Zeit aufzuräumen: Privacy Shield fordert umfangreiche Maßnahmen – sonst droht erhebliches Bußgeld

Die Auswirkungen des EuGH-Urteils zum Privacy-Shield sind doch gravierender als angenommen. Die Reaktionen der Aufsichtsbehörden verdeutlichen zwischenzeitlich, dass dies gravierende Auswirkungen auf Unternehmen hat.

Kurz nochmals zum Hintergrund: Im sog. Schrems II-Urteil vom 16.07.2020 hat der Europäische Gerichtshof das Privacy Shield, auf welches zahlreiche Datentransfers in die USA gestützt wurden, für unwirksam erklärt. Die Überwachungsmaßnahmen in den USA sind zu weitgehend, weshalb in der Regel weder vertragliche Verpflichtungen noch Selbstbindungen der Unternehmen (also gem. Privacy Shield oder Standardvertragsklauseln) daran etwas ändern. Hinzu kommt, dass seitens des europäischen Betroffenen kein wirksamer Rechtsschutz gegen solche Maßnahmen besteht.

Die Behörden bereiten sich bereits jetzt darauf vor, Prüfungen durchzuführen. Dabei gilt:

- Wer immer noch mit dem Privacy Shield rechtfertigt, wird zuerst geprüft
- Wer anlässlich des Schrems II-Urteils nichts machen, wird ebenfalls geprüft
- Wer die nachfolgenden Schritte durchführt, wird bei Prüfungen hintenan gestellt und/oder kommt ggf. ohne Bußgeld davon

Wir weisen darauf hin, dass Herr Schrems nun nach dem Urteil bei den Aufsichtsbehörden bereits 101 Beschwerden über europäische Unternehmen eingereicht hat, welche im Web immer noch über Google und Facebook Daten in die USA senden (Stand: 18.08.2020). Lassen Sie nicht zu, dass Sie auch in diesen Fokus geraten und machen Sie die Aufsichtsbehörde dadurch nicht auf Sie aufmerksam. Es handelt sich um einen besonders gravierenden Verstoß gem. Art. 83 Abs. 5 DSGVO, der nach den Bußgeldkriterien durchaus mit einem erhöhten Schweregrad bis tatsächlich zu den 4 % des Jahresumsatzes einhergeht.

I. PRÜFKATALOG

Hierauf basierend sind Unternehmen nun in der **PFLICHT**, bestimmte Prüfungen durchzuführen. Der Landesbeauftragte für Datenschutz in Baden-Württemberg hat daher nun folgenden Prüfkatalog vorgestellt:

1. **ERFASSEN SIE ZUNÄCHST ALLE DATENTRANSFERS IN DRITTSTAATEN, HIER: IN DIE USA.**

Hierbei reicht bereits der Zugriff auf Daten durch US-Unternehmen. Bitte beachten Sie, dass Sie auch Ihre Auftragsverarbeitungsverträge durchsehen müssen, ob Ihr Auftragsverarbeiter Daten an amerikanische Subunternehmer übermittelt!

To do
Erfassen Sie alle Datentransfers von sich und Ihren Auftragsverarbeitern in die USA!

Weisen Sie sodann die entsprechenden Auftragsverarbeiter an, die Übermittlung von Daten in die USA mit sofortiger Wirkung auszusetzen, bis der Auftragsverarbeiter ein entsprechendes Datenschutzniveau sichergestellt hat.

To do
Anweisung an die Auftragsverarbeiter, die US-Transfers auszusetzen!

2. **GIBT ES ZUMUTBARE ALTERNATIVEN FÜR SIE?**

Der Landesbeauftragte hat darauf hingewiesen, dass im Zentrum des weiteren Vorgehens des Landesamt die Frage stehen wird, ob es zumutbare Alternativdienstleister für die jeweiligen Dienste gibt. D.h. wenn Sie die Behörde nicht überzeugen können, dass der bereits genutzt Dienstleister/Vertragspartner kurz- oder mittelfristig unersetzlich ist, wird der Datentransfer untersagt.

So gibt es seiner Ansicht nach durchaus europäische oder in Drittländern mit angemessenem Datenschutzniveau vorhandene Alternativen zu GoogleAnalytics & Co., d.h. überlegen Sie sich, ob Sie entsprechende Tools austauschen bzw. Software/Server in den USA kündigen und sich Vertragspartner in der EU suchen, bspw.

- Reichweitenmessung von Websites – Matomo, Etracker
- Newsletterdienste – Sendinblue, CleverReach, rapidmail
- Videokonferenzdienste – Webex, TeamViewer (Blizz)
- Zahlungsdiensteanbieter – Heidelpay
- Soziale Netzwerke – Xing
- Nachrichtendienste auf dem Handy (statt WhatsApp) – Threema

Besteht für Sie ein Sonderkündigungsrecht aufgrund dessen, dass der Anbieter die datenschutzrechtlichen Vorgaben der DSGVO nicht einhalten kann?

Eine solche Kündigung ist dann zulässig, wenn Ihnen nach deutschem Recht die Fortführung des Vertrages nicht mehr zuzumuten ist. Im Arbeitsrecht gibt es bereits zahlreiche Urteile, wonach Datenschutzverstöße von Mitarbeitern mit einer fristlosen

Kündigung einhergehen dürfen. Im Übrigen muss sich die Rechtsprechung dazu erst entwickeln. Aber: Bei Verträgen mit US-Unternehmen kann es sein, dass Sie nicht unter deutschem Recht beurteilt werden, sondern nach amerikanischem Recht. D.h.es kommt immer zunächst auf den zugrundeliegenden Vertrag und die Frage an, welches Recht anzuwenden ist.

3. SAMMELN SIE FAKTEN ZU DEN DATENIMPORTEUREN IN DEN USA, D.H.

- Gab es schon Herausgabeverlangen gegen den Datenimporteur bzw. gibt es in der Branche des Datenimporteurs vermehrte Herausgabeverlangen?
- Kann der Datenimporteur die Datenherausgabe verhindern? Hat der Datenimporteur in der Vergangenheit gegen etwaige Herausgabeverlangen Rechtsschutz ersucht?
- Auf welche Art und Weise informiert der Datenimporteur des Datenexporteur im Falle eines staatlichen Herausgabeverlangens

Sofern Ihre Auftragsverarbeiter Daten in die USA übermitteln, müssen diese die relevanten Informationen bei ihren Subunternehmern einholen!

To do

Sammeln Sie Informationen zu Ihren Datenimporteuren bzw. fordern Sie Ihre Auftragsverarbeiter auf, diese Informationen einzuholen und Ihnen vorzulegen!

4. SAMMELN SIE FAKTEN ZUR RECHTSORDNUNG IN DEN USA, D.H.

- Identifizieren Sie die relevanten Überwachungsgesetz
- Identifizieren Sie Rechtsschutzmöglichkeiten der dortigen Unternehmen, Richtervorbehalte, Behördenaufsicht etc.
- Wie sind der datenschutzrechtliche Rechtsrahmen und das Datenschutzniveau generell?

Information

a) Überwachungsgesetze: u.a. Section 702 FISA, PPD-28, Patriot Act, US-CloudAct etc.
b) Rechtsschutzmöglichkeiten/Garantien/Datenschutzniveau: der EuGH hat bzgl. der US-Geheimdienstgesetze festgestellt, dass diese keinen konkret begrenzten Tatbestand haben und es am effektiven Rechtsschutz mangelt, wodurch kein gleichwertiger Schutz für Betroffene bestünde

5. VERGLEICHEN SIE DIE GEM. NR. 3 ERMITTELTEN RECHTSORDNUNGEN ZWISCHEN DEN USA UND DEUTSCHLAND!

⇨ Nach dem Schrems II-Urteil des EuGH ist der Vergleichsmaßstab wie folgt anzusetzen:
Die Garantien, durchsetzbaren Rechte, wirksamen Rechtsbehelfe nach Art. 46 I, II DSGVO müssen ein Schutzniveau bieten, das dem der DSGVO und der EU-Grundrechte-Charta gleichwertig ist.

Für die in den Ziff. 2-3 genannten Punkte können Sie einen Fragebogen erstellen, der Sie bei der Ermittlung der Punkte unterstützt.

	Achtung: Rechenschaftspflicht! Dokumentieren Sie alles und jeden Schriftverkehr und jeden Anruf und jede Prüfung und kontrollieren Sie kontinuierlich von Zeit zu Zeit alles!!!	

II. ANZUWENDENDE MASSNAHMEN

1. ERGÄNZEN SIE IHRE STANDARDVERTRAGSKLAUSELN!

Je mehr Risiko nach dem vorgenannten Prüfungsergebnis besteht, desto mehr Regelungen sollten Sie treffen. Nehmen Sie weitere Regelungen auf. Dies gilt auch gegenüber Google, Facebook & Co.

To do
Passen Sie die Standardvertragsklauseln an!

Hinweis: Facebook hat am 21.09.20 in der Presse verlauten lassen, dass diese sich überlegen, sich aus dem Europa-Geschäft zurückzuziehen, wenn man wegen der Datenschutzvorschriften nicht mehr so agieren könne, wie man möchte.

Die Einwilligung gem. Art. 49 DSGVO ist nach Angaben des Datenschutzbeauftragten nur in den seltensten Fällen und auch nur mit Einzelfallcharakter anwendbar, d.h. Sie können Ihre US-Cookies etc. nicht auf die Einwilligung nach Art. 49 DSGVO stützen. Wir hatten Ihnen diesbezüglich schon im letzten Newsletter mitgeteilt, dass wir hierin ein Risiko sehen.

2. ERGÄNZEN SIE SONSTIGE MASSNAHMEN

Die Standardvertragsklauseln sind mit weiteren Maßnahmen zu ergänzen, da sonst dennoch kein angemessener Schutz vorliegt!

- technische Maßnahmen (Verschlüsselung, Datenminimierung, Speicherung in der EU)

- organisatorische Maßnahmen (passt dieser seine Schutzmechanismen an; berichtet er über die ihn erreichten Behördenanfragen etc. so bspw. Microsoft)

To do
Prüfen Sie beim Datenimporteur ergänzende Maßnahmen oder vereinbaren Sie solche.

3. VERHALTEN DES DATENIMPORTEURS

Dokumentieren Sie das Verhalten des Datenimporteurs im Hinblick auf diese Vorgaben!

- Meldet er sich nicht zurück oder weist diese zurück -> machen Sie sich nochmals Gedanken zu Alternativen
- Nimmt er nicht alle Änderungen an, aber hat konstruktive Vorschläge, die der Sache ebenfalls dienlich sind und die Rechte wirksam durchsetzen -> Prüfen Sie die Vorschläge!

4. KONSEQUENZEN

Der Landesbeauftragte für den Datenschutz Baden-Württemberg schreibt ausdrücklich in seiner Richtlinie und hat dies diese Woche auch nochmals verbal explizit bestätigt:

WENN SIE KEINEN AUSREICHENDEN SCHUTZ VORSEHEN ODER DER DATENIMPORTEUR NICHT ANTWORTET, SIND SIE VERPFLICHTET, DEN TRANSFER AUSZUSETZEN UND/ODER ZU BEENDEN. Andernfalls kann die Aufsichtsbehörde den Transfer untersagen.

Das vorgenannte gilt natürlich auch für Datentransfers in alle anderen Drittstaaten, sofern nicht bereits ein Angemessenheitsbeschluss der EU-Kommission vorliegt (so bspw. für Kanada, Schweiz). Bitte beachten Sie dies v.a. auch dann, wenn es zu einem ungeregelten Brexit kommt. Die EU und Großbritannien verhandelt diesbezüglich derzeit noch, aber der Ausgang ist derzeit noch unklar.

Bei Fragen oder sofern Sie Hilfe benötigen, können Sie gerne jederzeit auf uns zukommen. Lassen Sie es uns anpacken!

Hinweis: Es handelt sich um eine Rechtsansicht der Autorin. Das Datenschutzrecht ist jedoch ein ungeformtes Rechtsgebiet, das erst noch zahlreicher Entscheidungen und Praxis bedarf, um sicher gehen zu können. Wir bitten, dies bei der Lektüre zu beachten.

© Dr. Carmen Fritz, LL.M.
Fachanwältin für Urheber- und Medienrecht
Fachanwältin für Gewerblichen Rechtsschutz
Zertifizierte Datenschutzbeauftragte (TÜV)
www.fritz-gern.de