Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

# DSG-Info-Service

Mai 2024 Ausgabe Nr. 112

*Liebe Leserinnen und Leser,*

*die neue Ausgabe der DSG-Info bietet interessanten Lesestoff für das kommende Pfingstwochenende! Der österreichische Datenschutzverein NOYB sorgt mit einer Beschwerde gegen das US-amerikanische KI-Unternehmen OpenAI wieder einmal für Schlagzeilen, der Europäische Datenschutzausschuss (EDSA) hat erneut eine umfangreiche Stellungnahme zur Thematik „Pay or Okay" herausgegeben und das österreichische Cybersicherheitsgesetz befindet sich nun in Begutachtung. Außerdem haben wir für Sie interessante Urteile aus der europäischen und österreichischen Rechtsprechung und wie gewohnt die Top-Bußgelder für datenschutzrechtliche Verstöße zusammengefasst.*

*Viel Spaß bei der Lektüre und bleiben Sie gut informiert!*

*Mag. Judith Leschanz*
*Geschäftsführung*

## 1. Der Kampf gegen falsche Informationen in KI-Systemen: NOYB reicht Beschwerde ein

Die fortschreitende Entwicklung von Künstlicher Intelligenz (KI) ermöglicht eine Vielzahl von Anwendungen in verschiedenen Bereichen, von der Medizin bis hin zur Unterhaltung. Eine der bemerkenswertesten Innovationen auf diesem Gebiet ist ChatGPT, ein leistungsstarker Chatbot des US-Unternehmens OpenAI.

Seit der Einführung im November 2022 hat ChatGPT weltweit Aufsehen erregt und wurde schnell zu einem integralen Bestandteil des täglichen Lebens vieler Menschen. Trotz ihres breiten Anwendungsspektrums sind LL-Modelle wie ChatGPT jedoch nicht fehlerfrei und ihre Ergebnisse gelegentlich problematisch. Dies betrifft auch die Einhaltung gesetzlicher Bestimmungen wie der EU-Datenschutz-Grundverordnung (DSGVO).

Der von Max Schrems gegründete Datenschutzverein NOYB wirft nun OpenAI vor, im Falle einer „Person des öffentlichen Lebens", die von NOYB vertreten wird, falsche Angaben zu persönlichen Daten (in diesem Fall das Geburtsdatum, das nicht öffentlich bekannt ist) zu machen und damit gleich mehrere Betroffenenrechte der DSGVO zu missachten.

Die DSGVO legt klare Richtlinien für den Schutz personenbezogener Daten fest. Unternehmen sind verpflichtet, sicherzustellen, dass die von ihnen verarbeiteten Informationen korrekt sind (Art. 5 Abs. 1 lit. d DSGVO), dass betroffene Personen Auskunft zu ihren Daten, deren Quellen und Empfängern erhalten (Art. 15 DSGVO) und fehlerhafte Daten berichtigt oder gelöscht werden können (Art. 16 und 17 DSGVO).

Trotz dieser klaren gesetzlichen Vorgaben hat OpenAI zugegeben, dass es nicht in der Lage ist, falsche Informationen, die von ChatGPT verbreitet werden, zu korrigieren oder die Herkunft dieser Informationen zu kontrollieren. Diese Tatsache ist nicht nur ein Verstoß gegen das geltende Datenschutzrecht, sondern wirft auch Fragen nach der ethischen Verantwortung von Unternehmen auf, die KI-Systeme entwickeln und einsetzen.

Die Datenschutzorganisation NOYB hat sich der Thematik angenommen, möchte nun gegen OpenAI rechtlich vorgehen und erhob daher Beschwerde[1] bei der österreichischen Datenschutzbehörde: *„Das Erfinden falscher Informationen ist schon für sich genommen höchst problematisch. Aber wenn es um falsche Informationen über Personen geht, kann das ernsthafte Konsequenzen haben.“*, so Maartje de Graaf, Datenschutzjuristin bei NOYB.

Das KI-Unternehmen wehrt sich in einer Stellungnahme gegen die Anschuldigungen und gibt an, es könne zwar alle Anfragen zum Beschwerdeführer blockieren, aber es sei technisch nicht möglich, einzelne Informationen (wie das Geburtsdatum) auszufiltern. NOYB bemängelte auch die unangemessene Reaktion auf das Auskunftsersuchen des Beschwerdeführers, dem eine Kopie über seine Daten, deren Quellen und Empfänger rechtlich zustünden. OpenAI hatte dem Beschwerdeführer zwar die Daten seines Benutzerkontos beauskunftet, nicht aber Angaben zu seiner Person, die sich in der Wissensbasis von ChatGPT befinden. Die Frage ist, ob dies angesichts der Menge an Daten und Verknüpfungen überhaupt möglich ist.

Trotz der Bemühungen einiger Datenschutzbehörden, die rechtlichen Probleme rund um ChatGPT anzugehen, bleibt die Situation vorerst ungelöst. Die italienische Datenschutzbehörde verhängte im März 2023 eine vorübergehende Einschränkung der Datenverarbeitung von ChatGPT[2], die nach der Erfüllung sämtlicher Auflagen wieder aufgehoben wurde. Weiters richtete der Europäische Datenschutzausschuss damals eine Taskforce[3] ein, um die nationalen Bemühungen der Behörden zu koordinieren.

Diese Maßnahmen sind ein wichtiger Schritt in die richtige Richtung, aber es bedarf weiterer Anstrengungen, um sicherzustellen, dass KI-Systeme den rechtlichen Standards der DSGVO entsprechen. Die Zusammenarbeit mit Datenschutzexperten und die Implementierung transparenter Prozesse zur Sicherstellung der Genauigkeit und des Schutzes personenbezogener Daten sind unerlässlich, um den rechtlichen Anforderungen gerecht zu werden und das Vertrauen der Nutzer zu erhalten.

## 2. EDSA gibt Stellungnahme zu „Pay or Okay“-Modellen ab

Am 17. April 2024 veröffentlichte der Europäische Datenschutzausschuss (EDSA) auf Antrag der Datenschutzbehörden der Niederlande, Norwegens und Hamburgs eine Stellungnahme[4]. Der Inhalt der Erklärung betrifft die Legitimität der Einwilligung zur Verarbeitung personenbezogener Daten zu Werbezwecken im Rahmen von „consent or pay“-Modellen, wie sie von vielen großen Online-Plattformen eingesetzt werden. In der Stellungnahme, die von der EDSA-Vorsitzenden Anu Talus präsentiert wurde, wird die Bedeutung einer echten Auswahlmöglichkeit für die Nutzer hervorgehoben. Die derzeitigen Modelle zwingen Individuen häufig dazu, entweder sämtliche Nutzungsdaten freizugeben oder eine Gebühr zu entrichten.

[1] https://kurzlinks.de/uzkt
[2] https://kurzlinks.de/wtdr
[3] https://kurzlinks.de/67x4
[4] https://kurzlinks.de/xn9n

In der Folge stimmen die meisten Nutzer der Datenverarbeitung zu, ohne die vollständigen Auswirkungen ihrer Entscheidung zu begreifen.

Der EDSA ist der Meinung, dass diese Modelle in den meisten Fällen nicht den Anforderungen an eine gültige Einwilligung entsprechen. Dies ist insbesondere dann der Fall, wenn den Nutzern lediglich die Wahl zwischen der Zustimmung zur Datenverarbeitung für verhaltensbezogene Werbezwecke und der Entrichtung einer Gebühr bleibt.

Die Stellungnahme betont, dass diese kostenpflichtige Alternative zur Verarbeitung personenbezogener Daten für Werbezwecke nicht als Standard betrachtet werden sollte. Stattdessen sollten Online-Plattformen in Erwägung ziehen, dem Betroffenen eine „gleichwertige Alternative" anzubieten, die nicht mit einer Gebühr verbunden ist. Diese sollte frei von verhaltensbezogener Werbung sein und weniger oder gar keine personenbezogenen Daten verarbeiten.

Des Weiteren wird betont, dass die Einholung der Einwilligung die Verantwortlichen nicht von der Einhaltung der Grundsätze der Datenschutz-Grundverordnung (Art. 5 DSGVO) entbindet. Insbesondere Zweckbindung, Datenminimierung und Verarbeitung nach Treu und Glauben müssen gewahrt bleiben. Online-Plattformen sind zudem verpflichtet, die Notwendigkeit und Verhältnismäßigkeit ihrer Verarbeitung nachzuweisen.

Der EDSA legt darüber hinaus Kriterien zur Bewertung der Einwilligung in diesen Fällen fest, darunter Konditionalität, Nachteil, Leistungsungleichgewicht und Granularität. Demnach müssen die Verantwortlichen prüfen, ob die Gebühr angemessen ist und ob die Verweigerung der Zustimmung negative Konsequenzen für die betroffene Person nach sich ziehen kann.

Außerdem sieht der EDSA eine Prüfung des Machtungleichgewichts zwischen Individuen und dem Verantwortlichen vor. Faktoren wie die Marktposition der Plattform, die Abhängigkeit der Nutzer von den Diensten und die Zielgruppe der Plattform sollten dabei berücksichtigt werden.

Nun arbeitet der EDSA weiter an Leitlinien für „consent or pay"-Modelle mit breiterem Anwendungsbereich und wird eine enge Zusammenarbeit mit Interessenträgern anstreben, um ein ausgewogenes und rechtskonformes Vorgehen sicherzustellen.

## 3. Grünes Licht für das NIS-2-Begutachtungsverfahren

Am 3. April 2024 hat die österreichische Regierung das Cybersicherheitsgesetz zur europäischen NIS-2-Richtlinie zur Begutachtung[5] vorgelegt. Die Richtlinie soll sicherstellen, dass Unternehmen und öffentliche Einrichtungen, die wichtige Dienste für wirtschaftliche oder gesellschaftliche Aktivitäten bereitstellen, auf potenzielle Cyberbedrohungen vorbereitet sind und angemessen auf Vorfälle reagieren können. Diese Richtlinie betrifft eine breite Palette von Akteuren[6], einschließlich Gebietskörperschaften, Vereine und insbesondere tausende Unternehmen. Waren bisher ca. 100 österreichische Unternehmen betroffen, dürften es mit dem neuen Gesetz 4.000 bis 7.000 werden.

Das vorgeschlagene Gesetz, das bis zum Oktober 2024 umgesetzt werden muss, verpflichtet die Akteure, angemessene Maßnahmen zur Cybersicherheit zu ergreifen. Vor allem Unternehmen, die als Teil der kritischen Infrastruktur gelten (zB Energie-, Wasser-, Stromversorgung)

[5] https://kurzlinks.de/7nwp

[6] https://kurzlinks.de/ibk5

sowie Einrichtungen auf Bundesebene müssen umfassende IT-Sicherheitsvorkehrungen implementieren.

Darüber hinaus sind sie angehalten, Cybersicherheitsvorfälle an eigens dafür geschaffene Meldestellen zu melden. Damit zielt die Gesetzgebung darauf ab, die Resilienz gegenüber modernen Cyberbedrohungen zu stärken und die Reaktionsfähigkeit auf Angriffe zu verbessern. Um Unternehmen bei ihren Anliegen und Fragen zu unterstützen, hat das Innenministerium eine Servicestelle für Cybersicherheit eingerichtet und Interessensvertretungen wie die Industriellenvereinigung, die Wirtschaftskammer sowie die Bundesländer in den Gesetzgebungsprozess eingebunden.

In unserer DSG-Info Ausgabe Nr. 108[7] haben wir die wichtigsten Inhalte der europäischen Verordnung unter die Lupe genommen – ein Blick lohnt sich auf jeden Fall!

## 4. Neues aus der Rechtsprechung

**TC-String als personenbezogenes Datum eingestuft**

Am 7. März 2024 hat der Europäische Gerichtshof (EuGH) im Rahmen eines Vorabentscheidungsverfahrens eine wegweisende Entscheidung (C-604/22)[8] getroffen, die erhebliche Auswirkungen auf die Online-Werbeindustrie hat. Das Urteil betrifft das „Transparency and Consent Framework“ (TCF) des Interactive Advertising Bureau (IAB) Europe und stellt fest, dass der TC-String als personenbezogenes Datum anzusehen ist.

Das IAB Europe ist ein Verband, der Unternehmen der digitalen Werbe- und Marketingindustrie auf europäischer Ebene vertritt. Seine Mitglieder, darunter Medien- und Technologieunternehmen, nutzen das TCF, um Einwilligungen für die Erhebung und Verarbeitung von Daten zu verwalten. Das TCF bietet einen Standard für die Abfrage und Übermittlung von Nutzereinwilligungen.

Dabei wird ein „Transparency and Consent String“ (TC-String) generiert, der die Einwilligungspräferenzen des Nutzers kodiert. Dieser TC-String wird von den Mitgliedsunternehmen des IAB Europe genutzt, um personalisierte Werbung auszuspielen. Neben dem TC-String wird auch ein Cookie – euconsent-v2 – auf dem Gerät des Nutzers hinterlegt.

Die belgische Datenschutzbehörde hatte zuvor festgestellt, dass die Speicherung des TC-Strings in Verbindung mit der IP-Adresse des Nutzers gegen die DSGVO verstößt. Das EuGH bestätigte diese Ansicht und stellte fest, dass der TC-String ein personenbezogenes Datum im Sinne der DSGVO ist. Laut EuGH enthält der TC-String benutzerspezifische Einstellungen, die wenn sie mit anderen Identifikatoren wie IP-Adressen verknüpft werden, zur Identifizierung einer bestimmten Person führen können.

Darüber hinaus sieht der EuGH das IAB Europe und seine Mitglieder als gemeinsame Verantwortliche für die im Rahmen des TCF verarbeiteten Daten an. Dies bedeutet, dass sie Vereinbarungen hinsichtlich ihrer gemeinsamen Verantwortlichkeit abschließen müssen.

Das Urteil hat weitreichende Konsequenzen für Unternehmen, die das TCF nutzen. Es wird erwartet, dass erhebliche Änderungen bei der Einholung von Einwilligungen und der Generierung des TC-Strings erforderlich sind.

[7] https://kurzlinks.de/tmy4

[8] https://kurzlinks.de/5tn4

**Nationale Datenschutzaufsichtsbehörden dürfen die Löschung unrechtmäßiger Daten anordnen**

Der Europäische Gerichtshof hat mit einem Urteil vom 14. März 2024 (C-46/23)[9] eine bedeutende Entscheidung getroffen, die die Befugnisse nationaler Datenschutzaufsichtsbehörden betrifft. In einem Vorabentscheidungsverfahren eines ungarischen Gerichts wurde klargestellt, dass diese Behörden die Löschung unrechtmäßig verarbeiteter personenbezogener Daten auch ohne Antrag der betroffenen Person anordnen dürfen.

Das Urteil bezieht sich auf einen Fall in Ungarn, bei dem die Verwaltung Újpest personenbezogene Daten im Rahmen eines Covid-19-Unterstützungsprogramms erhoben hatte. Die ungarische Datenschutzaufsichtsbehörde stellte daraufhin fest, dass die Verarbeitung der Daten gegen die Datenschutzgrundsätze verstieß und ordnete die Löschung an, obwohl keine entsprechenden Anträge betroffener Personen vorlagen.

Ein langwieriger Streit um die Auslegung der Datenschutzgrundverordnung (DSGVO) in Ungarn, an dem verschiedene Gerichte und Behörden beteiligt waren, war die Folge. Er drehte sich um die Frage, ob die Löschung unrechtmäßiger Daten nur auf Antrag der betroffenen Person erfolgen darf. Der Europäische Gerichtshof entschied nun, dass nationale Datenschutzaufsichtsbehörden unabhängig von solchen Anträgen handeln können.

Das Urteil unterstreicht die Rolle der nationalen Datenschutzaufsichtsbehörden bei der Gewährleistung der Einhaltung der DSGVO. Der EuGH hält es *„von besonderer Bedeutung, dass die Aufsichtsbehörde über wirksame Befugnisse verfügt, um wirksam gegen Verletzungen dieser Verordnung vorzugehen und insbesondere, um solche Verletzungen zu beenden, und zwar auch in den Fällen, in denen die betroffenen Personen nicht über die Verarbeitung ihrer personenbezogenen Daten informiert wurden, ihnen diese nicht bekannt ist oder sie jedenfalls die Löschung dieser Daten nicht beantragt haben.“*

**Unternehmen haften für Handlungen ihrer Mitarbeiter bei Datenschutzverletzungen**

In einem Urteil vom 11. April 2024 (C-741/21)[10] hat der Europäische Gerichtshof (EuGH) entschieden, dass der Verantwortliche für die Handlungen seiner Mitarbeiter haftet, selbst wenn das Unternehmen über Richtlinien zur Einhaltung des Datenschutzes verfügt.

In dem Fall ging es um einen Kunden des Verantwortlichen, der seine Einwilligung zur Direktwerbung widerrufen hatte. Trotzdem schickte der Verantwortliche weiterhin Postwerbung, was zur Klage auf Schadenersatz gemäß Art. 82 DSGVO vor dem Landgericht Saarbrücken führte.

Der Kläger machte geltend, dass der Verantwortliche seine personenbezogenen Daten unrechtmäßig verarbeitet und damit seine Rechte aus Art. 8 der Grundrechte-Charta verletzt habe. Er forderte sowohl materiellen als auch immateriellen Schadenersatz.

Die Entscheidung des EuGH, die sich auf Fragen des Landgerichts Saarbrücken stützt, stellt klar, dass sich ein Verantwortlicher nicht allein damit seiner Haftung entziehen kann, dass der Schaden durch das Fehlverhalten eines Mitarbeiters (iSv Art. 29 DSGVO) verursacht wurde. Die Haftung für Handlungen von Mitarbeitern fällt unter die „Haftung für fremdes Verschulden“, da Unternehmen (soweit sie keine Einzelunternehmen sind) durch ihre Mitarbeiter handeln. Ob die Handlungen im Rahmen vertraglicher Verpflichtungen („Erfüllungsgehilfenhaftung“) oder außerhalb davon („Besorgungs-

[9] https://kurzlinks.de/1t1e

[10] https://kurzlinks.de/u5lx

gehilfenhaftung“) erfolgen, ist nur für die Bestimmung des zivilrechtlichen Haftungsumfangs relevant, nicht aber für Schadenersatzansprüche aus dem Datenschutz. Der Verantwortliche (oder Auftragsverarbeiter) haftet nur dann nicht, „*wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist*“ (Art. 82 Abs. 3 DSGVO).

Das EuGH-Urteil verschiebt damit die Beweislast auf die Unternehmen, die umfassende Kontrollmaßnahmen, einschließlich Audits und die Überprüfung der Einhaltung angemessener Vorgaben, nachweisen müssen, um die Haftung zu mindern.

**BVwG mindert DSB-Strafe in E-Mail-Marketing-Fall**

Das österreichische Bundesverwaltungsgericht (BVwG) hat sich kürzlich mit einem Fall von E-Mail-Marketing befasst und eine ursprünglich von der Datenschutzbehörde verhängte Strafe von 4 Millionen Euro auf nur EUR 50.000,- reduziert (Entscheidung vom 26. März 2024, W 1372241630-1/48E).

In dem Fall ging es um eine Bank, die aufgrund des Fehlers eines Mitarbeiters eine Tabelle mit persönlichen Daten von fast 6.000 Kunden per E-Mail an 234 Personen verschickte. Die Datenschutzverletzung wurde der Datenschutzbehörde umgehend gemeldet und es wurden sofort Maßnahmen zur Minimierung des Schadens ergriffen, einschließlich der Anweisung an die Empfänger, die E-Mail zu löschen und die Löschung zu bestätigen.

Obwohl das BVwG die Feststellung der Datenschutzbehörde bestätigte, dass ein Verstoß gegen die DSGVO vorliegt, hielt es die ursprüngliche Strafe für überzogen. Das Gericht sah das proaktive Handeln der Bank, die Kooperation während des Verfahrens und die Maßnahmen zur Schadensminimierung als mildernde Umstände an. Insbesondere hob das BVwG die schnelle Reaktion der Bank nach Entdeckung des Vorfalls hervor, einschließlich der Pseudonymisierung der Daten und der Information der Aufsichtsbehörden.

Eine wichtige rechtliche Feststellung des BVwG betraf aber auch die Haftung der Bank als juristische Person. Es wurde erneut festgehalten, dass Bußgelder gegen Unternehmen auch verhängt werden können, wenn keine direkte Kenntnis oder Beteiligung der Geschäftsleitung vorliegt.

**EUGH genehmigt die Vorratsdatenspeicherung von IP-Adressen zu Zwecken der Durchsetzung von Urheberrechten**

In einem kürzlich ergangenen Urteil hat der Europäische Gerichtshof (EuGH) den Anwendungsbereich der Vorratsdatenspeicherung erweitert. Das Urteil erlaubt den Mitgliedstaaten das anlasslose Protokollieren von IP-Adressen zur Durchsetzung von Urheberrechten unter der Bedingung, dass die Privatsphäre der Betroffenen gewahrt bleibt. Das Gericht entschied, dass die Vorratsspeicherung von IP-Adressen nicht zwangsläufig einen schwerwiegenden Eingriff in die Grundrechte darstellt, sofern die nationalen Vorschriften eine strikte Trennung der verschiedenen Kategorien personenbezogener Daten vorsehen.

Der Fall betrifft Frankreichs Three-Strikes-System der Behörde Hadopi, die für die Durchsetzung des Urheberrechts im Internet zuständig ist. Hierbei erhalten Nutzer, die einer Urheberrechtsverletzung verdächtigt werden, zwei Verwarnungen, bevor beim dritten Verstoß rechtliche Schritte eingeleitet werden. Um den Täter zu ermitteln, muss Hadopi jedoch auf mit IP-Adressen verbundene Identitätsdaten zugreifen.

Das Dekret der französischen Regierung, das Hadopi den Zugang zu Identitätsdaten über IP-Adressen ermöglicht, wurde von Bürgerrechtsorganisationen wie La Quadrature du Net (LQDN) vor dem EuGH angefochten. Das Gericht sollte feststellen, ob eine solche Datener-

hebung und automatische Verarbeitung ohne vorherige gerichtliche Kontrolle mit dem EU-Recht vereinbar sind.

In seinem Urteil in der Rechtssache C-470/21[11] unterstreicht der EuGH, dass der Zugriff auf Daten nicht gerichtlich kontrolliert werden muss, wenn der Eingriff in die Grundrechte nicht als schwerwiegend anzusehen ist. Zum Beispiel kann das durch die strikte Trennung verschiedener Informationen und ein Verbot der Offenlegung von Dateiinhalten durch Mitarbeiter erreicht werden. Dennoch kann eine eingehende Prüfung erforderlich sein, wenn die Verknüpfung von Daten private Informationen offenbaren könnte.

**Tesla-Fahrer können wegen Autokameras für Datenschutzverletzungen haften**

Das BVwG hat vor kurzem eine wichtige Entscheidung getroffen, die Tesla-Fahrer und Fahrzeugbesitzer mit ähnlichen Überwachungssystemen in die Pflicht nimmt. Der Betrieb des sogenannten „Wächter-Modus", der Aktivitäten in der Nähe des Fahrzeugs aufzeichnet, kann einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO) darstellen, selbst wenn keine Aufnahmen gespeichert werden.

Der Fall begann damit, dass ein Passant das Blinken der Scheinwerfer eines geparkten Tesla bemerkte und feststellte, dass der Überwachungsmodus aktiviert war. Dieser Sachverhalt führte zu einem Beschwerdeverfahren vor der DSB (6. 7. 2022, Zl. D124.0655/22 2022-0.456.377) und später dem BVwG, welches nun am 4. 4. 2024 (GZ: W214 2259197-1/14E)[12] entschieden hat.

Obwohl im „Wächter-Modus" keine Aufzeichnung gemacht wurde, registrierten die Kameras des Fahrzeugs alle Bewegungen in der Umgebung. Das BVwG betonte, dass bereits die Beobachtung der Umgebung eine Datenverarbeitung darstellt und somit die Informationspflicht nach Art. 13 DSGVO auslöst. Diese Begründung verdeutlicht die weite Definition des Art. 4 Z 2 DSGVO. Das BVwG entschied außerdem, dass der Fahrzeughalter als Verantwortlicher anzusehen ist, da dieser die Entscheidung getroffen hat, den „Wächter-Modus" zu aktivieren.

Für Fahrzeughalter bedeutet dies, dass sie sich darüber im Klaren sein müssen, dass der Betrieb des Überwachungsmodus datenschutzrechtliche Verpflichtungen auslöst. Sie sollten ihn nur aktivieren, wenn es aufgrund der Situation erforderlich erscheint. Außerdem sind sie verpflichtet, Passanten durch ein gut sichtbar positioniertes Hinweisschild über die Bilderfassung zu informieren.

## 5. Top 3-Bußgelder

**Online-Händler missachtet Speicherbegrenzung[13]**

Ein Online-Händler wurde mit einer Geldbuße in der Höhe von EUR 856.000,00 wegen eines Verstoßes gegen Art. 5 Abs. 1 lit. e und Art. 25 Abs. 2 DSGVO von der finnischen Aufsichtsbehörde bestraft. Grund war, dass er seine Kunden dazu verpflichtete, für Bestellungen ein Kundenkonto einzurichten. Eine Option, als Gast zu bestellen, war nicht vorhanden. Der Händler machte außerdem keine Angaben, wie lange die Kontodaten gespeichert werden; wenn der Kunde ihre Löschung nicht verlangte, blieben sie auf unbestimmte Zeit gespeichert.

[11] https://kurzlinks.de/bcsv
[12] https://kurzlinks.de/7w6y
[13] https://kurzlinks.de/2mcr

Die finnische Aufsichtsbehörde ordnete zusätzlich zur Geldbuße an, dass eine angemessene Aufbewahrungsfrist festgelegt und die Verpflichtung zur Erstellung eines Kundenkontos aufgehoben werden muss. Der Online-Händler kündigte an, gegen die Entscheidung Rechtsmittel einzulegen.

**Fehlende TOM führen zu hoher Strafe**[14]

Die spanische Datenschutzbehörde Agencia Española de Protección de Datos (AEPD) hat eine Beratungsfirma mit einem Bußgeld von EUR 145.000,00 bestraft. Aus deren Büroräumen war ein Rucksack gestohlen worden, der einen USB-Stick mit unverschlüsselten, sensiblen Daten zu einem strafrechtlichen Gerichtsverfahren enthielt.

Die Sicherheitsmaßnahmen der Firma wurden als unzureichend bewertet. Die Daten waren nicht durch ein Passwort geschützt, wozu sie verpflichtet gewesen wäre. Wegen Verstößen gegen Art. 5 Abs. 1 lit. f DSGVO und Art. 32 Abs. 1 DSGVO verhängte die AEPD zwei Bußgelder in Höhe von EUR 90.000,- und EUR 55.000,-

**Bußgeld wegen unzureichender Datensicherheit**[15]

Die griechische Datenschutzbehörde hat ein Bußgeld von EUR 175.000,- gegen das Ministerium für Einwanderung und Asyl verhängt. Auf den Ägäischen Inseln werden zur Überwachung von Drittstaatsangehörigen die Systeme „Hyperion“ und „Centaurus“ eingesetzt. „Centaurus“ verarbeitet Bilddaten von Kameras und Drohnen und erstellt Verhaltensanalysen mittels künstlicher Intelligenz. „Hyperion“ nutzt RFID-Kennung und Fingerabdruck zur Zutrittskontrolle.

Nach einer Überprüfung stellte die griechische Datenschutzbehörde fest, dass die Datenschutz-Folgenabschätzungen des Ministeriums unvollständig waren und ein Verstoß gegen Art. 9 DSGVO vorlag. Außerdem gab es bei der Implementierung der Systeme schwerwiegende Versäumnisse in Bezug auf die Bestimmungen der Datenschutz-Grundverordnung. Die Einhaltung technischer Sicherheitsmaßnahmen ist insbesondere bei der Verarbeitung biometrischer Daten wichtig.

••••

## Save the Date

**Save the Date – Datenschutzseminar:**

Unser nächstes Datenschutzseminar findet am **11. und 12. Nov. 2024** im Vienna Hilton Plaza statt.

Wir freuen uns auf Ihre Anmeldung.

**Save the Date – Privacy Ring:**

Der Datenschutzverein Privacy Ring[16] lädt am **19. September 2024** zur inzwischen 12. Fachtagung in Wien im Campus der Universität Wien ein. Diesmal steht das Spannungsverhältnis zwischen Transparenzverpflichtungen und dem Datenschutz im Fokus.

Im Anschluss werden mit verschiedenen Expertinnen und Experten aus der Wirtschaft und dem öffentlichen Wesen eine Podiumsdiskussion sowie ein Get-together abgehalten.

[14] https://kurzlinks.de/f3h7
[15] https://kurzlinks.de/a0l3
[16] https://www.privacy-ring.uni-hannover.de/de/