Einleitung:

„Ungelöst, aber wieder in aller Öffentlichkeit! - Kurz mal durchgelüftet“

Wie war das noch? Ein paar Schlagzeilen dazu:

Über Datenschutzkreise hinaus sehr gut bekannt ist das (sogenannte) Schrems II Urteil des EuGH vom **16. Juli 2020** (C-311/18)[1]. Zu den Auswirkungen hat der Bundesbeauftragte (BfDI)[2] in einer 3-seitigen Stellungnahme Position bezogen und dazu ein „Prüfschema Drittstaatentransfers“ veröffentlicht[3].

Übrigens, die wissenschaftlichen Dienste des Deutschen Bundestages haben auf Anfrage aus dem Bundestag eine Stellungnahme / Dokumentation zum US-Datenrecht aus deutscher Datenschutzsicht erstellt[4]. Sehr interessante und übersichtliche Ausführungen zum Thema.

Das Handelsblatt berichtete unter dem **13. April 2021**[5] von Ausweitungen der Prüfung durch Aufsichtsbehörden, u. a. zur US – Cloud - Nutzung.

Wie haufe-online im **August 2021** berichtete[6], gibt es für Großbritannien einen Angemessenheitsbeschluss der EU, der aber nach 4 Jahren überprüft werden muss. Wenn die Briten allerdings, wie vorgesehen, sich durch eine Reformierung von der DS-GVO trennen wollen, kann dieser auch früher hinfällig werden und Großbritannien gilt dann als Drittland, was im Auge zu behalten ist.

Dann war und ist da noch **in 2022** die aktuelle Welle der Abmahnungen wegen Einbindung von „google-fonts“ in die eigene Website. Eine Vielzahl der Kommentierungen sieht eine Unrechtmäßigkeit wegen notwendiger Übermittlung der IP-Adresse darin, man sollte aber nicht zahlen (i.d.R. zwischen 100€ bis 200€). Jedoch sind die „google-fonts“ sofort lokal einzubinden, oder gleich eigene Schriftarten einbinden (z.B. siehe Fußnote[7]).

Aktuell – unter vielen anderen – berichtet die tageschau am **7. Oktober 2022** zum Vorstoß des US-Präsidenten mit einem neuen Dekret zum Datenschutzabkommen[8].

Inhalte

1. Grundsatz

Der Datenschutz reist mit den Daten! Bevor über den Transfer von personenbezogenen Daten in ein Drittland nachgedacht wird, müssen zunächst - selbstverständlich - die Voraussetzung für die „Rechtmäßigkeit der Verarbeitung“ nach Art.6 DS-GVO gegeben sein! Dazu kommt für besondere Kategorien von personenbezogenen Daten der Art.9 der DS-GVO und für Daten zu Straftaten der Art.10 DS-GVO (was ja immer gegeben sein muss!).

1 *Quelle: Info Curia: „EuGH Aktenzeichen = C-311/18“*
2 *Quelle: BfDI: Schrems II Urteil des EuGH (Urteil v. 16. Juli 2020, C-311/18) – Kernaussagen.“*
3 *Quelle: BfDI: „Prüfschema Drittstaatentransfers“*
4 *LINK: Wissenschaftliche Dienste des deutschen Bundestages: „US-Datenrecht, Zugriff von US – Behörden“*
5 *Quelle: Handelsblatt: „Deutsche Firmen in der Datenschutzfall – Behörden intensivieren Ermittlungen“*
6 *Quelle: haufe-online: „Großbritannien will Datenschutz reformieren und sich von der DSGVO lösen“*
7 *LINK: anwalt.de: „Abmahnungen wegen Google Fonts“*
8 *Quelle: tagesschau: „Vorstoß für ein neue Datenschutzabkommen (Vereinbarung mit der EU)“*

2. Checkliste zum Ankreuzen und Dokumentieren als Nachweis (-pflicht)

(a) Werden die personenbezogenen Daten rechtmäßig verarbeitet (Art.6, 9, 10 DS-GVO)

☐ **NEIN** Bitte prüfen und Rechtmäßigkeit schnellstmöglich erfüllen!

☐ **JA** Weiter mit (b)

(b) Werden personenbezogene Daten an Drittländer außerhalb der EU „offen gelegt“?

☐ **NEIN** Weiter mit (h)

☐ **JA** Weiter mit (c)

(c) Sind die Daten so verschlüsselt, dass kein Zugriff im Drittland möglich ist?

☐ **NEIN** Weiter mit (d)

☐ **JA** Weiter mit (h)

(d) Liegt für das Drittland ein Angemessenheitsbeschluss der EU vor?

LINK: *EU – Angemessenheitsbeschlüsse;EU Data Protection Supervisor: Erläuterung/Glossar*)

☐ **NEIN** Weiter mit (e)

☐ **JA** Weiter mit (h)

(e) Kann mit der Auswahl von bzw. der Schutzmaßnahmen nach Kapital V (Art.44-50) der DS-GVO ein gleichwertiges Schutzniveau gewährleistet werden?

Im besonderen Artikel 46 „Datenübermittlung vorbehaltlich geeigneter Garantien“ und Artikel 47 „Verbindliche interne Datenschutzvorschriften“, sowie Artikel 48 DS-GVO bei Gerichtsbeschluss im Drittland. (z.B. Standard – Datenschutzklauseln, interne Datenschutzvorschriften durchsetzbare Rechte, und Rechtsbehelfe mit wirksamen Mechanismen im Drittland).

LINK: EUR-Lex genehmigte Standard Vertragsklausel der EU

☐ **NEIN** Weiter mit (f)

☐ **JA** Weiter mit (g)

(f) Können zusätzliche Schutzmaßnahmen definiert und ergriffen werden, um ein gleichwertiges Schutzniveau der DS – GVO zu erlangen?

Damit ein gleichwertiges Schutzniveau erreicht wird, müssen nach dem EuGH – Urteil zusätzliche Maßnahmen in technischer, organisatorischer oder rechtlicher Hinsicht ergriffen werden, um die Gleichwertigkeit zu erreichen. Bei vertraglichen Anpassungen in Abweichung zu den Standard – Datenschutzklauseln sind diese als „ad-hoc-Klauseln“ VORAB durch die Aufsichtsbehörde zu genehmigen. (ergänzende Erläuterungen unter Punkt 4)

☐ **NEIN** Einsatz einer Alternative! Siehe Punkt 3 „Hinweise“

☐ **JA** Weiter mit (g)

(g) Sind die zusätzlichen Schutzmaßnahmen umgesetzt und praktisch wirksam?

☐ **NEIN** Wenn nicht kurzfristig wirksam: Einsatz einer Alternative! Siehe Punkt 3 „Hinweise“

☐ **JA** Weiter mit (h)

(h) Sind die Maßnahmen und die Prüfung dokumentiert?

☐ **NEIN** Es wird Zeit! (Mit einem ausgefüllte Druck starten, ist ein Anfang)

☐ **JA** Perfekt!

Ort / Datum Unterschrift (Verantwortliche)

3. Hinweise

Wird der Datentransfer in ein Drittland trotz Mängel im Schutzniveau (unzulässiger Weise) fortgeführt, besteht eine MELDEPFLICHT gegenüber der Aufsichtsbehörde!

Ja, es gibt eine Ausnahme nach DS – GVO Art. 49 „AUSNAHME FÜR BESTIMMTE FÄLLE“. Risikoaufklärung mit ausdrücklicher Zustimmung, (b) Vertragserfüllung oder (e) bei Rechtsansprüchen u. ä. Nach Art.49 (1) 2. Abs. „… darf eine Übermittlung an ein Drittland ... nur dann … wenn … nicht wiederholt erfolgt, nur eine begrenzte Zahl … betrifft, …“ - eben Ausnahmecharakter!

4. Was sind jetzt die, in komplexen Fällen noch notwendigen „zusätzlichen Schutzmaßnahmen“?

Der europäische Datenschutzausschuss (European Data Protection Board – edpb) hat von sich aus beschlossen, diese Frage zu untersuchen und nicht einfach so offenzulassen. Im November 2022 hat der edpb seine Empfehlungen für Verantwortliche, Unternehmen und die Aufsichtsbehörden in 46 Seiten zusammenfasst (Siehe Fußnote[9]) und erwartet von den Akteuren keine passive Haltung, sondern ein aktives Handel mit Nachweispflicht. Die Schlagzeilen:

Anmerkungen

- Fernzugriff aus einem Drittland (z. B. Support) und/oder Speicherung in einer Cloud (Wo? Vertragliche Whitelist/Blacklist?) außerhalb der EU ist immer als Übermittlung anzusehen!
- Immer ist die Wirksamkeit des nach Art.46 DS-GVO ausgewählten Übermittlungsinstruments im Hinblick auf die Gesamtumstände zu beurteilen (ggf. Rechtsgutachten einholen).
- Ergänzungen der Standardvertragsklauseln nach Art.46 Abs.2 c, d sind nicht genehmigungspflichtig, sofern keine Beeinträchtigung der genehmigten Klauseln besteht.
- Zusätzliche Maßnahmen sind nur als effektiv anzusehen im Sinne des EuGH, sofern genau die festgestellte Rechtslücke geschlossen wird. Sollte es letztendlich nicht möglich sein, ein im Wesentlichen gleichwertiges Schutzniveau zu erzielen, sind personenbezogenen Daten nicht zu übermitteln.

Empfehlungen und Beispiele

Technische Maßnahmen

✔ Verschlüsselung vor Transfer
(z.B. ein Backup mit personenbezogenen Daten wird vor Transfer (in eine Cloud) mit einer dem „Stand der Technik“ und den Zeitraum berücksichtigenden Verschlüsselung versehen und der Zugang ist nur über eine im Geltungsbereich der DS-GVO liegenden Berechtigung möglich.)

✔ Pseudonymisierung vor Transfer
(Vor Übermittlung u/o Analyse wird der Personenbezug derart entfernt, dass ohne Hinzuziehung zusätzlicher Daten eine Identifizierung der Person selbst, noch in einer größeren Gruppe möglich ist. Identifizierung nur über eine im Geltungsbereich der DS-GVO liegenden Berechtigung, die durch technisch – organisatorische Maßnahmen sichergestellt ist.)

✔ Transportverschlüsselung
(Auch wenn die Daten „nur“ über eine Land mit nicht angemessenem Schutzniveau geleitet werden könnten, gilt es einen Zugriffsschutz zu gewährleisten mittels einer Transportverschlüsselung mit dem Zeitraum angemessenem, effektiven Schutz nach dem Stand der Technik und Berechtigungen, die nur im Geltungsbereich der DS-GVO liegen.)

✔ Geschützter Empfänger
(Wenn sichergestellt ist, dass der Empfänger im Drittland über einen besonderen Schutz (Geheimhaltungspflicht auch gegenüber Behörden) verfügt, der einem Schutz nach DS-GVO gleich

9 *LINK: edpb: „Empfelung 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur …“*

kommt und den Zugriff von Dritten ausschließt, ist ein Datentransfer möglich. Voraussetzung ist eine Verschlüsselung nach dem „Stand der Technik“, mit exklusivem Zugriff nur durch Sender und Empfänger. (End-To–End).

✔ Verteilte Verarbeitung (Multi – Party – Processing)
(Ohne einen Personenbezug herstellen zu können, werden mehrere Auftragsverarbeiter mit der Verarbeitung von Teilmengen der Daten beauftragt, die ihnen und den Landesbehörden (auch gemeinsam) eine Identifizierung von Personen unmöglich machen. Eine Zusammenführung findet nur alleine beim Auftraggeber statt, was einen entsprechenden Nachweis erfordert)

✖ Auftragsverarbeitung mit Zugriff auf personenbezogene Daten in einem unsicheren Drittland ist nicht möglich!

✖ Auch innerhalb einer Unternehmensgruppe u/o eines gemeinsamen Geschäftszwecks können personenbezogen Daten nicht an unsichere Dritte oder Drittländer transferiert werden.

Vertragliche Maßnahmen

Da vertragliche Maßnahmen nur zwischen den Parteien und nicht auch gegenüber dem Drittland wirken, haben vertragliche Maßnahmen (Prüfung Wirksamkeit) i.d.R. unterstützende Wirkung.

✔ Transparenz
(Informationspflicht des Datenempfängers über ihm zugegangene und generelle behördliche Ersuchen, aktuelle rechtliche Regelungen, Zugriffe und Möglichkeiten von Behörden und Nachrichtendiensten, Gerichtsentscheidungen, entsprechende Informationen und Statistiken von Partnern u/o öffentlichen Quellen u. ä. zur aktuellen rechtlichen Einschätzung)

✔ Unterstützungspflichten
(Vertragliche Verpflichtungen, keine Hintertüren oder Ähnliches zu programmieren, keine Prozessänderungen für einen Personenbezug für sich selbst oder Dritte vorzunehmen und eine regelmäßige Prüfung zu ermöglichen. Pflicht zur sofortigen Information bei Auskunftsersuchen, Anwendung aller Rechtsmittel, sowie ggf. Information und rechtliche Unterstützung der Betroffenen. Dies verbunden mit einer Kündigungsklausel, um im Fall der Fälle den Transfer und die Verarbeitung sofort zu stoppen.)

Organisatorische Maßnahmen

Die vom europäischen Datenschutzausschuss vorgeschlagene (möglichen) Maßnahmen zielen auf die Ergänzung und Konkretisierung der Standardvertragsklauseln (Standard Contractual Clauses) ab. Dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 ist ein / sind genehmigte Muster beigefügt[10]. Der edpb schlägt dazu konkretisierte Maßnahmen in Bezug auf Transparenz, Rechenschaftspflicht, Datenminimierung, Normen und Verfahren vor. Neben den Einzelmaßnahmen ist sicherlich die Bildung eines gemeinsamen, entsprechend qualifizierten Datenschutzteams aus Juristen und IT – Spezialisten hervorzuheben. Das erleichtert die Einschätzung der aktuellen Lage, ermöglicht schnelle Reaktionen und die lokale Unterstützung für ggf. Betroffene.

Vorsichtiges Fazit:

Sofern die „Rechtsschutzlücken“ nicht durch Gerichte, Behörden oder andere vertrauenswürdige Institutionen eindeutig festgestellt wurden, ist m. E. ein Rechtsgutachten durch einen lokalen Juristen fast unumgänglich. Wie der Ausschuss (edpb) schreibt, bleibt es im Einzelfall zu prüfen, ob mit den zusätzlichen Maßnahmen die festgestellten Lücken im Datenschutz geschlossen werden.

Bei Bedarf, einfach einmal sprechen!

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

10 *Link: "Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021“*