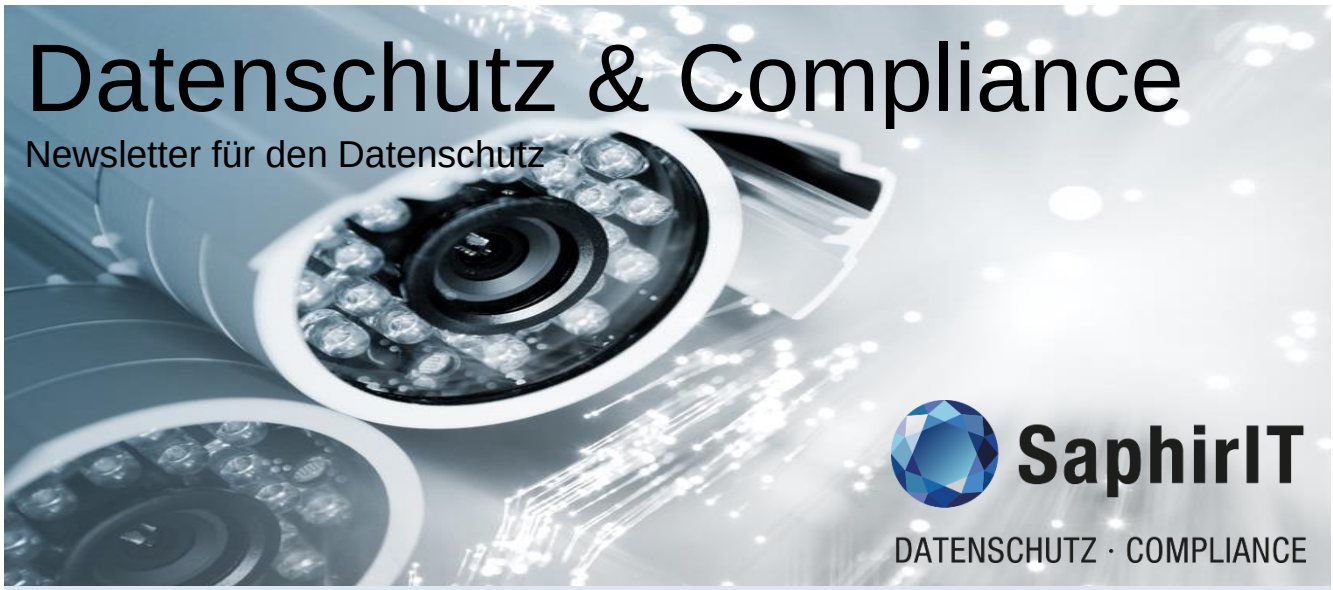

Ausgabe August 2020 | Seite 176 - 180

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter August 2020.

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

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Nutzung von Videokonferenzprogrammen nach Aus des Privacy-Shields

In unserem Newsletter vom Mai 2020 (abrufbar unter: https://www.saphirit.de/newsletter-flyer.html) haben wir Ihnen vorgestellt welche datenschutzrechtlichen Anforderungen an Videokonferenzprogramme zu stellen sind.

Bereits dort haben wir auf die rechtliche Problematik beispielsweise bei der Nutzung von Microsoft Teams oder Zoom hingewiesen. Eine datenschutzkonforme Nutzung konnte zu dem Zeitpunkt nur auf das umstrittene Privacy-Shield gestützt werden.

Das Privacy-Shield wurde in der Zwischenzeit vom Europäischen Gerichtshof (EuGH) gekippt. Wir berichteten dazu ausführlich in unserem Newsletter Juli 2020 (ebenfalls abrufbar unter: https://www.saphirit.de/newsletter-flyer.html).

Nun stellt sich die Frage, ob eine Nutzung von Videokonferenzprogrammen, die bisher auf

Grundlage des Privacy-Shields einen Datenaustausch zwischen den USA und Deutschland ermöglichten, datenschutzrechtlich noch zulässig ist.

Zunächst ist festzustellen, dass das Privacy-Shield als Rechtsgrundlage für einen sicheren Datentransfer in die USA nicht mehr zur Verfügung steht.

Ein datenschutzkonformer Transfer kann daher nur über wirksame Standardvertragsklauseln (SCCs) oder Binding Corporate Rules (BCRs) gewährleistet werden.

Nicht nur Videokonferenzprogramme sind hiervon aber betroffen. Jedwede Datenübertragung in die USA (die bisher auf Grundlage des Privacy-Shields gerechtfertigt wurde) erfolgt, wenn keine Maßnahmen getroffen werden, erst einmal ohne Rechtfertigung.

Die Berliner Beauftragte für den Datenschutz verkündete nun bereits, dass Unternehmen sich auf Einzelfallprüfungen von Übermittlungen in die USA einstellen müssten.

Der Abschluss von Standardvertragsklauseln (bzw. Binding Corporate Rules) ist jedoch auch nicht einfach. Insbesondere sollten einige Punkte beim Abschluss dieser Klauseln beachtet werden.

Generell bedarf es bei einer Übermittlung von Daten in ein Drittland (ein Land außerhalb der EU) einer Rechtsgrundlage im Sinne des Art. 6 Datenschutzgrundverordnung (DSGVO). Zudem muss der Verantwortliche dafür Sorge tragen, dass bei einer Datenübermittlung in ein Drittland geeignete Garantien vorliegen, um die Sicherheit der Daten bzw. ein angemessenes Schutzniveau zu gewährleisten.

Standardvertragsklauseln sind durch die EU-Kommission erlassen worden und behalten gemäß Art. 46 Abs. 5 DSGVO ihre Gültigkeit. Im Unterschied dazu sind Binding Corporate Rules nicht fest von der EU vorgegeben, sondern können selbst gestaltet werden. Dabei ist jedoch zu beachten, dass auch die individuell geschlossenen BCRs den datenschutzrechtlichen Mindeststandards, wie sie in den Standardvertragsklauseln zu finden sind, genügen müssen.

Ob und inwieweit die Anbieter von Videokonferenzprogrammen Standardvertragsklauseln mit ihren Nutzern abschließen bleibt fraglich. Schließlich ist es zudem Aufgabe des deutschen Verantwortlichen zu überprüfen, ob die vertraglich vereinbarten Garantien beispielsweise durch geeignete technische und organisatorische Maßnahmen auf Seiten der USA eingehalten werden.

Im Hinblick auf Videokonferenzprogramme empfiehlt es sich daher weiterhin nicht auf Programme zurückzugreifen, die Daten in den USA speichern. Vielmehr sollte auf europäische bzw. deutsche Anbieter zurückgegriffen werden um sichergehen zu können, dass ein angemessenes Datenschutzniveau vorliegt.

Aber auch jeder andere Datentransfer in die USA sollte einmal überprüft werden.

Sollte die Übertragung bisher auf das Privacy-Shield gestützt worden sein, so müssen Vorkehrungen getroffen werden um nunmehr einen angemessenen Datenschutz gewährleisten zu können.

Sollten Sie weiterhin Zoom oder andere nicht mehr datenschutzkonforme Videokonferenzprogramme nutzen wollen, ist dies zwingend zu dokumentieren und der Zweck unter Abwägung der Alternativen darzulegen.

Sollte Ihr Datenschutzniveau im Übrigen der DSGVO entsprechen, dürfte dieser Rechtsverstoß in der Gesamtschau aber eher zu vernachlässigen sein. Wir testieren Ihnen gerne ordnungsgemäßen Datenschutz.

Zur Umsetzung der hierfür noch notwenigen Maßnahmen sprechen Sie uns bitte an.

Europäischer Datenschutzausschuss veröffentlicht FAQ zum Privacy-Shield-Urteil des EuGHs

Der Europäische Datenschutzausschuss (EDSA) hat ein FAQ zu Fragen des Datentransfers in Drittländer herausgegeben.

Nach einem Urteil des EuGHs, wonach ein Datentransfer in die USA nicht mehr auf das Privacy-Shield gestützt werden kann, versucht der EDSA Antworten zu bieten.

Der EDSA stellt zunächst klar, dass es keine Übergangsfrist zur Umsetzung des Urteils gebe. Das Urteil müsse umgehend bei jeder Datenübertragung in die USA beachtet werden.

Standardvertragsklauseln seien grundsätzlich weiterhin gültig. Dennoch sei es vom Einzelfall abhängig, ob die bestehenden Regelungen ausreichend seien um ein angemessenes Schutzniveau gewährleisten zu können. In der EU geltende Vorschriften müssten aber eingehalten werden. Ist dies nicht der Fall, so sei der Datentransfer einzustellen.

Das gleiche gelte auch für Binding Corporate Rules. Sofern ein angemessenes Schutzniveau nicht gewährleistet werden könne, müsse der Datentransfer eingestellt werden.

Unternehmen, die beabsichtigen einen Datentransfer in die USA oder ein anderes Drittland dennoch aufrechtzuerhalten müssen die zuständige Aufsichtsbehörde benachrichtigen.

Was sollten Sie in der Praxis unternehmen?

Sie sollten jeden Transfer bei dem eine Übertragung personenbezogener Daten in ein Drittland, insbesondere die USA, stattfindet, überprüfen.

1. Ermitteln Sie alle Ihre Datentransfers in Drittländer bzw. die USA;

2. Stellen Sie fest auf welcher Rechtsgrundlage diese Datenübertragung bisher gestützt wird/wurde;

3. Sollte der Datentransfer auf Grundlage des Privacy-Shields erfolgt sein, so muss überprüft werden, ob nunmehr Standardvertragsklauseln oder Binding Corporate Rules in Frage kommen;

4. Erfolgt der Datentransfer bisher bereits auf Grundlage von Standardvertragsklauseln oder Binding Corporate Rules muss überprüft werden, ob diese noch den wesentlichen Anforderungen des EU-Rechts entsprechen;

5. Ist dies nicht der Fall, so muss überprüft werden, ob ein angemessenes Datenschutzniveau eventuell durch zusätzliche Maßnahmen erreicht werden kann;

6. Können zusätzliche Maßnahmen nicht getroffen werden muss noch überprüft werden, ob für eine Datenübertragung möglicherweise der Ausnahmetatbestand des Art. 49 DSGVO greift. Ist dies nicht der Fall, so muss der Datentransfer eingestellt werden;

7. Soll eine Datenübertragung trotz der Feststellung, dass ein angemessenes Schutzniveau nicht vorliegt, fortgesetzt werden so muss umgehend die Aufsichtsbehörde hierüber informiert werden.

Das vollständige Dokument mit allen beantworteten Fragen finden sie unter: https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en

Unterlassungsklagen im Bereich der DSGVO

Das Verwaltungsgericht (VG) Regensburg hatte einen Fall zu entscheiden in dem ein Kläger auf Unterlassung einer von der Stadt eingeführten Videoüberwachung des öffentlichen Raumes klagte (VG Regensburg, Bescheid v. 06.08.2020, Az. RN 9 K 19.1061).

Vor allem das Ergebnis der Entscheidung ist von Interesse. Das VG Regensburg geht davon aus, dass Art. 79 DSGVO weitere gerichtliche Rechtsbehelfe gegen Verantwortliche und Auftragsverarbeiter ausschließt.

Unterlassungsklagen nach §§ 1004 Abs. 1, 823 Abs. 2 BGB sollen im Bereich des Datenschutzes grundsätzlich nicht möglich sein.

Das VG bezieht sich zunächst auf den Wortlaut des Art. 79 Abs. 1 DSGVO wonach nur andere verwaltungsrechtliche oder außergerichtliche Rechtsbehelfe „unbeschadet“ blieben, nicht aber gerichtliche Rechtsbehelfe.

Gerichtliche Rechtsbehelfe bestünden nur bei einer Verletzung aufgrund einer Vorschrift der DSGVO.

Das VG führt hierzu aus:

„Jenseits der oben genannten Normen [genannt werden die Art. 12 bis 22 DSGVO] gewährt die Datenschutz-Grundverordnung keine Rechte, zu deren Durchsetzung ein wirksamer

Rechtsbehelf nach Art. 79 DSGVO zur Verfügung gestellt werden muss. In Betracht käme insbesondere ein Anspruch auf Unterlassung einer verordnungswidrigen Verarbeitung personenbezogener Daten, da gemäß Art. 8 Abs. 1 EU-GRCh, Art. 16 Abs. 1 AEUV jede natürliche Person Recht auf Schutz der sie betreffenden personenbezogenen Daten hat, wobei Inhalt des Schutzes auch das Erfordernis der Rechtmäßigkeit der Verarbeitung ist. Es müsste in einem solchen Fall daher die Möglichkeit bestehen, eine solche Verarbeitung für die Zukunft zu unterbinden, andernfalls der Grundrechtsschutz und der europarechtliche Effektivitätsgrundsatz nach Art. 4 Abs. 3 EUV beeinträchtigt wären.

Allerdings ist das Recht auf Unterlassung rechtswidriger Datenverarbeitung nicht als solches in der Datenschutz-Grundverordnung verankert. Diese konkretisiert zwar das primärrechtlich verbürgte Recht auf Schutz persönlicher Daten, aber eben nur, soweit sie die Ausprägungen dieses Rechts normiert. Dies spricht gegen die Annahme eines auf der Datenschutz-Grundverordnung basierenden Unterlassungsanspruchs bezüglich einer verordnungswidrigen Verarbeitung personenbezogener Daten.“

Demnach vertritt das VG die Auffassung, dass bei einer rechtswidrigen Datenverarbeitung zunächst eine Beschwerde bei der zuständigen Aufsichtsbehörde eingereicht werden müsste.

Erst wenn dann ein rechtsverbindlicher Beschluss der Aufsichtsbehörde vorliege könne gemäß Art. 78 Abs. 1 DSGVO vorgegangen werden, der einen gerichtlichen Rechtsbehelf vorsehe.

Eine Begründung dazu, warum Art. 79 DSGVO hinsichtlich gerichtlicher Rechtsbehelfe abschließend sei gibt das VG nicht. Es ist insbesondere fraglich, ob diese Auslegung Art. 47 Abs. 1 der EU-Grundrechte-Charta (GRCh) entspricht. Demnach sollen Betroffenen Rechtsbehelfe bei Verletzungen von durch das Recht der Union garantierten Rechten und Freiheiten zustehen. Hierzu dürfte auch das Recht auf Schutz personenbezogener Daten nach Art. 8 Abs. 1 GRCh zählen.

Aufgrund der grundsätzlichen Bedeutung dieser Fragestellung wurde die Berufung zugelassen. Es bleibt daher abzuwarten, ob die Ansicht des VG von den höheren Instanzen geteilt wird.

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