LOSCHELDER

Newsletter Datenschutzrecht

Juni 2021

Sehr geehrte Damen und Herren,

die letzten Wochen waren turbulent in Sachen Datenschutz: Max Schrems startet eine weitere Beschwerdeoffensive – diesmal nimmt er mit Hilfe von „Legal Tech“ die Gestaltung von Cookie-Bannern ins Visier und hat in der ersten aktiven Woche dem Vernehmen nach bereits 560 Beschwerden an verschiedene Unternehmen verschickt. Am 1. Juni dann der nächste Paukenschlag: Mehrere Datenschutzaufsichtsbehörden starten eine breit angelegte Schwerpunktprüfung „Drittstaatentransfer“, u.a. Bayern, BW, Berlin, Rheinland-Pfalz, Niedersachsen und Hamburg. Und nur 4 Tage später veröffentlichte die Europäische Kommission die (insofern wirklich hilfreichen) finalen Texte der neuen Standardvertragsklauseln für den Drittstaatentransfer sowie – erstmals – Musterklauseln für Auftragsverarbeitungsverträge.

Viel Stoff für unseren Newsletter. Wir wünschen viel Spaß bei der Lektüre, mag hier für die notwendige Umsetzung auch einiger weiterer Aufwand drohen.

Vor den Sommerferien melden wir uns zudem noch mit unserem nächsten Lunch@Loschelder-Webinar zu einem in der Praxis überaus wichtigen und regelmäßig wiederkehrenden Thema:

Die **Rollenverteilung im Datenschutzrecht** – Verantwortlicher, Gemeinsam Verantwortliche oder Auftragsverarbeiter, wer ist was?

Wann? 16.06.2021, 12:00-12:30 Uhr

Weitere Informationen dazu finden Sie unter https://loschelder.de/de/webinare.html, melden Sie sich gerne (kostenfrei) an unter webinare@loschelder.de.

Inhalt

Es wird ernst: Aufsichtsbehörden prüfen Drittlandtransfers

Kommt jetzt Schrems III? – Cookie-Banner auf dem Prüfstand

Neue Standardvertragsklauseln: Umstellung erforderlich

Auftragsverarbeitungsverträge: EU-Kommission veröffentlicht Muster

Zu guter Letzt

Es wird ernst: Aufsichtsbehörden prüfen Drittlandtransfers

Der Paukenschlag vom 1. Juni: Etliche Datenschutzaufsichtsbehörden machen ernst und starten eine Schwerpunktprüfung „Drittlandtransfer". Konkret geht es darum, ob die Konsequenzen aus dem EuGH-Schrems II-Urteil aus dem letzten Jahr umgesetzt wurden. Fand eine interne Analyse statt, wo personenbezogene Daten in Drittländer außerhalb des EWR übermittelt wurden? Ist das inzwischen ungültige EU-U.S.-Privacy Shield durch andere Instrumente ersetzt worden? Wie steht es um Vertragsstatus und Betroffeneninformationen? Was genau die Behörden wo unter die Lupe nehmen, haben wir nebst erster Handlungstipps zusammengefasst.

Quer durch die Republik erschienen Anfang Juni Pressemitteilungen auf den Homepages etlicher Datenschutzaufsichtsbehörden: Etwa in Baden-Württemberg, Bayern, Berlin, Brandenburg, Hamburg, Niedersachsen, Rheinland-Pfalz und dem Saarland verkündeten die Datenschutzaufsichtsbehörde ihre Teilnahme an der länderübergreifenden Kontrolle von Datenübermittlungen in Drittstaaten (also Länder außerhalb der EU und des EWR).

Verschickt werden seither Fragebögen an diverse Unternehmen, die sich mit der Übermittlung personenbezogener Daten in Drittstaaten unter spezifischen Schwerpunktthemen beschäftigen. Im Fokus stehen:

- Bewerberportale
- Konzerninterner Datenverkehr
- Mailhoster
- Tracking
- Webhoster

Die entsprechenden Fragebögen sind auf den Websites der Datenschutzaufsichtsbehörden abrufbar. Die Inhalte überraschen im Grundsatz nicht: Gefragt wird letztlich danach, ob die vom EuGH in seiner Schrems II-Entscheidung aus Juli 2020 festgehaltenen Maßstäbe eingehalten werden.

Die Beantwortung derartiger „Fragebögen" ist zunächst freiwillig. Allerdings steht den Behörden im nächsten Schritt der Erlass eines formalen Auskunftsersuchens offen, das dann auch (zwangsweise)

durchgesetzt werden kann. Es empfiehlt sich daher oft, die Fragebögen sorgfältig zu bearbeiten. „Sorgfalt“ bezieht sich dabei auch auf eine abgewogene Präsentation des Status quo und der seit dem EuGH-Urteil im vergangenen Sommer ergriffenen Maßnahmen.

Von zentraler Bedeutung ist dabei, dokumentieren zu können, dass

- im Unternehmen analysiert wird bzw. bestenfalls bekannt ist, wo welche personenbezogenen Daten in Drittländer übermittelt werden,
- bei US-Übermittlungen nicht mehr auf das vom EuGH für ungültig erklärte EU-U.S.-Privacy Shield gesetzt wird,
- die Transferprozesse geprüft und alternative Übermittlungsinstrumente (etwa Standardvertragsklauseln mit zusätzlichen Maßnahmen und Einzelfallprüfung, Einwilligungen o.ä.) im Blick sind,
- ein Wechsel auf EU-Anbieter zumindest geprüft wurde.

Etwa die am 7. Juni im Amtsblatt der EU verkündeten neuen Standardvertragsklauseln der EU-Kommission können hier nun Hilfestellung bieten, Drittstaatentransfers besser abzusichern. Wie genau, erläutern wir in unserem dritten Beitrag in diesem Newsletter – es empfiehlt sich, die neuen Standardvertragsklauseln möglichst zügig gerade für US-Transfers zu vereinbaren.

Kommt jetzt Schrems III? – Cookie-Banner auf dem Prüfstand

Am 31. Mai kündigte die NGO NOYB, hinter der Max Schrems steht, eine Beschwerdewelle an, gerichtet gegen Cookie-Banner. Konkret ist nach Ansicht der NOYB die weit verbreitete Ausgestaltung der Banner mit einem ersten Übersichtslayer und den Klickoptionen „Alle akzeptieren" – deutlich hervorgehoben – sowie – weniger augenfällig – „Einstellungen" oder „ablehnen" DSGVO-widrig. Über 500 Beschwerden sollen in der ersten Woche an diverse Websitebetreiber in der EU verschickt worden sein. Mit einer speziellen Software scannt NOYB dafür die Websites nach verschiedenen Kriterien. Die Drohung: Ändert euer Cookie-Banner oder wir beschweren uns bei der zuständigen Datenschutzaufsichtsbehörde. Droht hier Ungemach? Und wie kann reagiert werden, wenn ein solches Schreiben eintrifft?

Die datenschutz- und ePrivacy-konforme Ausgestaltung von Cookie-Bannern auf Websites ist ein Dauerbrenner. Von statischen Seiten mit wenigen Verarbeitungsvorgängen bis hin zu Websites mit umfangreichem Werbetracking begegnen Nutzern die Banner in der unterschiedlichsten Ausgestaltung. Eine optimale Lösung – benutzerfreundlich, transparent und wirkungsvoll im Betreibersinne – hat dabei wohl noch niemand gefunden.

Vermehrt durchgesetzt hat sich in den letzten Monaten eine Gestaltung auf mehreren Ebenen: Ebene 1 informiert im groben Überblick, mit einem kurzen Text und den Optionen „Alle akzeptieren" oder „Einstellungen", ggf. auch – meist weniger deutlich ersichtlich – „nur notwendige Cookies akzeptieren". Auf Ebene 2 und Ebene 3 gibt es dann zunehmend detaillierte Informationen mit einer Übersicht über die verschiedenen Zwecke (Ebene 2, etwa „Analyse – Marketing – Personalisierung") und dann auf Ebene 3 eine Listung aller einzelnen Anbieter mit den jeweiligen Verarbeitungszwecken. Diese Gestaltung dient zweierlei: dem Benutzer, der sich durch die Details nur nach Wunsch klicken muss; genauso aber auch dem Websitebetreiber, da die Conversion Rate bei derartiger Gestaltung oft besser ist.

Die Vorteile für den Benutzer jedenfalls sieht NOYB so nicht. Aus ihrer Sicht sind – verkürzt – derartige Cookie-Banner regelmäßig datenschutzrechtswidrig, da sie zu einem „Alle akzeptieren" verleiten und nicht genau so simpel einen Klick auf „Alle ablehnen"

ermöglichen. Es fehle an einer von der DSGVO geforderten simplen Ja/Nein-Option.

Die Vorgehensweise: NOYB schreibt die Unternehmen direkt an und offeriert einen Monat Umstellungszeit. Wenn diese nicht genutzt werde, würden Beschwerden bei den Datenschutzaufsichtsbehörden eingereicht. Geplant ist auf diesem Weg eine Zustellung von bis zu 10 000 Beschwerden weltweit inkl. Schritt-für-Schritt-Anleitung für die Unternehmen, wie sie ihre Softwareeinstellungen ändern können.

Es lohnt sich, die Entwicklung zu monitoren, werden vergleichbare Cookie-Banner genutzt. Sollte Ihr Unternehmen ein Beschwerdeschreiben von NOYB erhalten, ist eine konkrete Prüfung anzuraten: Die Rechtsposition der NOYB ist eine Auffassung der möglichen Lesarten der DSGVO. Hier sollte ein genauer Blick auf die konkrete Gestaltung des Cookie-Banners erfolgen und sorgfältig abgewogen werden, ob eine Umgestaltung tatsächlich angebracht ist.

Neue Standardvertragsklauseln: Umstellung erforderlich

Nach langem Warten ist es soweit: Neue Standardvertragsklauseln für internationale Datentransfers stehen zur Verfügung. Die finalen Texte hat die EU-Kommission am 4. Juni veröffentlicht, am 7. Juni folgte die formale Verkündung im Amtsblatt der EU. Die Texte bringen einige Neuerungen mit sich, mehr Aufwand in der Anwendung, aber auch mehr Rechtssicherheit etwa für US-Transfers. Nun gilt es, bestehende Verträge anzupassen und die geforderten Prüfungen und Dokumentation dafür zu erstellen. Das kostet Ressourcen, bringt aber auch die Chance auf einen sichereren Datentransfer und vielleicht sogar eine Lösung für die Nutzung einiger US-Tools mit sich … Wir stellen Ihnen in diesem Beitrag den wesentlichen Inhalt der Neuregelungen vor und erläutern, was jetzt zu tun ist.

Werden personenbezogene Daten in ein Drittland außerhalb der EU und des EWR übermittelt, haben Verantwortliche bzw. Auftragsverarbeiter dort ein angemessenes, den Gegebenheiten in der EU gleichwertiges Schutzniveau abzusichern. Art. 44 ff. DSGVO enthalten dafür diverse Instrumente, u.a. die sog. Standardvertragsklauseln. Bislang galten die alten Klauseln aus 2001 bzw. 2010 fort. Endlich hat die EU-Kommission nun neue Klauseln erlassen: Ganz offiziell ersetzen diese ab dem 28.09.2021 die alten Klauseln, spätestens zum 27.12.2022 müssen alle alten Vertragsklauseln durch die neuen ersetzt sein.

Sind aktuell Drittstaatentransfers nicht hinreichend abgesichert – wie in vielen Fällen bei US-Transfers derzeit der Fall – lohnt sich eine zügigere Umstellung auf die neuen Klauseln. Denn diese enthalten eine Reihe zusätzlicher Absicherungen, wie diese von den Datenschutzaufsichtsbehörden nach der EuGH-Entscheidung „Schrems II“ zum US-Transfer im letzten Sommer gefordert wurden. Und mehr noch: Die neuen Standardvertragsklauseln greifen den in der Praxis viel diskutierten, von den Aufsichtsbehörden bislang aber abgelehnten Gedanken einer Risikoabwägung auf (Abschnitt III, insb. Fn. 12): Wenn nationale Behörden qua Rechtslage zwar auf personenbezogene Daten in unverhältnismäßigem Umfang und ohne wirksame Rechtsbehelfe zugreifen dürften, dies aber aus dokumentierten Gründen praktisch quasi ausgeschlossen ist, kann u.U. doch ein angemessenes Schutzniveau angenommen werden …

Und auch weitere hilfreiche Anpassungen sind in den neuen Klauseln enthalten: Mehrparteienverhältnisse sind – endlich – konkret mit erfasst und auch die Option einer „Drittbegünstigung" ist – praxisnah – vorgesehen. Hierüber können etwa internationale Produktangebote abgesichert und ggü. den Kunden als „Drittbegünstigte" bereitgestellt werden. Abgedeckt werden nunmehr auch die unterschiedlichen Rollenkonzepte, etwa die Datenübermittlung von Auftragsverarbeitern an Verantwortliche im Drittstaat.

Nicht mehr möglich sein wird indes der in der Vergangenheit oft praktizierte schlichte Abschluss der Klauseln, ohne diese tatsächlich mit Leben zu füllen. Denn eine Prüfpflicht wird nun ebenso expressis verbis etabliert wie teils umfangreiche Dokumentations- und Informationspflichten etwa des Datenimporteurs im Drittland. Eine schlichte Unterschrift unter den Klauseln wird daher künftig nicht mehr ausreichen.

Dies bedeutet – zusammengefasst: Unsichere Datentransfers sollten möglichst zügig daraufhin geprüft werden, ob ein Abschluss der neuen Standardvertragsklauseln hier für eine verbesserte Situation sorgen kann. Alle übrigen auf Standardvertragsklauseln aufbauende Prozesse sollten im Verlauf der kommenden Monate überprüft und auf die neuen Klauseln umgestellt werden. Handlungsbedarf besteht hier in jedem Fall – spätestens bis Ende 2022.

Doch nun zu den Hintergründen:

Drittstaatentransfer – Modernisierungsbedarf und Schrems II-Urteil

Die alten Standardvertragsklauseln zum Drittstaatentransfer von 2001/2010 waren in zweierlei Hinsicht überarbeitungsbedürftig: Zum einen stammen die bisherigen Klauseln (Beschlüsse 2001/497/EG und 2010/87/EU) noch aus Zeiten vor Erlass der DSGVO. Deshalb war – so die EU-Kommission in ihrer Pressemitteilung – eine Anpassung an die Realitäten der modernen Datenübertragung und internationalen Interaktion von Unternehmen erforderlich. Besonders der zunehmende Einsatz von Verarbeitungsvorgängen mit mehreren Importeuren und Exporteuren und langen, komplexen Verarbeitungsketten musste abgebildet werden.

Zum anderen waren die Standardvertragsklauseln spätestens seit dem berüchtigten Schrems II-Urteil des EuGH aus dem letzten Jahr heftiger Kritik ausgesetzt. In diesem Urteil erklärte der EuGH das sog. EU-U.S.-Privacy Shield, den Angemessenheitsbeschluss zur Datenübertragung in die USA, unter anderem wegen umfassenden und mit den Standards der DSGVO nicht zu vereinbarenden Datenzugriffsrechten der US-Sicherheitsbehörden für unwirksam. Zwar wurden die Standardvertragsklauseln, die bei Fehlen eines Angemessenheitsbeschlusses eine geeignete Rechtsgrundlage für den Datentransfer in ein Drittland nach Art. 46 Abs. 2 lit. c DSGVO darstellen können, ausdrücklich nicht für unwirksam erklärt. Der EuGH äußerte aber hinsichtlich des Zugriffs der Sicherheitsbehörden ähnliche Bedenken wie beim Datentransfer auf der Grundlage des Angemessenheitsbeschlusses und verordnete bei Verwendung der Standardvertragsklauseln eine umfassender Einzelfallprüfung, ob die vertraglichen Vereinbarungen auch tatsächlich durchsetzbar sind. Denn Behörden können durch einen Vertrag zwischen zwei Unternehmen regelmäßig nicht in ihren nach nationalem Recht bestehenden Zugriffsrechte beschränkt werden.

Überarbeitete Klauseln für den Drittstaatentransfer personenbezogener Daten:

Die neuen Standardvertragsklauseln berücksichtigen all dies. Zu den wesentlichen Änderungen und Regelungen der nun beschlossenen neuen Standardvertragsklauseln gehören:

- **Modularer Ansatz**: Die neuen Klauseln sind als Module verfasst, d.h. neben allgemeinen Klauseln werden Klauselfassungen für unterschiedliche Datenübermittlungsszenarien und Verarbeitungsketten angeboten, unter denen die Vertragsparteien das Modul auswählen sollen, das am besten auf ihre jeweilige Situation passt. Darüber hinausgehende Modifikationen sind nach wie vor nicht zulässig.

- **Anwendung auf und Einbindung von Verarbeitungsketten:** Zudem werden nun Klauseln für die Anwendung auf unterschiedliche Verarbeitungsketten angeboten, etwa für die Beziehung zwischen Auftragsverarbeitern als Datenexporteur und Unterauftragsverarbeitern als Datenimporteur. In den bisherigen Standardvertragsklauseln war nur das

Übertragungsszenario vom Verantwortlichen zu Verantwortlichen oder Auftragsverarbeitern erfasst. Ketten, die in der Praxis häufig anzutreffen sind, waren damit kaum abzubilden. Hinzu kommt die neue Möglichkeit, dass mehrere Datenex- und -importeure während der Laufzeit eines Vertrages beitreten können.

- **Klare Regelung der Weiterübermittlung:** Die neuen Standardvertragsklauseln sehen Vorgaben über die Weiterübermittlung personenbezogener Daten an einen Datenimporteur in einem anderen Drittland vor. Dies soll nur zulässig sein, wenn der Empfänger ebenfalls dem Vertrag beigetreten ist, der Fortbestand des Datenschutzes etwa aufgrund eines Angemessenheitsbeschlusses der Kommission gewährleistet ist oder in bestimmten Situationen auch bei der ausdrücklichen Einwilligung des Betroffenen.

- **Vorherige Zusicherung der Einhaltung des Datenschutzniveaus:** Neu ist auch die Verpflichtung der Parteien, sich gegenseitig vor Abschluss des Vertrages zuzusichern, dass ihnen keine Gründe bekannt sind, aufgrund derer die vertraglichen Verpflichtungen nicht eingehalten werden können. Zu berücksichtigen haben die Vertragsparteien dabei:

    - Die konkreten Umstände des Datentransfers (etwa die Kategorie der verarbeiteten Daten, den Zweck der Übermittlung etc.);

    - Die Rechtslage und Behördenpraxis im Drittland vor allem hinsichtlich des Zugriffs von Behörden auf personenbezogene Daten nach zuverlässigen Informationen und gegebenenfalls praktischen Erfahrungen;

    - Ob und inwieweit zusätzliche Garantien und Maßnahmen zur Sicherstellung eines gleichwertigen Datenschutzniveaus ergriffen wurden (für diese kann sich an den Empfehlungen 01/2020 des EDSA orientiert werden).

  Der Datenimporteur hat dem Exporteur für diese Beurteilung sachdienliche Informationen zur Verfügung zu stellen, die

Einschätzung ist von den Parteien zu dokumentieren und auf Anfrage den Datenschutzbehörden darzulegen.

Die Beurteilung erfordert eine konkrete, dokumentierte Prüfung. Besonders deutlich wird das in Klausel 8, nach der der Datenexporteur versichern muss, „sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur – durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen – in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen" – dies muss dokumentiert werden.

- **Fortlaufende Transparenz- und Informationspflichten; Vertragslösung:** Der Datenimporteur wird zudem verpflichtet, die Entwicklungen der Rechtslage in seinem Land zu beobachten, zu dokumentieren und den Datenexporteur unverzüglich darauf hinzuweisen, wenn er befürchtet, die Verpflichtungen des Vertrages nicht länger einhalten zu können. Dem Importeur sollten im Gegenzug die Möglichkeit der Aussetzung der Datenübermittlung und gegebenenfalls auch das Recht zur Lösung vom Vertrag zustehen.

  Auch über etwaige Anfragen oder zwingende Verfügungen der nationalen Behörden zur Offenlegung der übermittelten Daten soll der Datenimporteur den Exporteur – soweit rechtlich zulässig – informieren, den Exporteur zumindest mit aggregierten Daten in regelmäßigen Abständen informieren, Anfragen und Antworten auf Offenlegungsgesuche dokumentieren und – sofern es entsprechende Zweifel an der Rechtmäßigkeit der Anfrage nach nationalem Recht gibt – den Rechtsweg gegen behördliche Offenlegungsanordnungen ausschöpfen. All dies soll der Datenimporteur in einer Art und Weise dokumentieren, in der sie den Datenschutzaufsichtsbehörden auf Anfrage vorgelegt werden kann.

- **Einbindung und Schutz der Betroffenen als Drittbegünstigte:** Unverändert bleibt, dass Betroffene als Drittbegünstigte in den Vertrag eingebunden werden und die Rechte des Vertrages geltend machen und durchsetzen können. Eine Verpflichtung, den Betroffenen bei der Wahrnehmung seiner Rechte im Drittland zu unterstützen,

wie es der EDSA in seinen Empfehlungen 01/2020 zur Ergänzung der Standardvertragsklauseln vorgesehen hat, wurde nicht aufgenommen.

- **Vertragliche Haftungsregelungen:** Die Standardvertragsklauseln sehen zudem Haftungs- und Entschädigungsklauseln vor, die im Wesentlichen an der DSGVO orientiert sind. Zum einen haften die Parteien untereinander für Vertragsverletzungen, zum anderen haften die Parteien jeweils auch gegenüber den durch die Datenverarbeitung Betroffenen für materielle und immaterielle Schäden, die durch die Verletzung ihrer Rechte aus dem Vertrage entstanden sind. Der Datenexporteur haftet davon unabhängig weiterhin nach den Vorschriften der DSGVO gegenüber den Betroffenen. Als Datenexporteure haften Verantwortliche für das Verhalten ihrer Auftragsverarbeiter und Auftragsverarbeiter für ihre Unterauftragsverarbeiter, wobei sie bei einer Inanspruchnahme durch die betroffenen Personen einen Ausgleich im Innenverhältnis abhängig vom Grad der Verantwortung des Datenimporteurs suchen können.

- **Einbindung in Verträge und Abweichungen:** Es ist ausdrücklich vorgesehen, dass die Standardvertragsklauseln in größere, umfassendere Verträge mit weiteren Verpflichtungen eingebunden werden können. Wesentliche Voraussetzung ist dabei jedoch, dass die sonstigen vertraglichen Bestimmungen nicht unmittelbar oder mittelbar im Konflikt mit den Standardvertragsklauseln stehen oder hierdurch die Grundrechte oder Grundfreiheiten der Betroffenen eingeschränkt werden. In Fällen des Widerspruchs oder des Konflikts der Standardvertragsklauseln zu anderen vertraglichen Regelungen genießen die Standardvertragsklauseln ausdrücklich Vorrang.

Umsetzungsfrist

Die neuen Standardvertragsklauseln treten am 27.06.2021 in Kraft (20 Tage nach Veröffentlichung im Amtsblatt der EU am 07.06.2021). Am 27.09.2021 werden die alten Klauseln von 2001/2010 aufgehoben, spätestens zum 27.12.2022 müssen bis dahin

abgeschlossene, „alte“ Standardvertragsklauseln durch die neuen ersetzt werden.

Eine „Amnestie“ ist mit diesen Umsetzungsfristen nur bedingt verbunden: Ist schon heute kein angemessenes Schutzniveau im Drittland abgesichert, wird dieses auch nicht für die Übergangsfrist fingiert. Konkret betrifft dies eine Vielzahl von US-Transfers. Dort wird es in etlichen Fällen ratsam sein, die neuen Klauseln so schnell wie möglich abzuschließen, wenn keine anderweitigen Absicherungen bestehen.

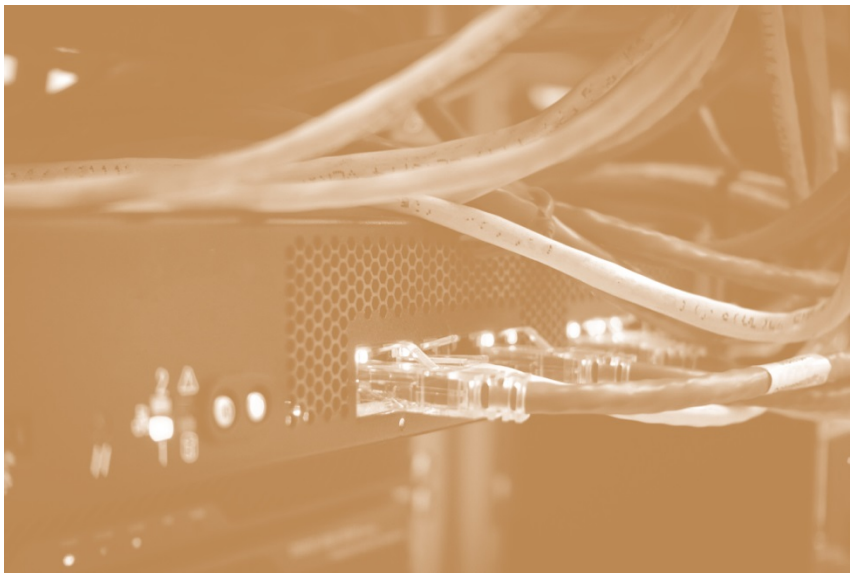
Erleichterung des Datentransfers in die USA?

Vorteil der neuen Standardvertragsklauseln ist, dass sie Unternehmen den Abschluss vertraglicher Vereinbarungen mit internationalen Partnern vereinfachen. Durch die Anerkennung der EU-Kommission können die Klauseln eingesetzt werden, ohne dass einer Prüfung oder Anerkennung durch die Datenschutzaufsichtsbehörden bedarf.

Zudem bieten die neuen Standardvertragsklauseln durch die Vielzahl neuer Verpflichtungen zur Überprüfung der Rechtslage im Drittstaat insbesondere für den Datentransfer in die USA eine rechtssichere Grundlage als die Vorgängerversion. Ob aber die Vereinbarung neuer Verträge auf der Grundlage der Standardvertragsklauseln allein ausreichen wird, um den Anforderungen des Schrems II-Urteils zu entsprechen, ist noch unklar. Der EDSA stellte in seinen Empfehlungen 1/2020 fest, dass rein vertragliche Verpflichtungen alleine regelmäßig nicht ausreichen werden, um ein mit der DSGVO vergleichbares Datenschutzniveau beim Datentransfer sicherzustellen. Der in Abschnitt III der neuen Standardvertragsklauseln zu findende risikobasierte Ansatz der EU-Kommission spricht dafür, wenn die Anforderungen dort eingehalten werden (insbesondere die Dokumentation durch den Datenimporteur, dass nach den „Gepflogenheiten“ und praktischen Erfahrungen nicht mit Zugriffen der US-Behörden zu rechnen ist. Ob den Gerichten das am Ende als Garantien für die Datensicherheit ausreicht, bleibt abzuwarten. Können zusätzlich technische Sicherungsmaßnahmen ergriffen werden, wird dies indes nach wie vor die Rechtssicherheit von Datentransfers weiterhin erheblich steigern.

Standardvertragsklauseln vs. Standarddatenschutzklauseln

Zum Abschluss noch ein Hinweis: Aufmerksamen Lesern der DSGVO-Vorschriften wird auffallen, dass Art. 46 DSGVO von „Standarddatenschutzklauseln“ und nicht, wie die Kommission, von „Standardvertragsklauseln“ spricht. Der Begriff „Standardvertragsklauseln“ kommt noch aus Zeiten der Datenschutzrichtlinie und wurde im Rahmen der DSGVO durch „Standarddatenschutzklauseln“ ersetzt. Inhaltlich beschreiben die Begriffe aber das gleiche, die Kommission nutzt aus Gewohnheit und auch wegen der verbreiteten englischen Abkürzung „SCCs“ (Standard Contractual Clauses) den alten Begriff als Synonym zu „Standarddatenschutzklauseln“ fort.



Auftragsverarbeitungsverträge: EU-Kommission veröffentlicht Muster

Vertragsmuster für Auftragsverarbeitungsverträge sprießen spätestens seit Inkrafttreten der DSGVO aus dem Boden. Auch viele Aufsichtsbehörden haben auf ihren Websites solche Vorlagen zum Download bereitgestellt. Erstmals hat nun die EU-Kommission – gemeinsam mit den Neuregelungen für internationale Datentransfers – auch Mustervorgaben für Auftragsverarbeitungsverträge veröffentlicht. Welche Bedeutung die Muster haben und ob bestehende Auftragsverarbeitungsverträge (national wie international) nun angepasst werden müssen, fassen wir nachfolgend zusammen.

Zunächst ist eine gewisse Vorsicht bei den Begrifflichkeiten geboten. Die Musterformulierungen zur Auftragsverarbeitung heißen „**Standardvertragsklauseln**“ (Beschluss vom 04.06.2021 sowie Anhang mit den Klauseln, jeweils in deutscher Sprache). Wie in unserem Beitrag 3 erwähnt, dürfen diese nicht mit den neuen „**Standarddatenschutzklauseln**“ für den Drittstaatentransfer, die auch häufig als Standardvertragsklauseln bezeichnet werden, verwechselt werden. Um Missverständnissen vorzubeugen, bezeichnen wir die neuen Klauseln zu Auftragsverarbeitungsverträgen hier als „Auftragsverarbeitungsvertragsklauseln“.

(Freiwillige) Rechtssicherheit

Wenn Unternehmen eine Auftragsverarbeitung vereinbaren wollen, geschieht dies in der Praxis auf der Grundlage von Vertragsmustern, die von Organisationen, Behörden oder Beratern entwickelt wurden. Auch wenn sich die meisten am Markt verfügbaren Muster gleichen, gibt es in den Details Divergenzen. Zum Beispiel beim Einsatz von Subunternehmern, bei der vertraglichen Verteilung der Haftung oder bei Überprüfung der TOMs. Unternehmen stehen dann vor der Frage, welches Muster zu nutzen ist bzw. ob ein bestimmtes Muster gesetzeskonform ist. In diesem Zusammenhang ist der Blick in Art. 28 Abs. 3 DSGVO regelmäßig wenig erhellend, da die Vorschrift sehr allgemein gehalten ist. Die neu veröffentlichten Auftragsverarbeitungsvertragsklauseln vermitteln den Verantwortlichen und Auftragsverarbeitern Rechtssicherheit, da sie die gesetzlichen Anforderungen an einen Auftragsverarbeitungsvertrag erfüllen (Art. 1 des oben verlinkten

Beschlusses). Unternehmen können sich also auf den neuen „Geldstandard“ verlassen, müssen dies aber nicht (Art. 2 des Beschlusses). Die Anwendung bleibt freiwillig.

Klauselwerk im Einzelnen

Auch bei den Auftragsverarbeitungsvertragsklauseln hat die Kommission einen modularen Ansatz gewählt, sodass die Vertragsparteien zwischen verschiedenen Klauselvarianten auswählen können. Dabei bestimmen die Auftragsverarbeitungsvertragsklauseln umfassend das in Art. 28 Abs. 3 und 4 DSGVO vorgegebene Pflichtenprogramm zum Auftragsverarbeitungsvertrag. Ähnlich wie die Standardvertragsklauseln zum Drittstaatentransfer bieten auch die Auftragsverarbeitungsvertragsklauseln die Möglichkeit zum Beitritt weiterer Parteien, Verantwortlicher oder Auftragsverarbeiter während der Laufzeit des Vertrages.

Hervorheben möchten wir die folgenden Klauseln:

- **Klausel 2**: Unabänderbarkeit: Die Klauseln sollen nicht verändert werden. Verantwortliche und Auftragsverarbeiter können aber einen individuellen Vertrag mit dem Inhalt der Art. 28 Abs. 3 und 4 DSGVO schließen oder die neuen Musterklauseln der Kommission ganz oder teilweise nutzen. Es ist den Parteien auch freigestellt, die vertraglichen Verpflichtungen noch zu erweitern. Es soll nur nicht zu Widersprüchen mit den Auftragsverarbeitungsvertragsklauseln kommen.

- **Klausel 4**: Bei Widersprüchen haben die Klauseln Vorrang vor Individualvereinbarungen.

- **Klausel 7.6**: Beide Parteien müssen die Einhaltung der Klauseln nachweisen können.

- **Klausel 7.7**: Zu begrüßen sind die klaren Regeln zum Einsatz von Subunternehmern und die Nennung der beiden möglichen Optionen: Vorherige gesonderte Genehmigung und allgemeine schriftliche Genehmigung. In vielen bisherigen Mustern und Individualvereinbarungen ist dies nicht derart klar herausgearbeitet.

Bemerkenswert ist, dass bei der Weitergabe von Unterauftragsverträgen der Schutz von Geschäftsgeheimnissen Berücksichtigung findet (lit. c), sodass hier ggf. Schwärzungen erfolgen können. Ebenfalls hervorzuheben ist die in lit. e) vorgesehene Drittbegünstigungsklausel, nach der der Verantwortliche, wenn der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

- **Klausel 9**: Das hier geregelte Procedere für den Umgang mit Datenpannen ist vergleichsweise detailliert und bereits deswegen sehr hilfreich.

Umsetzungsfrist und Empfehlung

Die neuen Auftragsverarbeitungsvertragsklauseln treten 20 Tage nach der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft. Für diese gilt keine Übergangsfrist.

Es bietet sich an, bestehende Auftragsverarbeitungsverträge auf die Vereinbarkeit mit den neuen Auftragsverarbeitungsvertragsklauseln zu überprüfen und gegebenenfalls neue Verträge unter Berücksichtigung der Musterklauseln zu schließen. Gerade das hohe Maß an Rechtssicherheit und die einfache Möglichkeit des Beitritts zu den Klauseln machen diese für die Praxis interessant.

Zu guter Letzt

Die NGO noyb.eu erregt diesen Monat besonderes Aufsehen. Nicht nur wurden durch eine von ihr entwickelte Software Beschwerden wegen ihrer Cookie-Banner direkt an Unternehmen verschickt (dazu unser erster Beitrag in diesem Newsletter). Auch erhob sie Beschwerde mit anderen europäischen Datenschutz-Organisationen gegen die Gesichtserkennungssoftware Clearview AI vor den nationalen Datenschutzbehörden. Darüber hinaus müssen sich die Datenschutzbehörden mit Beschwerden gegen die internationale Plattform Locatefamily.com auseinandersetzen und auch der italienische Grüne Pass bereitet datenschutzrechtliche Probleme. Und aus Österreich kommt Neues zum Auskunftsanspruch.

- **Beschwerden europäischer Datenschutz-Organisationen gegen Clearview AI**

Europäische Datenschutz-Organisationen wie die noyb.eu, Privacy International und Homo Digitalis haben jüngst Beschwerden gegen das US-Unternehmen Clearview AI in Frankreich, Österreich, Italien, Griechenland und dem Vereinigten Königreich wegen Verstoßes gegen die DSGVO eingereicht. Die KI-gestützte Gesichtssuchmaschine von Clearview AI kann anhand von Personenfotos innerhalb weniger Sekunden weitere Fotos derselben Person in Verbindung mit vernetzten Quellen wie Social Media-Profilen zur Verfügung stellen. Sie greift dabei auf eine eigene

biometrische Datenbank zurück, die sie durch Gesichtserkennungssoftware aufbaut. Insgesamt soll das Unternehmen so biometrische Daten von mehr als 3 Milliarden Menschen ohne deren Wissen oder Erlaubnis gesammelt haben – gegen die dadurch ermöglichte „Massenüberwachung" richten sich die Beschwerden.

Die Entwicklung dieser Beschwerden ist mit Spannung zu beobachten. Es könnte hieraus nicht nur hervorgehen, wo Clearview AI in Europa genutzt wird. Auch könnten die Ergebnisse in die aktuellen Vorschläge zur KI-Regulierung einfließen. Die Hamburger Aufsichtsbehörde hatte in einem konkreten Beschwerdeverfahren schon im Januar aufgrund fehlender Einwilligung die Löschung der Daten des Beschwerdeführers angeordnet.

- **Österreichischer OGH zum Auskunftsanspruch nach Art. 15 DSGVO**

Der österreichische Oberste Gerichtshof (OGH) hat in einem Verfahren über den Umfang des datenschutzrechtlichen Auskunftsanspruchs aus Art. 15 DSGVO gleich zweifach über datenschutzrechtliche Aspekte entschieden (Entscheidung vom 18.02.2021, Gz. 6Ob127/20z, hier abrufbar). Zum einen stellte der OGH fest, dass für datenschutzrechtliche Auskunftsbegehren nach Art. 79 DSGVO zwei Verfahrenswege offenstehen: Der Betroffene könnte sich an die zuständige Aufsichtsbehörde wenden, daneben aber auch den Auskunftsanspruch über den Zivilrechtsweg durchsetzen. Zum anderen entschied der OGH, dass die im Verfahren in Rede stehenden Informationen personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO sind. Konkret hatte der Beklagte, ein Postdienstleister, neben Adressdaten des Klägers auch marketing-relevante Informationen und Einschätzungen verarbeitet. Diese statistischen Einschätzungen, etwa dass der Kläger „investmentaffin", „bioaffin" und „Heimwerker" sei, seien als Einschätzungen und Urteile über die Person auch unabhängig von ihrem tatsächlichen Wahrheitsgehalt personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO, auf die der Auskunftsanspruch des Art. 15 DSGVO anwendbar ist.

- **Niederlande: Bußgeld i.H.v. 525.000 Euro und Verpflichtung zur Benennung eines Vertreters**

Die internationale Plattform Locatefamily.com ermöglicht es, den Kontakt zu Familienmitgliedern wiederherzustellen oder neue Bekanntschaften zu knüpfen. Hierfür greift sie auf einen Katalog mit Kontaktdaten zurück. Um als Nutzer auf diesen Zugriff zu haben, ist weder eine Registrierung noch eine andere Form des Beziehungsnachweises zur Person, deren Daten abgefragt werden, erforderlich. Hiergegen waren bei der niederländischen sowie anderen nationalen Datenschutzbehörden zahlreiche Beschwerden eingegangen. Die Kontaktdaten der betroffenen Personen sollen ohne ihr Wissen auf der Website veröffentlicht worden sein. Die Beantragung der Löschung war den Betroffenen nicht ohne weiteres möglich, die Plattform verfügt über keine Vertretung in der EU. Die Datenschutzbehörde in den Niederlanden hielt fest, dass internationale Unternehmen ohne Niederlassung in der EU dazu verpflichtet sind, einen in der EU niedergelassenen Vertreter zu benennen, sollten sie geschäftlich in der EU tätig sein und hierfür personenbezogene Daten verarbeiten. Schon das Fehlen eines solchen Vertreters genügte für die Verhängung des Bußgelds in Höhe von 525.000 Euro.

- **Polen: Bußgeld i.H.v. 250.000 Euro**

In Polen wurde ein Bußgeld von 250.000 Euro gegen das Medien- und Telekommunikationsunternehmen Cyfrowy Polsat S.A. aufgrund verschiedener Datenpannen verhängt. Immer wieder ging die postalische Korrespondenz mit Kundendaten inkl. Rechnungen und vertraglichen Informationen verloren oder wurde an die falschen Adressaten zugestellt. Die Datenschutzbehörde stellte fest, das Unternehmen habe es versäumt, angemessene technische und organisatorische Maßnahmen zum Schutz der Verarbeitung der Daten umzusetzen. Auch, wenn die Pannen vom beauftragen Lieferunternehmen verursacht worden seien, sei es Pflicht des Unternehmens als Verantwortlichem, Schutzvorrichtungen zu implementieren. Zudem hatte Cyfrowy Polsat die Datenschutzbehörde und die Betroffenen erst mit zwei- bis dreimonatiger Verzögerung informiert und daher auch gegen die Meldepflicht binnen 72 Stunden verstoßen.

- **Italien und Corona: Dekret zum „Grünen Pass“ verstößt gegen die DSGVO**

Im April 2021 verabschiedete die italienische Regierung ein Gesetzesdekret, mit dem Maßnahmen zur Eindämmung und Bekämpfung der Covid-19-Pandemie eingeführt wurden. Neben der Möglichkeit eines „Grünen Passes“, der dem Bürger nach erfolgreicher Impfung, Genesung oder negativem Testergebnis gewisse Freiheiten zugesteht, sollten auch technische Spezifikationen zur Gewährleistung der Interoperabilität dieses Grünen Passes mit der nationalen Plattform und solcher anderer EU-Mitgliedstaaten erlassen werden. Weiterhin sollte die Ausstellung dieser Pässe vorübergehend auch durch private Gesundheitseinrichtungen, Apotheken, Allgemeinmediziner und frei gewählte Kinderärzte möglich sein.

Die italienische Datenschutzbehörde stellte nun fest, dass die mit den geplanten Maßnahmen verbundenen Risiken für die Rechte und Freiheiten der Betroffenen nicht hinreichend berücksichtigt und auch nicht die geeigneten technischen und organisatorischen Maßnahmen zur wirksamen Umsetzung der Grundsätze des Datenschutzes getroffen worden seien. So sei etwa versäumt worden, die Datenschutzbehörde zu konsultieren und der Grundsatz der Datenminimierung nicht eingehalten worden. Informationen zur spezifischen Situation der betroffenen Person – ob sie geimpft ist, genesen ist oder negativ getestet wurde – seien nicht erforderlich. Es reichten persönliche Daten, die zur Identifizierung der betroffenen Person erforderlich sind, eine eindeutige Identifizierung des Zertifikats und das Ablaufdatum des Zertifikats. Darüber hinaus sei auch der Grundsatz der Transparenz verletzt. Es sei weder festgelegt, wer der für die Datenverarbeitung Verantwortliche ist, noch, wer die Zertifizierung aus welchen Gründen überprüfen kann oder welche Institution die Plattform für die Grünen Pässe betreibt. Auch die Grundsätze der Speicherbegrenzung, Integrität und Vertraulichkeit seien nicht berücksichtigt worden.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de