Zeitschrift für Datenschutz – ZD
www.zd-beck.de

ZD FOKUS

Axel Spies USA: Zusätzliche Anforderungen für die Online-Verarbeitung von personenbezogenen Daten in Kalifornien

ZD-Aktuell 2013, 03739

Am 27.9.2013 unterzeichnete der Gouverneur von Kalifornien, Brown, zwei Gesetzesnovellen mit zusätzlichen Anforderungen für die Sammlung von Online-Verbraucherdaten. Der erste Gesetzeszusatz (Assembly Bill – AB-370) zum bisher schon wegweisenden California Online Privacy Protection Act (CalOPPA) verlangt von den Betreibern von Webseiten, mobilen Anwendungen und anderen Online-Diensten u.a. eine Offenlegung der Praktiken, wie sie auf „Do-Not-Track"-Rückmeldungen oder die Erfassung der Online-Aktivitäten reagieren, womit zumindest in den USA gesetzliches Neuland betreten wird. Der zweite Gesetzeszusatz (Senate Bill – SB 46) beinhaltet zusätzliche Anforderungen an die schon bestehenden strengen Standards in Kalifornien, eine Verletzung der Datensicherheit (Data Breach Notification) z. B. durch Datenverlust, Diebstahl oder Hacking umgehend an die Betroffenen elektronisch zu melden.

Diese Zusätze ergänzen einen kürzlich ebenfalls verabschiedeten Zusatz SB 586 zum Schutz der „Privatsphäre von Kaliforniens Minderjährigen in der digitalen Welt". Die Initiativen zeigen, dass die Online-Privatsphäre – insbesondere im Hinblick auf Online-Aktivitäten – zunehmend im Fokus der kalifornischen Gesetzgebung steht. Kalifornien nimmt weiterhin eine Vorreiterrolle ein. Das gilt z.B. für das Verfolgen des Nutzers eines Diensts über einen gewissen Zeitraum oder über mehrere Webseiten hinweg (Tracking) zur Zusendung von u.a. individualisierter Werbung.

Mehr Pflichtangaben in der Privacy Policy nötig

CalOPPA – seit vielen Jahren eines der wegweisenden Privacy-Gesetze in den USA (vgl. *Spies*, ZD-Aktuell 2013, 03417 für mobile Apps) – legt bereits nach gegenwärtiger Rechtslage den Betreibern einer Webseite oder eines Online-Diensts, die personenbezogene Daten von Verbrauchern in Kalifornien sammeln, die Pflicht auf, ihre Datenschutzerklärung (Privacy Policy) auf der Webseite auffällig platziert zu posten. Die Privacy Policy muss schon heute mindestens folgende Angaben enthalten:

- eine Liste der Kategorien der gesammelten personenbezogenen Daten und die Parteien, mit denen diese Informationen geteilt werden können,
- eine Beschreibung, wie die Betroffenen die gespeicherten Daten einsehen und Änderungen geltend machen können,
- eine Beschreibung, wie die Betroffenen über wesentliche Änderungen der Privacy Policy informiert werden,
- das Datum des Inkrafttretens der Privacy Policy.

Die neuen Vorschriften der AB-370 erfordern zusätzlich folgende Angaben in der Privacy Policy zur besseren Transparenz der Datenverarbeitung:

- eine Offenlegung und Beschreibung, wie der Betreiber „Do-Not-Track"-Rückmeldungen oder andere Mitteilungen verarbeitet, die den Nutzern die Möglichkeit bieten, ihre Wahl in Bezug auf die Sammlung von persönlichen Informationen über ihre Online-Aktivitäten auszuüben (was natürlich voraussetzt, dass der Betreiber diese Informationen überhaupt sammelt) sowie
- eine Beschreibung, ob und wie Dritte personenbezogene Daten über die Webseite sammeln (z.B. die Zeit, die für Online-Aktivitäten verbraucht wird – oder ob der Nutzer eine Website anklickt).

Ein Betreiber kann die neuen Angaben zur Transparenz dadurch erfüllen, dass seine Privacy Policy klar und eindeutig mittels Hyperlink auf eine Beschreibung eines Protokolls des Betreibers verweist, das der Nutzer bei seiner Wahl zur vollen Information über die Sammlung von persönlichen Informationen über seine Online-Aktivitäten einsehen kann. Eine Pflicht, dem Verbraucher ein Opt-out anzubieten, besteht jedoch nicht. Er muss nur ausreichend informiert werden.

Darüber hinaus wird zum 1.1.2015 das Gesetz über die Begrenzung des Online-Marketing oder Werbung für Minderjährige (Personen unter 18 Jahren) in Kraft treten; es beinhaltet insbesondere, dass auch Minderjährige vom Betreiber verlangen können, dass ihre in einem Online-Dienst geposteten Informationen vom Betreiber wieder gelöscht werden. Gerade im Bereich Social Media, wenn ein Minderjähriger ein Posting z.B. auf

Facebook „bereut", hat diese Pflicht Bedeutung.
CalOPPA enthält keine besonderen Bestimmungen über die Durchsetzung der Vorschriften, aber Kaliforniens Generalstaatsanwältin *Harris* hat in der Vergangenheit auf Bestimmungen über den unlauteren Wettbewerb in Kalifornien zur Durchsetzung von CalOPPA zurückgegriffen. Dieses Gesetz sieht im Einzelfall Strafen von bis zu US-$ 2.500,– pro Verletzung vor. Vor einigen Monaten reichte die *Generalstaatsanwältin* eine viel beachtete Klage gegen *Delta Airlines* ein, der zufolge *Delta* durch die veröffentlichte Datenschutzerklärung in ihrer Fly Delta App gegen CalOPPA und Kaliforniens Wettbewerbsrecht verstoßen habe. (vgl. *Spies*, ZD-Aktuell 2013, 03417).
Die jüngsten Ergänzungen zu CalOPPA stellen in den USA erste Gesetzesregelungen des Konzepts des „Do-Not-Track" dar, das aktuell ein Schwerpunkt bei der *FTC* und für die Arbeit der Selbstregulierung durch die Industrie ist. Da CalOPPA sich auf die Datensammlung von Einwohnern Kaliforniens bezieht, können auch Unternehmen mit Sitz außerhalb Kaliforniens diesen neuen Anforderungen unterliegen.

Neue erweiterte Regeln bei einer Verletzung der Datensicherheit im Unternehmen

Zum zweiten Änderungszusatz zu CalOPPA (SB 46): Das geltende Recht erlegt denjenigen, die Geschäfte in Kalifornien führen und in diesem Zusammenhang personenbezogene Daten online verarbeiten, die Pflicht auf, eine Verletzung der Datensicherheit (Hacking, Verlust des Datenträgers usw.) an den Betroffenen elektronisch zu melden, sofern diese Daten nicht verschlüsselt sind. Der Terminus „persönliche Informationen" umfasst derzeit nur den individuellen Vornamen oder erste Initiale und Nachname in Kombination mit bestimmten unverschlüsselten Datensätzen wie Sozialversicherungsnummern, Führerscheinnummern, Kontodaten und medizinischen Informationen. Es gibt keine allgemeinen Regeln für personenbezogene Daten. Die neuen Änderungen der SB 46, die schon zum 1.1.2014 in Kraft treten, erweitern die Definition um den Benutzernamen oder eine E-Mail-Adresse in Kombination mit einem Passwort oder einer Sicherheitsfrage oder in Kombination mit Eingabeinformationen, die den Zugang zu einem Online-Konto (nicht nur ein Bankkonto) erlauben (gängiges Beispiel: E-Mail-Adresse als Login und Passwort).
Allerdings variieren die Verpflichtungen zur Benachrichtigung im Bereich Online-Kontoinformationen je nach Datentyp. Als wichtigstes Beispiel: Wenn in der Verletzung der Datensicherheit Online-Kontoinformationen und keine anderen persönlichen Daten involviert sind, kann das betroffene Unternehmen der Verpflichtung dadurch nachkommen, dass es die Verletzung der Datensicherheit „in elektronischer oder anderer Form der betroffenen Person prompt meldet und sie dazu auffordert, ihr persönliches Passwort und die Antwort auf die Sicherheitsfrage, soweit anwendbar, zu ändern, oder dass die Person in diesem Fall andere geeignete Maßnahmen zum Datenschutz selbst ergreift (z.B. indem sie das Online-Konto sicherheitshalber selbst löscht).
Im Lichte dieser neuen Vorschriften sollten die Unternehmen mit Geschäft in Kalifornien sorgfältig prüfen, ob CalOPPA mit den genannten neuen Vorschriften voll umgesetzt ist, und evtl. ihre Privacy Policy entsprechend anpassen bzw. aktualisieren.

■ Vgl. auch zu „Do-Not-Track" die Entschließung der Datenschutzkonferenz ZD-Aktuell 2013, 03746.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen LLP in Washington DC und Mitherausgeber der ZD.

EuGH: Aufnahme digitaler Fingerabdrücke in Reisepässe rechtmäßig

ZD-Aktuell 2013, 03771

Der *EuGH* hat (ZD 2013, 608 – in diesem Heft) festgestellt, dass die Erfassung und Speicherung von Fingerabdrücken in Reisepässen rechtmäßig ist. Die Maßnahmen seien gerechtfertigt, um die betrügerische Verwendung von Reisepässen zu verhindern.
Der Kläger, ein deutscher Staatsangehöriger, beantragte bei der Stadt Bochum die Erteilung eines Reisepasses, wobei er die obligatorische Erfassung seiner Fingerabdrücke verweigerte. Die Stadt lehnte dies unter Berufung auf das Passgesetz ab, weil ein Pass ohne die obligatorische Erfassung der Fingerabdrücke nicht erteilt werden könne. Mit einer Klage beim *VG Gelsenkirchen* (ZD 2012, 588 (Ls.)) begehrte der Kläger, die Stadt Bochum zu verpflichten, ihm einen Reisepass zu erteilen, ohne seine Fingerabdrücke zu erfassen. Er macht hierfür u.a. eine Verletzung seines Grundrechts auf Schutz personenbezogener Daten geltend. Das *VG* möchte nun vom *EuGH* wissen, ob die den Mitgliedstaaten unionsrechtlich auferlegte Verpflichtung nach Art. 1 Abs. 2 der VO 2252/2004/EG, der bei der Beantragung eines Reisepasses die Pflicht zur Abgabe von Fingerabdrücken und deren Speicherung im Pass vorsieht, insbesondere im Hinblick auf die Charta der Grundrechte der EU gültig ist.
Der *EuGH* war der Ansicht, dass zwar ein Eingriff in die Rechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten bestehe, dieser sei aber gerechtfertigt. Die Maßnahme sei auch verhältnismäßig, da wirksame Maßnahmen, die mit einem geringeren Eingriff verbunden wären, nicht ersichtlich seien. Insbesondere sei das Verfahren der Iris-Erkennung technisch noch nicht so ausgereift und wegen seiner derzeit noch deutlich höheren Kosten für eine allgemeine Anwendung weniger geeignet. Was die Verarbeitung von Fingerabdrücken betrifft, erfüllten Fingerabdrücke zwar eine besondere Aufgabe bei der Identifizierung von Personen im Allgemeinen.
Laut *EuGH* sieht die VO jedoch ausdrücklich vor, dass die Fingerabdrücke nur zu dem Zweck verwendet werden dürfen, die Authentizität des Reisepasses und die Identität seines Inhabers zu überprüfen. Außerdem sehe sie die Speicherung der Fingerabdrücke nur im Pass selbst vor, der im ausschließlichen Besitz seines Inhabers bleibt. Daher könne die VO als solche keine Rechtsgrundlage für eine etwaige Zentralisierung der auf ihrer Grundlage erfassten Daten oder für eine Nutzung dieser Daten zu anderen Zwecken als der Verhinderung der illegalen Einreise von Personen in das EU-Gebiet darstellen.
Die VO beruhe auch auf einer geeigneten Rechtsgrundlage und sei auch nicht wegen fehlender Anhörung des *EU-Parlaments* im Gesetzgebungsverfahren ungültig. Das Erlassverfahren sei fehlerfrei gewesen, jedenfalls hinsichtlich der VO 444/2009/EG, die den Wortlaut der streitigen Bestimmung der VO 2252/2004/EG ersetzt habe und auf den vorliegenden Fall anwendbar sei.

■ Vgl. zur Verwendung biometrischer Daten auch *BVerfG* ZD-Aktuell 2013, 03463.