

## Datenschutz-Newsletter II / 2022

### Aktuelles rund um den Datenschutz

#### Vorsicht bei Google Fonts

Bindet ein Verantwortlicher Google Fonts dynamisch in seine Website ein, sodass bei jedem Aufruf durch einen Nutzer eine Verbindung zu den Google Servern aufgebaut wird und die Schriftart von diesem geladen wird, ist zu bedenken, dass die IP-Adresse des Nutzers, also personenbezogene Daten, an Google weitergeleitet werden.

Das Landgericht München hat in diesem Zusammenhang in seinem Urteil vom 20. Januar 2022, 3 O 17493/20, entschieden, dass eine solche Weiterleitung datenschutzwidrig ist, sofern sie nicht auf einer Einwilligung beruht. Die Verarbeitung könne ausdrücklich nicht auf berechtigte Interessen des Verantwortlichen gestützt werden, da Google Fonts auch genutzt werden kann, ohne dass beim Aufruf der Website eine Verbindung zu einem Google Server hergestellt wird und eine Übertragung der IP-Adresse der Nutzer an Google stattfindet. Auch trete durch die Übermittlung an einen Server von Google in den USA ein Kontrollverlust ein. Ein angemessenes Datenschutzniveau könne nicht gewährleistet werden. Da eine Einwilligung im vorliegenden Fall unstreitig nicht eingeholt wurde und durch die Übermittlung der IP-Adressen das vom Nutzer empfundene Unwohlsein erheblich sei, wurde der Verantwortliche zu Schadensersatz und Unterlassen verurteilt.

Fazit: eine Verbindung zu Servern Dritter sollte ohne Einwilligung vermieden werden. Die Einbettung von Inhalten Dritter sehen Aufsichtsbehörden und Gerichte zunehmend kritisch.

Sollte sich der Verantwortliche dafür entscheiden, die Schriftarten auf einen eigenen Server zu laden, wird die Google Datei lediglich lokal in die Website eingebunden. Dies ist nach Ansicht des Gerichts datenschutzrechtlich nicht zu beanstanden. Andernfalls muss durch einen Cookie-Banner eine wirksame Einwilligung eingeholt werden.

#### Trans-Atlantic Data Privacy Framework

EU-Kommissionspräsidentin Ursula von der Leyen und US-Präsident Joe Biden haben verkündet, dass es eine grundlegende Übereinkunft für ein neues Abkommen über den sicheren Datentransfer zwischen der EU und den USA gebe.

Man einigte sich darauf, den grenzüberschreitenden Datenverkehr neu zu regeln, indem man EU-Bürgern mehr Rechte einräumt und es US-Geheimdiensten nicht mehr ganz so einfach macht, mit Daten von EU-Bürgern zu arbeiten. Das Ganze soll wieder in Form eines Abkommens geschehen, dem „Trans-Atlantic Data Privacy Framework.“ Beide Seiten haben Factsheets veröffentlicht, die die gemeinsamen Absichten

zur Sicherung der transatlantischen Datenflüsse stichpunktartig beschreiben:

- Es soll ein neues Regelwerk und verbindliche Garantien geben, um Zugriffsrechte der US-Sicherheitsbehörden auf personenbezogene Daten auf ein zum Schutz der nationalen Sicherheit erforderliches Maß zu begrenzen.
- Zudem soll ein neues zweistufiges Rechtsbehelfssystem zur Untersuchung von Beschwerden von EU-Bürgern über den Zugang zu Daten durch US-Nachrichtendienste eingeführt werden.
- Es soll strenge Verpflichtungen für US-Unternehmen geben, die aus der EU übermittelte Daten verarbeiten, einschließlich der Verpflichtung, ihre Einhaltung der Grundsätze durch das US-Handelsministerium selbst zu zertifizieren.
- Es sollen spezifische Überwachungs- und Überprüfungsmechanismen eingeführt werden.

Ob nach diesen Ankündigungen tatsächlich eine gemeinsame Lösung gefunden werden kann, bleibt abzuwarten.

### **Phishing-Angriffe auf E-Mail-Konten**

Dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) werden häufig erfolgreiche Angriffe auf E-Mail-Accounts bayerischer Unternehmen gemeldet. Das BayLDA hat daher im Mai 2022 nach Stichprobenprüfungen eine weitere Präventionsprüfung eingeleitet, um Verantwortliche zu sensibilisieren und Hilfestellungen zum Schutz gegen diese Form von Cyberkriminalität aufzuzeigen.

Die wichtigste Maßnahme zum aktiven Schutz vor solchen Cyberattacken stellt die Sensibilisierung des eigenen Personals dar.

Die Stabsstelle Prüfverfahren des BayLDA hat sich daher aufgrund der akuten Bedrohungslage im Cyberraum entschieden, die Absicherung von E-Mail-Accounts großflächig in Bayern zu kontrollieren. Im Rahmen der Präventionsprüfung werden grundlegende Sicherheitsmaßnahmen bei den geprüften Betrieben abgefragt. Dabei werden ihnen wie auch den unbeteiligten Unternehmen in Bayern Informationsmaterialien bereitgestellt, die eine eigenverantwortliche Kontrolle eines Sicherheitskonzepts erleichtern, etwa eine Checkliste zu den wichtigsten Handlungsfeldern, zum Beispiel Phishing-Awareness, Sicherheitsbewusstsein und Passwörter und vieles mehr. Die Informationsmaterialien können über die Homepage des BayLDA, [https://www.lida.bayern.de/de/kontrollen\\_stabsstelle.html](https://www.lida.bayern.de/de/kontrollen_stabsstelle.html), eingesehen werden.

Es ist Verantwortlichen zu raten, die dort abgefragten Punkte zu überprüfen und gegebenenfalls Verbesserungen vorzunehmen.

### **Stand: 24. Juni 2022**

Alle Beiträge sind nach bestem Wissen zusammengestellt. Eine Haftung für deren Inhalt kann jedoch nicht übernommen werden. Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

Thomas Hesz, RA/StB; Marcel Peetz (M.Acc.), WP/StB;  
Maria Gayer, RAin; Stefan Gräbe  
Zertifizierte Datenschutzbeauftragte (TÜV)  
Telefon: 09221 / 900 - 0  
[edsb@frtconsult.de](mailto:edsb@frtconsult.de) [www.frtpartner.de](http://www.frtpartner.de)