Ausgabe 06/2021

Liebe Leserin, lieber Leser,

mit unserem aktuellen Newsletter geben wir Ihnen einen Überblick über die neuen EU-Standardvertragsklauseln, die die Europäische Kommission kürzlich veröffentlicht hat. Auch für den Versand von E-Mails gibt es eine neue Orientierungshilfe, die wir Ihnen kurz erläutern.

Unsere Themen und Quellen im Überblick:

- **Das ist „neu“ an den neuen EU-Standarddatenschutzklauseln**
  https://www.datenschutz-notizen.de/das-ist-neu-an-den-neuen-eu-standarddatenschutzklauseln-4330214/

- **Neue Orientierungshilfe der DSK zur Sicherheit bei der E-Mail-Übermittlung**
  https://www.datenschutzticker.de/2021/06/neue-orientierungshilfe-der-dsk-zur-sicherheit-bei-der-e-mail-uebermittlung/

- **Technische und organisatorische Maßnahmen nach DSGVO**
  https://www.dr-datenschutz.de/technisch-und-organisatorische-massnahmen-nach-dsgvo/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ Das ist „neu“ an den neuen EU-Standarddatenschutzklauseln

Im Rahmen des Urteils „Schrems II“ wurde der Angemessenheitsbeschluss Privacy Shield vom EUGH für unwirksam erklärt und gleichzeitig festgestellt, dass Standardvertragsklauseln grundsätzlich ihre Gültigkeit behalten. Über die Auswirkungen hatten wir Sie bereits informiert. Die EU-Kommission hat nunmehr eine neue Version der sogenannten Standardvertragsklauseln veröffentlicht. Alte Standardvertragsklauseln können theoretisch noch bis Ende September 2021 abgeschlossen werden, müssen aber bis spätestens Ende des Jahres 2022 aktualisiert werden. Somit ist zu empfehlen, bei bereits bestehenden Verhandlungen die neuen Standardvertragsklauseln zu berücksichtigen.

Anders als die bisherigen Klauseln, die immer lediglich eine konkrete Verarbeitungskonstellation behandelten (Verantwortlicher – Verantwortlicher bzw. Verantwortlicher – Auftragsverarbeiter), sind die neuen Standardvertragsklauseln modular aufgebaut und decken folgende Situationen ab:

- Modul 1: Verantwortlicher – Verantwortlicher
  Diese Konstellation gab es auch bei den alten Standardvertragsklauseln.
- Modul 2: Verantwortlicher – Auftragsverarbeiter
  Auch diese Konstellation gab es zuvor schon. Nunmehr ist aber daneben kein zusätzlicher Auftragsverarbeitungsvertrag mehr erforderlich (Art. 28 Abs. 7 DSGVO).
- Modul 3: Auftragsverarbeiter – (Unter)Auftragsverarbeiter
  Nunmehr können die Standardvertragsklauseln in Konstellationen zwischen zwei Auftragsverarbeitern eingesetzt werden. Wie das Modul für den Verantwortlichen und den Auftragsverarbeiter, ist auch in dieser Konstellation der Abschluss eines (Unterauftrags-) Verarbeitungsvertrages nicht erforderlich. Zu beachten ist, dass im Anhang I A der Verantwortliche als Vertragspartei benannt werden muss.
- Modul 4: Auftragsverarbeiter – Verantwortlicher
  Diese Konstellation ist gänzlich neu und soll Fälle abdecken, in denen ein Unternehmen aus einem Drittland einen Auftragsverarbeiter in der EU beauftragt, personenbezogene Daten, die der DSGVO nicht unterfallen (z.B. Daten von US-Bürgern), zu verarbeiten. Fraglich ist, ob dies praxisrelevant ist.

Das bereits erwähnte „Schrems II“- Urteil ist in den neuen Klauseln berücksichtigt und führt zu folgenden Pflichten:

1. Verpflichtende Datentransfer-Folgenabschätzung (DTFA)
   Die Vertragsparteien müssen demnach zusichern, dass kein Grund zur Annahme besteht, dass Gesetze im Drittland den Datenimporteur daran hindern könnten, seinen Pflichten aus den Standardvertragsklauseln nachzukommen (Abschnitt III Klauseln 14 und 15). Ohne eine DTFA ist eine solche Beurteilung nicht möglich.
2. Pflicht zur Abwehr von Regierungsanfragen
   Die Datenimporteure müssen Anfragen von Behörden ablehnen, die den Standardvertragsklauseln widersprechen (z. B. Offenlegung von Daten) und den Datenexporteur unverzüglich darüber informieren.

Die wichtigsten Informationen zu den neuen Standardvertragsklauseln sowie eine Checkliste mit Handlungsratschlägen finden Sie hier!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist in ihrer Pressemitteilung vom 21. Juni 2021 darauf hin, dass auch bei Verwendung der neuen EU-Standardvertragsklauseln eine Prüfung der Rechtslage im Drittland und zusätzlicher ergänzender Maßnahmen erforderlich ist.

Neu: Angemessenheitsbeschluss der EU-Kommission vom 28. Juni 2021:

Die Europäische Kommission hat einen Angemessenheitsbeschluss für das Vereinigte Königreich erlassen, wodurch Großbritannien ein angemessenes Datenschutzniveau bescheinigt wird und die UK nunmehr als sicheres Drittland gilt. Somit muss bei der Übermittlung personenbezogener Daten nach dem Brexit nicht auf EU-Standardvertragsklauseln zurückgegriffen werden. (…mehr)

➢ Neue Orientierungshilfe der DSK zur Sicherheit bei der E-Mail-Übermittlung

Die Datenschutzkonferenz (DSK) hat die Orientierungshilfe: Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail veröffentlicht. Berücksichtigt werden hauptsächlich Risiken auf dem Transportweg, so dass die Orientierungshilfe hauptsächlich Hilfestellungen für die Verschlüsselungstechniken einer E-Mail gibt.

Grundsätzlich sollte beim Versand personenbezogener Daten per E-Mail insbesondere bei sensiblen Daten immer genau abgewogen werden, ob ein anderer Kommunikationsweg vorzuziehen ist (z. B. Bewerberportal).

Was ist noch grundsätzlich zu beachten:

- Öffentliche E-Mail-Dienstanbieter müssen die Anforderungen der TR 03108-1 des Bundesamtes für Sicherheit und Informationstechnik (BSI) einhalten -> *Nutzer des Anbieters hat grundsätzlich eine Sorgfaltspflicht bei der Auswahl*
- die unternehmenseigenen Systeme und Endgeräte müssen sicher an jene der Dienstanbieter angebunden sein
- ergeben sich für die Verarbeitung gesteigerte Risiken, sind ggf. die zusätzlichen Anforderungen (z. B. Konfigurationseinstellungen) zu berücksichtigen

In den folgenden Fällen ergeben sich zusätzliche Verpflichtungen:

Wer gezielt personenbezogene Daten per E-Mail empfängt muss einen verschlüsselten Kanal bereitstellen (mind. TSL-Verbindung). Weiterhin sollten Maßnahmen getroffen werden, die die Authentizität und Integrität der empfangenen E-Mails sicherstellt. Besteht ein hohes Risiko für den Betroffenen ist eine qualifizierte Transportverschlüsselung und eine Ende-zu-Ende-Verschlüsselung einzusetzen.

Für den Versand personenbezogener Daten gelten ähnliche Empfehlungen. Verantwortliche und Auftragsverarbeiter sollten sich auch bei normalem Risiko an der TR 03108-1 des BSI (s.o.) orientieren und eine obligatorische Transportverschlüsselung sicherstellen.

Bei **Berufsgeheimnisträgern** ist meist ein hohes Risiko für die Betroffenen anzunehmen und somit o. g. Empfehlungen zu berücksichtigen. In jedem Fall ist das Risiko besonders zu prüfen.

➢ Technische und organisatorische Maßnahmen nach DSGVO

Technische und organisatorische Maßnahmen, die sogenannten TOMs, sind in Unternehmen umzusetzen, um die Einhaltung der DSGVO zu gewährleisten und dies auch nachweisen zu können. Hierbei wird großen Wert auf ein angemessenes Schutzniveau gelegt, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessen ist. Sicherlich ist es nicht immer leicht, die richtige Auswahl an Maßnahmen zu treffen.

Hier eine kurze Abgrenzung der Begriffe:

- **Technische Maßnahmen**: Begrifflich beziehen sich technische Maßnahmen dabei regelmäßig auf Hard-, Software- und Netzwerk-Komponenten, die für die Datenverarbeitung genutzt und herangezogen werden. Technische Maßnahmen sorgen für die Sicherheit der eingesetzten IT-Systeme und für deren äußere Absicherung. Maßnahmen sind z.B. die Pseudonymisierung und die Verschlüsselung personenbezogener Daten, der Einsatz von Firewalls, die Erstellung von Protokollen (Logging), Vorgaben für die Passwortvergabe und -komplexität. Daneben können es aber auch Maßnahmen zur Sicherung der Datenverarbeitungsanlagen sein, wie z.B. Gebäudesicherheit durch Alarmanlagen, Fenster- oder Türsicherungen.

- **Organisatorische Maßnahmen**: Organisatorische Maßnahmen richten sich insbesondere an den Ablauf und die durchführenden Personen. Sie sind dementsprechend alle nichttechnische Maßnahmen mit denen die Datensicherheit erreicht werden soll, wie z.B. Mitarbeiterschulungen im Datenschutz, Vertraulichkeitsverpflichtungen der Mitarbeiter, das Vier-Augen-Prinzip oder die Aufstellung von Berechtigungskonzepten.

In Art. 32 DSGVO werden beispielhaft konkrete technische und organisatorische Maßnahmen benannt. Eine Checkliste des Bayerischen Landesamt für Datenschutzaufsicht gibt eine gute Übersicht über Maßnahmen aus der täglichen Praxis. Weiterhin werden in Art. 32 folgende Schutzziele definiert:

1. **Sicherstellung der Vertraulichkeit:**
   Daten werden nur Befugten verfügbar gemacht und sind für Unbefugte nicht zugänglich, z.B. durch Maßnahmen der Zutritts-, Zugangs- und Zugriffskontrolle sowie der Auftrags- und Trennungskontrolle.

2. **Sicherstellung der Integrität:**
   Umfasst Maßnahmen zum Schutz vor Verfälschung von Daten, wie etwa die Weitergabe- oder Eingabekontrolle.

3. **Sicherstellung der Verfügbarkeit von Systemen:**
   Maßnahmen, die sicherstellen, dass informationstechnische Systeme stets gemäß ihrem Zweck und Funktionsumfang genutzt werden können. Darunter fällt etwa der Schutz der Daten gegen zufällige Zerstörung oder Verlust durch Virenschutz, unterbrechungsfreie Stromversorgung, Brandschutzmaßnahmen oder Datensicherungen.

4. **Sicherstellung der Belastbarkeit der Systeme und Dienste:**
   Maßnahmen zur Sicherstellung der Widerstandsfähigkeit und zur Ausfallkontrolle von Systemen, z.B. Aufbau eines Notfallmanagements (BCM – Business Continuity Management)

Auch für die Auswahl der TOMs gibt der Artikel folgenden Hinweis:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."

Grundlagen für die Auswahl der TOMs bieten somit die Ermittlung des Schutzbedarfs der Daten und eine Risikoanalyse. Da es nicht möglich ist, die Daten von Betroffenen „absolut" zu schützen, muss ein Schaden und damit das Risiko genau abgewogen werden. Dieses ist natürlich umso höher, je sensibler die Daten sind und je größer die Eintrittswahrscheinlichkeit der Vernichtung, des Verlusts, der Veränderung oder der Offenlegung von Daten ist.

Der Prozess zur Auswahl angemessener Sicherungsmaßnahmen der Landesbeauftragten für den Datenschutz Niedersachsen bietet hier eine gute Hilfestellung.

➢ Urteile

Schmerzensgeld in Höhe von EUR 5.000 für unerlaubte Foto-Veröffentlichung eines Mitarbeiters

Eine universitäre Einrichtung hatte unerlaubt das Foto einer Mitarbeiterin in einer Werbebroschüre verwendet. Insbesondere stellte die Einrichtung ihre internationale Ausrichtung mit Verweis auf die farbige Hautfarbe der Mitarbeiterin heraus, sodass die Ethnie der Klägerin zur zentralen Aussage des Bildes wird.

Urteil des ArbG Münster vom 25. März 2021 – Az.: 3 Ca 391/20

Cookie-Banner „Durch die weitere Nutzung der Website stimmen Sie... zu" ist rechtswidrig

Bei der Formulierung fehle es an der notwendigen Einwilligung des Nutzers. In der bloßen Weiternutzung der Webseite könne keine konkludente Einwilligung gesehen werden.

Urteil des LG Köln vom 13. April 2021 – Az.: 31 O 36/21

➢ Weitere interessante Links

Digitaler Impfpass: Schlagen wir einen gefährlichen Weg ein?
Geimpfte können sich bei Apotheken ein Zertifikat ausstellen lassen. Zusammen mit der dazugehörigen CovPass-App oder der Corona-Warn-App entsteht der digitale Impfpass. Ein Kommentar hierzu…
https://www.dr-datenschutz.de/digitaler-impfpass-schlagen-wir-einen-gefaehrlichen-weg-ein/

Praxishinweise zum Fragebogen "konzerninterner Datenverkehr"
Die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) gibt Unternehmen Hinweise zur Beantwortung des Fragebogens der Aufsichtsbehörden zum konzerninternen Datenverkehr nach Schrems II.
https://www.gdd.de/aktuelles/startseite/praxishinweise-zum-fragebogen-konzerninterner-datenverkehr

Zoom vs. MS Teams 2:1
Vergleich der Videokonferenz-Tools…
https://www.datenschutz-notizen.de/zoom-vs-ms-teams-21-1230159/

TKG-Novelle verabschiedet
Der Bundestag hat mit den Stimmen der GroKo-Fraktionen den von der Regierung eingebrachten Gesetzentwurf zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) beschlossen. Die neuen Regelungen treten am 1. Dezember 2021 in Kraft.
https://www.datenschutzticker.de/2021/06/tkg-novelle-verabschiedet/

Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht
Hilfestellungen zum Datenschutz bei der Kontaktdatenerfassung und anderen infektionsschutzrechtlichen Aufgaben.
https://www.lda.bayern.de/media/pm/pm2021_04.pdf

Sind wir lästige Cookie-Banner bald los?
Nur zwei Wochen nach Bekanntgabe der automatisierten Überprüfung von Cookie-Bannern veröffentlicht die von dem Datenschutz-Aktivisten Max Schrems gegründete Organisation „noyb“ nun einen Vorschlag für ein neues automatisches Browser-Signal, das Cookie-Banner zukünftig obsolet machen könnte.
https://www.dr-datenschutz.de/sind-wir-laestige-cookie-banner-bald-los/