NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 2/2025

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Mitte Januar 2025 wurde die elektronische Patientenakte (ePA) für alle gesetzlich Versicherten in Deutschland nach dem neuen Opt-out-Modell eingeführt. Während bisher die Einrichtung einer ePA aktiv beantragt werden musste, erfolgt sie aktuell automatisch, sofern Versicherte nicht ausdrücklich widersprochen haben.
Versicherte haben nicht nur die Möglichkeit, die Einrichtung der ePA komplett abzulehnen, sondern können auch gezielt einzelne Datenverarbeitungen blockieren. Damit lässt sich die ePA individuell an die persönlichen Bedürfnisse und Datenschutzpräferenzen anpassen.
Das Bayerische Landesamt für Datenschutz hat neben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ein Papier veröffentlicht, das die neue Regelung detailliert erläutert und wichtige Fragen beantwortet („Aktuelle Kurz-Information 56“).
Zusätzlich zu den Widerspruchsrechten können Versicherte den Zugriff auf bestimmte Dokumente oder Kategorien von Dokumenten beschränken, sodass nur sie selbst darauf zugreifen können.
Es ist gesetzlich sichergestellt, dass Versicherte, die von ihren Widerspruchsrechten Gebrauch machen, weder bevorzugt noch benachteiligt werden dürfen.
Vor dem Hintergrund gewichtiger kritischer Stimmen (Ärzteblatt, Chaos Communication Congress) zur Sicherheit der ePA dürfte für die Betroffenen die Information wichtig sein, dass die Nutzung der ePA auch nach der Umstellung auf das Widerspruchsmodell freiwillig bleibt.
Versicherte haben die Möglichkeit, der Einrichtung einer ePA innerhalb von sechs Wochen nach Erhalt der entsprechenden Informationen zu widersprechen, was zur Löschung aller gespeicherten Daten führt. Es ist jedoch zu beachten, dass gelöschte Daten bei einer erneuten Einrichtung der ePA nicht wiederhergestellt werden können.

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: VideoFlow, Adobe Stock

Wegweiser stärkt Schutz von Kommunen vor Cyberangriffen

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben am 10. Dezember 2024 den Wegweiser „Kommunale IT-Krisen: Handlungsfähigkeit sichern“ ⭳ veröffentlicht.

Die Intention der Handreichung ist es, Kommunen gezielt dabei zu unterstützen, IT-Krisen zu bewältigen und die Folgen von Cyberangriffen auf ein Minimum zu reduzieren.
Tägliche Cyberangriffe auf IT-Infrastrukturen sind eine große Herausforderung, besonders für Städte und Gemeinden. Der Schutz kommunaler IT-Systeme ist essenziell, um die öffentliche Verwaltung funktionsfähig zu halten und den Alltag reibungslos zu gestalten.
IT-Krisen sind jedoch nicht allein ein technisches Problem, sondern betreffen auch die allgemeine Notfall- und Krisenorganisation. Eine enge Kooperation zwischen Verwaltung und IT-Betrieb ist entscheidend, um Prävention und Reaktion auf Cyberangriffe zu verbessern.
Der Wegweiser bietet eine praxisorientierte Hilfestellung, um Kommunen bei der Abwehr von Cyberangriffen zu unterstützen:

- **Bewältigung von IT-Krisen**: detaillierte Handlungsempfehlungen zur Reaktion auf Cyberattacken, einschließlich der Wiederherstellung der IT-Infrastruktur
- **Notwendige Voraussetzungen**: erfolgreiche Maßnahmen erfordern
  - geschulte Mitarbeitende,
  - klare interne Strukturen,
  - Unterstützung durch externe Partner wie Behörden oder Dienstleister.
- **Praktisches Lernbeispiel**: Ein fiktives Szenario eines Ransomware-Angriffs veranschaulicht Prozesse und Maßnahmen zur effektiven Bewältigung von IT-Krisen.

Der Leitfaden bietet Kommunen einen niedrigschwelligen Einstieg in das komplexe Thema kommunaler IT-Krisen. Er soll dazu beitragen, Daten und Infrastrukturen besser vor Cybergefahren zu schützen und negative Folgen zu minimieren. Darüber hinaus enthält die Veröffentlichung weiterführende Informationen und Hinweise zu verwandten Themenbereichen, die Kommunen bei der Entwicklung wirksamer Schutzmaßnahmen unterstützen.
Die Handreichung ist ein wichtiger Schritt, um Kommunen auf IT-Gefahrenlagen vorzubereiten und deren Handlungsfähigkeit auch in Krisenzeiten zu sichern. Auch wenn der Leitfaden primär auf Kommunalverwaltungen ausgerichtet ist, können die **Grundprinzipien und Strategien zur Stärkung der IT-Sicherheit und Krisenbewältigung** durchaus auch für Unternehmen relevant sein.

KI-Kompetenzen im deutschen Arbeitsmarkt

Ein neues Papier (Qualifizierungsbedarfe und Künstliche Intelligenz – Ein webanalytischer Ansatz mittels Generativer KI ⭳) des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation IAO untersucht den Bedarf an KI-Kompetenzen bei Fachkräften, insbesondere im Kontext neuer Technologien wie der generativen künstlichen Intelligenz (KI).

Foto: peshkova, Adobe Stock

Es konzentriert sich im Gegensatz zu allgemeiner KI-Literatur auf Expertenanforderungen und nutzt eine neuartige, auf Gen-AI-basierte Webanalyse von Stellenanzeigen, um aktuelle und zukünftige Kompetenzbedarfe effizient zu identifizieren. Die Methode ermöglicht nach Ansicht der Autoren eine präzise und skalierbare Analyse der dynamischen Entwicklungen auf dem Arbeitsmarkt.
Die Ergebnisse sollen Unternehmen und Bildungseinrichtungen einen detaillierten Überblick über die benötigten Kompetenzen liefern und das Potenzial der Gen-AI-Analyse für die Arbeitsmarktforschung aufzeigen. Das Ziel ist es, einen Beitrag zur besseren Ausrichtung von Bildungsangeboten und Unternehmensstrategien im Bereich KI zu leisten.
Zusammenfassend bietet das Diskussionspapier Unternehmen eine Grundlage für strategische Personalentscheidungen im Bereich KI. Es liefert wichtige Einblicke in die benötigten Kompetenzen und Methoden zur Analyse des Kompetenzbedarfs, die es Unternehmen ermöglichen, ihre KI-Strategie zu optimieren und den wachsenden Anforderungen des Arbeitsmarktes gerecht zu werden.

Foto: Imillian, Adobe Stock

Unzulässige Verarbeitung von Gesundheitsdaten per E-Mail: 10.000 Euro Schadensersatz

Das Arbeitsgericht Duisburg hatte jüngst darüber zu entscheiden, ob dem Kläger ein Ersatz eines immateriellen Schadens in Höhe von mindestens 17.000 Euro gegen die Beklagte zusteht, weil dieser in einer E-Mail an knapp 10.000 Empfänger Informationen über die Gesundheit des Klägers verbreitet hat.

Weiter auf DataAgenda lesen

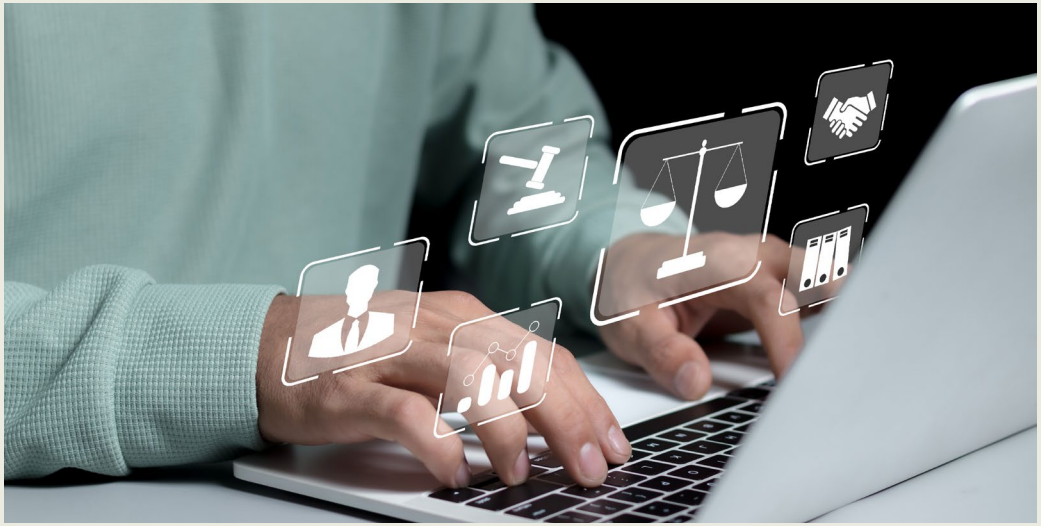

Foto: Ei, Adobe Stock

KI in der Anwaltskanzlei: Chancen verantwortungsvoll nutzen

KI-Anwendungen bieten vielfältige Möglichkeiten für den Einsatz in Anwaltskanzleien, bringen jedoch auch berufsrechtliche Herausforderungen mit sich.

Insbesondere „große" Sprachmodelle (Large Language Models (LLMs)) wie ChatGPT, bieten vielfältige Einsatzmöglichkeiten – von Recherche- und Analyse-Tools bis hin zur automatisierten Übersetzung von Rechtsdokumenten. Ein neuer Leitfaden der Bundesrechtsanwaltskammer (BRAK) unterstützt Anwältinnen und Anwälte dabei, KI-Tools rechtssicher und berufsrechtskonform zu nutzen.

Sprachmodelle generieren Texte auf Basis statistischer Wahrscheinlichkeiten, ohne den Inhalt tatsächlich zu „verstehen". Dies könne zu sogenannten „Halluzinationen" führen – der Erzeugung faktisch falscher, aber plausibel erscheinender Inhalte. In der rechtlichen Beratung können solche Fehler gravierende Konsequenzen haben, z. B. durch unrichtige Angaben in Schriftsätzen.

Zusätzlich existiere die Gefahr von Verzerrungen (Bias) durch einseitiges oder unzureichendes Trainingsmaterial. Trotz erheblicher Verbesserungen seit der Einführung von ChatGPT im November 2022 bleiben diese Herausforderungen bestehen.

Für Kanzleien sei es daher essenziell, KI-Ergebnisse sorgfältig zu prüfen und stets berufsrechtskonform einzusetzen, um haftungsrechtliche Risiken zu minimieren und von den Vorteilen der Technologie zu profitieren.

Insbesondere die Beachtung der anwaltlichen Verschwiegenheit nach § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO) muss auch beim Einsatz von KI und LLMs unbedingt sichergestellt sein. Dieses Gebot erstreckt sich auf alle Informationen, die der Rechtsanwältin bzw. dem Rechtsanwalt in Ausübung des Anwaltsberufs im Rahmen eines Mandats bekannt werden (§ 43a Abs. 2 Satz 2 BRAO). Die unbefugte Offenbarung eines der Rechtsanwältin bzw. dem Rechtsanwalt anvertrauten fremden Geheimnisses ist strafrechtlich abgesichert nach § 203 Abs. 1 Nr. 3 Strafgesetzbuch (StGB).

Der Leitfaden bietet Anwältinnen und Anwälten Orientierung zu zentralen Themen wie Prüfungs- und Kontrollpflichten, der Wahrung der anwaltlichen Verschwiegenheitspflicht sowie Transparenzpflichten beim Einsatz von KI. Darüber hinaus werden die wesentlichen Anforderungen der KI-Verordnung und deren Verhältnis zum Berufsrecht erläutert. Ergänzend enthält der Leitfaden Hinweise zu weiteren Risiken und verweist auf Leitfäden europäischer Anwaltsorganisationen sowie der Datenschutzkonferenz. Die Hinweise der BRAK können durchaus als Grundlage für die Erstellung einer knapperen Kanzlei-Policy genutzt werden.

Foto: E, Adobe Stock

Interessenkollision: Geheimschutzbeauftragter und Datenschutzbeauftragter in Personalunion

Die Problematik einer möglichen Interessenkollision, wenn sich der oder die Beauftragte für den Datenschutz im Rahmen einer weiteren Rolle im Unternehmen betätigt, ist hinlänglich bekannt.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beschäftigt sich jedoch in seinem Tätigkeitsbericht zum Datenschutz für das Berichtsjahr 2023 recht ausführlich mit einer Interessenkollision, die eher seltener besprochen wird.

Problemstellung: Wie ist eine mögliche Interessenkollision zu bewerten, wenn sowohl die Rolle des Geheimschutzbeauftragten als auch die des Datenschutzbeauftragten von derselben Person wahrgenommen werden soll?

Kurz: Der TLfDI sah nach Prüfung der Fragestellung, dass bei der Übertragung der Aufgaben eines Geheimschutzbeauftragten auf den behördlichen Datenschutzbeauftragten eine Inkompatibilität der beiden Aufgabenkomplexe und somit ein Interessenkonflikt, mithin eine Unvereinbarkeit im Sinne von Art. 38 Abs. 6 Satz 2 DS-GVO in Verbindung mit § 14 Abs. 7 Satz 2 Thüringer Datenschutzgesetz (ThürDSG) vorliegt.
Ein Interessenkonflikt nach den datenschutzrechtlichen Bestimmungen liegt nach Auffassung des TLfDI insbesondere dann vor, wenn ein (behördlicher) Datenschutzbeauftragter durch anderweitige Aufgaben und Pflichten, die er zusätzlich erfüllen soll, in seiner Aufgabenwahrnehmung nach Art. 39 DS-GVO in Verbindung mit § 15 ThürDSG derart eingeschränkt wäre, dass keine objektive Aufgabenwahrnehmung mehr vorliegt, er mithin die eigenständig vorgenommenen oder veranlassten Datenverarbeitungstätigkeiten selbst kontrollieren müsste.
Die ausführliche Bewertung des TLfDI finden Sie auf DataAgenda.

Foto: Stockfotos-MG, Adobe Stock

Anfertigung und Speicherung von Personalausweiskopien

In vielen Wirtschaftsbereichen wird zur Identifikation oftmals die Vorlage des Personalausweises verlangt und dieser dann auch gern kopiert oder fotografiert, vorgeblich zu Dokumentationszwecken. Nicht selten ergeben sich hier Unsicherheiten, hinsichtlich der Zulässigkeit von (vollständigen) Personalausweiskopien.

Weiter auf DataAgenda lesen

Foto: Nirusmee, Adobe Stock

Unzulässige Gesprächsaufzeichnungen in medizinischer Einrichtung

Eine Einrichtung zur Vermittlung ärztlicher Versorgung plante, sämtliche Telefongespräche mit medizinischem Personal aufzuzeichnen.

Dabei sollten auch Gesundheitsdaten der Anrufenden erfasst werden. Ziel war es, die ärztliche Dokumentationspflicht zu erfüllen, die Beschäftigten zu schützen und die Aufzeichnungen für Schulungen und Feedbackgespräche zu nutzen.

Ergebnis der Prüfung durch die Datenschutzbehörde

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit stellte fest (Jahresbericht 2023), dass die geplanten Gesprächsaufzeichnungen weder durch gesetzliche Vorschriften gedeckt noch datenschutzrechtlich erforderlich sind. Folgende Punkte wurden hervorgehoben:

- **Fehlende Erforderlichkeit für die ärztliche Dokumentationspflicht:**
  - Die ärztliche Dokumentationspflicht verlangt keine vollständige Aufzeichnung von Gesprächen.
  - Alternative, datensparsamere Verfahren zur Dokumentation sind ausreichend.
- **Kein Schutz der Beschäftigten:**
  - Die Aufzeichnungen waren nicht notwendig, um Beschäftigte vor möglichen Rechtsansprüchen zu schützen.
  - Ein potenzielles Risiko allein reicht nicht aus, um eine Erforderlichkeit nach der DS-GVO zu begründen.
- **Unzureichende Grundlage für Schulungszwecke:**
  - Es gibt keine Rechtsvorschrift, die die Verarbeitung von Gesundheitsdaten für Schulungen oder Feedbackgespräche rechtfertigt.
  - Solche Zwecke können nur mit ausdrücklicher Einwilligung der Betroffenen verfolgt werden.

Weiter auf DataAgenda lesen

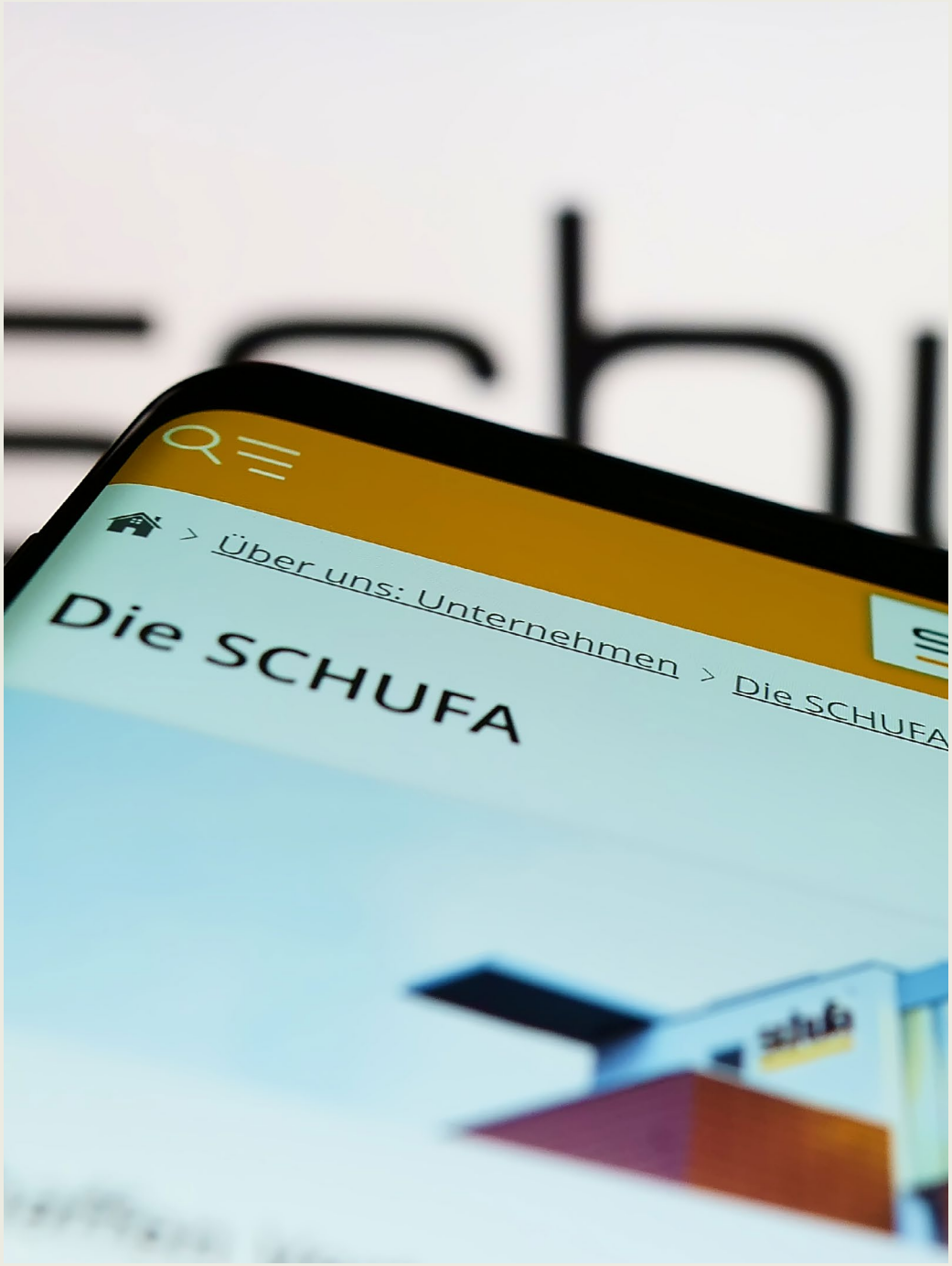

Foto: Timon, Adobe Stock

Verkürzte Speicherfristen bei der Schufa

Ab dem 1. Januar 2025 reduziert die Schufa Holding AG die Speicherfrist für ausgeglichene Forderungen in bestimmten Fällen von bisher 36 auf 18 Monate.

Diese Änderung betrifft etwa 120.000 Forderungen, die kurz nach der Übermittlung an die Auskunftei beglichen wurden. Zudem werden rund 56.000 Forderungen, die bereits länger als 18 Monate gespeichert sind, vorzeitig gelöscht.

Die Neuregelung ist Teil der überarbeiteten Verhaltensregeln für Wirtschaftsauskunfteien, die im Mai 2024 vom Verband „Die Wirtschaftsauskunfteien e. V." nach Intervention des Hessischen Datenschutzbeauftragten (HBDI), Prof. Dr. Michael Roßnagel, angepasst wurden.

Die Speicherfrist wird auf 18 Monate verkürzt, wenn folgende Bedingungen erfüllt sind:

- Die Forderung wurde innerhalb von 100 Tagen nach Übermittlung an die Schufa ausgeglichen.
- Innerhalb der 18 Monate wurden keine weiteren Negativdaten, wie neue Zahlungsstörungen, gemeldet.
- Es liegen keine Informationen aus dem Schuldnerverzeichnis oder Insolvenzbekanntmachungen vor.

Die neue Regelung soll sicherstellen, dass betroffene Personen, die ihre Forderungen schnell begleichen, ihre Bonität früher wiederherstellen können. Prof. Dr. Roßnagel betonte, dass die Halbierung der Speicherfrist ein zentrales Anliegen war, um die Verhältnismäßigkeit und Fairness im Umgang mit personenbezogenen Daten zu stärken.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat die überarbeiteten Verhaltensregeln zustimmend zur Kenntnis genommen. Die Änderungen gelten ab Januar 2025 und sind ein wichtiger Schritt zur Verbesserung der datenschutzrechtlichen Praktiken von Wirtschaftsauskunfteien.

Foto: svort, Adobe Stock

Bußgeld wegen Verstoßes gegen die Transparenzpflicht

Eine Bank wurde von der Berliner Beauftragten für Datenschutz und Informationsfreiheit mit einem Bußgeld in Höhe von 300.000 Euro belegt, da sie die Transparenzpflichten der DS-GVO bei einer automatisierten Einzelentscheidung missachtet hat.
Der Fall betrifft die automatisierte Ablehnung eines Kreditkartenantrags, bei der die Bank dem Antragsteller keine nachvollziehbaren Gründe für die Entscheidung mitteilte.

Weiter auf DataAgenda lesen

Foto: Johannes, Adobe Stock

Möglicher Datenschutzverstoß durch obligatorischen Gesichtsscan

Die Datenschutzorganisation noyb hat bei der italienischen Datenschutzbehörde (Garante per la Protezione dei Dati Personali – GPDP) eine Beschwerde gegen die Fluggesellschaft Ryanair eingelegt, da die Airline Kunden zwinge, Konten anzulegen und einen Gesichtsscan zur Verifizierung durchzuführen.

Ryanair verletze damit den Grundsatz der Datenminimierung und der freiwilligen Einwilligung, argumentiert noyb. Die verpflichtende Gesichtserkennung wird als besonders invasiv kritisiert, während alternative Verifizierungsmethoden unnötig erschwert würden. noyb fordert die italienische Datenschutzbehörde auf, gegen Ryanair vorzugehen, und verweist auf mögliche hohe Strafzahlungen. Folgende Verfahren werden von noyb im Wesentlichen kritisiert:

1. Obligatorische Kontoerstellung („Zwangskonten"):

- Ryanair zwingt Kunden, ein dauerhaftes Konto zu erstellen, um Flüge auf der Website oder App buchen zu können.
- Diese Praxis widerspricht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO), da ein solches Konto für die Flugbuchung nicht zwingend erforderlich ist.
- Andere Fluggesellschaften wie Lufthansa, easyJet, Air France und Norwegian verlangen keine Kontoerstellung für die Buchung.
- Die erfassten Daten werden in der Regel bis zur Löschung des Kontos gespeichert, was laut noyb selten der Fall ist.

2. Obligatorischer „Verifizierungsprozess" mit Gesichtsscan:

- Ryanair verlangt von Kunden einen „Verifizierungsprozess", bevor sie fliegen können.
- Dieser Prozess bietet theoretisch zwei Optionen, wobei Kunden jedoch praktisch zu einem Gesichtsscanner gedrängt werden.
- Biometrische Daten wie Gesichtsscans sind durch das EU-Recht besonders geschützt.
- Europäische Datenschutzbehörden warnen in der Regel vor „inakzeptabel hohen Risiken" durch Gesichtserkennung.

Weiter auf DataAgenda lesen

Data Agenda Podcast Folge 65: Justizbehörde gegen den Hass im Netz – Wie die ZAC NRW Onlinekriminalität bekämpft

Im Gespräch mit Staatsanwalt Dr. Christoph Hebbecker geht es um die Aufgabe eines Ermittlers gegen Hasskriminalität bei der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen. Das Spektrum der „ZAC NRW" reicht von Kooperationen mit Medienunternehmen und Fußballvereinen bis hin zur Zusammenarbeit mit Anbietern von Onlineplattformen unter der Digital Services Act (DSA). Allen, die sich dafür interessieren, wie zeitgemäße Bekämpfung der digitalen Hasskriminalität erfolgt erfolgen kann und wo deren Herausforderungen liegen, gewährt dieser Podcast Einblicke.
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter