



**Inhaltsverzeichnis** ++ Google Fonts und Schadensersatz ++ Compliance in KMU ++ Verschlüsselung durch Ransomware: Was tun? ++ Termine: UIMC vor Ort ++ Webinar-Angebote ++ **Inhaltsverzeichnis**



## Urteil sorgt für Verunsicherung und lockt „Abmahnindustrie“ Nutzung von Google Fonts datenschutzrechtlich bedenklich

Es wurde zu Google Fonts ein Urteil verkündet, das für erhebliche Aufmerksamkeit sorgt und inzwischen auch die sogenannte „Abmahnindustrie“ auf den Plan gerufen hat. „Daten und Fakten helfen auch bei diesem Thema weiter. Die genaue Betrachtung des Urteils lohnt, denn sie helfen beim richtigen Umgang.

Über Google Fonts werden vom US-amerikanischen Konzern Google weit über 1000 Schriftarten in Form von freien Lizenzen zur Verfügung gestellt. Gerade Webseitenbetreiber greifen gerne auf dieses Tool zurück. Es ist frei von Lizenzgebühren und das ist ein gewichtiges Argument. Ein vorhandener Nachteil, der in der Vergangenheit ausgeblendet und verdrängt wurde, ist die Serververbindung zu Google LLC in den USA. Von dort werden Schriften nachgeladen. Zumindest besteht dieser Nachteil dann, wenn die Schriften online eingebunden und nicht zuvor heruntergeladen und auf dem eigenen Webserver bereitgestellt werden. Fakt ist: Die IP-Adresse des Webseitennutzers wird an Google in die USA übertragen. Die USA sind bekanntlich kein EU-Land, sondern werden in Sachen Datenschutz als unsicherer Drittstaat betrachtet.

Nun hat das Landgericht München die Online-Nutzung von Google Fonts verboten. Begründung: Personenbezogene Daten werden unerlaubt an Google in die USA weitergegeben. Durch die Weitergabe der IP-Adresse des Webseitenbesuchers verletzte der Seitenbetreiber nach Auffassung der Richter das Recht des Klägers auf informelle Selbstbestimmung. Eine Rechtsgrundlage oder eine Einverständniserklärung habe es nicht gegeben. Folge: Dem Webseitenutzer wurde ein Schadensersatzanspruch in Höhe von 100 Euro zugesprochen.

Das Urteil rief die „Abmahnindustrie“ auf den Plan (Randbemerkung: Auch wenn es formal gesehen keine Abmahnungen sind, sondern eher Schadensersatzforderungen, wird in der Öffentlichkeit in der Regel von „Abmahnungen“ gesprochen.) Seitdem sind hunderte von solchen Schreiben bei Unternehmen und Webseiten-Betreibern eingegangen. Mal mit der Aufforderung 100 Euro zu bezahlen, weil eine Verletzung der Persönlichkeitsrechte vorliege und ein erhebliches „Unwohlsein“ bestehe. Ein anderes Mal beinhaltet das Schreiben gleich eine zu zahlende Summe von 500 Euro. Schließlich sollen gleich noch die Anwaltskosten übernommen werden.

Was ist nach Erhalt eines solchen Schreibens zu tun? „In jedem Fall nicht zahlen, sondern am besten zeitnah Fachwissen hinzuziehen, um zu schauen, welche juristischen und datenschutzrechtlichen Einfallstore die Abmahnung bzw. Schadensersatzforderung bietet“, beschreibt Dr. Jörn Voßbein. Tatsächlich ist eine Reihe von potenziellen Einwendungen denkbar. Einiges deutet daraufhin, dass die Schreiben rechtsmissbräuchlich sind, da die Webseiten-Nutzer die Homepage vorsätzlich besucht haben. Außerdem bleibt es fraglich, ob die juristisch bereits viel diskutierte Münchener Landgerichts-Entscheidung auch von anderen Gerichten in vergleichbaren Fällen übernommen wird. Experten gehen eher nicht davon aus.

„So oder so sollte ein Webseiten-Betreiber auf Google Fonts verzichten oder zumindest die Fonts lokal in die Webseite einbinden. Auch sollte die eigene Webseite einmal rechtlich geprüft werden,“ rät Dr. Voßbein, „schließlich lauern bei Tracking, embedded content durch Youtube-Videos oder Google Maps und anderen Techniken viele Fallen auf die Betreiber.“ Diese sind einfach zu beheben, wenn man sie denn kennt.

**Mehr Informationen** unter [www.uimc.de/news](http://www.uimc.de/news)



## kostenfreies web.eCollege-Seminar: Compliance in KMU

Nicht nur in KMU sind viele externe Anforderungen zu beachten, doch sollten diese besonders pragmatisch umgesetzt werden. Wir informieren Sie über die wichtigsten Vorgaben und empfehlenswerten Lösungsansätzen. Und natürlich UIMC-typisch aufbereitet: Praxisnah, lösungsorientiert und vor allem: verständlich. 14.09.2022 / 14 Uhr

[www.uimc.de/webecollege](http://www.uimc.de/webecollege)



Datenschutz



Informationssicherheit



Organisation / Strategie

**UIMC** | nachhaltig.gut.beraten.

UIMC DR. VOSSBEIN GMBH & CO KG, Otto-Hausmann-Ring 113, 42115 Wuppertal  
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: [consultants@uimc.de](mailto:consultants@uimc.de), Internet: [www.UIMC.de](http://www.UIMC.de)



## **Verschlüsselung durch Ransomware: Was tun?**

Bei Cyberangriffen werden immer wieder durch sog. „Ransomware“ die Daten/Systeme von Unternehmen so verschlüsselt, dass diese erst nach Zahlung einer bisweilen hohen Summe an die Erpresser wieder lauffähig sind.

### **Wie kann man solchen Attacken vorbeugen?**

Tatsächlich können Unternehmen schon heute viel für die Datensicherheit tun und somit Prävention gegen Cyber-Kriminalität leisten. Der Aufbau eines Informationssicherheits-Managements ist ein wichtiger Baustein zu einer deutlich verbesserten IT-Sicherheit im Unternehmen.

Dieses Vorgehensmodell kann sich an den gängigen Normen zum Informationssicherheits-Managementsystem (ISO/IEC 27001 und 27002) orientieren und ist seit Jahren aufgrund seiner Praktikabilität anerkannt.

Im Ergebnis entsteht ein Managementsystem, durch das sichergestellt werden kann, dass die Informationssicherheit im Unternehmen gelebt wird,

dass sie auf die Bedürfnisse des Unternehmens angepasst ist und dass alle wichtigen Aspekte erfasst werden.

**Was kann ich als Sofortmaßnahme tun?** Ein in letzter Zeit immer wichtiger werdender Bereich ist die Schulung und Sensibilisierung der eigenen Belegschaft für das Thema IT-Sicherheit und der richtige Umgang mit ihr. Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn die Mitarbeiter die Hintergründe verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig“/unsinnig empfunden werden, oder es wird unbewusst aus mangelndem Wissen gegen Vorgaben verstoßen.

**Gesamter Artikel** unter [www.uimc.de/news](http://www.uimc.de/news)

### **UIMC vor Ort:**

08.09.2022: IT-Sicherheitstag Mittelstand | Berlin

28./29.09.2022: Fachmesse Krankenhaus  
Technologie | Gelsenkirchen

25.-27.10.2022: it'sa | Nürnberg

06.12.2022: IT-Sicherheitstag NRW | Siegen

**Wir freuen uns auf Ihren Besuch!**

**Sie haben das letzte web.eCollege verpasst**, würden aber gerne noch mehr zum den vergangenen Themen erfahren? Dann schauen Sie sich die Unterlagen und/oder die Aufzeichnung an:

<http://update.uimcollege.de>

*Sie können sich als Gast anmelden. Hierzu geben Sie bitte den Code ein, den Sie bei uns erfragen können.*

*Sofern Sie als Kunde bereits Zugangsdaten für einen anderen Kurs im eCollege haben, können Sie sich auch „selbst einschreiben“. Die Einschreibung bleibt einen Monat bestehen.*

 **web.eCollege**  
kompakt praxisnah informieren

### **Die nächsten Termine [kostenfrei]**

14.09.2022: Compliance in KMU: Datenschutz,  
Informationssicherheit u. ä.

12.10.2022: 7 nützliche Tipps für eine Lieferant-  
bewertung / Dienstleister-Auditierung

09.11.2022: [Basics] Know What, Know How: Die  
10 wichtigsten Maßnahmen im Datenschutz

**Anmeldung unter [www.uimc.de/webecollege](http://www.uimc.de/webecollege)**



### **Aktuelles im Online-Formular-Center**

[neu] Neue Praxishilfe: Ablauf eines Outsourcing-Prozesses

**Um über Neuerungen zeitnah informiert zu werden**, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.



[www.uimcollege.de](http://www.uimcollege.de)

**Mehr Informationen, Hinweise & Tipps finden Sie hier: <https://www.UIMC.de/communication>**

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an [communication@uimc.de](mailto:communication@uimc.de) widersprechen.

