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

März 2024 Ausgabe Nr. 111

Liebe Leserinnen und Leser,

in der aktuellen Ausgabe unserer DSG-Info nehmen wir die jüngsten Entwicklungen im Bereich des Datenschutzes und der Künstlichen Intelligenz (KI) unter die Lupe. Ein besonderer Schwerpunkt liegt dabei auf das neu verabschiedete KI-Gesetz und möglichen Parallelen zur DSGVO.

Im nächsten Abschnitt widmen wir uns interessanten Fällen aus der Rechtsprechung, die nähere Einblicke in die praktische Umsetzung datenschutzrechtlicher Vorschriften erlauben. Außerdem richten wir unser Augenmerk auf die jüngsten Top-Bußgelder für Datenschutzverletzungen. Schließlich wollen wir auf unsere Datenschutz-Seminare hinweisen, die am 8. und 9. April stattfinden und ganz aktuelle Themen wie den soeben verabschiedeten AI-Act behandeln.

Wir hoffen, dass Sie diese Ausgabe ebenso informativ wie inspirierend finden und freuen uns auf Ihr Feedback und Ihre Gedanken zu den diskutierten Themen.

Viel Spaß bei der Lektüre wünscht

Mag. Judith Leschanz
Geschäftsführung

1. Newsmeldungen

KI-Gesetz beschlossen![1]

Nach knapp drei Jahren intensiver Debatten und Verhandlungen wurde am 13. März 2024 das KI-Gesetz (AI-Act) von den Abgeordneten des Europäischen Parlaments in Straßburg mit großer Mehrheit verabschiedet[2]. Für die einen stellt dieser Schritt ein historisches Ereignis dar, das die EU zum Pionier auf dem Gebiet der künstlichen Intelligenz macht. Kritiker bemängeln dagegen die vielen Ausnahmetatbestände im Regelwerk.

Vor allem die Bestimmungen über den Einsatz von biometrischer Massenüberwachung wurden im Trilog hitzig diskutiert. Diese Technologie ermöglicht das Scannen von Gesichtern im öffentlichen Raum, um die Identität der Betroffenen zu ermitteln. Das EU-Parlament wollte diese Praxis gänzlich verbieten, der EU-Rat sah sie im ursprünglichen Entwurf sogar als Präventivmaßnahme vor. Der schließlich gefundene Kompromiss sieht eine Erlaubnis für Strafverfolgungsbehörden vor, die jedoch davor eine Grundrechte-Folgenabschätzung durchführen

[1] https://digital-strategy.ec.europa.eu/de/policies/regulatory-framework-ai

[2] https://kurzelinks.de/u98o

und die Maßnahme in einer EU-Datenbank registrieren müssen. Bei entsprechender Begründung kann dies auch im Nachhinein erfolgen.

Die Verordnung tritt 20 Tage nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft und wird nach Ablauf von 24 Monaten in ihrer Gesamtheit uneingeschränkt anwendbar sein. Die Bestimmungen über verbotene KI-Praktiken werden bereits sechs Monate nach Inkrafttreten der Verordnung wirksam. Zusätzlich werden Verpflichtungen für Hochrisikosysteme erst 36 Monate nach Inkrafttreten bindend. In der Praxis bedeutet dies, dass ab dem Jahr 2026 Sanktionen für Verstöße gegen die Verordnung verhängt werden können.

Ebenfalls im Februar kündigte die Europäische Kommission die Einrichtung eines Europäischen KI-Büros[3] an. Das Büro soll sich für die Unterstützung und den verantwortungsbewussten Einsatz von vertrauenswürdiger KI engagieren, indem es parallel eine Schutzstrategie sowohl für Wirtschaftstreibende als auch Konsumenten gegenüber den Risiken der KI ausarbeitet.

Als integrierte Einrichtung der Europäischen Kommission fungiert das KI-Büro als Expertenhub für künstliche Intelligenz und bildet die Basis eines harmonisierten Steuerungssystems für KI in der gesamten Europäischen Union. Das Ziel ist, einheitliche, schlüssige und effiziente Strategien für den Umgang mit KI auf globaler Ebene zu formulieren, wobei ein internationaler, die EU-Grenzen überschreitender Ansatz verfolgt wird.

Die DSGVO und das KI-Gesetz bestehen nebeneinander, haben aber gemeinsame Schnittstellen. Diese ergeben sich, wenn auf der Entwicklungsebene personenbezogene Daten verwendet werden, beispielsweise für das Trainieren der KI, oder beim Echt-Einsatz, wenn personenbezogene Daten direkt verarbeitet werden (zB Müdigkeitserkennung von Autofahrern). Nur im Fall der Verarbeitung von anonymen, technischen oder synthetischen Daten kommt es zur alleinigen Anwendung des KI-Gesetzes.

KI-VO und die DSGVO

Im folgenden Abschnitt wollen wir Ihnen die Parallelität einiger Bestimmungen und Anforderungen der DSGVO und des KI-Gesetzes präsentieren. Diese Wechselwirkung wird vor allem für Datenschutzbeauftragte von Interesse sein, wenn es um die Umsetzung und Überwachung dieser Normen geht.

Beide Regelwerke basieren auf vergleichbaren Abläufen und zielen darauf ab, dieselben Grundrechte und Freiheiten zu sichern:

- Die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA), wie sie in **Art. 35 der Datenschutz-Grundverordnung** (DSGVO) festgelegt ist, erfährt im KI-Gesetz eine nähere Ausgestaltung. Diese betrifft insbesondere medizinische Fachkräfte, die personenbezogene Daten von Patienten mittels KI-Systemen verarbeiten. Gemäß KI-Gesetz sind Betreiber von als Hochrisiko eingestuften KI-Systemen – in diesem Kontext speziell Ärzte – angehalten, bei der Durchführung einer Datenschutz-Folgenabschätzung die dem System beiliegende Gebrauchsanweisung zu integrieren. Diese Gebrauchsanweisung muss als integraler Bestandteil des Prozesses herangezogen werden und alle notwendigen Informationen gemäß **Art. 13 Abs. 3 KI-VO** umfassen. Die darin enthaltenen detaillierten Angaben sind essenziell, um eine umfassende Bewertung der Datenschutzrisiken vorzunehmen, die mit dem KI-Einsatz in der medizinischen Praxis verbunden sind. Durch die Bereitstellung dieser Informationen sollen Transparenz geschaffen und die Einhaltung der daten-

[3] https://kurzelinks.de/8l9h

schutzrechtlichen Vorgaben sichergestellt werden, um den Schutz personenbezogener Patientendaten im Einklang mit den gesetzlichen Anforderungen zu gewährleisten.

- **Art. 15 KI-VO** bestimmt, dass KI-Systeme, die ein hohes Risiko darstellen, unter Berücksichtigung der Prinzipien der Genauigkeit, Robustheit und Cybersicherheit entworfen und entwickelt werden müssen. Ziel ist, dass diese Systeme ein angemessenes Sicherheitsniveau während ihres gesamten Einsatzzeitraums gewährleisten. Hierdurch werden spezifische Anforderungen an die Gestaltung der Sicherheit („Security by Design and by Default“) standardmäßig etabliert.

  Diese spezifischen Voraussetzungen übertreffen in Teilen die in **Art. 32 DSGVO** definierten technischen und organisatorischen Sicherheitsmaßnahmen (TOM). Daher kann es erforderlich sein, die nach der DSGVO eingeführten Sicherheitsvorkehrungen durch zusätzliche Maßnahmen zu stärken, die von der KI-Verordnung vorgegeben werden, um die Integrität und Sicherheit der KI-Systeme zu garantieren.

Auch wenn die Umsetzung der Verordnung in die Praxis noch offene Fragen birgt, kann ein etabliertes Managementsystem Unternehmen dabei helfen, ihre Risiken effektiv zu minimieren. Insbesondere bei Firmen, die bereits ein Datenschutzmanagementsystem (DSMS) umgesetzt haben, ergeben sich zahlreiche Parallelen in Bezug auf dokumentierte Informationen, Abläufe, Strukturen und Zuständigkeiten. Dies verschafft ihnen nicht nur bei der Einhaltung des neuen KI-Gesetzes Vorteile. Unternehmen, die bereits ein solides DSMS implementiert haben, können den neuen Regelungen der KI-VO mit mehr Zuversicht begegnen – ein überzeugendes Argument für Datenschutzbeauftragte, um die Verantwortlichen verstärkt zur Beschäftigung mit einem Datenschutzmanagementsystem zu bewegen.

Das KI-Gesetz tritt zwanzig Tage nach der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft und wird generell mit einer **Übergangsfrist von 24 Monaten** angewendet. Zu beachten sind jedoch einige unterschiedliche Übergangsfristen: Sechs Monate für die in der Verordnung festgelegten Verbote, zwölf Monate für die Bestimmungen zu allgemein verwendbaren KI (General Purpose AI) und 36 Monate für die in Anhang II aufgelisteten Hochrisiko-Systeme.

2. Neues aus der Rechtsprechung

Die österreichische Datenschutzbehörde verhängt Geldstrafe gegen Unternehmen wegen Verletzung der Meldepflicht[4]

Die österreichische Datenschutzbehörde (DSB) hat eine Geldstrafe in Höhe von EUR 5.900 gegen ein Unternehmen verhängt, weil es eine Datenschutzverletzung nicht ordnungsgemäß gemeldet hatte. Die Strafe wurde verhängt, nachdem das Unternehmen die DSB erst mehr als einen Monat nach dem Vorfall über einen Ransomware-Angriff informiert hatte.

Nach Ansicht der Datenschutzbehörde war die Benachrichtigung des Unternehmens über die Datenschutzverletzung zu allgemein gehalten und enthielt keine der wichtigen Informationen, die nach Art. 33 DSGVO erforderlich sind.

Der Verantwortliche hatte es nicht nur versäumt, die Sicherheitsverletzung innerhalb des

[4] Siehe dazu: https://kurzelinks.de/n2d1

vorgeschriebenen Zeitrahmens von 72 Stunden zu melden, sondern auch unvollständige Angaben zur Art der Sicherheitsverletzung, zu den Kategorien der betroffenen Personen und zu den Maßnahmen erteilt, die zur Behebung der Sicherheitsverletzung und zur Minderung ihrer Auswirkungen ergriffen wurden.

Nachdem das Unternehmen auf weitere Anfragen keine klaren Antworten gegeben hatte, leitete die Datenschutzbehörde ein Bußgeldverfahren ein. Trotz mehrfacher Aufforderungen arbeitete das Unternehmen nicht mit der Datenschutzbehörde zusammen und verstieß damit gegen Art. 31 DSGVO.

Darüber hinaus hat die Datenschutzbehörde festgestellt, dass das Unternehmen keine ordnungsgemäße Risikobewertung durchgeführt hatte, um festzustellen, ob die betroffenen Personen benachrichtigt werden mussten, wie es in Art. 34 DSGVO vorgegeben ist.

OLG Stuttgart: Direktmarketing auch ohne Einwilligung zulässig[5]

Das Landgericht Stuttgart hat in einem Urteil vom 25. Februar 2022 (Az. 17 O 807/21) einige wichtige Fragen rund um das Thema Brief- und Postwerbung behandelt. In der Entscheidung ging es unter anderem um die Rechtmäßigkeit postalischer Werbung basierend auf einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO sowie um die Möglichkeit, personenbezogene Daten in einer Blacklist zu speichern, um den Widerspruch gegen diese Werbung umzusetzen.

In dem Fall hatte der Kläger Schadenersatz eingeklagt, weil seine öffentlich zugängliche Anschrift ohne seine Einwilligung zu Zusendung postalischer Werbung verwendet wurde. Die Werbung wurde von einem Dienstleister versendet, der für verschiedene Werbetreibende tätig war. Der Kläger verlangte die Löschung seiner Daten gemäß Art. 17 DSGVO und forderte Auskunft über deren Verwendung.

Das Landgericht wies die Klage ab und sah keinen Verstoß gegen die DSGVO. Die Zusendung der Werbeschreiben und die damit verbundene Verarbeitung der Adressdaten waren nach Ansicht des Gerichts rechtmäßig gemäß Art. 6 Abs. 1 lit. f DSGVO. Die Beklagte könne ihre Interessen und die Interessen ihrer Kunden an der Werbemaßnahme als berechtigte Interessen im Sinne der DSGVO anführen. Auch eine Datenverarbeitung zur Umsetzung von Werbewidersprüchen sei nach Art. 6 Abs. 1 lit. c DSGVO gerechtfertigt.

Der Kläger hat dagegen Berufung eingelegt, die mit Beschluss des OLG Stuttgart (Az. 2 U 63/22) vom 2. Februar 2024 als offensichtlich unbegründet zurückgewiesen wurde. Der Beschluss bestätigt, dass das Landgericht Stuttgart in seinem Beschluss überzeugend dargelegt hat, dass sowohl die Erhebung der öffentlich zugänglichen Daten als auch die Verarbeitung für die Zusendung des Werbeschreibens gemäß Art. 6 Abs. 1 Satz 1 lit. f DSGVO rechtmäßig erfolgten. Es wird betont, dass für die Rechtmäßigkeit von Direktwerbung nicht zwingend eine bestehende Kundenbeziehung erforderlich ist. Vielmehr wurde unter Berufung auf Erwägungsgrund 47 der DSGVO klargestellt, dass Direktwerbung als berechtigtes Interesse anerkannt ist. Das Gericht hob hervor, dass sämtliche rechtlichen, wirtschaftlichen oder ideellen Interessen als berechtigte Interessen im Sinne des Gesetzes anzusehen sind.

Des Weiteren wurde festgestellt, dass die Verarbeitung der personenbezogenen Daten erforderlich war. Obwohl der Kläger argumentierte, dass die Werbung auch auf elektronischem Wege hätte versendet werden können, wies das Gericht darauf hin, dass die Versendung von E-Mails ohne ausdrückliche Einwilligung als unzumutbare Belästigung und stärke-

[5] Siehe auch: https://kurzelinks.de/ehqk

rer Eingriff in die Grundrechte[6] anzusehen ist. Die Zusendung eines Briefes wird dagegen als zulässig betrachtet.[7]

Das OLG wog die Interessen der Parteien ab und kam zu dem Schluss, dass die Interessen des Klägers nicht die der Beklagten überwogen. Dass der Kläger keine Werbung erhalten will, reicht allein nicht aus, um ein Überwiegen seiner Interessen zu begründen. Erst wenn er Widerspruch iSd Art. 21 Abs. 2 DSGVO erhebt, ist die künftige Direktwerbung unzulässig.

EuGH entscheidet über Entschädigung bei Datenschutzverletzungen

In einem kürzlich ergangenen Urteil hat der EuGH über die Voraussetzungen für die Geltendmachung von Schadenersatz für immaterielle Schäden gemäß Art. 82 DSGVO infolge von Datenschutzverletzungen entschieden.[8]

In dem Fall ging es um einen Verbraucher, der beim Kauf eines Haushaltsgeräts eine Datenschutzverletzung erlitt. Personenbezogene Daten, darunter der Name des Verbrauchers, seine Adresse und seine Bankverbindung, wurden von Mitarbeitern des Händlers versehentlich an einen Dritten weitergegeben. Obwohl die Datenschutzverletzung innerhalb kurzer Zeit behoben wurde, verlangte der Verbraucher Schadensersatz nach Art. 82 Abs. 1 DSGVO und machte einen immateriellen Schaden und potenzielle Risiken im Zusammenhang mit dem Verlust der Kontrolle über seine personenbezogenen Daten geltend.

Der EuGH befasste sich in dem Fall mit mehreren vom vorlegenden Gericht aufgeworfenen Schlüsselfragen. Er stellte klar, dass ein Kläger die negativen Folgen (Schäden) einer Datenschutzverletzung nachweisen muss, um Schadenersatz zu fordern. Der bloße Verstoß gegen die DSGVO-Bestimmungen reicht dazu nicht aus.

Der EuGH stellte außerdem fest, dass die Befürchtung eines möglichen Datenmissbrauchs nicht ausreicht, um Ersatz für immaterielle Schäden zu verlangen. Der Kläger muss eine begründete Furcht und ein tatsächliches Risiko des Missbrauchs seiner personenbezogenen Daten nachweisen.

Die Schwere des Verstoßes hat keinen direkten Einfluss auf die Entschädigung. Ihre Höhe richtet sich ausschließlich nach dem konkreten Schaden, den der Kläger erlitten hat. Die Entschädigung nach Art. 82 DSGVO hat ausgleichende und keine strafende Funktion.

Das Urteil des EuGH stellt die Bedingungen für die Geltendmachung von Schadenersatz für immaterielle Schäden infolge von Datenschutzverletzungen klar: Die Kläger müssen einen tatsächlichen Schaden nachweisen, um eine Entschädigung gemäß Art. 82 DSGVO zu erhalten. Darüber hinaus unterstreicht das Urteil die Bedeutung des Datenschutzes und die Verantwortung für den Schutz der personenbezogenen Daten.

OLG Düsseldorf entscheidet über Bestellbuttons bei Facebook und Instagram[9]

Der 20. Zivilsenat des Oberlandesgerichts Düsseldorf hat am 8. Februar 2024 einem Antrag teilweise stattgegeben, der sich mit Bestellbuttons auf Facebook und Instagram befasst. Das Urteil zur Unterlassungsklage, die von der Verbraucherzentrale Nordrhein-Westfalen e.V. eingereicht wurde, untersagt der Meta Platforms Ireland Limited (Meta), den Bestellprozess für die kostenpflichtige werbefreie Nutzung ihrer sozialen Netzwerke Facebook und Instagram zu gestalten, ohne dass auf dem

[6] EuGH, Urteil vom 4. Juli 2023 – C-252/21, Rn. 108, https://kurzelinks.de/nvfr

[7] BGH, Urteil vom 30. April 1992 – I ZR 287/90, juris Rn. 14 – Briefwerbung; BGH, Urteil vom 3. März 2011 – I ZR 167/09, juris Rn. 19 – Kreditkartenübersendung.

[8] Siehe dazu: https://kurzelinks.de/kag8

[9] Siehe auch https://kurzelinks.de/lr81

Bestellbutton ein eindeutiger Hinweis auf die Zahlungsverpflichtung ersichtlich ist.

Vor kurzem führte Meta neben den bestehenden kostenlosen werbefinanzierten Versionen von Facebook und Instagram eine kostenpflichtige werbefreie Option ein. Die Verbraucherzentrale argumentierte, dass die Nutzer nicht ausreichend darüber informiert würden, dass ein Klick auf die Bestellbuttons ein kostenpflichtiges Abonnement initiiert. Nach erfolglosen Verhandlungen brachte die Verbraucherzentrale eine einstweilige Verfügung ein, um dieses Vorgehen zu stoppen.

Der 20. Zivilsenat entschied zugunsten der Verbraucherzentrale und stellte fest, dass Unternehmen gesetzlich verpflichtet sind, Bestellbuttons im elektronischen Geschäftsverkehr klar zu kennzeichnen und Zahlungsverpflichtungen anzuzeigen. Der Button mit der Aufschrift „Abonnieren“ erfüllte diese Anforderung nicht, da kein Unterschied zwischen kostenlosen und kostenpflichtigen Abonnements bestand. Obwohl es an anderer Stelle im Bestellvorgang klare Hinweise auf die Abonnementkosten gab, wurde nur der Text auf dem Button als relevant erachtet.

Auch der Button „Weiter zur Zahlung“ in den Apps erfüllte nicht die Anforderungen des Verbraucherschutzes. Obwohl er auf die Zahlungsverpflichtung hinwies, wurden die Nutzer nicht ausreichend darüber informiert, dass ein Klick darauf nicht einfach zu einer weiteren Seite zur Dateneingabe führte, sondern einen verbindlichen Vertrag darstellte.

Das Urteil ist nun rechtskräftig und setzt einen Präzedenzfall für klarere und transparente Bestellvorgänge auf Social-Media-Plattformen.

3. Top 3 Bußgelder

32 Millionen! CNIL straft Amazon wegen unzulässiger Kontrollen ab

Die französische Datenschutzbehörde CNIL (Commission Nationale de l’Informatique et des Libertés) ließ mit einem hohen Pönale gegen Amazon France Logistique (AFL) aufhorchen[10]. Ganze **32 Mio. Euro** soll AFL für die unzulässige Videoüberwachung, Leistungs- und Verhaltenskontrollen seiner Mitarbeiter zahlen.

Die AFL führte in ihren Distributionszentren ein ausgeklügeltes Kontrollsystem ein, das die Handlungen und Leistungsfähigkeit ihrer Belegschaft präzise überwacht. Jeder Mitarbeiter im Lagerbereich bekam einen Handscanner, um Aufgaben wie das Laden und Entladen von Gütern unmittelbar zu verzeichnen. Die aus diesen Scans resultierenden Informationen bildeten die Basis für die Berechnung verschiedener Leistungsindizes, welche Einblicke in die Qualität der Arbeit, die Effizienz und die Pausenzeiten der Mitarbeiter lieferten.

Zusätzlich wurde dieses Kontrollsystem durch ein dreistufiges Alarmierungssystem verstärkt, das die Aktivitäten der Angestellten kontrolliert. Alarme wurden aktiviert, wenn ein Artikel in weniger als 1,25 Sekunden nach einem anderen gescannt wurde („Stow Machine Gun“). Ein anderer Alarm wurde bei Ruhezeiten von mehr als zehn Minuten ausgelöst („Idle Time“), und ein dritter registrierte kürzere Pausen („Latency under ten minutes“). Außerdem wurden die Arbeitsplätze mittels Videoüberwachung kontrolliert. Amazon verarbeitete die gesammelten Informationen zu Kennzahlen für die Arbeitsleistung, die anschließend für einen Zeitraum von 31 Tagen gespeichert wurden.

Die verhängte Geldstrafe mag auf den ersten Blick enorm erscheinen. Der Betrag relativiert

[10] https://kurzelinks.de/c6jm

sich, wenn man ihn mit dem globalen Jahresumsatz von Amazon, der über 500 Milliarden USD liegt, vergleicht, insbesondere unter Berücksichtigung des Art. 83 DSGVO. Die französische Datenschutzbehörde CNIL stellte fest, dass Verstöße gegen das Prinzip der Datensparsamkeit gem. Art. 5 und die Informationspflichten der Art. 12 und 13 DSGVO vorlagen. Besonders kritisiert wurde von der CNIL, dass Amazon die erhobenen Mitarbeiterdaten und die daraus generierten statistischen Auswertungen zu lange speicherte. Zudem ergaben Überprüfungen, dass die Videoüberwachung ohne vorherige Ankündigung und ohne angemessene Sicherheitsvorkehrungen nach Art. 32 DSGVO implementiert wurde. Das Passwort für den Zugang zur Videoüberwachungssoftware war nicht sicher genug und der Zugang wurde von mehreren Nutzern gemeinsam verwendet.

Fehlende Einwilligung für Werbe-Cookies

Zu Beginn des Jahres gingen – wieder bei der CNIL – insgesamt 27 Beschwerden gegen das Unternehmen Yahoo EMEA Ltd.[11] ein. Die Einwände bezogen sich primär auf unzulängliche Methoden bei der Einwilligung und dem Widerruf zum Cookie-Einsatz.

In den Jahren 2020 und 2021 durchgeführte Untersuchungen der CNIL deckten Verstöße gegen Art. 82 des französischen Datenschutzgesetzes auf. Rund 20 Werbe-Cookies wurden platziert, ohne Einwilligung der Seitenbesucher. Ferner war es für Nutzer des Yahoo E-Mail-Services problematisch, ihre Einwilligung zur Verwendung von Cookies zu widerrufen, da dies die weitere Verwendung des E-Mail-Services unmöglich machte. Ungeachtet der Schwere der begangenen Verstöße legte die CNIL die Geldstrafe auf lediglich **10 Mio. Euro** fest.

Zugangsdaten von Millionen Kunden veröffentlicht

Im August 2021 wurde ENDESA ENERGÍA, S.A.U., ein spanisches Energieversorgungsunternehmen, in Kenntnis gesetzt, dass Zugriffsdaten zu seiner Online-Plattform über eine Werbeanzeige auf Facebook angeboten wurden. Am 17. Januar 2022 stieß man auf eine weitere Facebook-Anzeige, in der eine Kundendatenbank, die Daten verschiedener Energieversorger enthielt, zum Verkauf angeboten wurde. Kurz darauf stellte ENDESA fest, dass personenbezogene Daten ihrer Kunden kompromittiert waren, darunter Namen, Geburtstage, Ausweisnummern, Passdaten, finanzielle Details und Adressen. Sofort nach Entdeckung des Datenlecks benachrichtigte das Unternehmen die spanische Datenschutzbehörde.

Die Untersuchung durch die Behörde deckte auf, dass ENDESA unzureichende Maßnahmen zur Datensicherheit ergriffen hatte. Beispielsweise wurden die Zugangsdaten erst einen Monat nach Aufdeckung des Vorfalls erneuert. Außerdem war es möglich, dass mehrere Personen denselben Nutzeraccount verwenden konnten. Diese Schwachstellen führten dazu, dass Unbefugte monatelang Zugang zu sensiblen Informationen hatten, was die Daten von etwa 4,8 Millionen Strom- und 1,2 Millionen Gaskunden gefährdete. Trotz des Wissens, dass Betrüger Verträge in Namen der Kunden abgeschlossen hatten, unterließ es ENDESA, die Betroffenen zu informieren.

Ferner rügte die spanische Datenschutzbehörde ENDESA dafür, dass es keinen Nachweis über die Einreichung eines Löschersuchens bei Facebook Ireland Limited vorlegen konnte. Als Konsequenz aus diesen Ereignissen und festgestellten Mängeln verhängte die Behörde gegen ENDESA ENERGÍA, S.A.U. eine Strafe in Höhe von **6,1 Millionen Euro.**[12]

[11] https://kurzelinks.de/oe2w

[12] https://kurzelinks.de/3464

••••

Datenschutz-Seminare 2024

Die Entwicklung des nationalen und internationalen Datenschutzes geht weiter, auch 2024 sind neue rechtliche Entscheidungen und Aktualisierungen zu erwarten. Lassen Sie sich im bewährt kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen in Angelegenheiten der Informationssicherheit und Datenschutzpraxis informieren! Neben praxisnaher Wissensvermittlung steht Secur-Data für State-of-the-Art-Anwendungstipps sowie praxistaugliche Muster und Vorlagen. Auch heuer wird Ihnen wieder **Herr Mag. Andreas Rohner von der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

8. April 2024, 9:15 – 17:00 Uhr:

„Rechtsentwicklung und Best Practices“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Menas Saweha, Rona Paca
Gastreferent: Mag. Andreas Rohner (Datenschutzbehörde Österreich)

9. April 2024, 9:15 – 17:00 Uhr:

„Praxis-Updates zu Datensicherheit & Informationssicherheit“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Krzysztof Müller, Friedrich Tuma, Menas Saweha

Ort: Hilton Vienna Plaza, Schottenring 11, 1010 Wien

Selbstverständlich stehen wir auch für Inhouse-Schulungen oder Seminare zu Spezialthemen zur Verfügung.

Hier geht’s zur Anmeldung: www.secur-data.at oder telefonisch unter (01) 533 42 07-0.