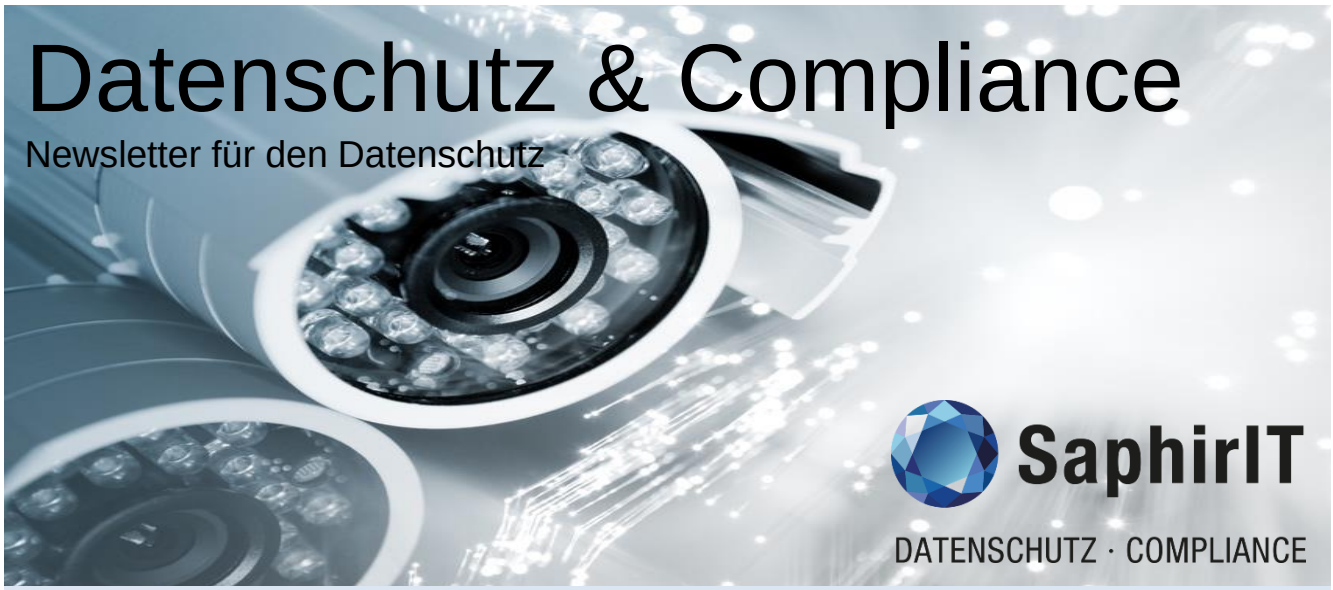

SONDERNEWSLETTER Juni 2021

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Sondernewsletter zum Thema „Auswirkungen des Schrems II - Urteils – Aufsichtsbehörden kündigen Kontrollen zur Umsetzung des Urteils an.“

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Aufsichtsbehörden kontrollieren Umsetzung des Schrems II - Urteils

Bereits in unserem Newsletter Juli 2020 hatten wir ausführlich über das Schrems II Urteil und seine Auswirkungen gesprochen.

Mit Urteil vom 16.07.2020 hatte der Europäische Gerichtshof das EU-US Privacy-Shield für rechtswidrig erklärt (EuGH, Urteil vom 16.07.2020, Az: C-311/18).

Jede Datenübertragung die bis zum Zeitpunkt des Urteils auf dem Privacy-Shield beruhte, war somit nunmehr rechtswidrig.

Auch der Einsatz der bisherigen Standardvertragsklauseln war nicht mehr ohne Probleme möglich. Es bedarf nun einer Einzelfallprüfung, ob ein Adressat im Drittland überhaupt in der Lage ist, die Pflichten aus den entsprechend

der Grundsätze des Urteils anzupassenden Standardvertragsklauseln, einzuhalten.

Bereits im Juli 2020 gaben wir den Ausblick, dass über kurz oder lang damit zu rechnen ist, dass die Aufsichtsbehörden diesbezüglich auch tätig werden und die Einhaltung überprüfen.

Nunmehr ein Jahr später ist der Zeitpunkt gekommen.

Die Landesbeauftragte für den Datenschutz in Niedersachsen teilte am 01.06.2021 mit, dass sich ihre Behörde an einer **länderübergreifenden Kontrolle** von Datenübermittlungen durch Unternehmen in Staaten außerhalb der europäischen Union oder des Europäischen Wirtschaftsraums, sog. Drittstaaten beteilige.

Ziel der Aufsichtsbehörden ist die breite Durchsetzung der im Urteil des Europäischen Gerichtshofs in seiner Schrems II-Entscheidung gestellten Anforderungen.

Das Urteil hat in vielen Unternehmen dazu geführt, dass grundlegende und lange praktizierte Prozesse überdacht und ggf. umgestellt werden mussten.

Neben der Landesbeauftragten für den Datenschutz in **Niedersachsen** haben sich auch die Landesdatenschutzbehörden aus **Baden-Württemberg, Bayern, Berlin, Bremen, Brandenburg, Hamburg, Rheinland-Pfalz** und dem **Saarland** der Prüfung angeschlossen.

Die Problematik wird aber auch an Unternehmen aus anderen Bundesländern nicht vorbeigehen.

Ausgewählte Unternehmen werden auf Basis eines gemeinsamen Fragenkatalogs angeschrieben. Hierbei werden unter anderem Fragen zum Einsatz von Dienstleistern zum E-Mail-Versand, zum Hosting von Internetseiten, zum Webtracking, zur Verwaltung von Bewerberdaten und zum konzerninternen Austausch von Kundendaten sowie Daten der Beschäftigten gestellt.

Dennoch entscheidet jede Aufsichtsbehörde selbst, in welchen Themenbereichen sie tätig werden möchte.

Falls Sie betroffen sind, melden Sie sich bitte sofort bei uns.

In Niedersachsen werden diese Fragebögen vorerst an 18 Unternehmen zu den Themen Mail- und Web-Hosting versendet.

Der Europäische Gerichtshof fordert in seinem Urteil klar von den Aufsichtsbehörden, dass diese unzulässige Datentransfers „aussetzen oder verbieten." Neben möglichen Bußgeldern ist dies die größte Gefahr für Ihr Unternehmen. Die Unterbrechung des Datentransfers in ein Drittland kann ein Unternehmen schwer schädigen.

Was tun?

Viele Unternehmen sind von dem Urteil des Europäischen Gerichtshofs betroffen. Nicht alle wird die Aufsichtsbehörde kontrollieren können. Dennoch ist Vorsicht geboten.

Sie sollten wie folgt vorgehen:

1. Zunächst sollten Sie alle Risiken identifizieren. Dies sind diejenigen Prozesse, bei denen personenbezogene Daten in ein Drittland gelangen könnten. Insbesondere sind hier Ihre Dienstleister **(Vorsicht bei Unterauftragnehmern!)** zu nennen. Neben den vorstehenden Fragen im Fragenkatalog gehören dazu u.a. auch die Cloud, der Messenger-Dienst, das Betriebssystem, die Anwendungsprogramme, das Videokonferenzsystem.

2. Sie müssen prüfen, ob es zu dem jeweiligen Prozess datenschutzkonforme Alternativen gibt.

3. Falls es diese gibt ist zu klären, ob diese in der Funktionalität, in der Anwendbarkeit, etc. vergleichbar sind mit der nicht datenschutzkonformen Lösung.

4. Falls eine Vergleichbarkeit da ist, werden Sie nicht umhinkommen spätestens in drei Jahren einen Wechsel vorzunehmen.

5. Falls keine Vergleichbarkeit vorliegt, ist eine umfassende datenschutzrechtliche Risikoabwägung durchzuführen. Vorstehende Punkte sind umfassend zu dokumentieren.

6. Wie bereits in unserem Newsletter Juli 2020 geschildert sollten Sie zudem in Ihrem Unternehmen prüfen, ob und inwieweit ein mögliches Bußgeld von der D&O Versicherung abgedeckt wäre oder ob gegebenenfalls zusätzliche Maßnahmen ergriffen werden müssen.

7. Zudem sollte jedenfalls die Möglichkeit in Betracht gezogen werden sog. „Binding Corporate Rules“ abzuschließen.

8. Zur Risikoeingrenzung sollten Sie zudem im Unternehmen im Übrigen ein ausreichendes Datenschutzniveau vorhalten. Dies wird helfen, bei den Aufsichtsbehörden ein Wohlwollen zu erhalten. Wir stellen Ihnen hierzu ein entsprechendes Testat aus.

Sprechen Sie uns zu diesem Problemkreis gerne an. Wir versuchen dann mit Ihnen gemeinsam eine Lösung für Ihr Unternehmen zu finden.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de

Unsere jeweils aktuellen Datenschutzinformationen finden Sie unter
https://www.saphirit.de/datenschutz.html