

Datenschutz & Compliance

Newsletter für den Datenschutz



SaphirIT

DATENSCHUTZ · COMPLIANCE

Ausgabe November 2017 | Seite 38-41

INHALT

SEITE 38

**Niedersachsen bestellt 500
Bodykameras für die Polizei**

SEITE 39

**Facebook muss sich in Deutschland an
deutsches Datenschutzrecht halten**

SEITE 40

**JEFTA: Kommt ein „zweites Privacy
Shield“ mit Japan?**

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter November 2017.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Niedersachsen bestellt 500 Bodykameras für die Polizei

- Landesdatenschutzbeauftragte Barbara Thiel reagiert „Irritiert und mit großer Verwunderung“ -

Der Innenminister Niedersachsens Boris Pistorius (SPD) ordnete nach dem erfolgreichen Politversuch mit 20 Körperkameras, die komplette Ausstattung der Polizei mit Bodycams an Brennpunkten und in den Ballungsgebieten Niedersachsens an. Dies ließ er vergangene Woche durch einen Ministeriumssprecher mitteilen.

Die Diskussion um das Beschaffen von Bodykameras hat in den letzten Monaten immer wieder für Diskussionen gesorgt. Mit der Verkündung dieser Anschaffung ist in Niedersachsen nun aber ein ganz neuer Streit entfacht. Insbesondere Datenschützer melden sich vermehrt zu Wort.

Der Hintergrund dürfte den meisten klar sein. Die Beschaffung der Kameras soll insbesonde-

re zur Abschreckung, Deeskalation und Prävention beitragen.

Nicht außer Acht gelassen werden darf dabei aber, wie die Landesdatenschutzbeauftragte nun verdeutlicht, der Datenschutz und der massive Eingriff in die Persönlichkeitsrechte jedes einzelnen Menschen, welcher sich in Reichweite dieser Kameras bewegt.

Der Innenminister ließ weiter verkünden, dass voraussichtlich noch weitere Kameras beschafft werden würden. Dass es nach momentaner Rechtslage dafür jedoch noch an einer rechtlichen Grundlage fehlt, scheint dabei vorerst keine Rolle zu spielen.

Thiel betonte, die Anschaffung der Bodycams dürfe nicht an Recht und Gesetz vorbei betrieben werden.

Anfang des Jahres, so Thiel, habe der Landtag über einen Gesetzentwurf der Landesregierung zur Überarbeitung des niedersächsischen Polizeigesetzes beraten. So lange ein solches Gesetz, welches den ausdrücklichen Einsatz von Körperkameras vorsehe jedoch nicht beschlossen sei, dürften diese rechtmäßig auch nicht im Dienst eingesetzt werden. Generell gegen einen Einsatz der Kameras sei der Landesdatenschutz aber nicht.

Die Kosten für die Anschaffung der 500 Kameras belaufe sich auf knapp eine halbe Million Euro (Pressemitteilung der Landesbeauftragten für den Datenschutz vom 10.11.2017).

Wir werden den Vorgang weiter beobachten.

Facebook muss sich in Deutschland an deutsches Datenschutzrecht halten

- Datenschutzeinwilligung in App-Zentrum ungenügend -

Das Kammergericht Berlin bestätigte nun die Rechtsauffassung der Vorinstanz durch das Landgericht Berlin gegen welche Facebook 2014 Revision eingelegt hatte.

Das Kammergericht entschied, dass Facebook User in Deutschland nicht ausreichend über den Umfang und Zweck der Datenweitergabe in deren App-Zentrum informiert wurden. Facebook, dürfe, so das Kammergericht die Daten seiner Nutzer nicht ohne deren ausdrückliche wirksame Einwilligung herausgeben.

Facebook bietet seinen Nutzern seit Jahren die Möglichkeit über das eigene App-Zentrum kostenfreie Spiele von anderen Anbietern zu spielen.

Um eines der Spiele spielen zu können müssen Nutzer den Button „Sofort spielen“ betätigen. Unter diesem wurden Hinweise angezeigt in welcher Art und Weise, welche personenbezogenen Daten an die Spielbetreiber weitergegeben würden. Unter anderem wurden E-Mail-Adressen und Statusmeldungen übermittelt.

Ein anderes Spiel verlangte bei Klicken des Buttons die Erlaubnis im Namen des Nutzers Statusmeldungen, Fotos und Anderes zu posten. Einen Hinweis über den Zweck der Datenverarbeitung blieb jedoch in beiden Fällen aus.

Der Bundesverband der Verbraucherzentralen war der Auffassung die bereitgestellten Informationen seien nicht geeignet um von einer informierten und freiwilligen Einwilligung der Nutzer über die Datenweitergabe ihrer personenbezogenen Daten auszugehen. Sie beanstandeten daher einen Datenschutzverstoß Facebooks gegen geltendes deutsches Datenschutzrecht.

Die Anwendbarkeit des deutschen Datenschutzrechts bejahte das Berliner Kammergericht unproblematisch mit der Begründung es reiche aus, dass das Unternehmen, mit seinem Sitz in Irland, deutsche Nutzer habe und ferner in Hamburg eine Schwestergesellschaft für die Förderung des Anzeigengeschäfts unterhalte.

Zur Begründung führte das Gericht an, die bereitgestellten Informationen reichten nicht aus, um bei den Nutzern von einer freien und informierten Entscheidung über die Genehmi-gung zur Erhebung und Weitergabe ihrer Daten auszugehen. Die ebenfalls von der Verbraucherzentrale beanstandete Berechtigung zum Posten von Inhalten hielt das Gericht für zu unbestimmt. Die Klausel verstoße gegen das AGB-rechtliche Transparenzgebot sowie gegen geltende Datenschutzvorschriften. Durch die Nutzung der verwendeten Klausel sei nicht eindeutig erkennbar, mit welchem Inhalt und in welcher Zahl besagte Posts getätigt würden. Von der Formulierung sei quasi jede mögliche Werbung umfasst.

Da dem Urteil eine enorme grundsätzliche Bedeutung zugesagt wird, ließ das Kammergericht die Revision zum Bundesgerichtshof zu. Wir werden weiter berichten (Kammergericht Berlin, Urt. v. 22.09.2017, Az. 5 U 155/14).

JEFTA: Kommt ein „zweites Privacy Shield“ mit Japan?

Die europäische Kommission hat erneut ihre Bemühungen um den Abschluss eines Abkommens zur Übermittlung von Daten auf Basis eines angemessenen Datenschutzniveaus verstärkt.

Inhalt der Datenschutzverhandlungen zwischen der EU und Japan ist das geplante Freihandels- und Investitionsabkommen JEFTA (Japan-EU-Free-Trade-Agreement), welches

insbesondere eine Vereinbarung zum Datenfluss zwischen beiden Parteien enthalten soll.

Der Kommission zufolge werde es sich bei JEFTA um das bedeutendste bilaterale Handelsabkommen handeln, welches jemals von der EU geschlossen wurde. Stellt die EU einmal ein angemessenes Datenschutzniveau für Japan fest, ist die Übermittlung von Daten ohne die Notwendigkeit weiterer Maßnahmen

aufgrund der internationalen Beziehung möglich.

Ein angemessenes Datenschutzniveau hat die EU längst noch nicht in allen Ländern festgestellt. Bezogen auf die USA löste das Mitte 2016 in Kraft getretene EU-US-Privacy Shield (s. unser Sonderrundbrief 02/2016) das für ungültig erklärte Vorgängerabkommen Safe Harbour (s. unser Sonderrundbrief 10/2015) ab. Weitere Drittländer in denen bereits ein angemessenes Datenschutzniveau festgestellt wurde sind: Argentinien, Australien, Guernsey, Isle of Man, Jersey und die Schweiz.

Das Europäische Parlament hält den Abschluss des Abkommens bereits für Anfang 2018 für möglich. Als Vorbereitung auf einen möglichen Abschluss entsandte das Parlament eine 8-köpfige Delegation um vor Ort in Tokio den Stand der aktuellen japanischen Bemühungen zu überprüfen.

Ziel der Reise, in welcher die europäischen Verantwortlichen sich mit Vertretern der japanischen Datenschutzbehörde und des japanischen Parlaments trafen war es, die Mitglieder des europäischen Parlaments über den aktuellen datenschutzrechtlichen Gesetzesrahmen der Japaner zu informieren.

Hintergrund ist, dass die Mitglieder des EU-Parlaments schließlich eine „Angemessen-

heitsentscheidung“ zu treffen haben werden, ob und inwiefern Japan die Voraussetzungen erfüllt als Drittland mit angemessenem Datenschutzniveau eingestuft zu werden.

Die Anforderungen an Japan seien dabei aber nicht so weit zu fassen, dass diese verpflichtet sind die ab 25.05.2018 in der EU geltende EU-Datenschutzgrundverordnung in ihrem nationalen Recht einzubinden. Vielmehr liege es (so auch schon der Europäische Gerichtshof in seiner Safe-Harbour Entscheidung) an der EU-Kommission ein im wesentlichen gleichwertiges Datenschutzniveau in Japan anzuerkennen. Es sei dabei unangemessen von Japan und auch anderen Drittländern ein zum europäischen Recht identisches Datenschutzniveau vorauszusetzen, um einen Datentransfer zu ermöglichen. Primär ginge es erst einmal darum ein zukunftsfähiges Modell aufzubauen, welches dann entweder in Form eines Privacy Shields oder aber in einer anderen Form über die Angemessenheit des Japanischen Datenschutzes entscheide.

Wir werden berichten, sobald eine neue Entwicklung in den Verhandlungen vorliegt.

Sollten Sie in Ihrem Unternehmen einen Datentransfer in die USA oder in ein anders Drittland betreiben müssen einige Besonderheiten beachtet werden. Sollten Sie dazu Fragen haben sprechen Sie uns gerne an.

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

