EUGH kippt "Privacy Shield" Und nun?

Urteil in der Praxis

EuGH-Urteil "Schrems II"

- Datentransfer zwischen EU und USA
- Hauptgrundlage für Austausch personenbezogener Daten

- Unwirksam
- keine Übergangsfrist
- sofort (seit 16.07.2020) anzuwenden

Übermittlung pbD in Drittländer

- Art. 44 DSGVO
- Datenübermittlung pbD außerhalb der EU (Drittland), wenn
- adäquates Datenschutzniveau
- im Zielland besteht

Übermittlung pbD in Drittland

- EU-Kommission stellte für USA adäquates Datenschutzniveau fest
- für Unternehmen, die bestimmte Vorgaben erfüllten
- Name "Privacy Shield"

- Vorteil für die EU-Vertragspartner: adäquates Datenschutzniveau durfte ohne weitere Prüfung angenommen werden

- Privacy Shield vom EuGH am 16.07.2020 unwirksam erklärt

EuGH: "Privacy Shield" unwirksam

- Befugnisse der US-Behörden
- Zugriff auf pbD von EU-Bürgern heimlich
- ohne effektiven Rechtsschutz
- Pflicht von US-Unternehmen auf Herausgabe pbD weltweit, auch wenn sich die Daten auf Servern in EU befinden

Risiko bei Nutzung von Privacy Shield

- Aufsichtsbehördliches Verfahren
- Untersagung der Verarbeitung pbD
- Bußgelder bis 4% des weltweiten Jahresumsatzes

- Zivilrechtliche Risiken durch Betroffene
- Durchsetzung der Rechte Betroffener (Löschung)
- Einstweilige Verfügung zur Untersagung der Verarb. pbD Betroffener
- Schadenersatz: Anwaltskosten

Adäquates Schutzniveau durch andere Mittel

- Möglichkeit: Standardvertragsklauseln
- engl. Standard Contractual Clauses (SCC)
- Standardschutzklauseln

- Musterverträge, die zwischen Verantwortlichen und Empfänger der pbD geschlossen werden
- Vertragsschluss reicht jedoch nicht aus
- Prüfung der weiteren Voraussetzungen notwendig

Standardvertragsklauseln

- Grundsätzlich anwendbar, wenn

- das selbe Schutzniveau personenbezogener Daten innerhalb der EU auch im Drittland garantiert werden kann
- Vertragspartner garantiert das Schutzniveau und hält es tatsächlich ein, Pflicht zur Prüfung durch den Verantwortlichen
- Voraussetzung: Vertragspartner hat Einfluss auf Datenschutz und Datensicherheit
- Vertragspartner hält entsprechende Maßnahmen vor und kann diese auch wirksam umsetzen

Standardvertragsklauseln

- Zugriff auf personenbezogene Daten durch NSA, Geheimdienste und weitere US-Behörden
- Pflicht zur Herausgabe der Daten weltweit (durch Anwendung von US-Recht, Cloud-Act)
- Kein wirksamer Rechtsschutz bzw. Rechtsbehelfe für Betroffene in den USA

- Pflicht des Verantwortlichen zu prüfen, ob das vom EuGH beschriebene Risiko des Zugriffs auf die pbD durch US-Behörden wirksam verhindert wird

Cloud Act

- erlaubt US-Behörden mit niedrigschwelligen Voraussetzungen die Herausgabe von pbD
- Unternehmen mit Sitz in USA
- weltweiter Zugriff (Herausgabepflicht)
- auch auf pbD, die sich auf EU-Servern befinden

- praktisches Problem: physische Herausgabe von Datenträgern?
- jedoch digitale Übermittlung

Prüfung in der Praxis

- Verfahrensverzeichnis aktualisieren
- Adressen, Datenkategorien, Angaben nach Art. 44 DSGVO

- Dienstleister auf Datentransfer überprüfen
- entweder direkter Datentransfer oder Einsatz von US-Dienstleistern
- Sub-Unternehmen

- Fragebögen nutzen und Dienstleister anschreiben

Prüfung in Praxis

- Erkennen von Datentransfers
- Eingesetzte Dienstleister prüfen

- US-Unternehmen erkennen (einfach bei Google, Facebook ect.)
- Subunternehmen herausfinden (Datenschutzerklärungen prüfen)

- Anschreiben der Unternehmen und Fragebögen ausfüllen lassen
- Alle Dienstleister abklopfen

Prüfung in Praxis

- Erste Hinweise auf Probleme: Nicht aktualisierte Datenschutzerklärungen
- Dienstleister beziehen sich immer noch auf Privacy Shield
- Telefonisches Nachfragen: Verwunderung und "Keine Ahnung"

Prüfung in Praxis

- Rechtsgrundlagen für Datentransfer ermitteln
- Standardvertragsklauseln
- Binding Corporate Rules (Verbindliche Datenschutzregeln im Unternehmen mit externer Zertifizierung und eigener Prüfung)
- Erforderliche Datentransfers (Transfer ist erforderlich und für Betroffenen erkennbar, z.B. bei Reise oder Versand von E-Mails zu Geschäftspartner)
- freiwillige, informierte Einwilligung
- Art. 49 DSGVO

Prüfung in Praxis

- Bestimmung des Risikos für Betroffene
- Verarbeitung von Daten besonderer Kategorien (Gesundheitsdaten, Leistungsbewertungen, Gewerkschaftszugehörigkeit, Religion, biometrische Daten ...)
- Nutzung von Videokonferenzen (berufliche E-Mail, berufliche Inhalte, jedoch sind Gesichter biometrische Daten ...)
- Newsletterdienste (welche Daten werden erhoben, Analysetools, Microzensus)

Prüfung in Praxis

- Bewertung von Schutzmaßnahmen
- Rückläufe von Antworten auf Versand des Fragebogens
- Auswertung der Rückläufer
- schwierigster Teil der Prüfung, setzt technische Kenntnisse voraus

- keine Backdoor
- Verschlüsselung von Daten
- Umgang mit Anfragen von US-Behörden (Abwehr mit Hilfe gerichtlicher Prüfung)

Prüfung in Praxis

- Standardvertragsklauseln sind anwendbar auf Auftragsverarbeiter in der ersten Linie (Verantwortlicher - Auftragsverarbeiter)

- Keine Anwendung auf Unterauftragnehmer (Verantwortlicher - Auftragsverarbeiter - Unterauftragnehmer)

- Keine Änderungen der Klauseln, da diese mit Behörden abgestimmt sind
- Zahlung von Vertragsstrafen (Bereitschaft des Dienstleisters)

Prüfung in Praxis: Beispiele

- Google
- Facebook: Untersagung der Verarbeitung am 10. September 2020

- Cloudservices (Dropbox)
- Amazon Web Services
- Datensicherung (Verschlüsselung?)
- Bewerbungsplattformen
- WebShop
- Newsletter

Nutzung von Alternativen

- Google Analytics: Matomo

- Alternative Drittländer mit anerkannten Datenschutzniveau (Schweiz, Kanada, Japan, Israel, Neuseeland)

Videokonferenzen

- Zoom, Teams ect. problematisch

- soweit möglich selbst hosten