

DATENSCHUTZ-NEWS – MÄRZ 2017

EU-Kommissarin erwägt Kündigung des Privacy Shields

Die EU-Justizkommissarin Věra Jourová wird das Privacy Shield Abkommen unverzüglich außer Kraft setzen, falls sich die US-Regierung nicht an die getroffenen Zusagen hält.

Grund hierfür ist die von Präsident Trump unterzeichnete Anordnung vom 25.01.2017, in welcher ein Passus vorhanden ist, der die Datenschutzrechte von Ausländern beschränkt. Da die Anordnung sich aufgrund ihres Wortlautes auch auf EU-Bürger bezieht, ist es sehr umstritten, ob sie den Grundsätzen des Privacy Shield Abkommens entgegensteht.

Sollte das Privacy Shield Abkommen tatsächlich aufgehoben werden, bliebe zunächst nur der Abschluss von EU-Standardvertragsklauseln zur Legitimation von Datenübermittlungen in die USA. Deren Zukunft ist allerdings ebenfalls ungewiss.

Quelle: intersoft consulting services AG

Unangekündigte Vor-Ort-Kontrolle in Zahnarztpraxis

Das Bayerische Landesamt für Datenschutzaufsicht schickte die Polizei zu einer Zahnarztpraxis in einem Mehrfamilienhaus. Basis dafür war, dass ein Bürger das BayLDA darauf aufmerksam machte, dass in einem leicht zugänglichen Treppenhaus die Patientenakten in unverschlossenen Metallaktenschränken aufbewahrt wurden. Die Polizei forderte

den Zahnarzt auf, die Metallschränke unverzüglich zu schließen.

Trotz vorhergehender Polizeianordnung wurde die Aufsichtsbehörde darauf aufmerksam gemacht, dass die Aktenschränke immer noch unverschlossen sind. Aufgrund dessen kam es zu einer unangekündigten Vor-Ort-Kontrolle durch das BayLDA, woraufhin der Zahnarzt die Akten aus den Schränken in seine Praxisräume und in einen mit einer Metalltür gesicherten Kellerraum brachte.

Nach derzeitiger Rechtslage kann ein Verstoß gegen die Anforderungen der Datensicherheit nicht unmittelbar mit einem Bußgeld sanktioniert werden. Aufgrund des EU-Datenschutzgrundverordnung (unmittelbares Recht ab dem 25.05.2018) können derartige Verstöße mit einem Bußgeld von bis zu 10. Mio. Euro bestraft werden.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Speicherung von Fluggastdaten

Das Bundeskabinett hat beschlossen, dass ab Mai 2018 alle Daten von Fluggästen gespeichert werden, die bei Buchung oder Check-in angegeben wurden. Dies umfasst bspw. Name, Adresse, Konto- oder Kreditkartenverbindung, Reiseweg, Telefonnummer.

Diese Daten dürfen dann auch mit ausländischen Behörden innerhalb Europas ausgetauscht

werden. Ziel des Beschlusses ist, dass Terror und Kriminalität grenzüberschreitend bekämpft werden können.

Quelle: www.swr.de

Vorratsdatenspeicherung für Fahrzeugdaten?

Bundesverkehrsminister Alexander Dobrindt will Haftungsfragen des automatisierten Fahrens künftig mit einer Blackbox klären lassen. Dies wurde bereits von mehreren zuständigen Datenschutz-Aufsichtsbehörden kritisiert, denn bisher sind die folgenden Punkte unklar:

- Wo wird sich der Datenspeicher befinden (im Fahrzeug oder auf Server des Fahrzeugherstellers)?
- Welche Daten werden gespeichert (bspw. Geschwindigkeit, Bremseninsatz, Positions- und Sensordaten, Sitzeinstellungen)?
- Wie groß ist der Umfang der gespeicherten Daten?
- Wer ist Adressat der Herausgabepflicht der Daten?
- Der Zweck der Datenspeicherung ist mit „zur Kontrolle“ unklar gefasst.

Quelle: www.heise.de

Massive Zunahme gemeldeter Datenpannen in Bayern

Die Anzahl der gemeldeten Datenpannen ist stark angestiegen. Dabei gehen viel der Pannen auf Hacking-Angriffe zurück. Durch Bürgerbeschwerden kam das Bayerische Landesamt für Datenschutzaufsicht auch nicht gemeldeten Angriffen auf die Spur.

Laut Bericht des BayLDA melde-
ten allein im vergangenen Jahr 85
Unternehmen eine Datenpanne.
Im Jahr zuvor waren es erst 28
Unternehmen.

Quelle: m.heise.de

Mailserver des Bundestags lahmgelegt

Anfang des Monats konnten Ab-
geordnete des Bundestages keine
E-Mails mehr senden und emp-
fangen. Das Internet als auch das
Intranet funktionierten nicht
mehr.

Es wird nunmehr von der Bundes-
tagsverwaltung geprüft, ob es
sich hierbei um ein Hardware-
Problem oder einen Hackerangriff
von außen auf das Parlament
handelte.

Die bisher größte Hackerattacke
wurde im Dezember 2014 und Ja-
nuar 2015 auf das interne Netz-
werk des Bundestages gestartet.
Dabei soll von einem ausländi-
schen Nachrichtendienst ein Tro-
janer auf die Rechner von Frakti-
onen platziert worden sein.

Quelle: www.welt.de

Google nützt Datenschutz

Google plant, Programme ohne
Datenschutzerklärung aus seinem
App-Store zu werfen. Das Unter-
nehmen stellt hierbei sehr
strenge Anforderungen und ist
dabei auf einer Linie mit den
deutschen Datenschutzbehörden.

Bisher konnten sich schwarze
Schafe sehr einfach in den Google
Play Store einschleichen. Nun will

Google jedoch hart durchgreifen.
Bereits in den vergangenen Wo-
chen erhielten die ersten App-
Entwickler E-Mails, in denen
Google ankündigte, ihre App aus
dem Katalog von Google Play zu
streichen, wenn nicht umgehend
eine Datenschutzerklärung er-
gänzt wird.

Zwar wird Google nicht alle Da-
tenschutzerklärungen inhaltlich
prüfen können, jedoch erhöht
sich für App-Entwickler das prak-
tische Risiko von Datenschutzver-
stößen signifikant.

Quelle: www.lto.de

Datenbank mit 1,37 Mrd. E- Mail-Adressen veröffentlicht

Aufgrund eines Back-up-Fehlers
veröffentlichte das Unternehmen
„River City Media“ versehentlich
seine komplette Spammer-Daten-
bank mit über 1,37 Mrd. Einträ-
gen. Hierbei wurden hauptsäch-
lich E-Mail-Adressen veröffent-
licht. Teilweise waren diese auch
mit IP-Adressen, Namen oder ei-
ner Postanschrift verknüpft.

Die Marketingfirma „River City
Media“ dient als Fassade für eines
der größten Spam-Netzwerke der
Welt, welches täglich mehrere
Milliarden E-Mails versendet. Um
an die entsprechenden Daten der
Betroffenen zu gelangen, nutzte
das Unternehmen die Teilnahme
an Gewinnspielen als Vorwand.
Dabei wurde im Kleingedruckten
eingewilligt, dass die Daten auch
für Werbezwecke an Dritte wei-
tergegeben werden dürfen.

Bei einer Anzahl von aktuell unge-
fähr 3,4 Mrd. Internetnutzer ist

somit theoretisch jeder Dritte von
der Offenlegung seiner Daten be-
troffen.

Quelle: intersoft consulting services AG

NSA bescheinigt Windows 10 und Surface hohe Sicherheit

Der US-Geheimdienst NSA hat
Windows 10 und die Surface-Ge-
räte als besonders sicher einge-
stuft und sie auf die CSfC-Liste
(Commercial Solutions for Classi-
fied Programs) gesetzt. Diese
Liste beschreibt kommerzielle
Produkte, die für den geheimen
Einsatz geeignet sind.

Nach eigener Aussage der NSA
nimmt diese nur Produkte auf die
Liste, die bestimmte Kriterien er-
füllen und zugleich zeitnah Up-
dates bereitstellen, um Sicher-
heitslücken zügig zu schließen.

Quelle: www.golem.de

Google setzt Richtlinie für Werbeanzeigen um

Betrüger und Kriminelle können
Werbebereiche nutzen, um Wer-
bung mit eingebettetem
Schadcode auszuspielen, der
Schwachstellen im verwendeten
Browser ausnutzt. Aufgrund des-
sen hat Google einen Beitrag ver-
öffentlicht, in dem die Maßnah-
men zur Filterung von böswilliger
und betrügerischer Werbung in
Google AdSense beschrieben
werden. Insgesamt hat Google im
Jahr 2016 1,7 Mrd. Werbeanzei-
gen ausgefiltert und damit mehr
als das Doppelte vom Vorjahr.

Quelle: datenschutz nord GmbH