FRT CONSULT GMBH
IT Dienstleistungen & Business Dienstleistungen

frtpartner

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

Datenschutz-Newsletter 2025 / I

Aktuelles rund um den Datenschutz

Data Privacy Framework wieder unter Prüfung

Im Juli 2023 trat das Data Privacy Framework (DPF) basierend auf einer Executive Order von US-Präsident Joe Biden in Kraft, um den EU-US-Datentransfer zu erleichtern. Ende Januar 2025 forderte die neue Trump-Administration demokratische Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) zum Rücktritt auf. Das PCLOB ist zentral für die Überwachung behördlicher Praktiken und den Schutz der Privatsphäre im Rahmen des DPF zuständig. Diese Entwicklung könnte die Stabilität des DPF gefährden. Das EU-Parlament hat die EU-Kommission aufgefordert, die Tragfähigkeit des DPF unter diesen Umständen zu prüfen. Mögliche Klärungswege umfassen Stellungnahmen nationaler und europäischer Aufsichtsbehörden sowie gerichtliche Überprüfungen durch nationale Gerichte oder direkt beim Europäischen Gerichtshof. Die Zukunft des Data Privacy Frameworks ist daher ungewiss. Politische Eingriffe in die Datenschutzaufsicht der USA könnten dazu führen, dass das DPF bald erneut rechtlich angefochten wird. Insofern sollten aufgrund dieser Unsicherheit Unternehmen ihre Datenübertragungen in die USA weiterhin überprüfen und ggf. zusätzliche Schutzmaßnahmen wie Standardvertragsklauseln implementieren, um sich gegen rechtliche Risiken abzusichern.

NOYB: Beschwerden gegen TikTok, AliExpress und Co.

Die Datenschutzorganisation noyb hat am 16. Januar 2025 Beschwerden gegen sechs chinesische Unternehmen eingereicht: TikTok, Xiaomi, AliExpress, SHEIN, WeChat und Temu. Der Vorwurf lautet, dass diese Unternehmen personenbezogene Daten europäischer Nutzer unrechtmäßig nach China übertragen, ohne ein angemessenes Datenschutzniveau sicherzustellen. Gemäß DSGVO dürfen Daten nur in Länder außerhalb der EU transferiert werden, wenn dort ein vergleichbares Datenschutzniveau gewährleistet ist oder geeignete Schutzmaßnahmen, wie Standardvertragsklauseln (SCCs), implementiert sind. noyb argumentiert, dass China diese Anforderungen nicht erfüllt und die Unternehmen keine ausreichenden zusätzliche Schutzmaßnahmen ergriffen haben. Zudem haben die betroffenen Unternehmen auf Auskunftsersuchen europäischer Verbraucher nicht oder nur unzureichend reagiert und ihre Datenschutzerklärungen seien intransparent. noyb fordert von den europäischen Datenschutzbehörden, die Datenübertragungen nach China sofort zu stoppen, die Datenverarbeitungspraktiken der Unternehmen zu untersuchen und gegebenenfalls Geldstrafen zu verhängen.

Schwärzung als rechtswidrige Datenverarbeitung?

Gemeinderäte einer sächsischen Gemeinde beschwerten sich bei dem Sächsischen Datenschutz- und Transparenzbeauftragten (SDTB), weil ein Bürgermeister sitzungsrelevante Unterlagen vor der Übergabe teilweise schwärzte. Geschwärzt wurden u. a. Firmendaten, Firmenname und -adresse. Begründet wurde dies mit der Sächs. Gemeindeordnung, wonach personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse bei der Veröffentlichung von Beratungsunterlagen nicht offenbart werden dürfen. Diese Ansicht teilte der SDTB nicht. Den Gemeinderäten können sitzungsrelevante

Unterlagen in ungeschwärzter Form zur Verfügung gestellt werden. Rechtsgrundlage sei Art. 6 Abs. 1 e) DSGVO iVm. SächsGemO: Für die Beratung im Gemeinderat sind erforderlichen Unterlagen zu übergeben, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Der „Informationsbedarf des verständigen Ratsmitglieds“ ist im Rahmen der gewissenhaften ehrenamtlichen Ausübung der Tätigkeit in wichtigen Angelegenheiten der Gemeinde auf dem Laufenden zu halten. Demnach ist eine Schwärzung von sitzungsrelevanten Unterlagen nicht erforderlich. Auch sind die Gemeinderäte als Teil der Verwaltung nach der SächsGemO gesetzlich zur Verschwiegenheit verpflichtet. Unterlagen sind daher entgegen der Auffassung des Bürgermeisters erst bei deren Veröffentlichung in Bezug auf personenbezogene Daten bzw. Betriebs- und Geschäftsgeheimnisse zu bereinigen und nicht bei der Übergabe an die Gemeinderäte. Das Verhalten des Bürgermeisters sei daher ein Verstoß gegen Art. 6 DSGVO in Form einer „unzulässigen Datenminimierung“, da keine Rechtsgrundlage für die Schwärzung gegeben sei. Auch eine Schwärzung bedarf einer Rechtsgrundlage, ebenso wie die Löschung von Daten. Die Schwärzung personenbezogener Daten ist damit nicht immer eine datenschutzkonforme Handlung.

DSGVO-Ansprüche können arbeitsrechtlich verfallen

Eine Arbeitnehmerin forderte ca. fünf Monate nach Ende ihres Arbeitsverhältnisses eine Abgeltung von nicht genommenem Urlaub. Arbeitsvertraglich war eine Ausschlussfrist vereinbart, die eine Geltendmachung von Ansprüchen nur bis drei Monate nach Fälligkeit des Anspruchs vorsah. Dem Gericht nach seien die Ansprüche der Arbeitnehmerin verfallen, da die Abgeltung erst nach Ablauf der Ausschlussfrist geltend gemacht wurde. Das Berufungsgericht LAG Hamburg entschied, dass die Klausel zur Ausschlussfrist zu weit gefasst sei und unzulässigerweise auch Auskunfts- und Schadensersatzansprüche aus der DSGVO erfasse. Eine derartige Verkürzung verstoße gegen den europäischen Äquivalenz- und Effektivitätsgrundsatz, beide seien nach ständiger Rechtsprechung des EuGH zu beachten. Vertragliche Ausschlussfristen beschränken sich jedoch auf die Regelung des Fortbestands bereits entstandener Ansprüche und führen keine zusätzlichen Voraussetzungen für deren Entstehung ein. Demnach sind sie mit dem Äquivalenzgrundsatz vereinbar, da nicht zwischen Ansprüchen aus Unionsrecht und innerstaatlichem Recht unterschieden wird. Der Effektivitätsgrundsatz sei ebenfalls eingehalten, da die Ausschlussfristen der Rechtssicherheit dienen und die Ausübung unionsrechtlicher Ansprüche weder unverhältnismäßig noch praktisch unmöglich machen. Damit stellt das Urteil klar, dass auch Ansprüche aus der DSGVO nach bestimmten Fristen verfallen können, nicht jedoch ein pauschaler Ausschluss von Ansprüchen nach einer starren Frist.

Die neue Einwilligungsverwaltungsverordnung – Was nun mit dem Consent-Banner?

Auf Basis von § 26 Abs. 2 TDDDG wurde die Einwilligungsverwaltungsverordnung (EinwV) erlassen. Ein rechtlicher Rahmen für ein alternatives Verfahren zur Verwaltung von Nutzereinwilligungen. Die Verordnung wird voraussichtlich am 1. April 2025 in Kraft treten. Beim Besuch von Webseiten werden Nutzer mit zahlreichen Einwilligungsbannern konfrontiert. Mit der EinwV soll eine nutzerfreundliche und rechtssichere Alternative zu Consent-Bannern geschaffen werden und mehr Kontrolle über die erteilten und nicht erteilten Einwilligungen gem. § 25 Abs. 1 TDDDG gegenüber Anbietern von digitalen Diensten verschaffen. Die Entscheidungen zu den Einwilligungen sollen dabei dauerhaft gespeichert und verwaltet werden und bei Bedarf an die Anbieter digitaler Dienste übermittelt werden können. Im Idealfall muss der Nutzer nur einmal seine Bereitschaft zu einwilligungsbedürftigen Trackings erklären. Weitere Einwilligungsabfragen würden vermieden. Derartige Dienste zur Einwilligungsverwaltung können sich durch einen elektronischen Antrag bei der Bundesbeauftragten für Datenschutz und Informationssicherheit (BfDI) anerkennen lassen. Anerkannte Dienste zur Einwilligungsverwaltung werden dann zukünftig in einem öffentlichen Register von der BfDI geführt.

Bereits in 2023 kritisierte u. a. die Datenschutzkonferenz (DSK) den Referentenentwurf der EinwV des Bundesministeriums für Digitales und Verkehr (BMDV) und erklärte, dass das Ziel der Einwilligungsverwaltungs-

verordnung nicht erreicht werden könne. Es bleibt abzuwarten, ob und wie viele Dienste zur Einwilligungsverwaltung sich von der BfDI anerkennen lassen. Die Freiwilligkeit der Einbindung solcher Dienste würde nur dazu führen, dass Anbieter digitaler Dienste weiterhin auf herkömmliche Consent-Banner setzen. Jedoch bieten anerkannte Einwilligungsdienste grundsätzlich eine Möglichkeit, dass Nutzer eine informierte und selbstbestimmte Entscheidung hinsichtlich ihrer Einwilligung nach § 25 Abs. 1 TDDDG treffen. Die Flut an Consent-Bannern im Internet könnte damit reduziert werden.

Manipulierte Rechnungen – Augen auf!

Das Manipulieren von Rechnungen nimmt weiter zu. Am 08.11.2023 um 14:14 Uhr versandte ein Handwerksbetrieb eine E-Mail mit einer PDF-Datei, die eine Abschlagsrechnung und die korrekte Bankverbindung enthielt. Um 14:35 Uhr erhielt der Kunde eine fast identische E-Mail mit einer gefälschten PDF-Datei, die eine abweichende Bankverbindung auswies. Die PDF-Datei war optisch nahezu identisch (abgesehen von den Bankverbindungsdaten), die E-Mail erhielt jedoch Hinweise auf eine fehlerhafte HTML-Formatierung. Der Kunde gab an, nur die manipulierte E-Mail erhalten zu haben. Der Handwerksbetrieb habe durch mangelnde IT-Sicherheit die Ursache für die Fälschung gesetzt. Das LG Rostock verurteilte den Kunden mit Urteil vom 20.11.2024 zur erneuten Zahlung. Die Überweisung auf die falsche Bankverbindung führte nicht zur Begleichung der Schuld. Der Handwerksbetrieb habe auch nicht schuldhaft verursacht, dass der Kunde auf das falsche Konto zahlte. Das Gericht stellte auf vertragliche Schutzpflichten ab: Beide Parteien hatten sich auf E-Mail-Kommunikation geeinigt, trotz der allgemein bekannten Unsicherheiten. Feste Sicherheitsvorgaben für den E-Mail-Verkehr gibt es nicht. Es war auch unklar, ob der Handwerksbetrieb seine Systeme durch ein höheres Sicherheitsniveau besser absichern und Angriffe verhindern hätte können. Zudem ergibt sich auch aus der DSGVO keine Pflichtverletzung, da sie nur den Schutz personenbezogener Daten betrifft. Hingegen wurde ein erhebliches Verschulden des Kunden festgestellt. Er ignorierte deutliche Hinweise auf eine Manipulation der E-Mail mit auffälligen Zeichenfehlern, wie die Umlaute in der E-Mail als „Ü“ für „Ü“ oder „ “ für ein „geschütztes Leerzeichen“. Auch hätte dem Kunden die veränderte Bankverbindung gegenüber früheren Zahlungen auffallen können. Alles Anzeichen für eine bessere Überprüfung der Kontodaten durch den Kunden.

Wer angreifbare Kommunikationsmittel nutzt, muss auch erhöhte Aufmerksamkeiten an den Tag legen und mit etwaigen Folgen auskommen. Es ist allgemein bekannt, dass E-Mails mit Postkarten verglichen werden und mit technischem Know-how einfach gelesen werden können. Manipulationen gehen Angriffen auf Mail-Systeme voraus. Unternehmen sollten ihre Systeme sorgfältig und laufend überwachen. Webmailer sollten vermieden werden. Bei Fehleranzeichen ist eine sofortige und umfassende Warnung und Information des Partners zwingend. Andererseits sollten Rechnungsmails kritisch geprüft werden, insbesondere je höher der Rechnungsbetrag ist.

Stand: 28. März 2025

Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

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