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 / I

Aktuelles rund um den Datenschutz

Google reCAPTCHA wird Auftragsverarbeiter

Google reCAPTCHA wird zum Schutz von Websites vor Spam eingesetzt. Die Anwendung soll erkennen, ob ein Nutzer menschlich ist. Google hat angekündigt, dass es beim Einsatz von reCAPTCHA ab April 2026 von der Rolle des Verantwortlichen in die eines Auftragsverarbeiters wechselt und einen AVV zur Verfügung stellt.

Um die Umstellung zu erreichen, aktualisiert Google seine Google Cloud Platform Service Specific Terms, welche die Nutzung von reCAPTCHA regeln. Dann unterliegen Nutzer, die auf reCAPTCHA-geschützte Websites zugreifen, nicht mehr den Datenschutzbestimmungen und Nutzungsbedingungen von Google.

Mit der Umstellung von Google reCAPTCHA auf den Auftragsverarbeitungsmodus reagiert Google auf die Kritik an der fehlenden Transparenz bezüglich der Nutzung der über reCAPTCHA erhobenen Daten. Zudem werden Websitebetreibern (formell) mehr Rechte in Bezug auf die über reCAPTCHA gesammelten Daten eingeräumt.

US-Firmen und deren EU-Töchter dürfen Auskünfte verweigern

Das LG Bonn hat mit Urteil vom 3. Juni 2025 entschieden, dass US-Firmen und deren europäische Töchter Auskünfte über Zugriffe US-amerikanischer Behörden verweigern dürfen, sofern ihnen dies gemäß Section 702 des US Foreign Intelligence Surveillance Act (FISA) verboten ist.

Im konkreten Fall hatte ein Nutzer eines sozialen Netzwerks Auskunft nach Art. 15 DSGVO verlangt, insbesondere darüber, ob US-Behörden auf seine Daten zugegriffen haben. Das Unternehmen verweigerte diese Information jedoch mit Verweis auf US-Recht, konkret auf Section 702 des Foreign Intelligence Surveillance Act (FISA). Dieses Gesetz verpflichtet bzw. erlaubt US-Unternehmen, mit Geheimdiensten zusammenzuarbeiten, verbietet ihnen aber gleichzeitig, über solche Zugriffe zu informieren.

Das Gericht stellte fest, dass hier eine sogenannte „Pflichtenkollision“ vorliegt: Einerseits besteht nach der DSGVO eine Auskunftspflicht gegenüber Betroffenen, andererseits eine gesetzliche Geheimhaltungspflicht nach US-Recht. Diese beiden Pflichten lassen sich nicht gleichzeitig erfüllen. Nach Auffassung des Gerichts kann eine solche unauflösbare Kollision einen Rechtfertigungsgrund für eine Auftragsverweigerung darstellen.

Bei der Abwägung entschied das Gericht zugunsten der Einhaltung des US-Rechts. Ein Unternehmen sei nicht gezwungen, gegen verbindliche ausländische Gesetze zu verstoßen. Zudem konnte der Kläger keine konkreten Hinweise auf tatsächliche Zugriffe von US-Geheimdiensten oder daraus entstandene Schäden vorlegen. Es überwog das Interesse an der Auskunftsverweigerung.

Datenschutz bei Ärzten

Datenschutz bei Ärzten ist ein zentraler Schutzbaustein für Patientinnen und Patienten. Die Anzahl an sensiblen Informationen in der medizinischen Versorgung ist enorm, zugleich handelt es sich um besonders schützenswerten personenbezogenen Daten (Befunde, Diagnosen, Medikationen, psychische Erkrankungen). Die Prinzipien der Vertraulichkeit, Datenminimierung, Zweckgebundenheit sind strikt einzuhalten. Klare Zugriffsregelungen auf Patientenakten nur durch befugtes

Personal (Need-to-know-Prinzip) sind ebenfalls nicht wegzudenken, wie eine sorgfältige Identitätsprüfung bei telefonischen Auskünften, bevor Informationen weitergegeben werden. Technische und organisatorische Maßnahmen bewahren elektronische Patientenakten vor unbefugtem Zugriff, Datenverlust oder Manipulation. Ein Missbrauch oder ungewollte Offenlegungen sensibler Informationen können so vermieden werden.

Im Alltag beim Arzt zeigt sich allerdings leider das Gegenteil. Die Anmeldung am offenen Tresen sind tägliche Realität.

Bereits einfache organisatorische und räumliche Maßnahmen können dies ändern: das Einrichten von Abstandszonen durch Bodenmarkierungen oder Hinweisschilder, Sichtschutzwände oder die Ausrichtung des Bildschirms, die Abfrage von Diagnosen oder Beschwerden nicht im öffentlichen Bereich, der Aufruf der Patienten mit Nummern oder Initialen.

Datenschutzprobleme werden oft aus Routine oder Zeitdruck hervorgerufen, selten aus Absicht. Dennoch helfen datenschutzrechtliche Regelungen einen klaren Rahmen zum Schutz von Patientinnen und Patienten zu gewährleisten. Eine Umsetzung der Maßnahmen verhindert Bloßstellung, Diskriminierung und Datenmissbrauch. Datenschutz entsteht nicht durch Paragraphen, sondern dort, wo die Regelungen akzeptiert und im Alltag konsequent angewendet werden. Insbesondere bei Ärzten zeigt angewendeter Datenschutz eine professionellere und vertrauenswürdigere Behandlung.

DSGVO und Kopplungsverbot: AG Nürnberg hält Einwilligung für wirksam

Mit Urteil vom 09.07.2025 des AG Nürnberg wurden Klarstellungen zur Reichweite der DSGVO und dem Kopplungsverbot im unternehmerischen Alltag getroffen. Die Parteien stritten über die Rechtmäßigkeit der Übermittlung von sogenannten Positivdaten an eine Wirtschaftsauskunftei im Rahmen eines Mobilfunkvertrags.

Klargestellt wurde im Urteil, dass eine datenschutzrechtliche Einwilligung auch dann freiwillig im Sinne des Art. 7 DSGVO sein kann, wenn sie an einen Vertragsschluss gekoppelt ist. Die DSGVO enthalte kein absolutes Kopplungsverbot, welches jede Verknüpfung von Verträgen mit datenschutzrechtlichen Erklärungen untersage. „Unfreiwilligkeit“ ist erst dann gegeben, wenn für den Betroffenen eine unangemessene Drucksituation oder eine faktische Alternativlosigkeit bestehe. Der Kläger hatte allerdings die Wahl zwischen zahlreichen Mobilfunkanbietern. Eine Beeinträchtigung der Entscheidungsfreiheit war nicht gegeben.

Eine Datenübermittlung war auch über das berechtigte Interesse des Unternehmens erfüllt. Die Übermittlung von Informationen über eine ordnungsgemäße Durchführung eines Vertrags ohne Zahlungsstörungen, dient legitimen Zwecken der Betrugsprävention. Das Telekommunikationsunternehmen hat ein erhebliches Interesse daran, massenhafte Vertragsabschlüsse zur Erlangung subventionierter Endgeräte frühzeitig zu erkennen.

Auch einen Schadensersatzanspruch nach Art. 82 DSGVO erkannte das Gericht nicht, da ein bloßes Unbehagen oder ein abstraktes Gefühl des Kontrollverlusts nicht ausreiche. Erforderlich sei der volle Nachweis eines konkret-individuellen Schadens.

Folge ist, dass Datenschutzinformationen transparent, zweckgebunden und in einfacher Sprache zu formulieren sind. Einwilligungen sind im Vertragstext deutlich hervorzuheben. Datenübermittlungen auf Basis des berechtigten Interesses sind sorgfältig zu dokumentieren.

Insofern kann der Unternehmer bei der Nutzung von Daten für legitime wirtschaftliche Zwecke gestärkt hervorgehen. Und: Die DSGVO gibt keinen Spielraum für pauschale Schadensersatzforderungen ohne realen Schaden.

Datenschutz bei Clean-Desk-Policy und Desksharing

Moderne Arbeitswelten sind geprägt vom mobilen Arbeiten, Homeoffice, Teil- und Gleitzeiten mit neuen datenschutzrechtlichen Herausforderungen. Hierbei sind Desksharing-Modelle und Clean-Desk-Policy entscheidende Bausteine.

Desksharing bedeutet grundsätzlich, dass es im Office keine festen Arbeitsplätze oder Schreibtische mehr gibt. Auch die Dienstgeräte könnten geteilt werden. Mitarbeitende wählen insofern täglich einen freien Arbeitsplatz. Das erhöht auch die datenschutzrechtlichen Herausforderungen, da Dokumente oder Datenträger mit

sensiblen Informationen versehentlich zurückgelassen werden können.

Bei einem ständigen Wechsel von Arbeitsplätzen und Dienstgeräten, muss sichergestellt sein, dass persönlichen Daten oder Dateien des vorherigen Nutzers nicht abrufbar sind. Desksharing benötigt daher klare datenschutzrechtliche Regeln.

Clean-Desk-Policy bedeutet, dass Arbeitsplätze ohne Einsicht in vertrauliche Daten hinterlassen werden, weder Papierakten oder Notizzettel noch mobile Datenträger oder ungesperrte Bildschirme. Auch hier sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten erforderlich.

Entscheidend sind klar definierte Verhaltensregeln: Vertrauliche Unterlagen dürfen zu keiner Zeit offen liegen bleiben, Dokumente gehören in abschließbare Schränke, und Ausdrucke sind sofort abzuholen oder bei Nichtverwendung direkt zu vernichten. Bildschirme sind zu sperren, wenn der Arbeitsplatz verlassen wird, oder werden bei Inaktivität automatisch gesperrt.

Auch das sog. „Pull-Printing“ verhindert, dass Ausdrucke unkontrolliert im Drucker verbleiben. Auch Schulungen und regelmäßige Sensibilisierungen fördern eine Clean-Desk-Policy unter Mitarbeitern.

Die Konzepte haben nur Erfolg, wenn auch das Unternehmen klare Standards definiert, wie der Arbeitsplatz nach der Nutzung auszusehen hat, hinsichtlich der physischen Ordnung als auch der digitalen „Sauberkeit“.

Zur Unterstützung sind zentrale Schließfächer oder abschließbare Rollcontainer sinnvoll. Maßgebend ist jedoch, dass alle Mitarbeitenden die Bedeutung dieser Maßnahmen verstehen und daran mitarbeiten. Führungskräfte sollten Vorbildcharakter haben.

Eine moderne Arbeitswelt mit zunehmender Flexibilität und Mobilität berücksichtigt auch den datenschutzkonformen Umgang mit Daten. Eine klar geregelte „Clean-Desk-Policy“ mit „Desksharing“ schützt personenbezogene Daten und fördert insgesamt die Informationssicherheit des Unternehmens. Ordnung, Klarheit und Verantwortungsbewusstsein am Arbeitsplatz vermeiden Datenschutzverstöße.

Stand: 31. März 2026

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