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 2026 / II

Aktuelles rund um den Datenschutz

Datenschutz-Folgenabschätzung: Einheitliche EDSA-Vorlage

Der Europäische Datenschutzausschuss (EDSA) hat am 14. April 2026 eine Vorlage für die einheitliche Durchführung einer Datenschutz-Folgenabschätzung (DSFA) veröffentlicht. Bis zum 9. Juni 2026 befindet sich der Entwurf in der öffentlichen Konsultation.

Ziel dieser Vorlage ist es, die bislang unterschiedlichen Herangehensweisen der Datenschutzaufsichtsbehörden und Unternehmen in den EU-Mitgliedstaaten zu standardisieren und die Durchführung von DSFAs vergleichbarer und nachvollziehbarer zu machen.

Nach Abschluss der Konsultation übernehmen Aufsichtsbehörden die EDSA-Vorlage entweder als Standard oder nutzen sie als Vorlage für ihre eigenen nationalen Vorlagen.

Die Vorlage führt durch den Bewertungsprozess und umfasst die Beschreibung der geplanten Datenverarbeitung, die Analyse von Zweck, Rechtsgrundlage und Datenflüssen, die Prüfung von Notwendigkeit und Verhältnismäßigkeit sowie die Identifikation und Bewertung möglicher Risiken für die Rechte und Freiheiten betroffener Personen. Darüber hinaus werden Maßnahmen zur Risikominderung dokumentiert und die Einbindung relevanter Beteiligter wie Datenschutzbeauftragter oder Aufsichtsbehörden berücksichtigt.

Die Vorlage ist jedoch nicht verpflichtend und führt keine neuen rechtlichen Pflichten ein, sondern dient als praxisorientierte Hilfestellung.

OLG Hamm zur Zulässigkeit appbasierter Kundenprogramme

Mit Urteil vom 16. April 2026 hat das Oberlandesgericht Hamm (Az. I-13 UKl 7/25) eine Entscheidung zur Frage getroffen, ob appgebundene Rabattaktionen im Einzelhandel gegen das Allgemeine Gleichbehandlungsgesetz (AGG) verstoßen können, konkret im Fall von Penny.

Ausgangspunkt war eine Klage des Verbraucherzentrale Bundesverbands (vzbv). Dieser hatte argumentiert, dass App-exklusive Rabatte eine Diskriminierung darstellen könnten, insbesondere gegenüber älteren Menschen oder Menschen mit Behinderung, da diese möglicherweise weniger Zugang zu Smartphones oder digitalen Anwendungen haben. Daher wurde ein Verstoß gegen das Allgemeine Gleichbehandlungsgesetz (AGG) geltend gemacht.

Das OLG Hamm wies die Klage jedoch ab. Nach Auffassung des Gerichts liegt weder eine unmittelbare noch eine mittelbare Benachteiligung im Sinne des AGG vor. Entscheidend sei, dass die Nutzung der App grundsätzlich allen Personen offensteht und die Rabatte nicht an ein Merkmal wie Alter oder Behinderung anknüpfen, sondern allein an die Entscheidung, die App zu verwenden.

Nutzung von Diagnosedaten für Präventionsprogramme durch die Krankenkasse?

Eine private Krankenversicherung bietet Gesundheitsprogramme, wie z. B. Coaching bei Diabetes, Asthma oder Rückenleiden, an. Welche Versicherten könnten davon profitieren und wie werden diese identifiziert?

Die Versicherung analysierte dafür die Rechnungsunterlagen, die Versicherte zur Leistungserstattung einreichten. Hiernach ermittelte die Versicherung potenzielle

Programmteilnehmer. Bei Neukunden und bei Vertragsänderungen holte sie dafür eine Einwilligung ein – bei den übrigen Bestandskunden allerdings nicht.

Genau darin wurde vom Landesbeauftragten für den Datenschutz Rheinland-Pfalz ein Verstoß gegen die DSGVO gesehen. Das Bundesverwaltungsgericht (BVerwG) hob die Urteile der Vorinstanzen auf und prüfte die Zulässigkeit der Datenverarbeitung auf mehreren Ebenen der DSGVO. Zunächst bestätigte das BVerwG, dass die Datenanalyse dem Ausnahmetatbestand des Art. 9 Abs. 2 lit. h DSGVO unterfällt. Sie dient Zwecken der Gesundheitsvorsorge. Damit wurde aber zugleich eine erforderliche Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO eröffnet und daran scheiterte die Versicherung. Das BVerwG kam zu dem Ergebnis, dass die Interessen der Versicherten überwiegen. Der erhöhte Schutz sensibler Gesundheitsdaten nach Art. 9 DSGVO strahlt auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO aus und erhöht die Anforderungen an deren Rechtfertigung erheblich.

- Die Vorsorgeprogramme gehören nicht zum medizinischen Kernbereich der Krankenversicherung.
- Die Datenverarbeitung trifft potenziell alle Bestandskunden – ohne deren Wissen und in erheblicher Streubreite.
- Die Versicherung hatte ihre Verarbeitungszwecke den Versicherten nicht hinreichend transparent gemacht und damit gegen Art. 13 Abs. 1 lit. d DSGVO verstoßen.

Damit wurde auch das Verhältnis zwischen Art. 9 DSGVO und Art. 6 Abs. 1 DSGVO entschieden und die Rechtsprechung des Europäische Gerichtshof aufgenommen. Das BVerwG löst das Spannungsverhältnis, indem es den erhöhten Schutzstandard des Art. 9 DSGVO als gewichtenden Faktor innerhalb der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO einsetzt: Der besondere Schutz sensibler Daten strahlt auf die Abwägung aus und erhöht die Anforderungen an das überwiegende Interesse des Verantwortlichen erheblich. Art. 6 Abs. 1 lit. f DSGVO ist damit bei Gesundheitsdaten formal anwendbar und die Interessen abzuwägen. Die Frage zur Zweckänderung und dem Verhältnis von Art. 9 Abs. 2 DSGVO zu Art. 6 Abs. 1 lit. f DSGVO ergibt sich möglicherweise aus den Urteilsgründen, die noch nicht veröffentlicht sind. Jedenfalls ist zu beachten, dass Präventionsangebote möglich sind, jedoch nur mit einem ausdrücklichen „Ja“ und der Einwilligung der Versicherten.

Der Restaurantbesuch im Urlaub

Mittlerweile kennt man dies im In- und Ausland. An vielen Tischen in den Restaurants befinden sich QR-Codes zum Aufruf des Menüs und für die Bestellung. Die verlinkten Webseiten/Anwendungen benötigen eine Internetverbindung, die via WLAN vom Gastrobetreiber oder Einkaufszentrum angeboten werden. Die Nutzung des kostenlosen WLAN erfolgt nur gegen Anmeldung zum eigenen Newsletter oder gegen Registrierung mit diversen Pflichtfeldern. Doch nicht jeder QR-Code ist auch in Ordnung. Nunmehr verbreiten sich auch Betrugsmaschen damit, das sog. „Quishing“, die dann auf täuschend echt aussehende Seiten verweisen und darüber Daten abgreifen und später missbrauchen. Daher sollte lieber geprüft werden, ob der aufgeklebte QR-Code auch der echte ist.

Und wer sich mit einem öffentlichen und eventuell unsicheren WLAN verbindet, sollte auch die Gefahr des verdeckten Trackings des Geräts kennen, das metergenaue Bewegungsprofile und eine Wiedererkennung und Überwachung ermöglicht.

Auch die Verwendung von Zahlungsdiensteanbietern vor Ort im fernen Urlaubsland kann unangenehme Folgen haben. Wichtig ist, gelegentlich auch an den Datenschutz im Ausland zu denken und manchmal das „uncoole“, aber (anonyme) Bargeld im Ausland als Zahlungsmittel zu verwenden.

Stand: 20. Juli 2026

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

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