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

Juli 2024 Ausgabe Nr. 113

Liebe Leserinnen und Leser,

vor der Sommerpause möchten wir Ihnen noch eine hochinteressante Lektüre in die Hand drücken. Diese Ausgabe widmet sich datenschutzrechtlichen Schadenersatzansprüchen, Google's Privacy Sandbox- und der aktuellen Rechtsprechung unter anderem zur Thematik Datenübermittlung, Auskunftsrecht und rechtskonformer Cookie-Einsatz.

Viel Spaß bei der Lektüre und bleiben Sie gut informiert!

Mag. Judith Leschanz
Geschäftsführung

1. News

1. Schadenersatzforderungen nach der DSGVO: Aktuelle Herausforderungen durch neue Technologien und wegweisende Urteile

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2018 hat der europäische Gesetzgeber die Rechte der betroffenen Personen erheblich gestärkt und die Pflichten für Verantwortliche und Auftragsverarbeiter von personenbezogenen Daten verschärft. Eine zentrale Neuerung ist das Recht auf Schadenersatz bei Datenschutzverletzungen.

Zunehmende Digitalisierung und der Einsatz moderner Technologien wie Künstliche Intelligenz (KI) bieten Unternehmen spannende Möglichkeiten für Wachstum und Innovation, setzen sie aber gleichzeitig neuen und sich stetig entwickelnden Bedrohungen aus. Wir beleuchten für Sie aktuelle Probleme und wegweisende Urteile des Europäischen Gerichtshofs (EuGH) sowie österreichischer Höchstgerichte und geben Ihnen praxisnahe Empfehlungen, wie Sie Schadenersatzforderungen vorbeugen können.

Rechtsgrundlage und Voraussetzungen für Schadenersatzansprüche

Art. 82 der DSGVO bildet die Grundlage für Schadenersatzansprüche. Demnach hat jede Person, die wegen eines Verstoßes gegen die Verordnung einen materiellen oder immateriellen Schaden erlitten hat, Anspruch auf Schadenersatz. Drei Voraussetzungen müssen erfüllt sein:

1. **Verstoß gegen die DSGVO**: Ein rechtswidriger Umgang mit personenbezogenen Daten, zB unrechtmäßige Verarbeitung oder mangelhafte Datensicherheit.
2. **Nachweis eines Schadens**: Ein tatsächlich eingetretener materieller (zB finanzieller) oder immaterieller Schaden (zB psychische Belastung) muss nachgewiesen werden.

3. **Kausalität**: Der Schaden muss durch den Datenschutzverstoß verursacht worden sein.

Aktuelle Herausforderungen durch moderne Technologien

Das Aufkommen moderner Technologien wie Künstlicher Intelligenz (KI), Big Data, Internet der Dinge (IoT) und Blockchain eröffnet nicht nur neue Möglichkeiten, sondern führt auch zu erheblichen Datenschutzrisiken. Diese Technologien können Datenschutzverstöße begünstigen, die wiederum zu hohen Schadenersatzforderungen führen können.

Im Folgenden werden die spezifischen Risiken neuer Technologien beleuchtet und erläutert, welche datenschutzrechtlichen Herausforderungen mit ihnen verbunden sind.

Künstliche Intelligenz und maschinelles Lernen

KI-Systeme benötigen große Mengen an Daten, um effektiv arbeiten zu können. Diese Daten stammen aus unterschiedlichsten Quellen, oft einschließlich sensibler personenbezogener Informationen. Die Risiken umfassen dabei:

- **Unbefugte Datenverarbeitung**: KI-Modelle können personenbezogene Daten ohne ausreichende rechtliche Grundlage verarbeiten, was einen Verstoß gegen die DSGVO darstellt. Daher ist wichtig, dass vor dem Einsatz eines KI-Modells die Zwecke und Rechtsgrundlagen der Verarbeitung geklärt werden.
- **Datenlecks** und unzureichende Sicherheit: Die Speicherung großer Datenmengen birgt das Risiko von Datenlecks. Ein bekanntes Beispiel ist der Verstoß von Facebook gegen die DSGVO durch die unerlaubte Weitergabe von Nutzerdaten, der zu erheblichen Schadenersatzforderungen führte (EuGH, C-311/18[1]).
- **Diskriminierung und Bias**: KI-Systeme können auf Basis fehlerhafter oder unvollständiger Daten trainiert werden, was zu diskriminierenden Entscheidungen führen kann. ZB könnten Kreditentscheidungen oder Bewerbungsverfahren, die unter Einsatz von KI erfolgen, voreingenommen sein und bestimmte Bevölkerungsgruppen benachteiligen. Gemäß Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden. Um mögliche Schadenersatzansprüche zu vermeiden, ist es wichtig, dass die KI-Ergebnisse durch MitarbeiterInnen zumindest kontrolliert werden.
- **Mangelnde Transparenz:** Viele KI-Algorithmen arbeiten als „Black Boxes“, deren Funktionsweise für Nutzer und sogar für die Betreiber selbst kaum nachvollziehbar ist. Diese Intransparenz kann zu Problemen führen, wenn betroffene Personen ihre Rechte auf Auskunft, Berichtigung und Löschung geltend machen möchten.

Internet der Dinge (IoT)

IoT-Geräte, die zB in Haushalten, Fahrzeugen oder im Rahmen öffentlicher Infrastrukturen eingesetzt werden, sammeln und übertragen kontinuierlich Daten. Diese Geräte sind häufig nicht ausreichend gegen Cyberangriffe abgesichert, was zu Datenschutzverletzungen führen kann.

- **Datenlecks durch Sicherheitslücken**: Schwachstellen in IoT-Geräten können genutzt werden, um auf personenbezogene Daten zuzugreifen oder diese zu stehlen. Ein prominentes Beispiel sind Hackerangriffe auf Smart-Home-Systeme, bei denen Videoaufnahmen oder Gesundheitsdaten kompromittiert wurden.

[1] https://kurzlinks.de/93k2

Der Cyber Resilience Act soll Sicherheitsanforderungen für Hardware- und Softwareprodukte mit digitalen Elementen regeln, die in der Europäischen Union auf den Markt gebracht werden. Hersteller sind nun verpflichtet, die Sicherheit während des gesamten Lebenszyklus eines Produkts zu berücksichtigen.

- **Kontrolle über Daten der IoT Geräte**: Nutzer haben oft keinen Einblick in die Datenverarbeitung durch IoT-Geräte und können diese nur schwer kontrollieren. Dies widerspricht dem Transparenzgebot der DSGVO und kann zu immateriellen Schäden wie Vertrauensverlust und psychischen Belastungen führen. Auch für nichtpersonenbezogene Daten wird durch die Umsetzung des Data Acts das gleiche Schutzniveau wie in der DSGVO gewährleistet.

Blockchain-Technologie

Die Blockchain-Technologie zeichnet sich durch die Unveränderlichkeit der gespeicherten Daten aus. Dies stellt eine Herausforderung dar, wenn es zB um das Recht auf Löschung und Berichtigung geht.

- **Löschanspruch**: Da Blockchain-Daten nicht ohne weiteres gelöscht werden können, kann es schwierig sein, den gesetzlichen Anforderungen der DSGVO gerecht zu werden. Dies kann zu Konflikten führen, wenn Betroffene ihr Recht auf Datenlöschung durchsetzen wollen.
- **Datenminimierung**: Die Speicherung von Daten in der Blockchain widerspricht oft dem Prinzip der Datenminimierung, da bereits gespeicherte Daten nicht mehr geändert oder entfernt werden können. Dies kann rechtliche Konsequenzen haben, wenn es um die langfristige Speicherung personenbezogener Daten geht.

Konkrete Risiken und Folgen für Unternehmen

Datenschutzverletzungen können zu erheblichen finanziellen Belastungen führen. Neben unmittelbaren finanziellen Folgen können Datenschutzverletzungen das Vertrauen der Kunden und Geschäftspartner erheblich beeinträchtigen. Dieser Vertrauensverlust kann langfristig negative Auswirkungen auf die Marktposition eines Unternehmens haben und seine Geschäftstätigkeit gefährden.

Zusätzlich zu Schadenersatzforderungen können Datenschutzverstöße zu hohen Bußgeldern durch die zuständigen Aufsichtsbehörden führen. Diese Bußgelder können je nach Schwere des Verstoßes bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens betragen.

Prävention und Risikominderung

- **Datenschutz durch Technikgestaltung**: Unternehmen müssen den Grundsatz „Privacy by Design“ umsetzen, der vorsieht, Datenschutzmaßnahmen bereits bei der Entwicklung neuer Technologien und Systeme zu integrieren. Dies umfasst den Einsatz von Verschlüsselungstechnologien, datenschutzfreundliche Voreinstellungen und regelmäßige Sicherheitsüberprüfungen.
- **Transparente Datennutzung und Einwilligungsmanagement:** Transparenz ist ein wesentlicher Aspekt der DSGVO. Unternehmen sollten sicherstellen, dass ihre Kunden umfassend über die Datenverarbeitung informiert wurden und ihre Einwilligung einholen, wenn dies erforderlich ist. Ein effektives Datenschutzmanagement hilft, die Rechte der betroffenen Personen zu wahren und rechtlichen Problemen vorzubeugen.
- **Schulung und Sensibilisierung:** Mitarbeiter müssen regelmäßig geschult und für Datenschutzfragen sensibilisiert werden. Dies hilft, das Bewusstsein für Datenschutzrisiken zu erhöhen und sicherzustellen, dass

personenbezogene Daten gemäß den gesetzlichen Anforderungen verarbeitet werden.

- **Kontinuierliche Überwachung und Anpassung:** Datenschutz ist ein kontinuierlicher Prozess. Unternehmen müssen ihre Datenschutzmaßnahmen regelmäßig überprüfen und an neue rechtliche und technologische Entwicklungen anpassen. Die laufende Überwachung und Anpassung hilft, Risiken frühzeitig zu erkennen und zu minimieren.

Abschließend ist zu sagen, dass neue Technologien wie KI, Big Data, IoT und Blockchain viele Vorteile bieten, aber auch erhebliche Datenschutzrisiken nach sich ziehen. Verantwortliche müssen sich der potenziellen Gefahren bewusst sein und geeignete Maßnahmen ergreifen, um Datenschutzverletzungen zu vermeiden und Schadenersatzforderungen vorzubeugen. Die Implementierung umfassender Datenschutzstrategien, die Schulung der Mitarbeiter und die kontinuierliche Verbesserung der Datenschutzpraxis kann rechtliche und finanzielle Risiken minimieren und das Vertrauen der Kunden erhalten. Wegweisende Urteile des EuGH und anderer Höchstgerichte unterstreichen immer wieder die Bedeutung der sorgfältig geplanten und rechtskonformen Datenverarbeitung.

2. Google's Privacy Sandbox: Eine Verbesserung des Datenschutzes?

Google hat mit dem Privacy Sandbox-Projekt ein Vorhaben gestartet, das die Online-Tracking-Praxis revolutionieren soll. Anstatt auf traditionelle Methoden wie Cookies zurückzugreifen, die häufig als invasive Form der Datenerfassung kritisiert werden, verspricht Google mit diesem Projekt eine sichere und datenschutzfreundlichere Zukunft für das Internet. Trotz dieser Ansprüche gibt es erhebliche Bedenken hinsichtlich der tatsächlichen Auswirkungen auf den Datenschutz. Die österreichische Datenschutzorganisation NOYB (Max Schrems) hat eine detaillierte Analyse durchgeführt und dabei verschiedene Aspekte des Projekts kritisch beleuchtet. Wir haben für Sie eine ausführliche Zusammenfassung der Ergebnisse zusammengestellt.

Hintergründe und Ziele der Privacy Sandbox

Googles Privacy Sandbox zielt darauf ab, den Einsatz von Cookies zu ersetzen, die traditionell für Online-Werbung eingesetzt werden. Diese Cookies sind bei Datenschutzaktivisten stark in die Kritik geraten, da sie es Werbetreibenden ermöglichen, Aktivitäten der Nutzer über verschiedene Websites hinweg zu verfolgen und detaillierte Benutzerprofile zu erstellen. Google will nun diese Cookies durch eine neue Technologie ersetzen, die angeblich die Privatsphäre der Nutzer besser schützt, gleichzeitig aber personalisierte Werbung ermöglicht. Dabei wird das Surfverhalten laufend vom eigenen Browser (Google Chrome) getrackt, um den Nutzern anschließend bestimmte Werbekategorien zuzuordnen.

Hauptkritikpunkte von NOYB

a) Mangel an Transparenz und Kontrolle

NOYB kritisiert, dass die Privacy Sandbox Nutzern unzureichende Kontrolle über ihre Daten gibt. Obwohl Google behauptet, dass die Sandbox die Privatsphäre der Nutzer schützt, bleibt unklar, wie diese neuen Technologien genau funktionieren und welche Daten tatsächlich gesammelt und verarbeitet werden. Nutzer werden weiterhin verfolgt, nur eben auf andere, weniger transparente Weise. Die Technologie mag zwar Drittanbieter-Cookies eliminieren, aber sie führt eine andere, ebenso invasive Technik zur Datenerfassung ein.

b) Gefährdung der Wettbewerbsgleichheit

Ein weiterer Kritikpunkt betrifft die potenziellen Auswirkungen auf den Wettbewerb. Google könnte durch die Einführung der Privacy Sandbox seine Marktmacht weiter ausbauen, indem es den Zugriff auf Nutzerdaten noch stärker kontrolliert. Dies könnte kleinere

Wettbewerber benachteiligen, die weniger Zugang zu den Daten haben und daher weniger präzise Werbung anbieten können.

c) Mangelnde Einhaltung der DSGVO

NOYB hebt hervor, dass die Einführung der Privacy Sandbox nicht den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entspricht. Insbesondere die Prinzipien von Transparenz und Treu und Glauben werden verletzt, da Google umfangreiche Nutzerdaten sammelt, ohne die betroffenen Personen hinreichend zu informieren oder ihre gültige Zustimmung einzuholen. Es gibt Bedenken, dass die Datenschutzrechte der Nutzer nicht ausreichend gewahrt werden.

Technische und rechtliche Herausforderungen

a) Neue Tracking-Technologien

Die Privacy Sandbox führt mehrere neue Technologien ein, darunter das Federated Learning of Cohorts (FLoC) und das Topics API, die darauf abzielen, Nutzerdaten in Kohorten zu gruppieren. Diese Ansätze sollen es ermöglichen, weiterhin zielgerichtete Werbung zu schalten. Allerdings bleibt fraglich, wie effektiv diese Technologien dabei sind, Datenschutz zu gewährleisten. Es besteht der Verdacht, dass die neuen Methoden nicht weniger invasiv sind als traditionelle Tracking-Technologien.

b) Rechtliche Unsicherheiten

Rechtlich gesehen wirft die Privacy Sandbox viele Fragen auf. Eine zentrale Frage ist, ob die neuen Tracking-Methoden den strengen Datenschutzvorgaben der DSGVO entsprechen. Insbesondere wird in Frage gestellt, ob die Nutzer ausreichend informiert wurden, um eine rechtsgültige Einwilligung für die Datenverarbeitung geben zu können. NOYB betont, dass ohne klare rechtliche Rahmenbedingungen und wirksame Kontrollmechanismen die Datenschutzrechte der Nutzer gefährdet sind.

Fazit und Empfehlungen

Die Analyse von NOYB zeigt, dass Google's Privacy Sandbox trotz der versprochenen Verbesserungen im Datenschutzbereich erhebliche Risiken birgt. Es besteht die Gefahr, dass die neuen Technologien die bestehenden Datenschutzprobleme nicht lösen, sondern lediglich in eine andere Form überführen. Nutzer könnten weiterhin verfolgt und ihre Daten genutzt werden, ohne dass sie dies ausreichend verstehen oder kontrollieren können.

Es ist entscheidend, dass die Aufsichtsbehörden und Datenschutzaktivisten die Entwicklung der Privacy Sandbox genau beobachten und sicherstellen, dass sie den gesetzlichen Anforderungen entspricht und die Rechte der Nutzer schützt. Unternehmen sollten ebenfalls wachsam sein und sich mit den technischen und rechtlichen Aspekten der neuen Technologien auseinandersetzen, um sicherzustellen, dass sie ihre Datenschutzpflichten einhalten und das Vertrauen ihrer Kunden bewahren.

Erfüllung der Pflichten der NIS-2-Richtlinie: Unsere Beratungsangebot

Ab voraussichtlich Oktober 2024 wird in Österreich ein neues Gesetz für Informationssicherheit (NISG 2024) in Kraft treten, das deutlich mehr Unternehmen betrifft als sein Vorgänger.

Unternehmen müssen sich auf umfassende neue Anforderungen einstellen, um die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten. Unsere Beratung steht Ihnen zur Seite, um diese Herausforderungen erfolgreich zu meistern.

Wichtige Pflichten des neuen Gesetzes:

- Risikomanagement: Unternehmen müssen Risiken für ihre IT-Systeme analysieren und geeignete Maßnahmen zur Risikominimierung ergreifen.
- Vorfallmeldung: Sicherheitsvorfälle, die den Betrieb beeinträchtigen könnten, müssen unverzüglich gemeldet und zügig behoben werden.
- Krisenmanagement: Pläne zur Wiederherstellung und Minimierung von Ausfällen müssen entwickelt und regelmäßig getestet werden.
- Informationsaustausch: Unternehmen sind verpflichtet, mit Behörden und Partnern zusammenzuarbeiten und Informationen über Bedrohungen und Vorfälle auszutauschen.
- Lieferkettensicherheit: Auch die Sicherheit von Lieferanten und Drittanbietern muss überwacht und sichergestellt werden.
- Compliance: Alle Maßnahmen müssen dokumentiert werden und nachweislich den gesetzlichen Vorgaben entsprechen.

Unsere Beratung unterstützt Sie in allen Bereichen:

- Individuelle Risikobewertungen: Wir analysieren Ihre spezifischen Risiken und entwickeln maßgeschneiderte Sicherheitskonzepte, die den Anforderungen des NIS 2 Gesetzes gerecht werden.
- Effektives Vorfallmanagement: Wir helfen Ihnen, ein effizientes Vorfallmanagement aufzubauen und unterstützen Sie bei der Einhaltung der strengen Meldepflichten.
- Krisen- und Wiederherstellungsplanung: Wir entwickeln robuste Krisenpläne und Wiederherstellungsstrategien, die sicherstellen, dass Ihr Betrieb im Ernstfall schnell lauffähig gemacht wird.
- Umfassende Schulungen: Wir bieten Schulungen und Sensibilisierungsprogramme an, um Ihr Team auf die neuen Anforderungen vorzubereiten und die Cybersicherheitskultur in Ihrem Unternehmen zu stärken.
- Dokumentation und Compliance: Wir unterstützen Sie bei der Erstellung und Pflege der erforderlichen Dokumentation, um sicherzustellen, dass Sie jederzeit nachweisen können, dass Sie alle gesetzlichen Vorgaben erfüllen.

Unser umfassendes wissenschaftliches Know-how und unser praxisorientierter Ansatz machen uns zum idealen Partner für die Umsetzung der NIS-2-Anforderungen. Mit unserer Unterstützung sind Sie bestens vorbereitet, um die neuen gesetzlichen Pflichten effizient und nachhaltig zu erfüllen.

Kontaktieren Sie uns für eine individuelle Beratung und lassen Sie uns gemeinsam Ihre IT-Sicherheitsziele erreichen!

2. Neues aus der Rechtsprechung

EuGH-Urteil: Auch die mündliche Datenübermittlung unterliegt der DSGVO

Der Europäische Gerichtshof (EuGH) hat in einem Urteil vom 7. März 2024 (C-740/22)[2] entschieden, dass die mündliche Übermittlung personenbezogener Daten, insbesondere von Daten über strafrechtliche Verurteilungen, als Datenverarbeitung im Sinne der Datenschutzgrundverordnung (DSGVO) anzusehen ist.

Der Fall begann, als Endemol Shine Finland bei einem finnischen Gericht mündlich Auskunft über das Strafregister einer Person verlangte, die an einem von Endemol organisierten Wettbewerb teilnehmen wollte. Das Gericht verweigerte die Auskunft mit der Begründung, dass es keine Rechtsgrundlage für das Auskunftsverlangen gebe und dass die Betroffenenrechte gewahrt werden müssten. Zudem handele es sich bereits bei der Suchanfrage im Informationssystem des Gerichts um eine Datenverarbeitung.

Der Fall gelangte vor den EuGH, der klarstellte, dass der Begriff „Datenverarbeitung" weit auszulegen ist und jede Art von Vorgang umfasst. Selbst eine mündliche Übermittlung gilt als Verarbeitung, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der EuGH betonte, dass es dem Ziel der Verordnung widersprechen würde, die Anwendung der DSGVO durch die mündliche Weitergabe personenbezogener Daten zu umgehen.

Anschließend führte der EuGH aus, dass der Begriff „Verarbeitung" gemäß Art. 4 Z 2 DSGVO weit gefasst ist und jede Art von Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten umfasst. Auch nichtautomatisierte Verarbeitungen fallen in den sachlichen Anwendungsbereich der DSGVO, sofern die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Eine mündliche Weitergabe gilt daher als Datenverarbeitung, außer die Informationen waren weder vorher in einem Dateisystem gespeichert noch sollen sie nach der Weitergabe gespeichert werden. Letzteres betrifft insbesondere private Unterhaltungen ohne jegliche Speicherung der Daten.

Erkennbarkeit in sozialen Medien

Das Oberlandesgericht (OLG) Dresden hat am 23. April 2024 (Az. 4 W 213/24)[3] eine Entscheidung zur Erkennbarkeit von Personen durch Äußerungen in sozialen Medien getroffen.

Der Antragsteller, bekannt als „Mr.K…" auf der Social-Media-Plattform TikTok, beantragte eine einstweilige Verfügung gegen die Antragsgegnerin „A…", die ebenfalls auf TikTok aktiv ist. Die Antragsgegnerin hatte sich in einem Livestream über „Mr.K…" geäußert, zwar ohne seinen Namen zu nennen, jedoch auf eine Weise, die ihn für einen bestimmten Personenkreis identifizierbar machte. Nach einem Rechtsstreit vor dem Landgericht Chemnitz schlossen die Parteien einen Vergleich, der der Antragsgegnerin bestimmte Äußerungen untersagte.

Das OLG Dresden stellte klar, dass die Nennung des Namens nicht zwingend erforderlich ist, um eine Person erkennbar zu machen. Es sei auch nicht entscheidend, ob alle oder ein erheblicher Teil der Adressaten die betroffene Person identifizieren können. Es genügt, wenn Teilinformationen (zB beschriebene Merkmale) den Betroffenen innerhalb eines bestimmten Bekanntenkreises identifizierbar machen.

Der Antragsteller konnte in dem Fall anhand von Beschreibungen und früheren Äußerungen der Antragsgegnerin identifiziert werden, was

[2] https://kurzlinks.de/ubp0

[3] https://kurzlinks.de/9xcw

auch Kommentare von Zuschauern bestätigten. Das Gericht befand, dass die Äußerungen der Antragsgegnerin das Persönlichkeitsrecht des Antragstellers erheblich verletzten. Sie beschuldigte ihn, an der Planung schwerer Straftaten gegen sie beteiligt zu sein, ohne dafür Beweise vorzulegen. Diese Beschuldigungen stellten eine schwere Ehrverletzung dar, unabhängig davon, ob die Rachepläne tatsächlich nachweisbar sind.

Die Entscheidung des OLG Dresden betont die Notwendigkeit des sorgfältigen Umgangs mit Informationen und Äußerungen über andere Personen in der digitalen Welt. Insbesondere wird hiermit deutlich gemacht, dass auch indirekte oder verschlüsselte Aussagen rechtliche Konsequenzen haben können, wenn die betroffene Person identifizierbar ist.

BVwG bestätigt die Rechtsmäßigkeit von Pop-up zur Einwilligung von Cookies

Das Bundesverwaltungsgericht (BVwG) hat am 26. April 2024 (W211 2281997-1)[4] entschieden, dass die Anzeige eines Pop-ups, das Nutzer zur Einwilligung zu Tracking-Cookies auffordert, nachdem diese bereits Cookies abgelehnt haben, zu einer gültigen Einwilligung führen kann.

Beim Aufruf der Website eines österreichischen Nachrichtenportals erschien ein Cookie-Banner mit den Optionen „Alle akzeptieren“ oder „Einstellungen verwalten“. Wählte der Nutzer „Einstellungen verwalten“ und lehnte Cookies ab, erschien ein weiteres Banner, das erklärte, dass die Plattform nur mit bestimmten Tracking-Cookies sinnvoll betrieben werden könne und daher eine Einwilligung erforderlich sei.

Der betroffene Nutzer reichte eine Beschwerde bei der österreichischen Datenschutzbehörde (DSB) ein und behauptete, dass dies gegen Art. 5 Abs. 1 und Art. 6 Abs. 1 DSGVO verstoße, da er gezwungen werde, seine Einwilligung zu Tracking-Cookies zu erteilen, um auf die Inhalte der Website zugreifen zu können.

Die DSB stellte fest, dass das Medienprivileg gemäß Art. 85 DSGVO nicht anwendbar sei, da die Datenverarbeitung nicht zur Verbreitung journalistischer Informationen, sondern zu Werbe- oder Analysezwecken erfolgte. Zudem erklärte die DSB, dass die betroffenen Cookies nicht unbedingt erforderlich seien und ihre Nutzung daher der Einwilligung des Nutzers bedürfe. Diese Einwilligung wurde jedoch nicht freiwillig erteilt, da der Nutzer keine echte Wahl hatte. Schließlich kam die DSB zu dem Schluss, dass berechtigte Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO nicht relevant seien, da bereits ein Verstoß gegen die ePrivacy-Richtlinie vorliege, die eine Einwilligung erfordert. Der Betreiber legte gegen diese Entscheidung Berufung beim BVwG ein.

Das BVwG entschied, dass die Einwilligung nicht erzwungen wurde, sondern freiwillig war. Es betonte, dass Daten als Gegenleistung für den Zugang zu Inhalten angeboten werden könnten und der Betreiber das Recht habe, selbst Bedingungen für den Zugang zu seinen Inhalten festzulegen. Nutzer hätten alternative Zugangswege wie eine Printausgabe oder ein digitales Abonnement. Das BVwG wies darauf hin, dass das Nachrichtenportal im Vergleich zu großen Plattformen[5] nicht in einer dominanten Marktposition sei und somit die Wahlfreiheit der Nutzer nicht im gleichen Ausmaß einschränkt.

Das BVwG annullierte damit die Entscheidung der DSB. Diese hat Berufung beim Verwaltungsgerichtshof (VwGH) eingelegt.

Auskunftsrecht genießt Vorrang vor dem Geschäftsgeheimnisinteresse eines Glücksspielanbieters

Das Oberlandesgericht Wien hat in einem Urteil vom 10. Juni 2024 (GZ 14 R 48/24t)[6] ent-

[4] https://kurzlinks.de/m72r
[5] S. dazu EuGH C-252/21 „Pay or Okay“ Modell von Meta
[6] https://kurzlinks.de/x5v0

schieden, dass einer von einem Glücksspielanbieter geschädigten Person das Recht auf Auskunft nach Art. 15 DSGVO zusteht. Der Anbieter argumentierte, dass die betroffene Person das Auskunftsrecht lediglich zur Erlangung von Beweismitteln für einen Zivilprozess missbrauchen wolle und daher kein legitimes Auskunftsbegehren vorliege. Das Gericht wiederholte die Auffassung des EuGH, dass ein Auskunftsersuchen auch dann zulässig ist, wenn es datenschutzfremde Ziele verfolgt. Da es aber seit der Veröffentlichung des EuGH-Urteils noch keine Entscheidung eines österreichischen Höchstgerichts gibt, erklärte das Gericht die ordentliche Revision für zulässig.

Der Fall begann, als ein Geschädigter vom Glücksspielanbieter Auskunft über seine personenbezogenen Daten forderte, um eine mögliche Rückforderungsklage vorzubereiten. Der Anbieter verweigerte diese Auskunft mit der Begründung, dass dem Kläger kein Auskunftsrecht nach Art. 15 DSGVO zustehe. Er argumentierte, der Kläger wolle nur Beweismittel für einen drohenden Zivilprozess erlangen und nicht die Rechtmäßigkeit der Datenverarbeitung überprüfen, was das Auskunftsrecht rechtsmissbräuchlich mache. Darüber hinaus gab der Anbieter an, dass die angeforderten Informationen einem berechtigten Geheimhaltungsinteresse gemäß § 4 Abs. 6 DSG iVm Art. 15 Abs. 4 DSGVO unterlägen, da eine Schwächung seiner Rechtsposition drohe.

Das Oberlandesgericht Wien lehnte diese Argumentation ab. Es betonte, dass das berechtigte Geheimhaltungsinteresse des Anbieters gemäß § 4 Abs. 6 DSG iVm Art. 15 Abs. 4 DSGVO zwar die Rechte und Freiheiten anderer Personen, einschließlich Geschäfts- und Betriebsgeheimnissen schützen solle, jedoch nicht dazu führen dürfe, dass der betroffenen Person jegliche Auskunft verweigert wird. Dies werde insbesondere im letzten Satz von Erwägungsgrund 63 der DSGVO deutlich gemacht.

In der Begründung verweist das Gericht auf das EuGH-Urteil (C-307/22)[7] vom 26. Oktober 2023.[8] In einem ähnlich gelagerten Fall hatte der EuGH entschieden, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten zur Verfügung zu stellen, auch dann gilt, wenn der Antrag mit anderen als den in Satz 1 von ErwGr 63 DSGVO genannten Zwecken begründet wird. Es wurde klargestellt, dass betroffene Personen das Recht auf freien Zugang zu ihren Daten haben, ohne dass sie ihren Antrag begründen müssen. Eine Ausnahme besteht nur, wenn der Antrag offenkundig unbegründet oder exzessiv ist.

[7] https://kurzlinks.de/l5sn

[8] S. auch unser DSG-Info Nr. 108

3. Bußgelder des Monats

Videoaufnahme in Chatgruppe gestellt

In einer Nudelfabrik des Unternehmens CUI ZSQ Food, S.L. südlich von Madrid kam es zu einem Vorfall im Zusammenhang mit der Videoüberwachung der Produktionsstätte. Ein Mitarbeiter des Unternehmens hatte Videoaufnahmen aus der Überwachungskamera der Fabrik in eine interne Chatgruppe gepostet, die allen Mitarbeitern des Unternehmens zugänglich ist.

In den hochgeladenen Videos war zu sehen, dass ein Kollege am Fließband über einen längeren Zeitraum hinweg seinen Arbeitsplatz verlassen hatte. Der Zweck des Postings bestand nach Aussage des Mitarbeiters darin, die anderen Kollegen zu warnen und ähnliche Verhaltensweisen zu verhindern.

Die spanische Datenschutzbehörde, die Agencia Española de Protección de Datos (AEPD)[9], stellte fest, dass es für die Verbreitung des Videos in der Chatgruppe keine rechtliche Grundlage gab. Die Behörde bewertete den Vorfall als Verstoß gegen die Vertraulichkeit der personenbezogenen Daten des betroffenen Mitarbeiters sowie derjenigen, die in dem Video zu sehen waren.

Ursprünglich wurde eine Geldstrafe von EUR 70.000 gegen CUI ZSQ verhängt. Nach einem Schuldeingeständnis des Unternehmens wurde diese Summe jedoch auf EUR 42.000 reduziert.

Die Behörde unterstrich in ihrem Urteil, dass die Überwachung des Verhaltens von Mitarbeitern am Arbeitsplatz durch Videoaufnahmen nicht ohne weiteres zulässig ist. Es muss stets eine sorgfältige Abwägung zwischen den berechtigten Interessen des Arbeitgebers an der Überwachung und dem Schutz der Privatsphäre der Arbeitnehmer vorgenommen werden. Im vorliegenden Fall überwog das Interesse des Arbeitnehmers, sich vor Überwachung zu schützen.

Italienische Behörde verhängt Millionenstrafe wegen unrechtmäßiger Werbeanrufe

Die italienische Datenschutzbehörde, Garante per la Protezione dei Dati Personali, hat ein Unternehmen, das im Verkauf und Marketing von Gas- und Stromverträgen tätig ist, wegen unrechtmäßiger Werbeanrufe mit einer Geldstrafe von EUR 6.419.631 bestraft.[10]

Das Unternehmen wurde aufgrund von 108 Meldungen und 7 Beschwerden über unerwünschte Telefonanrufe von der Behörde geprüft. Es stellte sich heraus, dass zahlreiche Anrufe an Personen gerichtet waren, die entweder keine Zustimmung gegeben oder ihre Telefonnummer im öffentlichen Einspruchsregister hinterlegt hatten. Die Prüfung ergab auch, dass von 747 abgeschlossenen Verträgen 657 aus unzulässigen Kontaktaufnahmen stammten.

Neben der Verhängung der Geldstrafe hat die Behörde dem Unternehmen jegliche Weiterverarbeitung der Daten der Beschwerdeführer und Hinweisgeber verboten.

Arbeitnehmer setzt Gesichtserkennung am Arbeitsplatz ein

Ein Autohändler in Süditalien implementierte ein Gesichtserkennungssystem, um die Anwesenheit seiner Mitarbeiter zu überwachen und ihre Arbeitsleistung zu bewerten. Dieses Vorgehen wurde durch die Beschwerde eines Mitarbeiters bekannt, die zur Untersuchung durch die italienische Datenschutzbehörde führte.

Laut Aussage der Mitarbeiter wurden neben der Zugangskontrolle mittels Gesichtserken-

[9] https://kurzlinks.de/iz20

[10] https://kurzlinks.de/a934

nungssystem auch detaillierte Protokolle über die durchgeführten KFZ-Reparaturen geführt. Diese Protokolle umfassten die Arbeitszeiten, die angewandten Mittel sowie Ausfallzeiten und deren konkrete Gründe.

Das Unternehmen rechtfertigte die Verwendung des Systems mit der Notwendigkeit, die Zuverlässigkeit der Mitarbeiter zu prüfen und etwaigem Fehlverhalten entgegenzuwirken. Die Datenschutzbehörde sah jedoch keinen legitimen Grund, der die Rechte und Freiheiten der betroffenen Mitarbeiter überwiegen würde. Die Verarbeitung der biometrischen Daten durch das Gesichtserkennungssystem erfolgte somit ohne rechtliche Grundlage.

Im Ergebnis verhängte die Behörde ein Bußgeld in Höhe von EUR 120.000[11] gegen das Unternehmen.

Biometrische Daten, wie sie bei der Gesichtserkennung verwendet werden, unterliegen nach DSGVO einem besonderen Schutz. Die Identifizierung mittels Gesichtserkennung stellt einen deutlich stärkeren Eingriff in die Privatsphäre der Mitarbeiter dar als die Verwendung eines Passworts oder übliche Verfahren zur Multi-Faktor-Authentifizierung.

Aufgrund ihrer Einstufung unter Art. 9 DSGVO sind bei der Verarbeitung biometrischer Daten strenge Datenschutzanforderungen zu beachten. Der Auswahl einer geeigneten Rechtsgrundlage gemäß Art. 9 Abs. 2 DSGVO kommt besondere Bedeutung zu.

••••

Save the Date

Save the Date – Datenschutzseminar:

Es freut uns, Ihnen unser nächstes Datenschutz-Praxisseminar am **11. und 12. November 2024** im Vienna Hilton Plaza anzukündigen. In unserem bewährten Seminar vermitteln wir Ihnen den neuesten Stand von Recht und Technik, indem wir auf aktuelle Entwicklungen, Rechtsprechung und Praxisbeispiele eingehen.

Wir freuen uns auf Ihre Anmeldung.

Save the Date – Privacy Ring:

Der Datenschutzverein Privacy Ring[12] 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.

Die Teilnahme an der Veranstaltung ist kostenlos. Wir freuen uns auf Ihre Anmeldung.

[11] https://kurzlinks.de/a934

[12] https://www.privacy-ring.uni-hannover.de/de/