IT-SICHERHEIT UND DATENSCHUTZ (TEIL 1)

Praktische Lösungen für aktuelle Probleme mit Google Fonts, Facebook und Co.

von RAin Heike Mareck, Dortmund

| Feierabend oder Pause gemacht und auf dem Schreibtisch sensible Mandantendaten liegen gelassen bzw. den Computer nicht gesperrt? Solche Situationen betreffen die IT-Sicherheit und den Datenschutz in der Anwaltskanzlei. Der AK-Leitfaden mit insgesamt fünf Teilen beantwortet deshalb die wichtigsten IT- und Datenschutz-Fragen und erläutert, welche technischen und organisatorischen Maßnahmen die Kanzlei unbedingt beachten muss. Teil 1 gibt Ihnen praktische Tipps bei typischen, aktuellen Problemen u. a. mit Google Fonts, einem Datenleck bei Facebook und der Anwendung von Microsoft Office 365. |

1. Deshalb sind auch Kanzleien betroffen

Dies kann und sollte jeder Kanzleiinhaber überprüfen!

In den letzten Wochen ist im Bereich IT-Sicherheit und Datenschutz viel passiert. Das betraf vor allem die Nutzung von Google-Schriften auf Websites oder den Einsatz von Microsoft Office 365. Denken Sie jetzt etwa: „Betrifft mich nicht"? Das ist leider nicht korrekt! Denn häufig werden Google Fonts oder Inhalte von Drittanbietern (z. B. wenn die Kanzleiadresse mit Google Maps angezeigt wird) auch auf vielen Kanzleiwebsites falsch eingebunden. Oder Sie betreiben über facebook eine Fanpage und die dort angegebene Handynummer ist „geleakt" worden. In diesen Fällen haben auch Sie ein DS-GVO-Problem!

2. Darauf sollten Sie beim Einsatz von Google Fonts achten

Die Übertragung personenbezogener Daten in die USA ist oft nicht legal

In den letzten Monaten wurden systematisch Websites im sog. Seitenquelltext nach den Links fonts.gstatic oder fonts.googleapis.com durchsucht. Bei Treffern wurden die Websitebetreiber abgemahnt – verbunden mit der Aufforderung, zwischen 150 bis 270 EUR zu zahlen. Hintergrund ist: Das LG München bejaht einen Schadenersatzanspruch wegen Verstoßes gegen die DS-GVO, wenn die IP-Adresse auf einer Website rechtswidrig in die USA übermittelt wird (20.1.22, 3 O 17493/20; vgl. zur unzulässigen Übertragung personenbezogener Daten in die USA auch: EuGH 16.7.20, Rechtssache C-311/18, Schrems II). Über Google Fonts können Schriften auf einer Website frei genutzt werden, ohne sie auf den eigenen Server laden zu müssen. Allerdings werden die Schriften bei einem Aufruf der Webseite über einen externen Google-Server nachgeladen und dabei werden Daten an Google übermittelt.

Google-Schriften auf den eigenen Server hochladen

PRAXISTIPP | Wenn Sie Google-Schriften einbinden, dann bitte nur statisch auf Ihrem Server! Kontrollieren Sie deshalb die Schriften auf Ihrer Website: Unter iww.de/s7407 können Sie dazu Ihre URL eingeben. Hier erhalten Sie in wenigen Sekunden angezeigt, ob Ihre Website abmahngefährdet ist. Achtung: Damit wird zwar nicht die komplette Website überprüft, sondern nur einige Seiten. Diese Prüfung gibt aber schon einen guten Überblick!

3. Diese anderen Schauplätze könnten akut werden

Nach den oben geschilderten Erfahrungen ist leider zu befürchten, dass sich die Protagonisten „neue" Ziele suchen werden. Dieses könnten z. B. Inhalte auf Ihrer Website sein, die Sie von dritten Servern einbinden. Neben Google Fonts geht es z. B. auch um:

- JavaScript-Dateien
- Bilder
- Videos
- Like-Buttons
- Google Maps
- Recaptcha
- Eingebettete Newsletter-Anmeldeformulare

PRAXISTIPP | Auch wenn die Abmahnwelle zu Google Fonts gerade gebrochen ist (siehe auch: AG Charlottenburg 20.12.22, 217 C 64/22), sollten Sie Ihre Website auf den Einsatz von Drittanbietern überprüfen. Befragen Sie dazu Ihren Webtechniker, Webdesigner bzw. Ihre Internetagentur, wenn Sie dafür technisches Know-how brauchen. Es kommt unterm Strich nur darauf an, dass Sie die Drittinhalte lokal einbinden!

Auch Drittinhalte immer lokal einbinden

4. Datenleck bei Facebook hat Millionen Kunden geschädigt

In den vergangenen Wochen war in sozialen Medien die Rede von einem angeblichen Datenleck bei WhatsApp. Ein Hacker soll Nutzerdaten im Netz zum Verkauf für 2.000 EUR angeboten haben – darunter seien auch rund sechs Millionen deutsche Nummern. An dieser Version gibt es nun Zweifel. „Es gibt kein WhatsApp-Datenleck!" sagte jüngst RA Christian Solmecke von der Kölner Medienrechtskanzlei WBS.LEGAL. Sein Team war an den Hacker herangetreten, der ein Sample von hunderten Datensätzen zur Überprüfung bereitstellte. Dabei kam heraus, dass die Reihenfolge der Betroffenen komplett identisch mit der der Opfer des Facebook-Datenlecks aus dem vergangenen Jahr gewesen ist. Es fehlten lediglich einige Namen.

Es gibt zwar kein WhatsApp-Datenleck ...

Demgegenüber gab es das Facebook-Datenleck tatsächlich. Ende November 2022 verhängte die irische Datenschutzbehörde gegen den Meta-Konzern ein Bußgeld in Höhe von 265 Mio. EUR. Die Aufsichtsbehörde sah es als erwiesen an, dass Facebook nicht sorgsam mit den Daten seiner Kunden umgegangen ist. Facebook hätte das sog. Scraping (= Extrahieren, Kopieren, Speichern und Verwenden fremder Inhalte online) und den Abruf von Millionen Kundendaten und Handynummern verhindern können.

... Facebook hat aber Sorgfalt bei Kundendaten vernachlässigt

PRAXISTIPP | Wenn Sie ein Facebook-Konto haben, sollten Sie überprüfen, ob auch Sie von diesem Datenleck betroffen sind. Auf einer Website von WBS.LEGAL unter iww.de/s7406 können Sie Ihre Telefonnummer eingeben und diese überprüfen lassen.

Eigene Telefonnummer überprüfen

MERKE | Die EU-Kommission hat am 13.12.22 den ersten Entwurf für einen „Angemessenheitsbeschluss“ für die USA veröffentlicht (iww.de/s7409). Dieser könnte im Laufe des Jahres 2023 in Kraft treten. Damit sollen sichere transatlantische Datenströme gefördert und die Bedenken des EuGH im „Schrems II“-Urteil ausgeräumt werden.

5. Auch Microsoft (Office) 365 birgt Datenschutz-Gefahren

DSK-Urteil: Microsoft-Terms bleiben Datenschutznachweis schuldig

Ende November 2022 veröffentlichte die extra für Microsoft-Onlinedienste eingesetzte Arbeitsgruppe der Datenschutzkonferenz (DSK) ihre Ergebnisse zu Untersuchungen beim Einsatz des Cloud-Dienstes Microsoft Office 365 (jetzt: Microsoft 365). In 14 mehrstündigen Terminen zwischen der DSK-Arbeitsgruppe und Microsoft-Vertretern waren ausschließlich die Vertragsinhalte der Microsoft-Terms (speziell das Microsoft Products and Services Data Protection Addendum [DPA], vgl. iww.de/s7408) geprüft worden. Die DSK stellte *„unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrags vom 15. September 2022‘ nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“*

Zeitgleich veröffentlichte Microsoft unter dem Titel „Microsoft erfüllt und übertrifft europäische Datenschutzgesetze“ eine Gegendarstellung. Damit liegen jetzt zwei unterschiedliche Sichtweisen zum datenschutzkonformen Einsatz von Microsoft 365 auf dem Tisch.

Behörden prüfen jetzt Datenschutz beim Einsatz von Microsoft 365

Bisher gibt es kaum Kontrollen der Aufsichtsbehörden in Bezug auf Microsoft 365. Auch in der Bußgeld-Datenbank (vgl. unter iww.de/s7410) wird bezüglich Microsoft 365 kein Treffer angezeigt. Aber die ersten Aufsichtsbehörden rühren sich. Laut Mitteilung des LfDI Baden-Württemberg soll ein neuer Fokus auf besonders sensible Daten im öffentlichen Dienst sowie auf die Sozialverwaltung gelegt werden. Und die Aufsichtsbehörde in Thüringen plant eine Untersuchung dazu, wie stark Microsoft 365 in der Unternehmerschaft verbreitet ist. Letztlich muss abgewartet werden, wie sich die Aufsichtsbehörden positionieren.

Nicht ohne Ihren DSB oder Ihren Anwalt!

PRAXISTIPP | Auch Kanzleiinhaber sollten ihre Risiken zum Gebrauch von Microsoft 365 mit der Unterstützung ihrer Datenschutzbeauftragten Anfang des Jahres 2023 analysieren. Da ein Nachweis der Datenschutzkonformität von Microsoft-365-Diensten allein mittels Microsoft-Terms laut DSK nicht erbracht werden kann, muss dieser händisch erfolgen. Es gilt, die bestehenden Risiken in einer Risikoanalyse abzuwägen. Sollte Ihnen die Aufsichtsbehörde einen Fragenkatalog zukommen lassen, sollten Sie diesen nur unter Hinzuziehung eines Datenschutzbeauftragten (DSB) oder eines Datenschutzrechtlers beantworten. Denn in der Regel sind die Fragen sehr genau aufeinander abgestimmt – Fehler sind so quasi vorprogrammiert.