Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Bericht zum zweiten Swiss-US Privacy Shield Review (2019)

I. Überblick

Am 14. September 2019 fand der zweite, jährliche Joint Review des Swiss-US Privacy Shields der Schweizer Delegation und der US-Regierung in Washington D.C. statt.

Seit Inkraftsetzung des Swiss-US Privacy Shield Rahmenwerks am 17. April 2017 haben sich über 3'300 Unternehmen dem Swiss-US Privacy Shield Programm angeschlossen, seit dem letzten Review (Oktober 2018) ist die Anzahl um fast 1'000 Zertifizierungen angestiegen. Bei über 70% der Mitglieder handelt es sich um KMUs aus unterschiedlichen Sektoren, insbesondere aus den Bereichen Informations- und Kommunikationstechnologie, unternehmensbezogene und professionelle Dienstleistungen, Medien und Unterhaltung sowie Bildung. Auch Konzerne wie Facebook Inc. und Google LLC sind nach wie vor Privacy Shield zertifiziert.

Der EDÖB ist Ansprechstelle für Betroffene in der Schweiz und Unternehmen.

Hinsichtlich des kommerziellen Teils des Swiss-US Privacy Shield ist beim EDÖB im Berichtsjahr lediglich ein Fall zur Weiterleitung an das Department of Commerce (DoC) eingegangen. Es handelte sich hierbei um einen «false claim» (Unternehmen, das sich fälschlicherweise als Privacy Shield zertifiziert ausgibt). Der Fall konnte in Zusammenarbeit mit dem DoC gelöst werden (vgl. auch unten Ziff. 1.4.).

Ferner sind ungefähr zehn berechtigte Beschwerden gegen zertifizierte Unternehmen bei privaten, unabhängigen Stellen für die alternative Streitbeilegung (ADR) betreffend das Swiss-US Rahmenwerk eingereicht worden. Beschwerden betreffend zertifizierte Unternehmen, die den EDÖB als unabhängige Beschwerdestelle gewählt haben, oder Beschwerden in Bezug auf arbeitsrechtliche Daten von Arbeitnehmern (zwingende Aufsicht durch EDÖB) sind keine eingegangen. Hingegen wurde der EDÖB mehrfach von Unternehmen mit Sitz in der Schweiz konsultiert betreffend Unklarheiten im Datentransfer in die USA.

Bezüglich den Zugriff auf Personendaten durch US Behörden zum Zweck der nationalen Sicherheit ist seit Inkraftsetzung des Rahmenwerks kein Fall beim EDÖB eingegangen.

Nach wie vor ist es schwierig abzuschätzen, aus welchen Gründen die zur Verfügung stehenden Rechtsinstrumente durch Betroffene in der Schweiz wenig genutzt werden. Zum einen könnte dies an der Komplexität des Rahmenwerks liegen und der Schwierigkeit, allfällige Datenschutzverletzungen festzustellen. Bei Fragen steht der EDÖB wie erwähnt als Ansprechstelle für Betroffene in der Schweiz sowie Unternehmen zur Verfügung. Zum anderen gilt es aber auch zu bedenken, dass vor einer allfälligen ADR/EDÖB zuerst das zertifizierte Unternehmen selbst angegangen werden sollte. Es ist deshalb davon auszugehen, dass eine quantitativ schwer abschätzbare Anzahl von Datenschutzverletzungen bereits auf diesem Weg beseitigt werden konnte.

Die Schweiz war am zweiten Review wie bereits im Vorjahr durch das SECO (Lead) und den EDÖB (datenschutzrechtliche Optik/Aufsicht) vertreten. Auf der US Seite nahmen Vertreter des DoC teil.

Das Treffen erfolgte im Nachgang des dritten Joint Reviews des EU-US Privacy Shields, an dem die Schweizer Delegation mit Beobachterstatus anwesend war, sich jedoch nicht äussern durfte. Am EU-US Joint Review 2019 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 Liberities Oversight Board (PCLOB, unabhängige Stelle zur Überwachung des Schutzes der Privatsphäre und den bürgerlichen Freiheiten),
- Ombudsperson (und Mitarbeiter),
- Inspector General für Intelligence Community

Für die EU nahmen Vertreter der nachfolgenden Gremien teil:

- EU-Kommission,
- acht Vertreter des Europäischen Datenschutzausschusses (EDSA/engl. EDPB)

Wie bereits im Vorjahr wurde aufgrund der Übereinstimmung des Schweizer und des EU Rahmenwerks in praktisch allen inhaltlichen Belangen ein Grossteil der Themen wie zum Beispiel der behördliche Zugriff auf Personendaten oder wichtige datenschutzrechtliche Aspekte des kommerziellen Teils (z.B. Tätigkeitsbereich der FTC/des DoT) ausschliesslich am EU-US Reviews behandelt (vgl. auch Bericht des EDÖB zum ersten Joint Review des Privacy Shield, 2018[1]).

Auf Stufe der EU haben sowohl die Kommission als auch der EDSA (bis 25. Mai 2018: Artikel 29 Arbeitsgruppe [WP29]) je eigene Berichte im Rahmen ihrer bisherigen Joint Reviews (2017[2], 2018[3] und 2019[4]) verfasst.

Die wichtigsten datenschutzrechtlichen Erkenntnisse des EDSA resultieren aus vorgängigem schriftlichem Austausch mit den USA sowie der Diskussion anlässlich des dritten EU-US Joint Reviews. Sie gelten im Allgemeinen analog für das Swiss–US Privacy Shield. Die US-Behörden nehmen ihre Anpassungen denn auch für beide Rahmenwerke nach Massgabe ihrer Gleichheit vor.

Die Funktion des EDÖB entspricht grösstenteils derjenigen des EDSA (vormals WP29).

Folglich entspricht der nachfolgende Bericht zu grossen Teilen demjenigen Bericht des EDSA.

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.

Nachdem beim ersten Review des Swiss-US Privacy Shield Rahmenwerks (2018) insbesondere die Einrichtung und der Ablauf der Prozesse des kommerziellen Teils des Privacy Shield Programms sowie die persönliche Kontaktaufnahme mit den US Vertretern im Vordergrund stand, wurde in diesem Jahr auch intensiv über die Nutzung des Privacy Shield Rahmenwerks durch Unternehmen mit Sitz in der Schweiz sowie über spezifische Anpassungen und Entwicklungen des kommerziellen Teils diskutiert.

---

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

[2] WP29: 2017https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf
EU Kommission: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[3]EDSA:https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en
EU Kommission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[4] EDSA: https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en
EU Kommission: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

Der Vollständigkeit halber zu erwähnen ist, dass sich ein in der Schweiz wohnhafter Schiedsrichter im Verlauf des Berichtjahres von der Liste hat löschen lassen. Die US-Behörden beschlossen, diesen vorläufig nicht zu ersetzen. Der Schiedsrichtermechanismus bleibt nichtsdestotrotz für das Swiss–US Privacy Shield vollständig operativ.[5]

Aus datenschutzrechtlicher Sicht sind insbesondere folgende Punkte relevant:

II. Datenschutzrechtliche Prüfung

1. Kommerzielle Aspekte

1.1. Informationen und Anleitungen für US Unternehmen

Da das Datenschutzniveau in den USA im Vergleich zu demjenigen der Schweiz als nicht gleichwertig gilt, ist ein Datentransfer von der Schweiz in die USA grundsätzlich nur unter den in Art. 6 des Bundesgesetzes über den Datenschutz (SR 2 235.1, DSG) aufgeführten Bedingungen erlaubt. Daher soll das Privacy Shield Rahmenwerk ein ausreichendes Datenschutzniveau zur Erleichterung des Datentransfers in die USA für die zertifizierten Unternehmen in dem im Privacy Shield Text festgelegten Rahmen gewährleisten. Angesichts dessen sowie der Tatsache, dass das datenschutzrechtliche Verständnis der USA sich grundlegend von jenem der Schweiz (und der EU) unterscheidet, ist die Sicherstellung der einheitlichen Interpretation des Privacy Shield Textes von grösster Bedeutung.

Aufgrund dessen und auf Verlangen der WP29 und des EDSA (vgl. ihre Berichte) hat das DoC seit der in Kraftsetzung des Privacy Shield Rahmenwerks leicht zugängliche und verständliche Leitfäden für zertifizierte Unternehmen in Form von FAQs zur Verfügung gestellt (z.B. „Accountability for Onward Transfer Principle“ , „Processing Guidance“).

Im vergangenen Jahr hat das DoC auch ein Merkblatt in Form von FAQs zum Thema Privacy Shield und Grossbritannien (Brexit) publiziert .

Der EDÖB begrüsst das aktive Vorgehen des DoC für ein besseres Verständnis des komplexen Privacy Shield Textes für Unternehmen und Interessierte.

Aufgrund der Anfragen, die den EDÖB auch von Unternehmen mit Sitz in der Schweiz erreicht haben, schliesst sich der EDÖB insbesondere dem Vorschlag des EDSA an, dass das DoC unter anderem das Verfahren bei der Auftragsdatenbearbeitung oder die Verwendung von Standardvertragsklausen (SCC) etc. näher erläutere.

1.2. Klare und einfach zugängliche Informationen für Schweizer Betroffene

Wie unter Ziff. I erwähnt, kann es sich aufgrund der Komplexität des Privacy Shield Rahmenwerks für Betroffene in der Schweiz und der EU schwierig gestalten, ihre Rechte geltend zu machen. Auf Verlangen der WP29 und später des EDSA (vgl. ihre Berichte) hatten die US Behörden bereits im Verlauf des ersten Anwendungsjahres des EU-US Privacy Shields sowie im ersten Anwendungsjahr des Swiss-US Privacy Shields leichter verständliche Informationen über die Rechte von Betroffenen, die verfügbaren Mittel und Rechtsbehelfe auf ihrer Webseite publiziert. Auch die verschiedenen Beschwerdemöglichkeiten werden erläutert und teilweise die entsprechenden Links direkt angegeben. Nach den ersten jährlichen Überprüfungen des Rahmenwerks und als Reaktion auf die Vorschläge der WP29 hat das DoC auf seiner Website ein einseitiges Dokument hinzugefügt, das einen Überblick über das Programm gibt, wobei der Schwerpunkt auf den Rechten des Einzelnen liegt und wie er diese ausüben kann .

[5] vgl. hier 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

Weitere Leitfäden werden erwartet.

Zusätzliche Informationen zu den Rechten von Schweizer Betroffenen finden sich auf der Website des EDÖB . Wie erwähnt, kann der EDÖB bei Unklarheiten auch schriftlich oder telefonisch konsultiert werden.

1.3. Selbstzertifizierung und Rezertifizierung

Bei der Zertifizierung und Rezertifizierung gab es bei der Überprüfung der Privacy Shield Konformität der Unternehmen durch das DoC keine Veränderungen im Vergleich zum letztjährigen Privacy Shield Review. Folgende Punkte werden durch das DoC sowohl bei der Zertifizierung als auch bei der Rezertifizierung geprüft:

- Registrierung bei einem unabhängigen Regressunternehmen (IRM)
- Entrichtung des Beitrags betr. Annex I Arbitral Fund Contribution
- Einhaltung des Privacy Shield “Supplemental Principle 8“ (Zugang zu personenbezogenen Daten)
- Vollständigkeit und Konsistenz der “Certification Information”
- Datenschutzerklärung (Vorhandensein der 13 Elemente, die der Privacy Shield verlangt, wird auch in den Datenschutzrichtlinien der Unternehmen überprüft)

Nach wie vor verlangt das DoC bei Bedarf von den Unternehmen, die über Links abrufbaren Informationen zu präzisieren, um den Betroffenen die Ausübung ihrer Rechte zu erleichtern. Zudem überprüft das DoC die Anmeldungen auf Inkonsistenzen zwischen den Angaben in den Privacy Policies der Unternehmen und jenen auf der Privacy Shield Liste (z.B. Angaben zur Zertifizierung für HR/non HR Data). Mittels solcher Überprüfungen war es dem DoC auch in diesem Berichtsjahr möglich, diesbezügliche Nichterfüllungen der Anforderungen festzustellen und nicht Privacy Shield konforme Unternehmen als Mitglied abzulehnen. Das DoC verbietet den US Unternehmen auch weiterhin, 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 veröffentlicht worden ist, damit Widersprüchlichkeiten zwischen Angaben in Privacy Policies und tatsächlichem Stand der Erstzertifizierungen vermieden werden.

Diese Massnahmen erachtet der EDÖB als wertvoll. Nichtsdestotrotz bleibt aus Sicht des EDSA wie auch des EDÖB problematisch, dass die durch das DoC vorgenommenen Überprüfungen gemäss den am Review erhaltenen Informationen hauptsächlich formelle Kriterien betreffen und kaum die Einhaltung der Privacy Shield Grundsätze in ihrem Inhalt materiell tangieren.

Eine solche materielle Kontrolle wäre aber angezeigt, insbesondere weil die meisten Unternehmen kein Compliance Assessment über externe Firmen vornehmen lassen, sondern dies selber durchführen.

Wie beim letztjährigen EU-US Privacy Shield Review wurde das Problem diskutiert, dass es bei der Rezertifizierung vorkommt, 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. Gemäss den Informationen anlässlich des dritten EU-US Privacy Shield Reviews kann der Prozess der Rezertifizierung bis zu 105 Tage ab dem tatsächlichen Fälligkeitsdatum dauern. Während dieses gesamten Zeitraums bleiben die Unternehmen auf der Liste „aktiv“.

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 Privacy Shield Grundsätze verpflichtet. Der EDÖB geht mit dem EDSA weiter überein, dass es aber wünschenswert wäre, eine Lösung dahingehend zu finden, dass der Schutz der Betroffenen zu jedem Zeitpunkt sichergestellt ist und keine Unsicherheit darüber existiert. In der Zwischenzeit sollten sowohl die Betroffenen als auch Unternehmen in der Schweiz und der EU, die Personendaten an zertifizierte US Unternehmen übermitteln, darauf aufmerksam gemacht werden, die Gültigkeit der Zertifizierung jeweils zu überprüfen.

Ebenfalls wurde im Rahmen des dritten EU-US Privacy Shield Reviews festgestellt, dass auf der Liste des Privacy Shields mehrere als "aktiv" eingestufte Unternehmen standen, deren Rezertifizierung im 2018 fällig war. Der EDSA forderte das DoC anlässlich des diesjährigen Reviews auf, Verfahren einzuführen, die sicherstellen, dass die "aktive" Teilnehmerliste immer auf dem neuesten Stand ist.

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

Anlässlich des ersten EU-US Privacy Shield Reviews (2017) kritisierte die WP29, dass sich die Aufsicht über die kommerziellen Aspekte des Privacy Shields hauptsächlich auf die Drittunternehmen stützte, die einen Independent Recourse Mechanism (IRM) zur Verfügung stellten, und dass es seitens des DoCs an ausreichender ex officio Aufsicht und Überwachung mangle.

Im darauffolgenden Privacy Shield Review 2018 (der erste für das Swiss-US Privacy Shield) konnten signifikante Verbesserungen in der Aufsicht durch die US-Behörden bezüglich beider Rahmenwerke festgestellt werden (vgl. Bericht EDÖB, 2018 Ziff. 1.4.).

Gemäss den diesjährigen Informationen hat das DoC im vergangenen Jahr die Anzahl der Stichprobenkontrollen auf 30 zufällig ausgewählte Unternehmen pro Monat erhöht und insgesamt mehr als 670 Abmahnungen erteilt, wovon die meisten "false claims" betrafen. Zwar sind diese durch das DoC vorgenommenen Verbesserungen zur Gewährsleitung der formellen Einhaltung der Grundsätze des Privacy Shield, wie im letzten Bericht ausgeführt, zu begrüssen. Als problematisch erachten aber sowohl der EDSA als auch der EDÖB die Tatsache, dass der Fokus der Kontrollen weiterhin auf die zu erfüllenden Formalitäten und nicht auf dem Inhalt der Grundsätze liegt. Daher fordert der EDSA das DoC im Rahmen ihres dritten Reviews weiterhin auf, seine Aufsichtsaktivitäten auch auf materielle Elemente wie zum Beispiel das Prinzip der Zweckbindung auszudehnen. Auch im Zusammenhang mit dem „Onward Transfer“ habe das DoC beispielsweise noch immer 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 überwacht werden. Das DoC hält an seiner Auffassung fest, dass die Unternehmen mit ihrer Zertifizierung rechtlich durchsetzbare Verpflichtungen eingehen. Die Betroffenen müssen dementsprechend auch selber aktiv werden. Das Rahmenwerk sehe indes keine substanzielleren Kontrollen vor (vgl. auch Ziff. 1.4. S.5 des Berichts 2018). Es gäbe aber Möglichkeiten, den Inhalt der Stichproben zu erweitern.

Wie der EDSA erachtet es auch der EDÖB als angezeigt, dass substanzielle Kontrollen durch das DoC vorgenommen werden, damit überprüft werden kann, dass selbstzertifizierte Unternehmen die materiellen Anforderungen des Privacy Shield konkret umsetzen. Er wird die weitere Entwicklung verfolgen und bleibt im Austausch mit Vertretern der EU und der USA.

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

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

Seit der letzten Überprüfung des Privacy Shields hat die FTC insgesamt sieben neue Fälle verzeichnet. Bei der Nichtkonformität handelte es sich jeweils um administrative Fehler und nicht um materielle Verletzungen der Privacy Shield Prinzipien. Der EDSA empfiehlt, dass weitere Kontrollen der Weiterleitung durchgeführt werden könnten, da die von den zertifizierten Unternehmen geschaffenen Lösungen auch nicht vom DoC überprüft werden.

In der FTC Abteilung für Datenschutz und Identitätsschutz (Bureau of Consumer Protection) befassen sich 40 Anwälte fast ausschliesslich mit dem Thema Datenschutz. Sie werden dabei unter anderem von technischen Experten unterstützt. Bezüglich des im letzten Jahr erzielten Facebook-Vergleichs stellte die FTC am diesjährigen Review klar, dass der durch den Vergleich abgedeckte Bereich ausserhalb des Geltungsbereichs des Privacy Shield liege.

Der EDSA begrüsste, dass die FTC vermehrt von Amts wegen tätig wird. Da die FTC aber weiterhin keine Details bekanntgibt, ist eine Beurteilung der konkreten Fälle und der Tätigkeiten der FTC nach wie vor 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 (IRM)

Die Anzahl der Beschwerden, die bei IRM Anbietern eingegangen ist, ist seit dem letzten Review leicht gestiegen. Die Beschwerden scheinen jedoch hauptsächlich verfahrenstechnische Aspekte zu betreffen und nicht die materielle Einhaltung der Grundätze. Das Instrument der IRM vermag daher eine verstärkte materielle Kontrolle durch die US Behörden nicht zu substituieren (vgl. Ziff. 1.4. und 1.5.).

Wie im Bericht zum Review 2018 ausgeführt, sind die IRM Firmen angehalten, in ihren jährlichen Berichten zu beschreiben, wie sie allfällige Interessenkonflikte vermeiden oder zu lösen gedenken (vgl. dazu Ziff. 1.6. S. 6 des Berichts 2018). Das DoC führte hierzu aus, dass es seine Leitlinien für den jährlichen IRM-Bericht aktualisiert hat, damit Interessenkonflikte und mögliche Lösungen aufgezeigt werden. Die Leitlinien decken jedoch nicht alle Aspekte der Berichte ab. Insbesondere stellte der EDSA fest, dass zu diesem Aspekt noch kein einheitliches Vorlagenformat für die Berichte eingeführt wurde. Um eine vollständige Vergleichbarkeit zu gewährleisten, empfiehlt der EDSA dem DoC daher, für den jährlichen IRM-Bericht ein standardisiertes Vorlagenformat einzuführen, das auch Erläuterungen enthält, wie mögliche Interessenkonflikte ausgeschlossen werden.

1.7 Personaldaten

Wie bereits im vorangegangenen Bericht erwähnt (vgl. Ziff.1.7. Bericht 2018), wird der Begriff der Personaldaten im Zusammenhang mit dem Privacy Shield von der EU und der Schweiz, und von den US-Behörden unterschiedlich ausgelegt. Das DoC und die EU-Behörden haben die Diskussionen über ihre unterschiedlichen Interpretationen von HR-Daten im vergangenen Jahr fortgesetzt, ohne dass eine Einigung erzielt worden ist. Aufgrund dieser nicht gelösten Diskrepanz in der Definition lag der Fokus beim letzten wie auch bei diesem Review weniger auf dem Begriff als vielmehr auf den Folgen, zu denen die unterschiedlichen Definitionen führen können. Der EDSA und der EDÖB befürchten, dass die im Rahmenwerk für Beschäftigungsdaten festgelegten zusätzlichen Schutzmassnahmen (z.B. Opt-in statt Opt-out zu Marketingzwecken) bei Nicht-HR Daten von keiner US-amerikanischen oder EU-Behörde durchgesetzt würden. Der EDÖB vertritt die gleiche Meinung wie der EDSA, nämlich dass Personaldaten strengeren Anforderungen unterstehen sollen, unabhängig davon, ob sie vom Arbeitgeber oder von einem Auftragsbearbeiter bearbeitet werden (vgl. auch Bericht 2018, Ziff. 1.7.). Die Diskussionen zwischen der EU und den US-Behörden zu diesem Thema werden fortgesetzt.

2. Behördliche Zugriffe auf Personendaten/nationale Sicherheit

Seit dem letzten Review hat sich der Rechtsrahmen der USA nicht entscheidend geändert. Die wesentlichen Vorbehalte, die von der WP29 resp. des EDSA und vom EDÖB in den letztjährigen Berichten betreffend die behördlichen Zugriffe auf Personendaten im Rahmen des Privacy Shield zum Zweck der nationalen Sicherheit oder der Strafverfolgung geäussert wurden, bestehen daher nach wie vor. Insbesondere betreffen die Bedenken betreffend die Datenerhebung, die Aufsicht, den Rechtbehelf und den Ombudspersonmechanismus. Ferner ist zu beachten, dass derzeit der Fall „Schrems II“ (Rechtssache C-311/18) vor dem Gerichtshof der Europäischen Union (EuGH) hängig ist, der auch den EU-US Privacy Shield betrifft und so indirekt auch für den Swiss-US Privacy Shield Bedeutung hat. Das Urteil wird für März bis Mai 2020 erwartet.

Die für die nationale Sicherheit zuständigen US Vertreter waren einzig am EU-US Review anwesend, an welchem der EDÖB als Beobachter anwesend war und sich nicht äussern durfte. Angesichts der Tatsache, dass die Rahmenwerke sich entsprechen, schliesst sich der EDÖB hinsichtlich der behördlichen

Zugriffe den Ausführungen zu den Analysen des EDSA an, sofern nachfolgend nicht etwas anderes explizit erwähnt wird. Es wird daher insbesondere auf den Bericht des EDSA vom 12. November 2019 verwiesen, vgl. Ziff. I, vgl. auch die Berichte vom 22. Januar 2019 und Bericht der WP29 vom 28. November 2017, vorne Ziff, I).

2.1. Erhebung von Daten für Zwecke der nationalen Sicherheit

2.1.1 *Erhebung von Daten gemäss Section 702 Foreign Intelligence Surveillance Act (FISA)*

Der EDSA betont erneut die Notwendigkeit einer unabhängigen Beurteilung der Verhältnismässigkeit und der Erforderlichkeit bezüglich der Definition von "targets" und des Konzepts der "foreign intelligence" gemäss Section 702 FISA (auch im Rahmen des UPSTREAM-Programms). Ferner hält er an seiner Forderung nach einer weiteren unabhängigen Beurteilung der Anwendung von „selectors“ in Einzelfällen fest („tasking of Selectors“, z.B. Telefon, E-Mailadresse etc.)". Er verlangt auch weiterhin weitere Klarstellungen/Erläuterungen betreffend das Überwachungsprogramm UPSTREAM, um auszuschliessen, dass willkürliche (Massen-)Erhebungen zu personenbezogenen Daten von Nicht-US Personen nach Section 702 erfolgen (vgl. auch Bericht 2018, Ziff.2.1.).

Im Hinblick auf Section 702 FISA wurde in den Diskussionen der diesjährigen Überprüfung klargestellt, dass sich eine als „target“ zu identifizierende "Person" auf mehrere Personen mit demselben Identifikator beziehen könnte, sofern alle diese Personen Nicht-US Personen wären und die anwendbaren Kriterien für die Zielerreichung erfüllen.

Der EDSA begrüsst, dass der inzwischen vollständig funktionsfähige PCLOB als unabhängige Aufsichtsbehörde beschlossen hat, die Abfrage (Suche) der gemäss Section 702 erlangten Daten durch das FBI zu überprüfen, sowie die Tatsache, dass der PCLOB angab, nachzuverfolgen, inwiefern die in ihrem Bericht zu Section 702 ausgesprochenen früheren Empfehlungen berücksichtigt worden seien. Jedoch bedauert der EDSA, dass der PCLOB nicht beabsichtigt, einen aktualisierten Gesamtbericht über die Section 702 zu erstellen und herauszugeben, der sich auf den im Jahr 2014 vorgelegten Bericht stützt. Ein allgemeiner aktualisierter Bericht würde dazu beitragen, eine Bewertung der neuen Bestimmungen in Abschnitt 702 (Reauthorisierung 2017) sowie der Verfahren von Nachrichtendiensten vorzunehmen.

2.1.2. *Erhebung von Daten gemäss der Executive Order 12333 (EO12333)*

Der EDSA hält an der Auffassung fest, dass sich die Angemessenheit des Datenschutzniveaus nicht auf die Überwachung innerhalb der physischen/geographischen Grenzen eines Drittstaats beschränken solle. Vielmehr sollten auch die Rechtsgrundlagen analysiert werden, die diesem Drittstaat ermöglichen, eine Überwachung ausserhalb seines Hoheitsgebiets in Bezug auf EU-Daten (resp. Schweizer Daten) durchzuführen. Beschränkungen des staatlichen Zugangs zu Personendaten sollten sich auf jene Daten erstrecken, die "auf dem Weg" in ein Land sind, für welches eine Angemessenheit anerkannt wird.

Anlässlich der letzten Reviews betonten die US-Behörden, dass die EO 12333 nicht als Grundlage für die Erhebung von Daten innerhalb des US-Gebietes verwendet werden kann und dass die Erhebung von Daten im Rahmen dieser EO nicht in den Anwendungsbereich des Privacy Shield falle (vgl. auch letztjähriger Bericht des EDÖB, Ziff. 2.1.).

Angesichts der nach wie vor bestehenden Unsicherheit und Unvorhersehbarkeit bezüglich der Anwendung der EO 12333 betonte der EDSA zwar erneut die Wichtigkeit von klarstellenden Berichten des PCLOB zu diesem Text. Es ist aber davon auszugehen, dass entsprechende Berichte geheim bleiben werden und keine weiteren Informationen über die konkrete Funktionsweise der EO12333 (und deren Notwendigkeit und Verhältnismässigkeit) der Öffentlichkeit oder Vertretern von Drittstaaten zugänglich gemacht werden.

2.1.3. *Schutzmassnahmen gemäss Presidential Policy Directive 28 (PPD-28)*

Die von den US Behörden bestätigte (grundsätzliche) Anwendung der PPD-28 begrüsste der EDSA (vgl. auch Bericht des EDÖB zum ersten Review, 2018), insbesondere weil nur sie Garantien und Beschrän-

kungen für die Erhebung und Verwendung von Daten ausserhalb der USA vorsieht (die Beschränkungen der FISA oder anderer spezifischerer US-Gesetze gelten hierfür nicht).

Die massenhafte Erhebung von Daten wird durch die PPD-28 auf sechs nationale Sicherheitszwecke beschränkt (Spionage, Terrorismus, Massenvernichtungswaffen, Cybersicherheit, Gefahren für die Streitkräfte, grenzüberschreitende kriminelle Bedrohungen), um die Privatsphäre aller Personen, einschliesslich Nicht-US-Bürgern, besser zu schützen. Im Rahmen des dritten EU-US Privacy Shield Reviews fand keine neue substanzielle Diskussion über die Auslegung und Anwendung der sechs Sicherheitszwecke statt, die eine Einschätzung zu den Zusicherungen der US-Behörden ermöglicht hätte.

Die US-Behörden machen zwar geltend, dass die Executive Orders und Presidential Policy Directives "rechtsverbindlich" seien. Es gilt aber zu bedenken, dass diese Rechtsinstrumente keine durchsetzbaren Rechte begründen. Daher wäre es für Betroffenen in der Schweiz oder der EU nicht möglich, sich vor einem US-Gericht z.B. direkt auf die Verletzung der PPD-28 zu berufen (vgl. auch Bericht des EDÖB, 2018, Ziff. 2.3.).

2.2. Aufsicht über Überwachungsprogramme der US Behörden

Der EDSA erinnert daran, dass eine umfassende Aufsicht über alle Überwachungsprogramme von entscheidender Bedeutung ist.

Bereits während der beiden vorangegangenen jährlichen gemeinsamen Überprüfungen wurden die Aufsichtsaktivitäten mehrerer Instanzen/Einheiten vorgestellt. Nach Ansicht des EDSA besteht eine umfassende Aufsichtsstruktur, die sich aus verschiedenen, zum Teil von der Nachrichtendienstgemeinschaft unabhängigen Einheiten zusammensetzt, darunter die Privacy and Civil Liberty officers, die Inspector Generals, der PCLOB, der FISC und der Kongress.

Der EDSA begrüsst auch die Ernennung der letzten fehlenden Mitglieder des PCLOB, der nun vollständig funktionsfähig ist. Der PCLOB stellte erstmals sein Arbeitsprogramm vor, und der EDSA äusserte sich positiv über die Transparenz dieses Aufsichtsorgans. Der EDSA erachtet den PCLOB als wichtiges unabhängiges Organ der «Aufsichtsstruktur».

Hingegen fordert der EDSA erneut die Veröffentlichung von Berichten wie auch Aktualisierungen früherer Berichte (Section 702 FISA, PPD-28).

Im Allgemeinen ist anzumerken, dass eine sinnvolle Überprüfung der Aufsicht über Überwachungsprogramme der US Behörden kaum möglich ist, weil Vertretern von Drittstaaten nur Zugang zu öffentlichen Dokumenten gewährt wird.

2.3. Rechtsweg für Schweizer Betroffene

Wie im letztjährigen Bericht des EDÖB erwähnt (Ziff. 2.3.) ist für die Bejahung eines adäquaten Datenschutzniveaus eines Drittstaates zentral, dass in der Schweiz Betroffene Zugang zu einer unabhängigen und unparteiischen Beschwerdestelle haben.

Da sich der Rechtsrahmen gemäss Auskunft der US Behörden seit dem letzten Review nicht verändert hat, ist auf die Ausführungen im Rahmen des letzten Reviews zu verweisen (vgl. Bericht EDÖB 2018, Ziff. 2.3.).

Eine gerichtliche Überprüfung der Überwachungsangelegenheiten (Section 702 FISA, EO12333, etc.) ist nach wie vor aufgrund der derzeitigen sehr restriktiven Interpretation der Verfahrensvoraussetzungen («standing requirements») nicht realistisch. Anlässlich des EU-US Reviews wurde bestätigt, dass sich die Auslegung des Begriffs «standing» in Überwachungsfragen in der Entwicklung befindet, wobei die Fälle noch anhängig sind .

2.4. Ombudspersonmechanismus

Im Rahmen des dritten EU-US Privacy Shield Reviews begrüsste der EDSA die Ernennung von Herrn Keith Krach am 18. Januar 2019 zur "permanenten" Ombudsperson.

Da der Ombudspersonmechanismus momentan praktisch die einzige direkte Möglichkeit zur Überprüfung der Einhaltung der datenschutzrechtlichen Grundsätze gemäss PPD-28, EO 12333, Section 702 FISA, etc. durch US Behörden darstellt, ist es von zentraler Bedeutung, dass die Ombudsperson unabhängig und unparteiisch ist.

Herr Keith Krach ist als Under Secretary of State for Economic Growth, Energy, and the Environment zwar unabhängig von den Nachrichtendiensten, jedoch nicht von der US Regierung.

Betreffend die Behandlung von Anträgen von Betroffenen wurde bereits an den letzten Reviews von den jeweiligen Ombudspersonen und der US-Regierung die Sicherstellung der rechtmässigen und effizienten Bearbeitung von Anträgen erläutert. Die Mitarbeiter der Ombudsperson erläuterten anhand eines abstrakten Falls, wie Anfragen behandelt werden (vgl. auch Bericht EDÖB 2018, Ziff. 2.4.). Herr Keith Krach bestätigte die Aussagen der letzten Ombudspersonen, dass er Schreiben zum Abschluss von Fällen nur dann unterzeichne, wenn er überzeugt sei, dass sie ordnungsgemäss behandelt wurden, und dass er die Streitfrage bis vor die höchste Ebene der zuständigen US Regierungsstelle bringe, wenn er von dem ihm vorgelegten Ergebnis nicht überzeugt sei.

Die Verfahren betreffend den Zugang der Ombudsperson zu relevanten Informationen und für die Interaktion der Nachrichtendienstgemeinschaft einschliesslich Aufsichtsbehörden, bleiben teilweise geheim, was eine Einschätzung des Verfahrens stark erschwert.

Wenngleich keine konkreten Indizien bestehen, an der Integrität der neuen Ombudsperson zu zweifeln, fordert der EDSA daher mehr Informationen über die Befugnisse der Ombudsperson gegenüber der Nachrichtendienstgemeinschaft.

Auf der Grundlage der verfügbaren Informationen kann nach wie vor nicht zum Schluss gekommen werden, dass die Kompetenzen der Ombudsperson gegenüber den Nachrichtendiensten ausreichend sind, da ihre «Befugnis» im Falle einer Rechtsverletzung darauf beschränkt zu sein scheint, zu entscheiden, die Einhaltung der Grundrechte gegenüber dem Antragsteller nicht zu bestätigen. Darüber hinaus können die Entscheidungen der Ombudsperson nicht vor Gericht gebracht werden.

Dies erweist sich als problematisch im Hinblick auf die grundrechtlich verankerten Garantien auf ein Verfahren vor einem unabhängigen und unparteiischen Gericht.

III. Fazit:

Der EDÖB begrüsst Der EDÖB begrüsst die Bemühungen der US-Behörden zur Verbesserung des Privacy Shield Programms, insbesondere die von Amtes wegen durchgeführten Aufsichts- und Durchsetzungsmassnahmen sowie die Ernennung der letzten fehlenden Mitglieder des PCLOB und der permanenten Ombudsperson.

Nach wie vor gibt es allerdings verbesserungswürdige Punkte. Was die kommerziellen Aspekte betrifft, so bleiben beispielsweise die Durchführung materieller Kontrollen durch das DoC, die Einhaltung der Anforderungen beim Onward Transfer oder die Lösung der Problematik HR Daten Anliegen des EDSA wie auch des EDÖB.

Was die Erhebung von Daten durch US Behörden angeht, wären unter anderem Berichte hilfreich, zum Beispiel zu den Garantien in der PPD-28.

Was den Ombudspersonmechanismus betrifft, kann aus den Informationen am EU-US Review nicht geschlossen werden, dass die Ombudsperson über ausreichende Befugnisse verfügt, um Zugang zu Informationen zu erhalten und Datenschutzverletzungen zu beheben. Ob mit dem Ombudspersonmechanismus die Anforderungen an eine unabhängige unparteiische Beschwerdeinstanz Rechnung getragen wird, kann daher derzeit auch für das Swiss-US Privacy Shield nicht bejaht werden.

Es sei an dieser Stelle daran erinnert, dass die am EuGH hängigen Fälle, insbesondere der Fall «Schrems II», die indirekt auch auf die Schweiz Auswirkungen haben werden, abzuwarten sind.

Im März 2020