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

September 2024 Ausgabe Nr. 114

Liebe Leserinnen und Leser,

der Sommer ist vorbei und wir hoffen Sie konnten sich gut erholen! In der Herbst-Ausgabe des DSG-Info bieten wir Ihnen interessante Einblicke in den zweiten Bericht der Europäischen Kommission zur Anwendung der Datenschutz-Grundverordnung und aktuelle Rechtsprechung zu den Themen Verbandsklagen, Cookie-Einsatz und Auskunftsbegehren. Wie immer präsentieren wir Ihnen auch die Top-Bußgelder für datenschutzrechtliche Verstöße.

*Im November informieren wir Sie im Rahmen unseres **Datenschutzpraxisseminars** über aktuelle Entwicklungen und Best Practices im Datenschutz. Nähere Infos finden Sie am Ende der DSG-Info.*

Wir wünschen eine angenehme Lektüre!

Mag. Judith Leschanz
Geschäftsführung

1. Zweiter Bericht zur Anwendung der Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die am 25. Mai 2018 in Kraft trat, markierte einen entscheidenden Schritt im europäischen Datenschutzrecht. Ziel der Verordnung ist es, den Schutz personenbezogener Daten innerhalb der EU zu stärken und gleichzeitig den freien Datenverkehr im Binnenmarkt zu gewährleisten. Am 25. Juli 2024 veröffentlichte die **Europäische Kommission** ihren *„Zweiten Bericht zur Anwendung der Datenschutz-Grundverordnung (DSGVO)"*. Dieser Bericht gibt Aufschluss über den aktuellen Stand der Umsetzung der DSGVO, analysiert Herausforderungen und identifiziert Handlungsfelder für die Zukunft.

Gemäß **Art. 97 der DSGVO** ist die Europäische Kommission verpflichtet, dem Europäischen Parlament und dem Rat alle vier Jahre über die Anwendung der Verordnung zu berichten. Diese Berichte dienen nicht nur der Evaluierung der bisherigen Umsetzung, sondern sollen auch Möglichkeiten zur Anpassung und Weiterentwicklung aufzeigen. Der erste Bericht[1], der im Juni 2020 veröffentlicht wurde, lieferte erste Erkenntnisse zur Implementierung und Anwendung der DSGVO in den Mitgliedstaaten. Der zweite Bericht[2] baut auf diesen Erkenntnissen auf und reflektiert die Entwicklungen und Erfahrungen der vergangenen vier Jahre.

[1] https://kurzlinks.de/kl8b

[2] https://kurzlinks.de/72z6

Die wichtigsten Punkte

Bestätigt wird, dass die DSGVO im Wesentlichen ihre Ziele erreicht hat. Sie hat das Bewusstsein für den Schutz personenbezogener Daten in der EU erheblich gesteigert und die Rechte der Bürgerinnen und Bürger gestärkt. Unternehmen und Organisationen haben ihre Datenschutzpraxis verbessert, und eine Harmonisierung der Datenschutzvorschriften in der gesamten EU hat stattgefunden.

Die Kommission stellt fest, dass die DSGVO sowohl auf europäischer als auch auf globaler Ebene Maßstäbe gesetzt hat. Viele Länder außerhalb der EU haben ähnliche Datenschutzgesetze erlassen oder ihre bestehenden Gesetze an die DSGVO angepasst, um den Handel mit der EU zu erleichtern und einen vergleichbaren Datenschutzstandard zu gewährleisten.

Durchsetzung und Sanktionen

Ein zentrales Thema des Berichts ist die Durchsetzung der DSGVO. Die Kommission hebt hervor, dass seit 2018 mehrere hochkarätige Fälle von Datenschutzverletzungen aufgedeckt wurden, die zu signifikanten Bußgeldern geführt haben. Insbesondere gegen große Technologiekonzerne wurden teils sehr hohe Geldstrafen verhängt und der Stellenwert der DSGVO-Compliance verdeutlicht. Dies erfolgte u.a. für Verstöße gegen die Rechtmäßigkeit und Sicherheit der Verarbeitung, Verstöße gegen die Verarbeitung besonderer Kategorien personenbezogener Daten und Verletzungen der Rechte des Einzelnen.

Ein Beispiel ist die Verhängung einer Geldstrafe in dreistelliger Millionenhöhe gegen ein globales Unternehmen, das gegen Vorschriften zur Datenübermittlung in Drittländer verstoßen hatte. Der Fall unterstreicht die strengen Anforderungen der DSGVO an den internationalen Datentransfer und die Notwendigkeit, robuste Datenschutzmaßnahmen im Unternehmen zu implementieren.

Die Durchsetzung in Zahlen:

- EU-Datenschutzbehörden haben über 20.000 Untersuchungen aus eigener Initiative eingeleitet.
- Insgesamt gehen bei ihnen mehr als 100.000 Beschwerden pro Jahr ein.
- Über 20.000 Beschwerden wurden im Wege der gütlichen Einigung beigelegt. Diese wird am häufigsten in Österreich, Ungarn, Luxemburg und Irland angewandt.

Trotz dieser Erfolge weist der Bericht auch auf Unterschiede in der Durchsetzung zwischen den Mitgliedstaaten hin. Während einige Länder proaktive Maßnahmen ergriffen haben, sind andere aufgrund begrenzter Ressourcen oder unterschiedlicher rechtlicher Interpretationen langsamer in der Umsetzung und Durchsetzung der DSGVO. Dies führt zu einer ungleichen Handhabung und möglicherweise zu Lücken im Datenschutz innerhalb der EU.

Zusammenarbeit der Aufsichtsbehörden

Ein weiterer wesentlicher Punkt des Berichts betrifft die Zusammenarbeit zwischen den nationalen Datenschutzbehörden. Die DSGVO sieht Mechanismen wie das Kohärenzverfahren und den Europäischen Datenschutzausschuss (EDSA) vor, um sicherzustellen, dass die Verordnung einheitlich angewendet wird.

Hier einige Zahlen zum Einsatz der Kooperationsinstrumente durch die Behörden:[3]

- Federführende Datenschutzbehörden haben rund 1.500 Beschlussentwürfe herausgegeben, von denen 990 zu endgültigen Beschlüssen führten, mit denen ein Verstoß gegen die DSGVO festgestellt wurde.

[3] Siehe https://kurzlinks.de/72z6

- Datenschutzbehörden aus 18 Mitgliedstaaten erhoben „maßgebliche und begründete Beschwerden“ gegen Beschlüsse der federführenden Aufsichtsbehörde.
- Die Datenschutzbehörden haben fast 1.000 „formelle“ Amtshilfeersuchen und rund 12.300 „informelle“ Ersuchen gestellt.
- Fünf gemeinsame Maßnahmen wurden eingeleitet, an denen Datenschutzbehörden aus sieben Mitgliedstaaten beteiligt waren.

Der Bericht zeigt, dass die Zusammenarbeit zwischen den Aufsichtsbehörden in vielen Fällen funktioniert, es aber auch Herausforderungen gibt, insbesondere bei grenzüberschreitenden Fällen. Ein Beispiel dafür sind langwierige Entscheidungsprozesse in Fällen, die mehrere Länder betreffen, wie z.B. die Untersuchung von großen Technologieunternehmen, deren Geschäftstätigkeiten sich über mehrere Mitgliedstaaten erstrecken. Die Koordination dieser Fälle erfordert erheblichen Aufwand und kann zu Verzögerungen bei der Durchsetzung führen. Aus diesem Grund nahm die Kommission im Juli 2023 einen Vorschlag für eine Verordnung über Verfahrensregeln[4] an. Dieser Vorschlag soll die DSGVO ergänzen, indem er detaillierte Regeln für grenzüberschreitende Beschwerden und die Zusammenarbeit zwischen den Datenschutzbehörden festlegt.

Technologische Entwicklungen und Herausforderungen

Seit dem Beschluss der DSGVO hat sich die Technologie rapide weiterentwickelt, was neue Herausforderungen für den Datenschutz nach sich zieht. Der Bericht behandelt intensiv die Auswirkungen von Technologien wie Künstliche Intelligenz (KI), Big Data und Internet der Dinge (IoT) auf den Datenschutz. Diese neuen Verarbeitungsmethoden haben das Potenzial, große Mengen an personenbezogenen Daten zu verarbeiten und neue Risiken für die Privatsphäre zu bewirken.

Um die DSGVO in dieser Hinsicht zu ergänzen und konkretisieren, hat die EU eine Reihe von Initiativen angenommen, um bestimmte Ziele der Digitalpolitik zu verfolgen. Einige Beispiele:

- Das Gesetz über digitale Dienste[5] (Digital Services Act, DSA) zielt darauf ab, ein sicheres Online-Umfeld für Einzelpersonen und Unternehmen zu schaffen. Es untersagt Online-Plattformen, Werbung basierend auf Profiling zu schalten, wenn dafür „besondere Kategorien personenbezogener Daten“ verwendet werden.
- Das Gesetz über digitale Märkte[6] (Digital Markets Act, DMA) zielt darauf ab, digitale Märkte gerechter und wettbewerbsorientierter zu gestalten. Es verbietet Betreibern, die als Gatekeeper eingestuft wurden, personenbezogene Daten zwischen ihren zentralen Plattformdiensten und anderen Diensten zu „verknüpfen“ und „intern zu verwenden“, es sei denn, der Nutzer hat ausdrücklich zugestimmt.
- Das KI-Gesetz[7] (Artificial Intelligence Act, AI Act) definiert die EU-Datenschutzbestimmungen in speziellen Bereichen, in denen Künstliche Intelligenz zum Einsatz kommt, wie etwa bei biometrischer Fernidentifizierung, der Analyse besonderer Datenkategorien zur Bias-Erkennung sowie der Weiterverarbeitung personenbezogener Daten in KI-Reallaboren.

Daraus ergibt sich für Unternehmen auch die Notwendigkeit, datenschutzfreundliche Technologien zu entwickeln und einzusetzen. Beispielsweise enthält die DSGVO den Grundsatz der Datenminimierung, der sicherstellen soll, dass nur die Daten verarbeitet werden, die für

[4] https://kurzlinks.de/7v9p
[5] https://kurzlinks.de/ec5z
[6] https://kurzlinks.de/8zuf
[7] https://kurzlinks.de/ldrq

einen bestimmten Zweck erforderlich sind. Unternehmen müssen daher bei der Gestaltung ihrer Systeme und Prozesse Anforderungen des Datenschutzes von Anfang an berücksichtigen („Privacy by Design“).

Praktisches Beispiel: Ein Unternehmen, das KI-basierte Personalisierung in seinem Online-Shop nutzt, muss sicherstellen, dass die verwendeten Algorithmen transparent dargestellt und erhobene Daten auf das notwendige Minimum beschränkt werden. Zudem muss sichergestellt werden, dass die Nutzer klar und verständlich über die Datenverarbeitung informiert wurden und ihre Einwilligung erteilt haben.

Einwilligung und Betroffenenrechte

Ein weiteres zentrales Element der DSGVO ist die Stärkung der Betroffenenrechte, insbesondere auf Information, Auskunft, Berichtigung, Löschung und Datenübertragung. Der Bericht stellt fest, dass diese Rechte weitgehend in die Praxis umgesetzt wurden, allerdings gibt es auch hier Herausforderungen.

Viele Unternehmen haben Schwierigkeiten, die Einwilligung der Nutzer auf eine Art und Weise einzuholen, die den Anforderungen der DSGVO entspricht. Einwilligungen müssen ausdrücklich, informiert und freiwillig sein, was in der Praxis oft schwer umzusetzen ist. Der Bericht betont, dass viele Unternehmen ihre Prozesse anpassen mussten, um den strengen Anforderungen gerecht zu werden.

Zum Bewusstsein der Einzelnen für die DSGVO und die Datenschutzbehörden hält der Bericht folgende Zahlen fest:

- 72 % der Befragten in der gesamten EU gaben an, von der DSGVO gehört zu haben, darunter 40 %, die wissen, worum es sich dabei handelt.
- In Schweden ist das Bewusstsein mit 92 % am stärksten, während in Bulgarien mit 59 % das Bewusstsein am schwächsten ausgeprägt ist.
- 68 % der Befragten in der EU geben an, von einer nationalen Behörde gehört zu haben, die für den Schutz ihrer Datenschutzrechte zuständig ist, wobei 24 % aller Befragten angeben, dass sie auch wissen, welche Behörde zuständig ist.

Datentransfers in Drittländer

Die Kommission hält fest, dass der Datentransfer in Drittländer weiterhin eine zentrale Herausforderung darstellt. Der Bericht hebt hervor, dass die Kommission intensiv an der Sicherstellung der Angemessenheit solcher Datentransfers arbeitet, um den Schutz personenbezogener Daten auch außerhalb der EU zu gewährleisten.

Besonders im Fokus stehen die USA. Hier wird der neue Angemessenheitsbeschluss „EU-U.S. Data Privacy Framework“[8] erwähnt, der im Juli 2023 in Kraft trat und als wichtiger Schritt zur Erleichterung von Datentransfers in die USA angesehen wird. Die Kommission betont jedoch, dass die kontinuierliche Überwachung und Evaluierung dieses Rahmens erforderlich ist, um sicherzustellen, dass die Datenschutzstandards auch eingehalten werden.

Zusammenfassend weist der Bericht darauf hin, dass trotz Fortschritten weiterhin sorgfältig geprüft werden muss, ob der Schutz personenbezogener Daten in Drittländern den Anforderungen der DSGVO entspricht. Insbesondere für die USA bleibt dies ein Bereich erhöhter Aufmerksamkeit, um eine sichere und rechtskonforme Datenverarbeitung zu gewährleisten.

Fazit und Ausblick

Der „Zweite Bericht zur Anwendung der Datenschutz-Grundverordnung“ zeigt, dass die DSGVO in den ersten sechs Jahren seit ihrem Inkrafttreten maßgeblich zur Verbesserung des Daten-

[8] www.dataprivacyframework.gov/Program-Overview

schutzes in der EU beigetragen hat. Dennoch bleiben verschiedene Herausforderungen, insbesondere in Bezug auf die Durchsetzung, die Anpassung an neue Technologien und die Harmonisierung zwischen den Mitgliedstaaten. Die Kommission betont die Notwendigkeit, die Anwendung der DSGVO kontinuierlich zu überwachen und bei Bedarf anzupassen, um sicherzustellen, dass der Datenschutz auch in einer sich schnell verändernden digitalen Welt gewährleistet bleibt.

2. Update zu den Änderungen im Datenschutzgesetz

Eine Entscheidung des Verfassungsgerichtshofs[9] (VfGH) machte die Änderung des Datenschutzgesetzes[10] notwendig, indem sie die bisherige Formulierung von § 9 DSG mit Juni 2024 aufhob. Die Entscheidung betrifft die nationale Umsetzung einer der Öffnungsklauseln der DSGVO, die journalistische Tätigkeiten von den strengen Datenschutzregelungen ausnimmt.

Art. 85 DSGVO wurde ursprünglich so umgesetzt, dass alle Regelungen der DSGVO für den Bereich der journalistischen Zwecke für unanwendbar erklärt wurden. Diese Pauschalausnahme ging dem VfGH jedoch zu weit. Stattdessen müsse eine gesetzliche Interessensabwägung vorgenommen werden, um den Schutz personenbezogener Daten und das Recht auf freie Meinungsäußerung angemessen in Einklang zu bringen.

Das neu geregelte Medienprivileg verpflichtet nun auch Medien und deren journalistische Mitarbeiter zur Einhaltung der DSGVO-Bestimmungen. Das Redaktionsgeheimnis bleibt aber geschützt, indem Medien nicht verpflichtet sind, ihre Informationsquellen bekanntzugeben, zB bei Auskunftsbegehren vor Veröffentlichung des Beitrags. Neu ist auch, dass Bürgerjournalisten, darunter Privatpersonen und NGOs, von den Regelungen profitieren sollen. Die Ausnahmen und Abweichungen von der DSGVO für diese Gruppen sind zwar weniger umfassend als für professionelle Medienunternehmen und -dienste. Die Regelung soll aber sicherstellen, dass auch nicht-professionelle Journalisten einen Beitrag zur öffentlichen Debatte leisten können.

Eine weitere Änderung des Datenschutzgesetzes kommt im Gefolge eines EuGH Urteils vom 16. 1. 2024 (C-33/22)[11], das klarstellte, dass die DSGVO auch für die Verarbeitung personenbezogener Daten durch parlamentarische Gremien gilt. Bei der Änderung handelt sich um die Schaffung eines parlamentarischen Datenschutzkomitees, das ab 2025 als eigenständige Aufsichtsbehörde im Bereich der Gesetzgebung fungieren wird und für den Nationalrat, den Bundesrat, den Rechnungshof und die Volksanwaltschaft zuständig ist.

Im Zuge der Gesetzesänderung wurden auch die Rechte der Betroffenen angepasst. Die Novelle zum Informationsordnungsgesetz[12] sieht im Einklang mit der DSGVO eine Beschränkung von Auskunfts-, Löschungs- und Berichtigungsrechten vor, um die parlamentarische Arbeit nicht zu beeinträchtigen. Allerdings können in besonderen Fällen Anträge auf Entfernung von Inhalten von der Parlamentswebsite gestellt werden. Der Nationalratspräsident oder die Nationalratspräsidentin entscheidet über datenschutzrechtliche Anträge, wobei die jeweils zuständigen Datenschutzbeauftragten und Antragsteller einbezogen werden müssen.

[9] https://kurzlinks.de/ypui
[10] https://kurzlinks.de/aiq6
[11] https://kurzlinks.de/mie3
[12] https://kurzlinks.de/mi9x

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!

3. Neues aus der Rechtsprechung

EuGH stärkt Verbandsklagen

Der Europäische Gerichtshof (EuGH) hat in einem neuen Urteil vom 11. Juli 2024 (C-757/22)[13] die Klagebefugnis von Verbraucherschutzverbänden bei Verstößen gegen die Informationspflichten nach Art. 12 und 13 DSGVO bestätigt und damit die Anwendung von Art. 80 Abs. 2 DSGVO weiter gestärkt.

Hintergrund des Verfahrens war ein Rechtsstreit zwischen dem Bundesverband der Verbraucherzentralen (vzbv) und Meta Platforms Ireland Limited. Im sogenannten App-Zentrum von Facebook sah der vzbv eine unrechtmäßige Datenverarbeitung, da Nutzer unzureichend über die Erhebung und Weitergabe ihrer Daten informiert wurden. Die Einwilligung, die in diesem Kontext eingeholt wurde, erachtete der vzbv als unwirksam. Der Bundesgerichtshof (BGH), der sich in dritter Instanz mit dem Rechtsstreit befasst hat, hielt die Klage des vzbv für begründet. Er fragte den EuGH jedoch, ob der Verband auch nach Inkrafttreten der DSGVO noch berechtigt ist, eine solche Klage zu erheben.

Mit seinem Urteil aus dem Jahr 2022 (C-319/20)[14] hatte der EuGH klargestellt, dass solche Klagen zum Schutz von Verbraucherinteressen keine konkrete Verletzung des Rechts auf Datenschutz oder einen entsprechenden Auftrag der betroffenen Personen erfordern. Es reiche aus, dass die fragliche Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen nach der DSGVO beeinträchtigen könne.

Nun bezweifelte der BGH, ob eine Verletzung der Informationspflichten als Verstoß „infolge einer Verarbeitung“ angesehen werden kann, der eine Verbandsklage rechtfertigt.

Der EuGH entschied, dass die Nichteinhaltung von Informationspflichten wie das Versäumnis, klare Informationen über Verarbeitungszwecke und Datenempfänger gem. Art. 12 und 13 DSGVO bereitzustellen, als Verstoß „infolge der Verarbeitung“ angesehen werden kann. Die Verarbeitung von Daten kann als unrechtmäßig angesehen werden, wenn diese Rechte verletzt werden. Sie fällt in den Anwendungsbereich des Art. 80 Abs. 2 DSGVO und eröffnet damit die Möglichkeit von Verbandsklagen.

Kein überwiegendes Geheimhaltungsinteresse für Detektivberichte

Ein aktuelles Urteil (13 U 48/23)[15] des 13. Zivilsenats des Oberlandesgerichts Oldenburg behandelt den Anspruch auf Offenlegung eines Detektivberichts. Im konkreten Fall hatte eine Versicherung ein Detektivbüro mit der Observierung einer Person beauftragt, die nach einem Verkehrsunfall Ansprüche wegen Verletzungen geltend gemacht hatte. Die Versicherung vermutete, dass die tatsächliche Beeinträchtigung des Klägers geringer war als angegeben, und beauftragte daher eine Detektei, dessen Alltag über mehrere Wochen hinweg zu überwachen.

Nach Abschluss der Observation erstellte die Detektei einen Bericht über die gesundheitlichen Einschränkungen des Klägers. Dieser forderte im Rahmen einer Klage vor dem Landgericht Osnabrück Einsicht in die gesammelten personenbezogenen Daten und eine Kopie des Ermittlungsberichts. Die Versicherung verweigerte die Herausgabe mit dem Argument, dass die Informationen sensible medizinische Daten enthielten, deren Offenlegung im Hinblick auf mögliche spätere Rechtsstreitigkeiten die

[13] https://kurzlinks.de/phn4
[14] https://kurzlinks.de/s0lf
[15] https://kurzlinks.de/9vsf

Geheimhaltungsinteressen der Versicherung verletzen könnte.

Das Landgericht hatte ein überwiegendes Geheimhaltungsinteresse der Versicherung anerkannt und die Klage abgewiesen. Die daraufhin eingelegte Berufung des Klägers war jedoch erfolgreich. Das Oberlandesgericht entschied, dass dem Kläger nach Art. 15 DSGVO ein Auskunftsanspruch zustehe. Es stellte klar, dass personenbezogene Daten grundsätzlich offengelegt werden müssen, um die Rechtmäßigkeit ihrer Verarbeitung zu überprüfen. Die Geheimhaltungsinteressen der Versicherung gegenüber dem Betroffenenrecht auf Auskunft würden in diesem Fall nicht überwiegen, nicht zuletzt, da die Daten dem Kläger im Fall eines zukünftigen Rechtsstreits ohnehin zugänglich gemacht werden müssten.

Softwareanbieter haftet für rechtswidrig eingesetzte Cookies

In einem wegweisenden Urteil (Az. 6 U 192/23)[16] hat das Oberlandesgericht Frankfurt am Main entschieden, dass Microsoft Advertising haftet, wenn Cookies ohne Zustimmung der Nutzer auf deren Geräten gespeichert werden. Dies gilt auch, wenn diese Cookies durch Drittwebsites gesetzt werden, die den Microsoft-Dienst nutzen.

Cookies werden auf Endgeräten der Nutzer gespeichert und ermöglichen personalisierte Werbung und das gezielte Ausspielen von Anzeigen. Microsoft Advertising bietet Unternehmen die Möglichkeit, ihre Werbung auf Webseiten zu platzieren und den Erfolg dieser Kampagnen zu messen. Dabei wird von Microsoft ein Code zur Verfügung gestellt, der in die Websites der Kunden integriert wird. Anschließend kommen Cookies zum Einsatz, die vom Microsoft-Programmcode auf diesen Webseiten gesetzt und ausgelesen werden.

Eine Klägerin hatte Microsoft Advertising verklagt, weil auf ihren Geräten Cookies gespeichert wurden, ohne dass sie ihre Einwilligung gegeben hatte. Microsoft Advertising fordert in seinen Allgemeinen Geschäftsbedingungen (AGB), dass die Webseitenbetreiber dafür sorgen, dass die erforderliche Einwilligung eingeholt wird.

Das OLG Frankfurt am Main hat jedoch entschieden, dass Microsoft Advertising durch die AGB nicht von seiner Verantwortung entbunden ist. Das Gericht stellte klar, dass Microsoft die gesetzliche Verpflichtung gem. § 25 Abs. 1 Satz 1 TTDSG erfüllen muss, wonach jeder, der Cookies speichert oder darauf zugreift, die ausdrückliche Einwilligung der Nutzer einholen muss. Microsoft Advertising könne sich nicht auf die Verpflichtung der Webseitenbetreiber verlassen. Das Urteil, das im Eilverfahren gefällt wurde, bestätigte die Haftung des Unternehmens für die Speicherung und Auswertung der Cookies ohne Einwilligung.

4. Top Bußgelder

1. Verbotene Werbeanrufe

Die spanische Datenschutzbehörde (Agencia Española de Protección de Datos, AEPD)[17] ging auf eine Beschwerde eines Bürgers ein, der wiederholt unerwünschte Werbeanrufe von Vodafone erhalten hatte, obwohl er dafür nie seine Einwilligung gegeben hatte. Die betroffenen Telefonnummern waren zudem in einer Sperrliste eingetragen, um solche Anrufe zu verhindern.

Die AEPD forderte das Unternehmen auf, Informationen über die durchgeführten Anrufe und

[16] https://kurzlinks.de/digs

[17] https://kurzlinks.de/m77n

die damit verbundene Datenverarbeitung bereitzustellen, doch trotz mehrmaliger Anfrage blieb eine Antwort von Vodafone aus. Dies führte zu einer Geldbuße in der Höhe von **EUR 200.000** auf Grund eines Verstoßes gegen Art. 58 Abs. 1 DSGVO.

2. Löschbegehren versagt

Eine Privatperson beschwerte sich ebenfalls bei der spanischen Datenschutzbehörde, nachdem das FinTech-Unternehmen ID Finance Spain ihre wiederholte Aufforderung zur Löschung personenbezogener Daten ignoriert hatte. Das Unternehmen begründete dies mit einer angeblichen Schuld der Person, die jedoch auf Identitätsdiebstahl zurückzuführen war. Die AEPD stellte fest, dass die Daten ohne gültige Einwilligung gespeichert worden waren und daher nicht hätten gespeichert werden dürfen. Zudem fehlte ein Datenschutzbeauftragter bei ID Finance Spain. Aufgrund dieser Verstöße (Art. 6, Art. 17, Art. 37 Abs. 7 DSGVO) gegen die DSGVO verhängte die Behörde ein Bußgeld von **EUR 180.000**.

3. Entlassener Mitarbeiter mobbt Kundin

Eine Dame beschwerte sich über den Lebensmittelgroßhändler Metro, nachdem ein entlassener Lieferant des Unternehmens ihre im Firmensystem gespeicherten Daten missbraucht hatte, um ihr sarkastische SMS zu schicken und die Schuld für seine Entlassung zu geben. Die Frau verlangte daraufhin die Löschung ihrer personenbezogenen Daten, was Metro mit der Begründung ablehnte, dass ihr Ehemann der eigentliche Kunde sei. Die griechische Datenschutzbehörde[18] stellte fest, dass Metro der Anfrage hätte nachkommen müssen und dass es an ausreichenden Maßnahmen zum Schutz der Daten mangelte. Außerdem meldete Metro den Vorfall nicht. Dies führte zu einem Bußgeld von **EUR 50.000** auf Grund der Verletzung der Art. 15, 17, 24, 32 und 33 DSGVO**.**

4. Fehlende Schutzmaßnahmen für Datentransfers

Die niederländische Datenschutzbehörde Autoriteit Persoonsgegevens (AP)[19] hat Uber Technologies und Uber BV wegen eines Verstoßes gegen die DSGVO mit einer hohen Geldstrafe in der Höhe von **290 Mio. EUR** belegt. Der Grund dafür war die Übermittlung von Mitarbeiterdaten in die USA ohne angemessene Schutzmaßnahmen gemäß Art. 44 ff. DSGVO. Über einen Zeitraum von rund zwei Jahren wurden Daten zahlreicher Uber-Mitarbeiter an die US-Muttergesellschaft und andere Unternehmen in den USA weitergeleitet, ohne dabei die erforderlichen Datenschutzvorkehrungen zu treffen. Zu den betroffenen Daten gehörten nicht nur Stammdaten wie Name und Führerscheininformationen, sondern auch sensible Daten wie Standort- und Kontodaten, Vorstrafen und Gesundheitsinformationen.

Ursprünglich war Uber im Rahmen des Privacy Shield-Abkommens zertifiziert, doch nach dessen Aufhebung versäumte das Unternehmen, alternative Schutzmaßnahmen zu ergreifen. Seit Ende des letzten Jahres ist Uber jedoch nach dem neuen Data Privacy Framework zwischen der EU und den USA zertifiziert.

••••

[18] https://kurzlinks.de/n4wf

[19] https://kurzlinks.de/y5bs

Privacy Ring: Transparenz im Spannungsfeld des Datenschutzes

Der Datenschutzverein Privacy Ring[20] lädt am **19. September 2024** zur inzwischen 12. Fachtagung in Wien am 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.

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 **ein Vertreter der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

11. November 2024, 9:15 – 17:00 Uhr:

„Rechtsentwicklung und Best Practices“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Menas Saweha, Rona Paca
Gastreferent: Vertreter der Österreichischen Datenschutzbehörde

12. November 2024, 9:15 – 17:00 Uhr:

„Updates zur praktischen Anwendbarkeit und Use-Cases“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, 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.

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