

Datenschutz-Newsletter 2026 / 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

Das berechtigte Interesse: Weit mehr als eine Auffangregelung

Jede Verarbeitung personenbezogener Daten erfordert eine Rechtsgrundlage. In der Praxis wird oft versucht, Lücken durch eine Einwilligung zu schließen. Doch gerade im Arbeitsverhältnis ist dies fehleranfällig: Da eine Freiwilligkeit zwischen Arbeitgeber und Arbeitnehmer nicht ohne weiteres anzunehmen ist, erweist sich die Einwilligung hier oft als rechtliches Luftschloss.

In solchen Fällen rückt Art. 6 Abs. 1 lit. f DSGVO in den Fokus: die Verarbeitung auf Basis eines berechtigten Interesses. Doch entgegen der verbreiteten Annahme ist dies kein einfacher „Rettungsanker“, sondern an strikte Bedingungen geknüpft. Nach der aktuellen Rechtsprechung des EuGH (u. a. Urteil vom 04.07.2023) müssen drei Kriterien kumulativ erfüllt sein:

Drei Voraussetzungen für das berechtigte Interesse:

1. Es muss ein legitimes Interesse des Verantwortlichen oder eines Dritten vorliegen.
2. Die Verarbeitung muss zwingend erforderlich sein, um dieses Ziel zu erreichen.
3. Die Grundrechte und Freiheiten der betroffenen Person dürfen nicht überwiegen.

Ein häufiger Fehler ist die sogenannte „verkürzte Prüfung“, bei der lediglich das eigene Interesse benannt, die Erforderlichkeit und die Abwägung jedoch vernachlässigt werden. Das Ergebnis ist eine Datenverarbeitung ohne Rechtsgrundlage.

Orientierungshilfen von EDSA und HmbBfDI (LIA)

Um hier mehr Sicherheit zu schaffen, hat der Europäische Datenschutzausschuss (EDSA) im Oktober 2024 eine Orientierungshilfe veröffentlicht. Darauf aufbauend bietet der Hamburgische Beauftragte für Datenschutz und

Informationsfreiheit (HmbBfDI) einen detaillierten Fragenkatalog für das sogenannte Legitimate Interests Assessment (LIA) an, auch für die notwendigen unternehmenseigenen Dokumentationen.

Fazit: Letztlich zeigt der Umfang dieses Prüfprozesses, dass das „berechtigte Interesse“ keine einfache Checkliste ist, sondern eine anspruchsvolle juristische Analyse. Die Anforderungen an die berufliche Qualifikation eines Datenschutzbeauftragten sind nicht ohne Grund so hoch: Um eine Interessenabwägung rechtssicher zu gestalten, ist eine tiefe Expertise an der Schnittstelle von Datenschutzrecht und betriebsorganisatorischen Prozessen unerlässlich.

Das unterschätzte Risiko: Unzureichendes Verarbeitungsverzeichnis

In vielen Unternehmen wird das Verzeichnis von Verarbeitungstätigkeiten (VVT) lediglich als formale Pflicht wahrgenommen. Es wird einmalig erstellt, in einer Schublade oder einem digitalen Ordner abgelegt und selten wieder angeführt. Diese passive Herangehensweise ist jedoch gefährlich. Eine aktuelle Entscheidung der luxemburgischen Datenschutzaufsicht (CNPd) verdeutlicht, dass ein formal vorhandenes VVT keinen Schutz bietet, wenn die inhaltliche Qualität fehlt.

Die Falle der „formalen Compliance“

Im Kern des Falles stand ein Unternehmen, das zwar ein VVT führte und sogar ein spezielles Verwaltungstool einsetzte. Dennoch wertete die Aufsichtsbehörde das Register als unzureichend. Das Problem war nicht das Fehlen des Dokuments, sondern seine mangelhafte Pflege und inkonsistente Ausführung.

Die Behörde rügte insbesondere die Verwendung zu pauschaler Begriffe. Angaben wie „interne Abteilungen“ oder „Service Provider“ sind rechtlich nicht ausreichend; die DSGVO verlangt eine präzise und nachvollziehbare Kategorisierung der Empfänger. Besonders kritisch wurden Defizite bei den Drittlandtransfers bewertet: Fehlende Angaben zu den konkreten Empfängern oder nicht benannte Zielländer machten eine Prüfung der Rechtmäßigkeit unmöglich. Die Folge waren nicht nur konkrete Nachbesserungsanordnungen, sondern auch ein Bußgeld aufgrund eines Verstoßes gegen Art. 30 DSGVO.

Das VVT als strategisches Kontrollsystem

Diese Entscheidung unterstreicht, dass das VVT weit mehr ist als eine bloße Dokumentationspflicht. Es ist das zentrale Nervensystem des Datenschutzmanagements. Nur wer seine Verarbeitungstätigkeiten vollständig, korrekt und aktuell erfasst hat, ist überhaupt in der Lage zu beurteilen, ob die Datenverarbeitung rechtmäßig ist und wo potenzielle Risiken liegen. Ein lückenhaftes VVT ist somit gleichbedeutend mit einem Kontrollverlust über die eigenen Datenströme. Es genügt nicht, die entsprechenden Informationen in anderen internen Dokumenten zu verstecken. Die relevanten Details müssen widerspruchsfrei direkt im Verzeichnis integriert sein, da jede Inkonsistenz unmittelbar als Compliance-Verstoß gewertet werden kann.

Handlungsempfehlungen für die Praxis

Um aus der Falle der formalen Compliance auszubrechen, sollten Unternehmen ihr VVT als ein sich selbst fortführendes datenschutzrechtliches Werkzeug einführen:

Dynamische Pflege: Das Verzeichnis muss an die tatsächlichen Geschäftsprozesse gekoppelt sein. Änderungen in der Software-Landschaft oder neuen Dienstleistern müssen unmittelbar ins VVT einfließen.

Präzision statt Pauschalisierung: Verzicht auf vage Begriffe. Empfänger und Datenkategorien müssen konkret benannt werden, um die Transparenzpflicht zu erfüllen.

Fokus auf Drittländer: Eine detaillierte Kartierung aller Datenflüsse außerhalb der EU/des EWR ist essenziell, inklusive der Benennung der Rechtsgrundlagen für diese Transfers.

Qualitätssicherung: Regelmäßige Stichproben und Abgleiche mit der Realität in den Fachabteilungen verhindern, dass das VVT zur „Phantomkartei“ verkommt.

Rechtssichere Hilfe für den Verantwortlichen

Um solche Qualitätsmängel zu vermeiden, empfiehlt sich die Orientierung an offiziellen Standards. So stellt beispielsweise der Bundesbeauftragte für den Datenschutz und die

Informationsfreiheit (BfDI) in Zusammenarbeit mit der Datenschutzkonferenz (DSK) standardisierte Musterformulare und Leitlinien zur Verfügung. Diese Vorlagen bieten ein rechtssicheres Grundgerüst.

Zwischen Pflicht und Verstoß: Das fehlende VVT

Besonders kritisch ist jedoch die Situation von Unternehmen, die gar kein VVT vorweisen können. Da die Pflicht zur Führung eines Verzeichnisses nicht nur für Organisationen mit mehr als 250 Mitarbeitern gilt, sondern auch für kleinere Unternehmen, sobald die Verarbeitung nicht mehr nur gelegentlich erfolgt oder Risiken für Betroffene bestehen, wird das vollständige Fehlen oft als systematisches Versagen gewertet und zieht drastischere Sanktionen nach sich als ein lediglich lückenhaftes Register.

Fazit: Das VVT ist ein zentraler Baustein der DSGVO-Konformität. Seine Qualität entscheidet darüber, ob ein Unternehmen seine Rechenschaftspflicht erfüllen kann. Die Entscheidung der CNPD zeigt deutlich, dass auch vermeintlich kleine formale Mängel schwerwiegende rechtliche und finanzielle Folgen haben können. Wer sein VVT nur formal führt, schafft sich eine gefährliche Illusion von Sicherheit.

Fehlende Rollenabgrenzung: Verantwortlicher statt Auftragsverarbeiter

Die korrekte Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter ist eine der zentralen Unterscheidungen der DSGVO. Sie entscheidet darüber, wer die Informationspflichten erfüllt, Betroffenenrechte bearbeitet und die Rechtmäßigkeit der Datenverarbeitung nachweisen muss. Eine aktuelle Entscheidung der belgischen Datenschutzbehörde (APD) verdeutlicht, dass eine falsche Einordnung schwerwiegende finanzielle Folgen haben kann.

Der Fall Isabel SA

Gegen das Fintech-Unternehmen Isabel SA wurde eine Geldbuße in Höhe von 120.000 Euro verhängt. Das Unternehmen bot mit „TruliUs“ einen digitalen Identifizierungsdienst an und stufte sich dabei als reinen Auftragsverarbeiter ein. Damit wälzte Isabel die zentralen DSGVO-Pflichten auf seine Kunden ab. Ein Nutzer stellte jedoch fest, dass mehr Daten erhoben wurden als angegeben und forderte Auskunft. Da Isabel sich selbst nicht als Verantwortlichen sah, blieb diese Anfrage unbeantwortet.

Die Entscheidung der Behörde

Die belgische Aufsichtsbehörde widersprach der Selbsteinschätzung von Isabel. Entscheidend war nicht die vertragliche Bezeichnung, sondern die tatsächliche Entscheidungsgewalt über Zweck und Mittel der Verarbeitung:

Strukturelle Prägung: Isabel hatte den Dienst konzipiert und betrieben. Das Unternehmen legte fest, wie die Authentifizierung abläuft und welche Daten erfasst werden.

Standardisierung: Da es sich um einen standardisierten Dienst mit eigenem Konzept handelte, konnten weder die Nutzer noch die Kunden den Prozess maßgeblich mitbestimmen. Hinweise auf die Komplexität der Rollenabgrenzung oder eine interne Dokumentation der falschen Einordnung entlasteten das Unternehmen nicht. Gerade bei neuartigen Diensten sei eine sorgfältige Risikoanalyse zwingend erforderlich.

Folgefehler durch falsche Einordnung

Die fehlerhafte Rollenbestimmung zog eine Kette weiterer Verstöße nach sich:

Mangelnde Transparenz: Die Datenschutzhinweise waren unzureichend.

Verletzung von Betroffenenrechten: Das Auskunftersuchen wurde ignoriert.

Verstoß gegen die Datenminimierung: Es wurden unnötig umfangreiche Daten (z. B. Nationalität, Geburtsort) erhoben, die für den Zweck der Authentifizierung nicht erforderlich waren.

Die Geldbuße wurde letztlich direkt an den Grundverstoß gegen die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) geknüpft, da daraus alle anderen Defizite resultierten.

Fazit: Der Fall unterstreicht, dass die Rollenverteilung in der DSGVO materiell-rechtlich und nicht formal-vertraglich bestimmt wird. Wer ein System inhaltlich und technisch prägt, übernimmt die Rolle des Verantwortlichen. Eine saubere rechtliche Analyse zu Beginn ist essenziell.

Prävention von Datenpannen im Gesundheitswesen

Die Verarbeitung von Gesundheitsdaten unterliegt aufgrund ihrer Sensibilität einem besonderen Schutz. Fehler bei der Handhabung dieser Daten können für Betroffene schwerwiegende Folgen haben. Angesichts steigender Fallzahlen von Datenpannen hat der LfDI Baden-Württemberg in seinem Tätigkeitsbericht 2025 gezielte Maßnahmen zur Vermeidung unbefugter Offenlegungen definiert.

Die Problematik: Sensibilität und Risiken

Gesundheitsdaten lassen unmittelbare Rückschlüsse auf Diagnosen und den körperlichen oder psychischen Zustand einer Person zu. Menschliche Fehlleistungen, technische Mängel oder organisatorische Lücken führen hier oft zu einer schwerwiegenden Verletzung der Privatsphäre.

Besonders kritisch sind dabei „klassische“ Fehlerquellen wie der unsichere Versand oder die Verwechslung von Patienten.

Sicherer Versand physischer Datenträger

Wenn Gesundheitsdaten postalisch auf mobilen Datenträgern (z. B. USB-Sticks) versendet werden, ist eine Kombination aus technischem und physischem Schutz zwingend:

1. Verschlüsselung: Ein Versand ohne Verschlüsselung nach aktuellem Stand der Technik ist unzulässig.

2. Physische Barrieren: Da USB-Sticks in Briefumschlägen leicht ertastbar sind, empfiehlt der LfDI die Nutzung von gepolsterten Umschlägen mit verstärkten Seiten. Zudem sollte der Datenträger fest am Anschreiben fixiert werden, um ein „Herumschieben“ im Umschlag zu erschweren.

3. Nachverfolgbarkeit: Bei umfangreichen oder besonders sensiblen Datenübermittlungen sollte konsequent eine Sendungsverfolgung genutzt werden, um im Verlustfall den Verbleib der Daten klären zu können.

4. Digitale Portale: Der Versand über Webportale ist eine sichere Alternative, sofern eine verschlüsselte Übertragung (auch gegenüber dem Anbieter) und eine starke Authentifizierung gewährleistet sind.

Strategien gegen den Fehlversand

Fehlversände entstehen häufig durch Tippfehler, Namensgleichheiten oder das Vermengen von Patientenunterlagen bei unzureichender Benennung oder fehlender Ordnungsstruktur. Da die bloße Sensibilisierung der Beschäftigten oft nicht ausreicht, müssen prozessuale Sicherungen greifen:

- **Das Vier-Augen-Prinzip:** Die Implementierung eines Kontrollschritts durch eine zweite Person kann menschliche Versehen beim Versand effektiv abfangen.

- **Eindeutige Patientenidentifikation:** Der Name allein ist als Identifikationsmerkmal unzureichend. Er muss zwingend mit einem eindeutigen Datum (z. B. Geburtsdatum) oder einer eindeutigen Patienten-ID verknüpft werden.

- **Technische Validierung:** IT-Systeme sollten so konfiguriert sein, dass sie bei Namensgleichheiten automatisch Warnmeldungen ausgeben, um Verwechslungen zu vermeiden.

Fazit für die Praxis: Die Vermeidung von Datenpannen im Gesundheitswesen erfordert einen ganzheitlichen Ansatz. Es ergeben sich drei Kernsäulen der Prävention:

1. Technik: Verschlüsselung und Validierung.

2. Organisation: Vier-Augen-Prinzip und eindeutige IDs.

3. Dokumentation & Schulung (klare Richtlinien für alle Mitarbeiter).

Kennzeichnungspflicht ab August 2026: KI im Einsatz

Die fortschreitende Integration künstlicher Intelligenz in den unternehmerischen Alltag erhält einen verbindlichen rechtlichen Rahmen. Ab August 2026 greifen die neuen Transparenzpflichten der europäischen KI-Verordnung (AI-Act). Viele Unternehmen stehen nun vor der Aufgabe, ihre Prozesse anzupassen. Die gute Nachricht vorweg: Für den Großteil der kleinen und mittelständischen Betriebe reicht eine unkomplizierte, verständliche Kennzeichnung aus. Das Regelwerk unterscheidet im Wesentlichen drei Szenarien, in denen Transparenz rechtlich eingefordert wird.

KI-Texte im Fokus des öffentlichen Interesses

Nicht jeder digital optimierte Webseitentext erfordert ab 2026 ein Label. Die Pflicht beschränkt sich primär auf Texte, welche die breite Öffentlichkeit über gesellschaftlich relevante, politische oder nachrichtliche Themen informieren und per KI generiert oder maßgeblich bearbeitet wurden. Keine Kennzeichnung brauchen klassische Produktbeschreibungen, automatisierte Übersetzungen oder Texte, bei denen die KI lediglich zur Rechtschreibkorrektur genutzt wurde. Wichtige Ausnahme: Prüft ein Mensch das KI-Erzeugnis vor der Publikation final und übernimmt dafür die redaktionelle Verantwortung (Art. 50 Abs. 4 EU AI-Act), entfällt die Kennzeichnungspflicht komplett.

Kennzeichnung von Deepfakes und künstlichen Medien

Medieninhalte, die durch KI-Einsatz täuschend echt wirken und dadurch eine Verwechslungsgefahr mit der Realität bergen (sogenannte Deepfakes), müssen unmissverständlich deklariert werden. Das betrifft beispielsweise manipulierte Videos, künstlich erzeugte Interviews oder komplett synthetisch generierte Fotos von Firmengebäuden. Erlaubt sind weiterhin einfache technische Korrekturen wie Schärfen- oder Belichtungsanpassungen.

Offenlegung bei direktem KI-Kundenkontakt

Nutzer besitzen das Recht zu erfahren, ob sie mit einer Maschine oder einem Menschen kommunizieren. Setzen Unternehmen KI-Chatbots auf der Homepage, automatisierte E-Mail-Antworten oder KI-Sprachsysteme am Telefon ein, muss dies direkt zu Beginn der Interaktion offengelegt werden.

Fazit: Praxis-Tipp und Übergangsfristen

Um den bürokratischen Aufwand im Alltag zu minimieren, empfiehlt sich die Etablierung einer internen Transparenzstrategie. Feste Vorgaben – wie standardisierte Hinweise am Textende oder standardmäßige Bildunterschriften bei

generierten Fotos – nehmen Mitarbeitern die Einzelfallprüfung ab. Unternehmen sollten zudem die gesetzlichen Stichtage im Blick behalten: Während neue Systeme ab dem 2. August 2026 direkt konform laufen müssen, gewährt der Gesetzgeber für bereits vor diesem Datum veröffentlichte Medien eine Schonfrist zur Nachpflege bis zum 2. Dezember 2026.

Stand: 30. September 2026

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.

RA/StB Thomas Hesz; WP/StB Marcel Peetz (M.Acc.); RAin Kira Scheidt; Stefan Gräbe

Zertifizierte Datenschutzbeauftragte (TÜV)

Telefon: 09221 / 900 - 0

edsb@frtconsult.de www.frtpartner.de