darauf gestützten Datenerhebungen informiert.

[7] https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf

2.2. Aufsicht über Überwachungsprogramme der US Behörden

Der EDSA unterstreicht die Wichtigkeit der Aufsicht über die Überwachungsprogramme der US Behörden. Bereits anlässlich des EU-US Review 2017 wurden Aufsichtsaktivitäten von verschiedenen U.S Institutionen vorgestellt. Im Rahmen des zweiten EU-US Reviews wurden weitere Einheiten präsentiert, was zum besseren Verständnis der Funktionsweise der Inspector Generals (Aufsichtseinheiten) beitrug.

Der EDSA ist der Auffassung, dass die zuständigen Aufsichtsorgane genügend unabhängig von der Intelligence Community ist (inkl. the Privacy and Civil Liberty officers, the oversight of the Department of Justice und Inspector Generals).

Den PCLOB erachtet der EDSA als essentielles Element im Aufsichtsgefüge über die US Behörden. Nachdem beim ersten Review des EU-US Privacy Shield die WP29 gefordert hatte, die vier freien Sitze des PCLOB zu besetzen, hat der US Senat erfreulicherweise am 11. Oktober 2018 drei Mitglieder, inklusive neuer Chairman Adam Klein, bestätigt, womit das Quorum erreicht ist und der PCLOB beschlussfähig ist. Somit kann der PCLOB seine Aufgaben als unabhängiges Aufsichtsorgan wahrnehmen. Die freien Stellen bleiben zu besetzen.

2.3. Rechtsweg für Schweizer Betroffene

Im für den EU-US Privacy Shield (und für den Swiss-US Privacy Shield indirekt) relevante Schrems Urteil hat der Gerichtshof der Europäischen Union (EuGH) festgehalten, dass Betroffenen gemäss Art. 47 der Charta der Grundrechte der Europäischen Union der Rechtsweg zu einem nationalen Gericht offenstehen muss. Das heisst, es muss eine Möglichkeit für den Bürger vorgesehen werden, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen resp. ihre Berichtigung oder Löschung zu erwirken.

Auch die schweizerische Bundesverfassung garantiert das Verfahren vor einem unabhängigen und unparteiischen Gericht (Art. 29ff BV). Entsprechend hat auch ein Drittstaat, dessen Datenschutz als angemessen gelten soll, ein Gericht zur Verfügung zu stellen, vor dem ein wirksamer Rechtsbehelf eingelegt werden kann.

Die PPD-28 begründet keine durchsetzbaren Rechte. Eine rechtswidrige elektronische Überwachung gestützt auf die EO 12 333 bietet ebenfalls kein Rechtsschutzinstrument.
Eine gerichtliche Überprüfung der Überwachungsangelegenheiten durch FISA ist derzeit aufgrund der sehr restriktiven Interpretation der Verfahrensvorschriften nicht realistisch: Dem Supreme Court of the United States genügt die abstrakte Gefahr der Überwachung nicht für eine rechtliche Überprüfung, sondern die Überwachung der Kommunikation muss nachgewiesen werden.

Es gestaltet sich folglich für einen Schweizer (oder auch EU) Betroffenen als ausserordentlich schwierig, Überwachungsmassnahmen vor Gericht anzufechten, resp. überprüfen zu lassen. Dies erweist sich angesichts des Grundrechts auf wirksamen gerichtlichen Rechtsschutz als problematisch. Die weitere Entwicklung bezüglich der Interpretation der Klagebefugnis im Bereich der Überwachung ist (auch in hängigen Verfahren) weiterzuverfolgen.[8]

Der Ombudspersonmechanismus stellt für Schweizer Betroffene momentan praktisch die einzige (direkte) Möglichkeit der Überprüfung der Einhaltung der datenschutzrechtlichen Grundsätze (PPD-28, EO 12 333, FISA Section 702, etc.) durch US Behörden dar. Deshalb sind hohe Anforderungen an die

[8] vgl. auch Bericht des EDSA vom 22. Januar 2019, Ziff. 4.4. S. 18, insbesondere auch die Fälle ACLU v. Clapper und Wikipedia v. NSA

verfahrensrechtlichen Grundsätze dieses Ombudspersonmechanismus zu stellen. Diese werden nachfolgend analysiert.

2.4. Ombudsperson

Der Zugang zum Ombudsverfahren wurde im ersten Jahr seit der Inkraftsetzung des Swiss– US Privacy Shields umgesetzt. Der EDÖB geht mit den Vertretern des EDSA (und der WP29) einig, dass die Schaffung des Ombudspersonmechanismus als Rechtsbehelf für Betroffene bei Zugriffen der US Behörden auf ihre persönlichen Daten grundsätzlich zu begrüssen ist. Die Ombudsperson prüft Gesuche unter Einbezug des PCLOB und gelangt bei allfälliger Verletzung der Persönlichkeitsrechte an den (unabhängigen) Inspector General des entsprechenden Nachrichtendienstes, der die internen Richtlinien der Behörde überprüft (resp. das zuständige Privacy and Civil Liberties Office).

In Anbetracht der Verfahrensgarantien der Schweizerischen Bundesverfassung sind hohe Anforderungen an die Unabhängigkeit und die Unparteilichkeit der Ombudsperson zu stellen.

Am 28. September 2018 wurde eine neue vorübergehend amtierende («acting») Ombudsperson, Manisha Sing (Acting Under Secretary of State for Economic Growth, Energy, and the Environment), ernannt. Sie löste Judith Garber (acting Assistant Secretary for Oceans, Environment and Science at the Department of State) ab.

Anlässlich des zweiten Joint Review des EU-US Privacy Shield erklärten die Ombudsperson sowie andere Vertreter des US Regierung die Funktionsweise des Mechanismus anhand eines theoretischen Falls. Dabei wurde versichert, dass die Ombudsperson unabhängig von den US Nachrichtendiensten sei und die Anträge von Betroffenen betreffend Verletzung der zugesicherten datenschutzrechtlichen Grundsätze rechtmässig und effizient behandle. Sie antworte auf Anträge von Betroffenen in jedem Fall erst, wenn sie überzeugt sei, dass keine Datenschutzverletzung vorliege. Wenn nötig, würde sie von der präsidialen Vollmacht Gebrauch machen, die Streitfrage bis vor die höchste Ebene der zuständigen US Regierungsstelle zu bringen. Konkrete Fälle dürfen gemäss der Ombudsperson jedoch nicht publik gemacht werden, und auch die tatsächliche Vorgehensweise im Einzelfall und das Zusammenspiel zwischen der Ombudsperson und der Nachrichtendienstgemeinschaft der Vereinigten Staaten (Intelligence Community) sind teilweise geheim. Solange diese Prozesse nicht offengelegt werden, kann aber nicht abschliessend beurteilt werden, wie gross die Kompetenzen (powers) der Ombudsperson gegenüber der Intelligence Community tatsächlich sind, das heisst, ob sie mit ausreichenden Kompetenzen ausgestattet ist, sich die erforderlichen Informationen zu beschaffen und Mängel zu beseitigen.

Mithin ist zurzeit zweifelhaft, ob bei Nichteinhaltung der zugesicherten datenschutzrechtlichen Grundsätze durch US Behörden tatsächlich genügend Abhilfe geschafft werden kann. Dies erweist sich als problematisch u.a. im Hinblick auf die grundrechtlich verankerten Garantien auf ein Verfahren vor einem unabhängigen und unparteiischen Gericht, zumal anlässlich des EU–US Review bestätigt wurde, dass die Entscheidungen der Ombudsperson nicht vor Gericht gebracht werden können.

Zudem ist die Stelle des Under Secretary, der das Amt der Ombudsperson zugeordnet ist, noch nicht ständig besetzt. Es bleibt daher eine ständige (permanente) Ombudsperson zu ernennen.,

Präsident Donald Trump im Januar 2019 Keith Krach als Under Secretary of State for Economic Growth, Energy and the Environment nominiert. Dieser würde bei einer Bestätigung durch den US Senat, welche zum Zeitpunkt der Erstellung dieses Berichts hängig ist, als permanente Ombudsperson eingesetzt werden. Der EDÖB wird die Entwicklungen weiterverfolgen.

2.5. Zugriff auf Personendaten durch Strafverfolgungsorgane

Der EDÖB nimmt zur Kenntnis, dass die Rechte von Drittstaatsangehörigen mit Blick auf die nachträglichen Mitteilungen von Datenbeschaffungen, die bei Dritten stattfanden, im US-Strafprozessrecht gewissen Einschränkungen unterworfen sind. Solche Einschränkungen können sich grundsätzlich auch auf Betroffene mit Schweizer Staatsbürgerschaft negativ auswirken.

III. Fazit:

Der EDÖB begrüsst die Implementierung der im Swiss-US Privacy Shield Framework festgelegten Elemente des Swiss-US Privacy Shield Abkommens während des ersten Jahres sowie die Umsetzung von verschiedenen (von der EU vor und während des ersten Reviews verlangten) Verbesserungen, die auch in das Swiss-US Privacy Shield Framework eingebaut wurden. Es sind dies beispielsweise Anpassungen beim Zertifizierungsprozess, eine verstärkte Überprüfung durch die US Behörden von Amtes wegen sowie die Publikation/das zur Verfügung stellen von verschiedenen hilfreichen Dokumenten. Erfreulich ist auch die Besetzung von zwei vakanten Sitzen des PCLOB, womit das nötige Quorum erreicht ist.

Als positiv zu bewerten ist ferner die Ernennung der fünf Schiedsrichter für die Schweiz, welche die Liste der EU Schiedsrichter ergänzt und vor dem ersten Review erfolgreich abgeschlossen werden konnte.

Jedoch gibt es verschiedene verbesserungswürdige Punkte.

Beispielsweise wären substantielle Überprüfungen der Privacy Shield zertifizierten US Unternehmen durch die US Behörden wünschenswert.

Ferner wird der Verlauf der weiteren Diskussionen zwischen der EU Kommission und den US Behörden betreffend die Definition des Begriffs HR Daten für Arbeitnehmende in der Schweiz von Interesse sein.

Was den Zugriff auf Personendaten durch US Behörden betrifft, ist es wie der EDSA in seinem Bericht vom 22.1.2019 festgehalten hat, wichtig, dass der PCLOB als Aufsichtsorgan weitere Berichte verfasst, insbesondere auch über die Anwendung der Schutzmassnahmen nach der PPD-28, sowie Berichte betreffend die Section 702 FISA und die EO 12 333.

Ferner ist eine permanente Ombudsperson zu ernennen.

Der EDSA verweist zudem auf die massgebenden, am Europäischen Gerichtshof (EuGH) hängigen Verfahren, z.B. betreffend Vertragsstandardklauseln, die es abzuwarten gilt, und die auf die Schweiz indirekt Auswirkungen haben.