

## Datenschutz-Newsletter 2023 / III

Telefon: 09221 / 900 - 0  
Telefax: 09221 / 900 - 111  
Kontakt: edsb@frtconsult.de  
Adresse: Kurt-Schumacher-Str. 23  
95326 Kulmbach

### Aktuelles rund um den Datenschutz

#### Datenschutzrahmen EU-US

Unter anderem in unserem Newsletter 2020 / III berichteten wir, dass das EU-US Privacy Shield vom EuGH im Juli 2020 für unwirksam erklärt wurde. Dies hatte zur Folge, dass ein Transfer von personenbezogenen Daten in die USA mit erheblichen Risiken und Unsicherheiten verbunden war.

Die Europäische Kommission hat nun im Juli 2023 in einem Angemessenheitsbeschluss festgelegt, dass die USA ein angemessenes Schutzniveau für die personenbezogenen Daten gewährleisten, die innerhalb des neuen Datenrahmens EU-US (EU-US Data Privacy Framework) übermittelt werden. Dieser sieht unter anderem vor, dass der Zugang von US-Nachrichtendiensten zu EU-Daten auf ein notwendiges und verhältnismäßiges Maß beschränkt ist und ein Rechtsbehelfsverfahren zur Datenschutzüberprüfung geschaffen wird. Ein Gericht kann bei Verstößen die Löschung der Daten anordnen. Unternehmen in den USA können sich dem Datenschutzrahmen EU-US anschließen, sofern sie sich zur Einhaltung verschiedener Datenschutzpflichten verpflichten, vgl. <https://www.dataprivacyframework.gov/s/participant-search>.

Rechtsfolge des Angemessenheitsbeschlusses ist, dass personenbezogene Daten innerhalb des Datenrahmens EU-US

ohne weitere Schutzmaßnahmen in die USA übermittelt werden können.

Die Präsidentin der Europäischen Kommission Ursula von der Leyen betonte, dass der neue Datenschutzrahmen EU-US einen sicheren Datenverkehr gewährleiste und Unternehmen Rechtssicherheit biete. Dies muss zumindest bezweifelt werden. Organisationen wie die von Max Schrems, Hauptkläger im oben genannten EuGH-Urteil, haben bereits angekündigt, gegen den Datenrahmen EU-US klagen zu wollen.

#### Auskunftsanspruch: Recht auf Kopie

Immer wieder erreichen uns Fragen zum Umfang des Auskunftsanspruchs. Konkret geht es hier oft um die Frage, ob sämtliche Dokumente, die personenbezogene Daten des Betroffenen enthalten, in Kopie zur Verfügung gestellt werden müssen. Im jüngst veröffentlichten Tätigkeitsbericht 2022 hat das Bayerische Landesamt für Datenschutzaufsicht dazu Stellung genommen:

Gemäß Art. 15 Abs. 3 DSGVO ist der Verantwortliche verpflichtet, eine „Kopie der personenbezogenen Daten“, die Gegenstand der Verarbeitung sind“, zur Verfügung zu stellen. Dies bedeute aber gerade nicht, dass sämtliche Originaldokumente kopiert und ausgehändigt werden müssten. Vielmehr genüge es, alleine die personenbezogenen

Daten, die in dem entsprechenden Schriftstück enthalten sind, zu beauskunften. Die Aufsichtsbehörde stützt sich hier auch auf das Urteil des EuGHs vom 04. Mai 2023, C-487/21, das dieselbe Rechtsauffassung vertritt.

### **OLG Karlsruhe: Sicherheitsmaßnahmen beim Versand von E-Mails im geschäftlichen Verkehr**

In einem Fall überwies ein Käufer Geld auf ein falsches Konto, das aus einer Fake-E-Mail stammte. Der Verkäufer klagte das ausstehende Geld ein.

Das OLG Karlsruhe entschied mit Urteil vom 27. Juli 2023, 19 U 83/22 zugunsten des Verkäufers, da dieser keine Pflichten in Bezug auf den Schutz seines E-Mail-Kontos verletzt habe.

Es gibt gemäß dem Urteil keine konkreten gesetzlichen Vorgaben, welche Sicherheitsvorkehrungen beim Versand von E-Mails im geschäftlichen Verkehr einzuhalten sind. Auch stellte das Gericht fest, dass die DSGVO nicht anwendbar ist, weil keine personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO verarbeitet wurden. Daher konnte auch die „Orientierungshilfe des Arbeitskreises Technische und organisatorische Datenschutzfragen“ nicht herangezogen werden.

Die berechtigten Sicherheitserwartungen im geschäftlichen Verkehr hat der Verkäufer erfüllt: Die Feststellungen des Gerichts zur Art des von dem Verkäufer verwendeten Passwortes für das E-Mail-Konto und deren regelmäßige Änderung, sowie zur Nutzung von Firewall und Virensoftware sprechen gegen eine Pflichtverletzung.

Die vom Käufer weiter angeführten Sicherheitsmaßnahmen waren im

geschäftlichen E-Mail-Verkehr nicht erwartbar gewesen. Der Käufer argumentierte, dass der Verkäufer zur Nutzung des Sender Policy Frameworks (SPF) verpflichtet gewesen sei. SPF ist ein Verfahren mit dem geprüft wird, ob der sendende E-Mail-Server berechtigt ist, für die Domäne E-Mails zu versenden. Endnutzer, wie der Verkäufer, die selbst keinen E-Mail-Server betreiben, haben auf die Verwendung jedoch keinen Einfluss, so dass dahingehend auch keine Sicherheitserwartung des Käufers bestehen kann. Auch die vorgebrachte Ende-zu-Ende Verschlüsselung ist im geschäftlichen Verkehr nicht erwartbar. Zwar wird diese vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen, gleichzeitig ist dem BSI bewusst, dass sie nur selten eingesetzt wird, was ebenfalls einer allgemeinen Sicherheitserwartung entgegensteht. Die Transportverschlüsselung „Transport Layer Security“ (TLS) gibt es nur im Verkehr zwischen bestimmten E-Mail-Anbietern. Da zwar der vom Verkäufer genutzte Anbieter, nicht aber der vom Käufer einem TLS nutzenden E-Mail-Anbieter angehört, ist die gescheiterte Transportverschlüsselung nicht dem Verkäufer anzulasten.

### **Stand: 15. September 2023**

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/FBISTr; Maria Gayer, RAin; Stefan Gräbe  
Zertifizierte Datenschutzbeauftragte (TÜV)  
Homepage: [www.frtpartner.de](http://www.frtpartner.de)