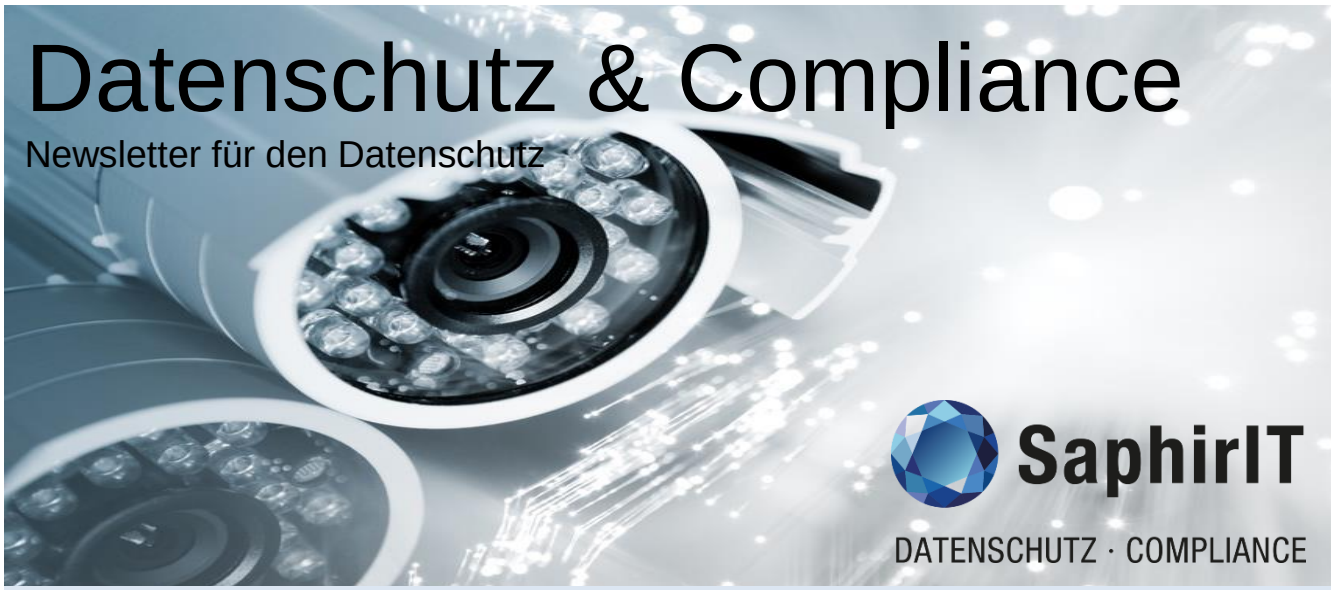

Ausgabe Juni 2018 | Seite 66 - 70

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Juni 2018.

Wie immer wünschen wir Ihnen viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Facebook äußert sich erstmals nach EuGH-Urteil zur gemeinsamen Verantwortlichkeit bei „Fanpages“

Der Europäische Gerichtshof (EuGH) hatte mit Urteil vom 05.06.2018 entschieden, dass der Betreiber einer Facebook-Fanpage schon durch die Eröffnung dieser Fanpage an der Entscheidung über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten aller Seitenbesucher neben Facebook mitverantwortlich ist.

Wie zu erwarten war hat sich nunmehr Facebook zu Wort gemeldet und ein Statement auf seinen Internetseiten bezüglich des Urteils abgegeben.

Facebook wolle Veränderungen vornehmen, um es Fanseiten-Betreibern zu ermöglichen, ihre Seiten konform der Datenschutzgrundverordnung (DSGVO) betreiben zu können.

Facebook führt aus: „Wir werden die notwendigen Schritte unternehmen, um es den Seitenbetreibern zu ermöglichen, ihren rechtlichen

Verpflichtungen nachzukommen. Unserer Ansicht nach ist es nicht sinnvoll, Seitenbetreibern eine gleichrangige Verantwortung für die von Facebook durchgeführte Datenverarbeitung aufzuerlegen; dies hat auch der EuGH anerkannt. Wir werden unsere Nutzungsbedingungen bzw. Richtlinien für Seiten aktualisieren, um die Verantwortlichkeiten sowohl von Facebook als auch von Seitenbetreibern klarzustellen, und damit auch die Einhaltung der rechtlichen Vorgaben für die Seitenbetreiber zu erleichtern. Details zu unseren aktualisierten Bedingungen werden wir in Kürze bekanntgeben."

Bereits zum Problem der Notwendigkeit des Abschlusses einer Auftragsdatenverarbeitungsvereinbarung hatte Facebook seine Nutzungsbedingungen dahingehend geändert, dass der Abschluss einer solchen Vereinbarung nicht notwendig sein soll.

Ob diese Änderung insbesondere nach den Regeln der DSGVO überhaupt zulässig ist wird abzuwarten bleiben.

Klar ist: Facebook selbst dürfte mit diesem Statement erst einmal versuchen seine Nutzer zu beruhigen und dem vorschnellen Löschen von Fanpages entgegenzuwirken. Ob und inwieweit es überhaupt möglich ist, dass Facebook die Verantwortlichkeit komplett auf sich nimmt, obwohl der EuGH eine gemeinsame Verantwortlichkeit annimmt, ist sehr fraglich.

Bis auf weiteres ist, was das Betreiben von Fanpages angeht, dennoch Vorsicht geboten. Sie sollten unternehmensintern abwägen ob das Bestehen einer solchen Fanpage tatsächlich notwendig ist und sich der Auftritt überhaupt rentiert.

Wir halten Sie auf dem Laufenden.

Privacy Shield vor dem Aus?

- EU-Abgeordnete nehmen die USA in die Pflicht -

Am 11.06.2018 beschloss der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des EU-Parlaments mit knapper Mehrheit eine Resolution zum transatlantischen Privacy Shield.

Die Übermittlung personenbezogener Daten in die USA stellt sich aus datenschutzrechtlicher Sicht seit jeher kritisch dar. Das einst gültige Safe-Harbour Abkommen ermöglichte, bis es am 16.10.2016 gekippt wurde, den Datentransfer in die USA.

Das Privacy-Shield ist der erste Angemessenheitsbeschluss seit dem in Kraft treten der Datenschutzgrundverordnung am 25.05.2016. Von der EU-Kommission beschlossen ermöglicht es US-Unternehmen sich auf der Privacy-Shield Liste eintragen zu lassen.

Hat der Datenexporteur aus der EU dann festgestellt, dass das betroffene Unternehmen in die Privacy-Shield Liste aufgenommen wurde kann der Datentransfer ohne eine weitere besondere Genehmigung erfolgen.

Das Privacy-Shield ist dennoch nicht weniger umstritten als sein Vorgänger. Insbesondere, da nicht festgestellt werden könne, ob die US-Behörden nicht weiterhin Daten von EU-Bürgern sammeln können.

Die Abgeordneten der EU erhöhen mit der Resolution nun den Druck auf die Kommission, die Einhaltung der Datenschutzgrundverordnung in den USA stärker zu kontrollieren. Dies sei eine zentrale Voraussetzung um den Transfer von Unternehmensdaten zwischen der EU und den USA aufrecht erhalten zu können.

Sollte die US-Seite bis zum 01. September diesen Jahres nicht in der Lage sein alle Vorgaben der 2016 in Kraft getretenen DSGVO einzuhalten müsse die Kommission das Datenschutzschild außer Kraft setzen.

Nachdem bereits das Safe-Harbour Abkommen gekippt wurde erscheint es, insbesondere aufgrund der nun geltenden DSGVO, durchaus möglich, dass auch das Privacy-Shield nach weniger als zwei Jahren ausgedient hat.

Ob die Kommission der Aufforderung des LIBE-Ausschusses das Privacy-Shield neu zu verhandeln und zu überarbeiten nachkommen wird, erscheint nicht nur wegen der aktuellen politischen Lage eher fragwürdig.

Ohnehin steht die Wirksamkeit des Privacy Shields in einem Verfahren zwischen Max Schrems und Facebook bereits vor dem EuGH auf dem Prüfstand.
Die momentan sicherste Variante scheint der Abschluss von EU-Standardvertragsklauseln zu sein. Viele große Unternehmen wie Google, Amazon oder Microsoft stellen eine solche Vereinbarung online zur Verfügung.

Die Problematik sollte trotzdem weiterhin wachsam verfolgt werden, denn auch wenn die Standardvertragsklauseln momentan als adäquatestes Mittel gelten, stehen auch diese in der Kritik und werden im gleichen Zug zur Wirksamkeit des Privacy-Shields vom EuGH auf ihre Wirksamkeit überprüft.

Es bleibt also spannend. Wir halten Sie auf dem Laufenden, sollten sich die aktuellen Begebenheiten ändern.

EMRK zur Einsichtnahme des Arbeitgebers in dienstliche Geräte seiner Arbeitnehmer

Immer wieder in der Diskussion steht die Frage ob und in welchem Umfang Arbeitgeber die Nutzung des dienstlichen PCs und anderer Geräte ihrer Mitarbeiter überwachen dürfen. Meist im Vordergrund steht dabei das private Nutzungsverhalten von Internet und oder E-Mail.

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat sich nun mit der Frage beschäftigt, wann diese Daten ausgewertet werden dürfen.

Vom Arbeitgeber zur Verfügung gestellte Hard- und Software darf grundsätzlich nur für betriebliche Zwecke verwendet werden. Eine private Nutzung ist nur erlaubt, wenn sie ausdrücklich gestattet ist.

Sofern die private Nutzung nicht gestattet ist, kann eine Einsichtnahme in das betroffene Gerät grundsätzlich immer erfolgen. Sofern dann erkennbar auch private Daten vorhanden sind, darf auf diese und damit das Gerät grundsätzlich nicht weiter zugegriffen werden.

Ein Zugriff darf jedoch dann weiter erfolgen, wenn ein konkreter Missbrauchsverdacht vorliegt (z.B. Vermutung betrieblicher Daten in privatem Ordner).

Bei einer gestatteten privaten Nutzung stellt sich die Rechtslage für die Einsichtnahme privater Daten wesentlich anders und komplizierter dar.

Die Einsichtnahme in ein Gerät, auf welchem sowohl private, als auch dienstliche Daten vermischt gespeichert sind, ist Arbeitgebern grundsätzlich nicht erlaubt. Diese ist wie bei der nicht gestatteten privaten Nutzung nur möglich, wenn die privaten Daten erkennbar von den betrieblichen Daten getrennt sind (beispielsweise mittels einer Software Container Lösung).

Aus vorgenannten Gründen sollte die private Nutzung ausdrücklich untersagt werden.

Der EGMR hat dies mit seinem Urteil vom 22.02.2018 bekräftigt.

Bei allen Daten auf einem dienstlichen Gerät sei grundsätzlich erst einmal davon auszugehen, dass diese auch dienstlicher Natur sind. Von diesem Grundsatz könne nur dann abgewichen werden, wenn die betreffenden Dateien ausdrücklich als „privat“ gekennzeichnet wurden.

Im Einzelfall kann es bei einer erlaubten privaten Nutzung durchaus zu Problemen kommen, wann es sich tatsächlich um private Daten handelt. Im betreffenden Fall hatte der Arbeitnehmer einen Ordner „persönliche Daten“ genannt. Diese Beschriftung, so das Gericht könne sich darauf beziehen, dass der Arbeitneh-

mer an diesem Ordner persönlich arbeite. Nicht aber, dass es sich konkret um sein Privatleben handele.

Knackpunkt der Entscheidung war die Feststellung, dass Arbeitgeber Daten die nicht eindeutig als „private Daten“ zu erkennen sind, grundsätzlich auch verwerten dürfen. Nur wenn festgestellt würde, dass die Daten „privat“ seien stünde der Schutz der Privatsphäre über dem Interesse des Arbeitgebers auf Datenerhebung.

Will ein Arbeitnehmer nicht, dass seine privaten Dateien auf Arbeitsgeräten durch den Arbeitgeber oder Kollegen geöffnet werden, sollte er idealerweise erst gar keine privaten Dateien auf dem Gerät abspeichern.

Geschieht dies doch, so sollte er sicherstellen, dass die Dateien eindeutig als „private Dateien“ gekennzeichnet sind.

Unsere Empfehlung: Regeln Sie die private Nutzung dienstlicher Geräte in Ihrem Unternehmen ausdrücklich. Ein komplettes Verbot der privaten Nutzung erscheint dabei am effektivsten. Sollten Sie die Nutzung zu privaten Zwecken doch gestatten sollte genau definiert sein wie, wann und in welchem Umfang dies erlaubt ist.

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