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 / IV

## Aktuelles rund um den Datenschutz

### Irish High Court stoppt vorläufig Maßnahmen gegen TikTok

TikTok hatte nach der Entscheidung der irischen Datenschutzbehörde (DPC) vom April 2025 nachzuweisen, dass in China ein dem EU-Niveau gleichwertiger Schutz für die dorthin fließenden Daten gewährleistet werden könne. Da TikTok gegen diese Entscheidung Berufung hatte, hat der Irish High Court im November 2025 die Maßnahmen der DPC gestoppt. Damit sind das Verbot der Datenübermittlung aus dem europäischen Wirtschaftsraum (EWR) nach China sowie das Bußgeld in Höhe von 530 Millionen Euro bis zum Abschluss des Hauptverfahrens ausgesetzt.

### LinkedIn verwendet Nutzerdaten zum KI-Training

LinkedIn nutzt seit November 2025 europäische Nutzerdaten zum Training seiner KI, um Dienste wie die Jobsuche zu optimieren. Das Unternehmen stützt sich dabei rechtlich auf das „berechtigte Interesse“ (Art. 6 I f) DSGVO). Diese Praxis wurde bereits von Konzernen wie Meta erfolgreich gerichtlich genutzt. Nutzer können dieser Verarbeitung in den Kontoeinstellungen unter „Datenschutz“ durch Deaktivieren der Option „Daten zur Verbesserung generativer KI“ widersprechen. Diese Nutzungsuntersagung gilt jedoch nur für die Zukunft. Was bereits an Daten in die KI-Modelle eingeflossen ist, wird nachträglich nicht mehr entfernt.

### Datenschutz im Alltag

Datenschutz gilt oft als praxisfern. Dennoch sichert Datenschutz auch im Alltag beim Einkaufen neben dem Komfort auch Kontrolle. Kundenkarten, mobile Bezahlvorgänge, Rabattaktionen und Online-Bestellungen hinterlassen massive Datenspuren. Das Datenschutzrecht dient hier als notwendiger Schutzschild für die Privatsphäre der Verbraucher.

Dabei garantiert das datenschutzrechtliche Prinzip der **Zweckbindung**, dass Daten nur für die Abwicklung des Kaufs genutzt und nicht ohne Einwilligung an Dritte weitergegeben werden. Ohne diesen Schutz könnten private Informationen über das Konsumverhalten an Versicherungen oder Banken verkauft werden.

Zudem verpflichtet das Prinzip der **Datenminimierung** Unternehmen dazu, nur die absolut notwendigen Informationen zu erheben. Die Erstellung von detaillierten Bewegungs- und Verhaltensprofilen aus Bezahlvorgängen wird damit verhindert. Die persönlichen Lebensgewohnheiten bleiben so privat und ein Missbrauch dieser Daten durch globale Analysekonzerne wird verboten.

Aufgrund des Datenschutzes sind Händler verpflichtet aufzudecken, welche Informationen sie sammeln und was sie damit vorhaben (**Transparenzpflichten**). Dies sichert die Freiheit der eigenen Entscheidung für den Rabatt oder die Anonymisierung.

Ohne Datenschutzrecht ließen sich für Supermärkte und Onlineshops aus den Einkaufsdaten, wie Gegenstand, Preis, Marke, Ort, Zeit, Standort oder der Zahlungsart ein genaues Personenprofil erstellen. Eine psychologische Manipulation würde durch zugeschnittene Produktempfehlungen oder Rabattaktionen möglich, die nicht auf Angebot und Nachfrage beruht, sondern auf den Schwächen und der Lebenssituation der Betroffenen. Preisanpassungen könnten auch anhand von technischen Merkmalen erfolgen (Bestellung über teures oder günstiges

Endgerät), der Bestellzeit oder auf Grundlage des bisherigen Kaufverhaltens, um Preise künstlich zu erhöhen (**Dynamic Pricing**) oder Rabatte oder Angebote bewusst zu verweigern. Diese Methoden sind grundsätzlich verboten. Erlaubt werden diese Methoden bei ausdrücklicher Einwilligung, z.B. durch das Bestätigen von Tracking Cookies im Banner einer Website.

Um den Schutz der persönlichen Daten zu wahren, sollte beim Onlinekauf nur das angegeben werden, was für den Kauf unbedingt nötig ist und optionale Daten ausgespart werden. Für personalisierte Werbung und Analyse-Tools sollte die Einwilligung nur erteilt werden, wenn diese auch jederzeit widerrufbar ist und der Zweck nachvollziehbar erscheint.

In den Geräteeinstellungen lässt sich für einzelne Einkaufs- und Liefer-Apps der Datenzugriff (Kontakte, ID, Kamera, Standort etc.) gesondert einstellen. Einer personalisierten Preisgestaltung kann man mit der stetigen Ablehnung von Tracking-Cookies und der regelmäßigen Löschung der Browserdaten ausweichen.

Nur durch Datenschutz ist heute gewährleistet, dass modernes Einkaufen nicht mit einer Durchleuchtung der eigenen Privatsphäre einhergeht. Es bedarf eines bewussten Umgangs mit den eigenen Einwilligungen und der Preisgabe von persönlichen Daten und den sich aus dem Datenschutz ergebenden Rechten. Andernfalls ist man personalisierter Preisgestaltung, algorithmischer Diskriminierung, Profiling und manipulativer Rabatt- und Preisgestaltung unwillkürlich ausgeliefert.

**Microsoft 365: Hessen geht voran**

Die datenschutzrechtliche Situation hinsichtlich Microsoft 365 hat in den letzten Jahren in Deutschland erhebliches Aufsehen erregt und wirft zahlreiche Fragen auf. Im November 2022 äußerte die Datenschutzkonferenz (**DSK**), dass Microsoft 365 nicht datenschutzkonform eingesetzt werden könne. Die DSK begründete diese Einschätzung damit, dass der Microsoft Datenschutznachtrag (englisch: Data Processing Addendum, **DPA**) nicht den Anforderungen der Datenschutzgrundverordnung (**DSGVO**) genüge.

Die DSK führte an, dass der DPA nicht die Mindestanforderungen erfüllt, die für eine rechtmäßige Auftragsverarbeitung nach Artikel 28 der DSGVO erforderlich sind. Unternehmen, die Daten an Dritte (wie Microsoft) übermitteln, müssen hiernach sicherstellen, dass die Dritten angemessene Sicherheitsvorkehrungen und zulässige rechtliche Rahmenbedingungen bieten. Trotz mehrerer Anpassungen des DPA durch Microsoft äußerte sich die DSK nicht erneut und hielt damit an ihrer früheren Bewertung fest. Dies führte bei den Unternehmen zu einer anhaltenden Unsicherheit.

Die Unternehmen, die sich trotzdem für Microsoft 365 entschieden haben, handelten aus Notwendigkeit, Innovation und Hoffnung auf zukünftige Klarheit.

In der Vergangenheit gab es Bestrebungen seitens einiger Datenschutzbehörden, den DPA direkt mit Microsoft nachzuverhandeln und auch unabhängige, datenschutzfreundliche Alternativen anzubieten, wie etwa eine eigene souveräne Cloud. Die Forderung nach einer datenschutzkonformen Nutzung von Microsoft 365 ist in der deutschen Öffentlichkeit und bei verschiedenen Organisationen vorhanden, was zusätzlichen Druck auf die DSK und andere Aufsichtsbehörden ausübt.

Am 14.11.2025 veröffentlichte der Hessische Beauftragte für Datenschutz und Informationsfreiheit (**HBDI**) dann eine Pressemitteilung, in der mehrfach explizit erklärt wurde, dass Microsoft 365 nun datenschutzkonform genutzt werden könne. Diese Entscheidung widerspricht der bisherigen Einschätzung der DSK und deutet darauf hin, dass sich relevante rechtliche Rahmenbedingungen geändert haben könnten. Der HBDI betont allerdings, dass Unternehmen eine vertiefte datenschutzrechtliche Prüfung durchführen sollten, um die Einhaltung der Anforderungen sicherzustellen. Damit wird erstmals ein Schritt in Richtung einer einheitlicheren Behandlung des Themas in Deutschland unternommen, auch wenn die Entscheidung lediglich für Hessen gilt. Eine technische Untersuchung einzelner Microsoft 365 Dienste ist allerdings laut Pressemitteilung nicht erfolgt. Damit lässt sich die Validität dieser datenschutzrechtlichen Einschätzung anzweifeln.

Die Auswirkungen dieser klaren und positiven Einschätzung für die Verwendung von Microsoft 365 in Hessen sind potenziell weitreichend. Unternehmen in der Region können nun erleichtert aufatmen, da das bisher bestehende Risiko eines unzureichenden Datenschutzvertrags verringert wird. Auch andere Bundesländer

könnten sich dadurch ermutigt fühlen, vergleichbare Entscheidungen zu treffen. Damit wird die Diskussion über die rechtliche Grundlage und die Nutzung von Microsoft 365 im gesamten Bundesgebiet neu entfacht. Der Fokus wird in der Folge auf eine einheitliche Regulierung und Position der DSK gelegt.

Ein Ausbleiben einer einheitlichen und klaren Antwort der DSK macht jedoch die rechtliche Lage langfristig für viele Unternehmen unübersichtlich und die rechtliche Bewertung schwer einschätzbar. Eine detaillierte Datenschutzfolgenabschätzung (**DSFA**) bleibt für den Einzelfall erforderlich, wie die datenschutzrechtliche Praxis mit Microsoft 365 zeigt.

**Bußgeld der kroatischen Aufsichtsbehörde**

Der mehrfache Verstoß eines kroatischen Telekommunikationsunternehmens gegen die DSGVO löste für dieses eine Geldstrafe in Höhe von 4,5 Millionen Euro aus, die die kroatische Datenschutzbehörde (AZOP) verhängte.

Gerügt wurde, dass das Unternehmen einen Teil seiner Datenverarbeitung an einen IT-Dienstleister in Serbien ausgelagert hatte. Dieser Dienstleister hatte Zugriff auf ein Customer-Relationship-Management-System (**CRM**), welches 847.862 Datensätze mit personenbezogenen Informationen, darunter Namen, Adressen, Telefonnummern und Bankverbindungen, enthielt. Obwohl Standardvertragsklauseln abgeschlossen wurden, versäumte es das Unternehmen, diese nach dem 27. Dezember 2022 zu erneuern. Des Weiteren informierte der Telekommunikationsanbieter die betroffenen Personen nicht über den Datentransfer in ein Drittland. Zudem stellte sich heraus, dass das Unternehmen Ausweiskopien seiner Mitarbeiter erstellt hatte, ohne sicherzustellen, dass dies erforderlich war. Zusätzlich setzte das Unternehmen einen **Auftragsverarbeiter** im telefonischen Vertrieb ein, ohne die erforderlichen Schutzmaßnahmen des Dienstleisters zu überprüfen.

Die datenschutzrechtliche Bewertung zeigt, dass aufgrund des fehlenden Angemessenheitsbeschlusses der EU-Kommission für Serbien oder anderweitiger Garantien der Abschluss von **Standardvertragsklauseln** notwendig war (Art. 46 II c DSGVO). Diese Klauseln waren jedoch nach dem 27.12.2022 nicht mehr gültig und boten damit keine rechtliche Grundlage für den Datentransfer. Eine an sich erforderliche Risikobewertung für den Datentransfer nach Serbien fehlte. Eine solche Bewertung, welche als „Transfer Impact Assessment“ (**TIA**) bekannt ist, wäre aber erforderlich gewesen, um sicherzustellen, dass im Drittland ein angemessenes Datenschutzniveau garantiert wird.

Das Unternehmen verstieß zudem gegen das Informationsrecht der Nutzer (Art. 13 DSGVO) sowie gegen den **Grundsatz der Datenminimierung** beim Anfertigen von Ausweiskopien.

Der Prozess wurde auch trotz eines hinweisenden Gesprächs mit dem Datenschutzbeauftragten nicht angepasst. Das Unternehmen bleibt bei der Auslagerung der datenschutzrechtlichen Pflichten selbst „**Verantwortlicher**“ der Daten. Damit hat das Unternehmen sicherzustellen, dass der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen (**TOM**) zum Schutz der personenbezogenen Daten trifft. Diese Prüfung wurde nicht vorgenommen, wodurch das Unternehmen seiner Verantwortung nicht nachgekommen ist.

Die kroatische Datenschutzbehörde hatte keine konkreten Gründe für ihre Untersuchung genannt. Es zeigt sich jedoch, dass im Rahmen von Aufsichtsmaßnahmen auch andere Datenschutzverstöße aufgedeckt werden können. Das Ignorieren von Hinweisen des Datenschutzbeauftragten kann, wie hier, schwerwiegende datenschutzrechtliche und wirtschaftliche Folgen haben. Die proaktive Herangehensweise im Datenschutz, sowie eine Unternehmenskultur, die Bewusstsein und Verantwortung fördert, sind von größter Wichtigkeit. Nur so kann langfristige Sicherheit und Compliance gewährleistet werden.

**Stand: 31. Dezember 2025**



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

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