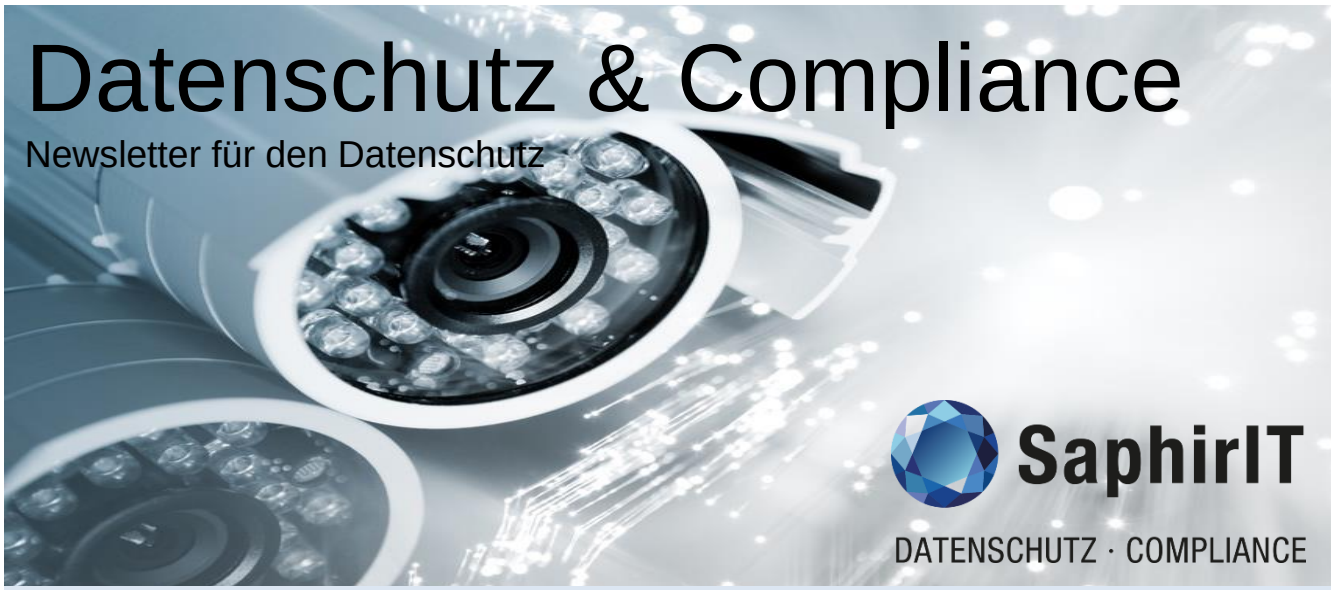

Ausgabe Februar 2021 | Seite 205 - 209

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Februar 2021.

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

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

LfD Niedersachsen zu Polizei-Messenger auf privaten Geräten

Bereits häufiger haben wir über die Problematik von einer „Bring Your Own Device“-Regelung (BYOD) berichtet.

Zusammengefasst geht es darum, dass Arbeitnehmer ihre eigenen Endgeräte wie beispielsweise Handys oder Laptops für dienstliche Zwecke verwenden dürfen.

Datenschutzrechtlich ist dieses Vorgehen sehr problematisch.

Nun hat sich die Landesbeauftragte für den Datenschutz (LfD) in Niedersachsen zu einem Messenger geäußert, der von Polizeibeamten auf privaten Endgeräten verwendet wird.

Explizit geht es um die Verwendung des Messengers „NIMes“. Die LfD Niedersachsen hat die Verwendung gegenüber dem Niedersächsischen Innenministerium beanstandet. Vor allem die Verwendung von BYOD bringe Risiken und Gefahren mit sich, denen die Polizei bisher nur mit unzureichenden Sicherheitsmaßnahmen begegne.

Die Landesbeauftragte für den Datenschutz Barbara Thiel führte dazu aus, die fehlende Kontrolle des Dienstherrn über die privaten Geräte der Beamtinnen und Beamten führe zu einem inakzeptablen Risiko für den Betrieb des hoch schutzbedürftigen Messenger-Dienstes.

Das Schutzstufenkonzept des LfD Niedersachsen hat Schutzstufen von A bis E. Die Messenger-App verarbeitet personenbezogene Daten der Schutzstufe D, welches die zweithöchste Stufe bei der Schwere eines möglichen Schadens für den Betroffenen darstellt.

In Stufe D werden Daten verarbeitet, deren unsachgemäße Handhabung die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.

Barbara Thiel kritisiert weiter: „Durch den BYOD-Ansatz ist im laufenden Betrieb eine unüberschaubare Kombination von verschiedenen Geräten, Betriebssystemen, sonstiger Software und Konfigurationen im Einsatz“.

„Gleichzeitig ist der jeweilige Anwender dafür verantwortlich, sein privates Endgerät vor Schadprogrammen zu schützen. Das wird dem Schutzbedarf der bedrohten Daten in keiner Weise gerecht.“

Die Übertragung von Daten könne jederzeit durch Schadsoftware angegriffen werden, ohne dass Dienstherr oder Anwender dies bemerkten.

Die Polizei führe zwar anlasslose Kontrollen der NIMes-Nutzer durch, diese beträfen jedoch nicht BYOD-Geräte.

Die Landesbeauftragte für den Datenschutz stellte klar, dass sie nicht generell gegen den Einsatz von NIMes sei. Der Messenger sei deutlich datenschutzfreundlicher als viele andere Messenger-Dienste. Dennoch sei es notwendig Polizistinnen und Polizisten endlich flächendeckend mit Dienstgeräten auszustatten.

Alternativ könne auf den privaten Geräten ein sogenanntes „Mobile Device Management“ aufgesetzt werden, dies würde jedoch voraussetzen, dass alle Polizistinnen und Polizisten diesem zustimmen, was eher fraglich sein dürfte, so Thiel.

Auch wenn die LfD Niedersachsen der Polizei den Einsatz der App auf privaten Geräten nicht untersagen kann ist das Innenministerium nach der geäußerten Beanstandung zumindest verpflichtet eine Stellungnahme abzugeben.

Diese Grundsätze müssen auch Sie in Ihrem Unternehmen beachten, wenn Sie BYOD praktizieren. Ihnen gegenüber hat die Aufsichtsbehörde sehr wohl die Möglichkeit rechtliche Maßnahmen bis hin zu Bußgeldern zu ergreifen.

CLOUD Act vs. DSGVO

Vor einiger Zeit hat der Europäische Gerichtshof das EU-US Privacy-Shield für unwirksam erklärt (wir berichteten in unserem Newsletter Juli 2020, abrufbar unter: https://www.saphirit.de/newsletter-flyer.html).

Seither ist es für viele Unternehmen noch schwieriger als vorher einen datenschutzrechtskonformen Datentransfer zwischen den Vereinigten Staaten und Europa aufrecht zu erhalten oder zu ermöglichen.

Viele Unternehmen setzen nun darauf ihre Server in europäischen Ländern aufzustellen, um dort dann die Regelungen der Datenschutzgrundverordnung (DSGVO) einhalten zu können.

Das Problem liegt jedoch im sog. Cloud-Act, der im März 2018 verabschiedet wurde. Dieser hat nichts mit einer Cloud zu tun, in der Sie vielleicht Ihre Daten speichern. CLOUD ist die Abkürzung für „Clarifying Lawful Overseas Use of Data Act“.

Der Cloud-Act gibt US-Strafverfolgungsbehörden praktisch eine ungehemmte Zugriffsmöglichkeit auf Daten von US-Unternehmen und Nutzern. Dies gilt auch wenn die Server der US-Anbieter in Europa stehen.

Der Cloud-Act verstößt damit eindeutig gegen die geltende Datenschutzgrundverordnung. Auch wenn ein amerikanisches Unternehmen Server in der EU aufstellt, um dort Daten seiner europäischen Nutzer zu speichern, verstößt dies gegen geltendes Datenschutzrecht.

Auch auf diese Daten können die Geheimdienste in den USA zugreifen.

Dies hat zur Folge, dass an sich nahezu alle Datenübertragungen mit einem US-Amerikanischen Unternehmen momentan nicht datenschutzkonform möglich sind. Auf der sicheren Seite ist nur, wer Lösungen von europäischen Anbietern nutzt.

Auch wenn es europäische Alternativen gibt, so werden diese häufig noch nicht genutzt. Jedes Unternehmen muss sein eigenes Risiko einschätzen, ob beispielsweise Software von US-amerikanischen Unternehmen (z.B. Microsoft, ZOOM, etc.) verwendet wird oder nicht.

Datenübertragung in das Vereinigte Königreich nach dem Brexit

Die EU-Kommission ist nach „gründlicher Überprüfung“ zu dem Ergebnis gekommen, dass das Vereinigte Königreich ein angemessenes Datenschutzniveau gewährleistet.

Nach dem Austritt des Vereinigten Königreichs aus der Europäischen Union bedurfte es einer Neubewertung des Datenschutzniveaus. Als ehemaliges Mitglied der Europäischen Union hatte sich das Vereinigte Königreich bisher immer auch an die Vorschriften der Datenschutzgrundverordnung (DSGVO) halten müssen.

Seit dem Austritt gilt das Vereinigte Königreich als Drittland im Sinne der Datenschutzgrundverordnung.

Zunächst war zwischen der EU und dem Vereinigten Königreich eine sechsmonatige Übergangsfrist vereinbart worden, um dann eine längerfristige Lösung aushandeln zu können. Ohne eine Vereinbarung bzw. die Feststellung eines angemessenen Datenschutzniveaus würde ein Datentransfer nur unter deutlich strengeren Bedingungen möglich sein (Über den Austritt Großbritanniens aus der EU berichteten wir bereits in unserem Newsletter Januar 2018, abrufbar unter: https://www.saphirit.de/newsletter-flyer.html).

Die EU-Kommission hat nunmehr zwei Entwürfe für sog. Angemessenheitsbeschlüsse veröffentlicht. Dabei wurde auch untersucht welchen Zugriff auf Daten die britischen Behörden haben. Die Kommission kam zu dem Ergebnis, dass auch insoweit das Datenschutzniveau dem der DSGVO „im Wesentlichen gleichwertig“ sei.

Dennoch dürfte dies einer der wichtigsten Punkte sein, die noch diskutiert werden müssen, bevor die EU das Vereinigte Königreich als sicheres Drittland einstufen kann.

In Großbritannien haben die Sicherheitsbehörden umfassende Befugnisse zur Massenüberwachung. Gemäß dem „Investigatory Powers Act“ darf die eng mit der NSA kooperierende GCHQ massive Eingriffe in technische Gerätschaften vornehmen.

Noch hat der Europäische Gerichtshof (EuGH) über einen sicheren Datentransfer nach Großbritannien nicht entschieden.

In einem Urteil hatte der EuGH Mitte letzten Jahres jedoch das EU-US Privacy Shield unter anderem deswegen gekippt, weil die US-Sicherheitsbehörden zu viele Befugnisse haben und dies mit den Grundsätzen der DSGVO nicht vereinbar ist.

Die Kommission ist dennoch der Auffassung, dass ein Angemessenheitsbeschluss wirksam wäre. Die Sicherheitsbehörden im Vereinigten

Königreich hätten bei den von ihnen durchgeführten Aktivitäten die Anforderungen immer analysiert und seien zu der Überzeugung gekommen, dass das Anfordern von Informationen in den betreffenden Fällen immer „notwendig und angemessen“ war. Gleiches gelte auch für den Inlandsgeheimdienst MI5.

Bisher ist der Angemessenheitsbeschluss jedoch noch nicht „in trockenen Tüchern“. Bis dahin besteht für Unternehmen, die Daten in das Vereinigte Königreich übertragen weiterhin Rechtsunsicherheit.

Auch wenn der Angemessenheitsbeschluss schließlich erstmal gebilligt wird, so bleibt abzuwarten wie der EuGH sich dazu äußern wird und ob er auch diesen Angemessenheitsbeschluss, ähnlich wie das EU-US Privacy-Shield kippen wird.

Falls Sie unseren Newsletter in Zukunft nicht mehr erhalten möchten, schicken Sie bitte eine kurze E-Mail an info@saphirit.de

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