Datenschutz-Depesche 2020/01:

Neustes EuGH-Urteil zum Datenschutz - das sollten Sie jetzt beachten!

Wer Amazon, Facebook, Google oder Microsoft oder andere US-amerikanische Produkte einsetzt und nicht ausschließen kann, dass personenbezogene Daten in den USA verarbeitet werden, tut dies auf Grund des Urteils des EuGH vom 17.07.2020 ab sofort ohne die Rechte und Sicherheit der Daten für seine betroffenen Interessenten und Kunden garantieren zu können. Damit verstößt der Verantwortliche gegen die Grundsätze der europäischen Datenschutz-Grundverordnung (Art. 5 Abs. 1 lit. f DSGVO) und das Unternehmen riskiert bis zu vier Prozent seines Jahresumsatzes.

Ohne auf die Details und Begründungen des Urteils einzugehen, kann man davon ausgehen, dass diese Entscheidung gefällt worden ist, um die EU-Bürger vor dem Zugriff der US-Geheimdienste zu schützen und dafür zu sorgen, dass die Rechte für die betroffenen Personen gewährt werden. Denn dies war auf der Grundlage des seit 2018 gültigen Angemessenheitsbeschlusses der EU, den sogenannten „US-Privacy-Shield“ nicht ohne Weiteres umzusetzen, oder haben Sie mal probiert von Ihrem Auskunftsrecht Gebrauch zu machen?

Wenn im Verzeichnis für Verarbeitungstätigkeiten bzw. im Auftrag mit dem US-Unternehmen bislang auf Basis des US-Privacy-Shields personenbezogene Daten in den USA verarbeitet wurden bzw. nicht ausgeschlossen werden kann, dass diese dort gespeichert werden, ist dies Datenschutz-rechtlich ab sofort nicht mehr möglich. Zwar haben die Datenschutz-Aufsichtsbehörden signalisiert im Moment keine Sanktionen zu verhängen, doch was muss jetzt getan werden, damit Sie eventuelle Risiken fürs Unternehmen erkennen und begrenzen können?

Hier erhalten Sie **neun Tipps aus der Praxis** zu diesem Thema in Form einer Checkliste:

1. Es handelt sich um personenbezogene Daten? Wenn ja, gehen Sie bitte weiter.
2. Sie haben die Datenflüsse in Ihrem Unternehmen analysiert und im Verzeichnis für Verarbeitungstätigkeiten gem. Art 30 DSGVO dokumentiert?
   Dazu gehören u.a., dass beispielsweise
   a. eine Rechtgrundlage festgelegt ist?
   b. die Kategorien der betroffenen Personen und der betroffenen personenbezogenen Daten beschrieben sind?
   c. der Zweck der Datenverarbeitung und deren Schutzbedarf definiert ist?
   d. nur die Daten verarbeitet werden, die notwendig sind?
   e. die Daten aktuell und richtig sind?
   f. die Datenweitergabe in ein Drittland dokumentiert wurde?

   Super, dann gehen Sie bitte zum dritten Punkt.
   Wenn nicht, wird es höchste Zeit dies jetzt zu tun.
3. Die personenbezogenen Daten wurden anonymisiert bzw. verschlüsselt bevor sie verarbeitet wurden (z.B. bei einem Cloud-Dienstleister gespeichert)? In diesem Fall brauchen Sie nichts weiter zu tun, sofern eine Zuordnung / Lesbarkeit für den Dienstleister nicht mehr ermöglicht ist.
4. Es wurde ein Auftragsverarbeitungsvertrag gem. Art 28 DSGVO mit dem Datenverarbeiter im In- oder Ausland geschlossen? Ein Muster zu diesem Vertrag

können Sie bei mir anfordern. Liegt diese Vereinbarung vor, können Sie zum nächsten Punkt gehen, wenn nicht, holen Sie dies bitte umgehend nach.

5. Jetzt gibt es zwei verschiedene Ansatzpunkte, die noch nicht rechtlich abgesichert, aber solange argumentier-bar sind, bis es eine andere (Gerichts-) Entscheidung gibt:
   a. Man geht aus dem geografisch-örtlichen Gültigkeitsbereich der EU-DSGVO aus und als „Aus- oder Drittland“ wird der ausländische Unternehmenssitz definiert, den das Unternehmen hat. Im Falle Microsoft z.B. Redmond, Washington, USA. Dies ist eine sehr übliche und unter den Aufsichtsbehörden sehr verbreitete Ansicht. Folgen Sie dieser Argumentation und wollen Sie das Risiko einer anderweiten Entscheidung vermeiden, gehen Sie bitte weiter zum nächsten Punkt (6.).
   b. Oder man geht vom Anwendungsbereich der EU-DSGVO aus und der Sinn und Zweck von Kapitel V der DSGVO ist es, den Schutz zu gewährleisten, wenn Daten aus dem „*Geltungsbereich“ der DSGVO* „hinausbefördert“ werden. Nun ist es im Beispiel von Microsoft so, dass Microsoft auch einen Sitz in Europa hat und wenn Sie als Vertreter des verantwortlichen Unternehmens eine Vereinbarung mit Microsoft abschließen, gilt die DSGVO als Grundlage. D.h. der unter Punkt 2. abgeschlossene Auftragsver-arbeitungsvertrag (AVV) fällt für beide Unternehmen unter den Geltungsbereich der DSGVO. Für beide Unternehmen gilt die DSGVO, da beide ihren Sitz in der EU haben, was ja auch gem. Art. 3 DSGVO so benannt ist. Das heißt die Daten würden nicht aus dem Geltungsbereich der EU heraus verarbeitet werden. Und wenn Sie dieser Argumentation folgen, benötigen Sie für diese Auftragsverarbeitung keine zweite „Sicherheitsstufe“ in Form von Standarddatenschutzvertragsklauseln oder dgl. (siehe nachfolgenden Punkt 6., da dies der Dienstleister (in diesem Beispiel Microsoft intern durch Binding Coperate Rules oder andere Maßnahmen gem. Kapitel V der DSGVO) sicherstellen selbst muss. M.E. können Sie also bei allen Verarbeitungen, die mit einem Dienstleister abgeschlossen werden, die eine Niederlassung in der EU haben auf dieser Basis zugrunde legen und es entfällt der nachfolgende Punkt und Sie haben die Sicherheit der Daten gewährleistet.

   Wenn Sie jedoch dem 5. Punkt im Buchstaben a. dieser Argumentation folgen gehen Sie bitte weiter zum Punkt 6.
6. Sie haben zusätzlich zu Ihrem Auftragsverarbeitungsvertrag eine internationale Sicherheitsmaßnahme als „2.Sicherheitsstufe“ gem. DSGVO Kapitel V zugrunde gelegt.
   Diese können sein:
   a. *Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses* gem. Art. 45 DSGVO., aktueller Stand siehe https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
      Dieser Punkt entfällt mit dem EuGH-Urteil vom 17.07.20.
   b. *Datenübermittlung vorbehaltlich geeigneter Garantien gem. Art. 46 DSGVO*
      - **ohne Genehmigung** der Aufsichtsbehörden auf Basis: Standarddaten-schutzklauseln der EU-Kommission, abgekürzt auch SCC, SDK oder SVK genannt.
      - **unter Genehmigung** der Aufsichtsbehörden für sonstige Vertragsklauseln. Diese individuellen, durch eine Aufsichtsbehörde angenommenen und damit genehmigten Vertragsklauseln, wie auch Alternativen, wie die verbindliche, interne Datenschutzvorschriften gem. Art. 47 DSGVO (BCR), genehmigte Verhaltensregeln (CoC) z.B. durch Branchenverbänden oder Zertifizierungen wurde zur

Vollständigkeit aufgenommen, sind aber aufgrund von sehr großem Zeitbedarf bzw. noch nicht verabschiedeten Zertifizierungen momentan (noch) nicht relevant.

c. *Datenübermittlung - Ausnahmen für bestimmte Fälle gem. Art. 49 DSGVO*
   - Ausdrückliche Einwilligung (💣) gem. Abs. 1 Buchstabe (lit.) a
   - Erfüllung eines Vertrages oder vorvertragliche Maßnahmen (!) gem. lit. b - auf Antrag der betroffenen Person

Mit dem o.a. Urteil des EuGH entfällt mit Unternehmen in der USA die Datenübermittlung gem. Buchstabe a. D.h. es verbleiben ab sofort nur die Standard-datenschutzklauseln, die Sie u.a. hier finden: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32001D0497. Sie erhalten den Link nur auf Set 1, da die Betroffenenrechte hier besser geregelt sind und die Aufsichtsbehörden aus Bayern den Abschluss dieser Standarddatenvertragsklauseln empfehlen.
Als zweite Lösungsvariante können Sie auch die Ausnahmeregelungen aus dem Buchstaben c. dieser Abhandlung verwenden. Bitte denken Sie an die Voraussetzung (Freiwilligkeit, Nachweis, Transparenz) einer Einwilligung, die bei dieser ausdrück-lichen Einwilligung für Datenübermittlung in die USA ebenfalls gilt und das ein Vertrag den Antrag der betroffenen Person enthalten muss, z.B. in den AGB oder den Datenschutzerklärungen.

7. Haben Sie die entsprechende Verarbeitung in den o.a. Datenschutzhinweisen mit aufgenommen? Wenn ja, ist alles in Ordnung und es geht zum nächsten Punkt. Wenn nein, ergänzen Sie bitte umgehend Ihre Datenschutzinformation und den entsprech-enden Hinweis und in den AGB (optionaler Hinweis), um die Transparenzgrundsätze sicherzustellen und beachten Sie Punkt neun.
8. Der vorletzte Punkt ist eine (Vor- und danach regelmäßige Über-)Prüfung der tech-nisch-organisatorischen Maßnahmen der vom Auftragsverarbeiter zugesicherten Sicherheit der Verarbeitung gerade, wenn sensible Daten wie Gesundheitsdaten verarbeitet werden. Wenn Sie dies initiiert haben, haben Sie ein DSGVO-gerechtes Datenschutzniveau erreicht.
9. Last but not least: Haben Sie den Datenschutzbeauftragten bestellt und angemeldet? Die Mitarbeitersensibilisierung und Einbindung in den Datenschutz im Unternehmen ist das A und O, deshalb lohnt es sich – auch für Fragestellungen, wie sie das aktuelle EuGH-Urteil aufwerfen, einen externen oder internen Datenschutzbeauftragten hinzuzuziehen. Darüber hinaus stehen Ihnen, als Datenschutz-Kunden, die Hinter-gründe dieses Artikel in Folienform oder als Workshop auf Nachfrage zur Verfügung.

Für alle Ihre Fragen wenden Sie sich jederzeit gerne an mich.

Ihr *Jens Wiemeyer*