

NoName e.V.: Chaotische Viertelstunde:01

Das Ende von Safe Harbour

Donnerstag 22 Oktober 2015

1 01 Das Ende von Safe Harbor

Created Dienstag 13 Oktober 2015

1.0.1 Teil 0: Disclaimer

- ich (die Vortragende bzw. Erstellerin dieser Notizen) habe keine juristische Ausbildung
- während ich versucht habe, nach bestem Wissen und Gewissen die Aussagen zusammenzutragen, bitte ich folgendes zu beachten
 - der Vortrag / diese Notizen können Aussagen enthalten, die nicht vollständig und / oder korrekt wiedergegeben wurden, oder die nicht mehr aktuell sind
 - * der Vortrag / diese Notizen enthalten Zusammenfassungen, und erheben damit keinen Anspruch auf Vollständigkeit
 - * der Vortrag / diese Notizen enthalten Aussagen, die aus dem Englischen in das Deutsch von mir übersetzt wurden, und die deswegen unter Umständen nicht korrekt wiedergegeben sind
- die Quellen zu den Aussagen befinden sich als Link in dem Punkt *vor* den Aussagen

1.0.2 Teil 1: Hintergründe

Was ist das "Safe Harbor Framework" noch gleich?

- <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE>
- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24 Oktober 1995

- "die Übermittlung personenbezogener Daten ... in ein Drittland ... zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet." (Artikel 25 Absatz 1)
 - * "Stellt die Kommission fest ..., daß ein Drittland kein angemessenes Schutzniveau ... aufweist, so treffen die Mitgliedsstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt." (Artikel 25 Absatz 4)
 - * "Die Kommission kann ... feststellen, daß ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ... hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau ... gewährleistet." (Artikel 25 Absatz 6)
- <http://www.export.gov/safeharbor/index.asp>
- "Safe Harbor Framework"
 - 7 Privacy Principles
 - Einhaltung dieser Privacy Principles kann u.a. begrenzt sein durch
 - * nationale Sicherheit
 - * öffentliches Interesse
 - * Strafverfolgung
 - * Rechtssprechung
 - * Notice
 - Zweck zu dem die Daten gesammelt werden
 - Kontakt
 - Typ von Dritten mit denen die Daten geteilt werden
 - * Choice
 - wenn die Daten an Dritte weitergegeben werden sollen / für einen anderen Zweck als die ursprünglich angegebenen
 - für nicht-sensible Daten opt-out Mechanismus
 - für sensible Daten opt-in Mechanismus
 - * Onward Transfer
 - wenn Daten an Dritte weitergegeben werden, muss sichergegangen werden, daß sie entweder
 - den EU-Datenschutzrichtlinien entsprechen, oder
 - dem "Safe Harbour Framework", oder
 - äquivalente Abkommen

- * Security
 - Daten müssen vor Verlust, Missbrauch, unberechtigtem Zugriff, Veröffentlichung, Veränderung und Zerstörung geschützt werden
- * Data Integrity
 - die Daten müssen für den Zweck, für den sie erhoben worden sind, relevant sein
 - die Daten müssen zuverlässig, korrekt, komplett und aktuell sein
- * Access
 - es muss Zugang zu den Daten bestehen, um sie gegebenenfalls verbessern, ergänzen oder löschen zu können, falls sie falsch sind
 - falls der Aufwand diesen Zugang zu ermöglichen vertretbar ist
 - falls nicht die Rechte einer anderen Person / Organisation dadurch verletzt werden
- * Enforcement
 - zugängliche und bezahlbare Einrichtungen um Beschwerden / Streitigkeiten zu untersuchen / Entschädigungen zu leisten
 - Kontrollmechanismen für die tatsächliche Umsetzung des "Safe Harbor Framework"
 - Verpflichtungen zur Umsetzung / Strafen für Nicht-Umsetzung
- * und 15 FAQ, betreffend
 - Sensible Daten
 - Fälle in denen der opt-in **nicht** nötig ist
 - Journalismus
 - Pressefreiheit steht über dem "Safe Harbor Framework"
 - Selbstzertifizierung
 - Verifizierung
 - in-house
 - externe Überprüfung
 - Access
 - Zugangsrecht ist **nicht** garantiert
 - z.B. bei Unverhältnismäßigkeit des Aufwands
 - z.B. wenn nicht-vertrauliche Informationen nicht von vertraulichen Informationen getrennt werden können
 - Choice
 - **opt-out** sollte jederzeit möglich sein

- wenn praktikabel
- ...
- freiwillige Selbstzertifizierung
 - * bei der U.S. Department of Commerce anzeigen
 - Brief mit
 - Daten des Unternehmens
 - Verarbeitung der Daten aus der E.U.
 - Datenschutzrichtlinien für die Daten aus der E.U.
 - Brief + Eintrag in U.S.-E.U. Safe Harbor List werden veröffentlicht
 - jährlich
 - * U.S.-E.U. Safe Harbor List
- Kontrollinstanz ist die U.S. Federal Trade Commission
- Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG)

PRISM

- im Juni 2013 werden den Zeitungen "The Guardian" und "The Washington Post" Details zu dem PRISM-Programm veröffentlicht
 - https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
 - <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>
- angebliche Kooperation von U.S.-amerikanischen Internet-Firmen mit der NSA und dem FBI / dem GCHQ
 - Zugang zu den Nutzerdaten von nicht-U.S.-amerikanischen Nutzern / U.S.-amerikanischen Nutzern in Kommunikation mit nicht-U.S.-amerikanischen Nutzern
 - * Audio + Video Chats
 - * Videos
 - * Fotografien
 - * E-Mails
 - * Dokumentübertragungen
 - * Verbindungsdaten

- * soziale Netzwerkdaten
- Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple
- * Dementi

Beschwerden und Klage

- [http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62014CJ0362\\$from=DE](http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62014CJ0362$from=DE)
- die Wiener Datenschutzorganisation [europe-v-facebook.org](http://www.europe-v-facebook.org) (<http://www.europe-v-facebook.org/DE/de.html>) gegründet von Max Schrems
- legt im Juni 2013 Beschwerde ein gegen:
 - Apple und Facebook (in Irland)
 - * Beschwerde gegen Facebook von Max Schrems persönlich
 - * bei Anmeldung Vertrag mit Facebook Irland
 - personenbezogene Daten werden in die U.S.A. zur Verarbeitung transferiert
 - diese Übermittlung von den Daten von Max Schrems soll die irische Datenschutzbehörde verhindern
 - Argument: PRISM
 - Skype und Microsoft (in Luxemburg)
 - * Bearbeitung der Beschwerde
 - PRISM wäre illegal
 - Teilnahme an PRISM wurde dementiert
 - Yahoo (in Deutschland)
 - * läuft
- die zuständige Datenschutzbehörde in Irland sieht keinen Handlungsbedarf
 - die Rechtsansicht, daß PRISM illegal ist, ist "frivol" – die Beschwerde muß nicht bearbeitet werden
- im Oktober 2013 wird die Klagschrift eingereicht
 - http://www.europe-v-facebook.org/JR_Grounding_Documents.pdf

1.0.3 Teil 2: Das Urteil und Reaktionen

Das Urteil

- am 6.10.2015 das Urteil des EuGH
 - <https://www.datenschutz-guru.de/2015/10/safe-harbor-webinar/>
 - <http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0362>
 - das "Safe Harbor Framework"
 - * bietet keine wirksamen Kontrollmechanismen
 - * ermöglicht unbeschränkten Zugang zu den Daten
 - kein angemessener Schutz
 - die Entscheidung der Kommission zu "Safe Harbor" ist ungültig

Die Reaktionen

- <https://www.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice>
- U.S. Secretary of Commerce Penny Pritzker
 - "deeply disappointed"
 - die Entscheidung schafft "significant uncertainty for both U.S. and EU companies and consumers"
 - und bringt die "thriving transatlantic digital economy" in Gefahr
 - eine geupdatete Version des "Safe Harbour Framework" soll so schnell wie möglich herausgebracht werden
- http://www.europe-v-facebook.org/CJEU_IR.pdf
- europe-v-facebook.org / Max Schrems
 - das Urteil unterstreicht
 - * daß Massenüberwachung eine Grundrechtsverletzung ist
 - U.S.-Firmen nicht behilflich dabei sein dürfen
 - * es möglich sein muss, rechtliche dagegen vorzugehen

- setzt Signale für Umgang mit vergleichbarer Überwachung durch E.U.-Mitgliedsstaaten
- http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm
 - Erster Vizepräsident Frans Timmermans (EU-Kommissar für "Better Regulation, Interinstitutional Relations, the Rule of Law and the Charter of Fundamental Rights")
 - * https://ec.europa.eu/commission/2014-2019/timmermans_en
 - Věra Jourová, EU-Kommissarin für "Justice, Consumers and Gender Equality"
 - * https://ec.europa.eu/commission/2014-2019/jourova_en/
 - Bestätigung für Bemühungen, das "Safe Harbor Framework" neu zu verhandeln
 - Prioritäten:
 - * Schutz der personenbezogenen Daten von E.U.-Bürgern bei Transfer in die U.S.A.
 - * ungestörter Datenfluss
 - * Verhandlungen mit jeweiligen Datenschutzbehörden um koordiniert Alternativen zu dem "Safe Harbor Framework" anzubieten
- andere Reaktionen: <https://netzpolitik.org/2015/safe-harbor-urteil-reaktionen-aus-presse-politik-ngos-und-verbaenden/>

1.0.4 Teil 3: Was dann?

Bisherige Alternativen zu dem "Safe Harbor Framework" <http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html>
http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm
[http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62014CJ0362\\$from=DE](http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62014CJ0362$from=DE)

- EU-Standardvertragsklauseln
 - <https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-was-sind-eu-standardvertragsklauseln/>
 - http://www.haufe.de/compliance/haufe-compliance-office-online/datenuebermittlung-ins-ausland-praktikabel-gestalten-32-eu-standardvertragsklauseln_idesk.PI28584_HI6735613.htm
 - Vertragsmuster von der Europäischen Kommission

- * EU-Standardvertrag I (2001)
- * EU-Standardvertrag II (2004)
- * EU-Standardvertrag für Auftragsverarbeitungen (2010)
- Binding Corporate Rules
 - http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm
 - https://de.wikipedia.org/wiki/Binding_Corporate_Rules
 - Regelwerk einer Unternehmensgruppe zum Schutz personenbezogener Daten
 - * Datenschutzrichtlinien
 - * Wirksamkeitwerkzeuge ("Tools of effectiveness")
 - * Beweis für Rechtskräftigkeit
 - werden verifiziert von § Datenschutzbehörde
 - alle Datentransfers **innerhalb** der Unternehmensgruppe müssen diese Regeln befolgen
 - * **kein** Datentransfer außerhalb der Unternehmensgruppe auf Basis von diesem Regelsatz möglich
- außerdem gibt es nach den Datenschutzrichtlinien Ausnahmen für:
 - zweifelsfreies Einverständnis der Person auf die sich die personenbezogenen Daten beziehen
 - Vertragserfüllung
 - * zwischen der betroffenen Person und dem Datenverarbeiter
 - * im Interesse der betroffenen Person zwischen dem Datenverarbeiter und einem Dritten
 - wichtiges öffentliches Interesse
 - lebenswichtiges persönliches Interesse
 - öffentliches Register / Register, daß allen mit berechtigtem Interesse zugänglich ist

Safe Harbor 2.0

- http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm
- http://www.europe-v-facebook.org/CJEU_IR.pdf
- als Folge der PRISM-Enthüllungen hat die EU-Kommission Verbesserungen an dem "Safe Harbor Framework" vorgeschlagen
 - "Making Safe Harbor safer"
 - * mehr **Transparenz**
 - * einfacherer Zugang zu/mehr Einsicht in die Arbeit von **Alternative Dispute Resolution**-Providern
 - * mehr **Kontrollen**
 - * Zugang zu Daten für **staatlichen Behörden** einschränken / transparenter machen
- seit 2013 Verhandlungen mit U.S.-amerikanischen Behörden
 - Deadlines in 2014/15 sind ohne Ergebnis verstrichen