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

August 2022 Ausgabe Nr. 103

Liebe Leserinnen und Leser,

diese DSG-Info widmet sich unter anderem der Abmahnwelle eines NÖ-Rechtsanwalts, der derzeit Unternehmen in großer Anzahl wegen des Einsatzes von Google Fonts und anderen Google-Online-Diensten anschreibt. Darüber hinaus bleibt das Thema Google Analytics und internationaler Datenverkehr weiterhin aktuell. Mittlerweile hat neben der österreichischen und niederländischen Datenschutzbehörde auch die italienische Behörde eine Entscheidung gegen den weiteren Einsatz des US-Webanalysedienstes getroffen. Auch die französische Behörde CNIL hat klar zu erkennen gegeben, dass das Thema nicht mehr übergangen werden kann.

Zusätzlich besprechen wir aktuelle Datensicherheitsvorfälle aus Österreich und wollen Sie auf gesetzliche Änderungen in den Bereichen Whistleblowing und Verbandsklagen sowie auf eine Änderung des Datenschutzrechts in Großbritannien hinweisen.

Abschließend möchten wir Sie herzlich zu unseren DSGVO-Praxisseminaren im Oktober einladen und wünschen Ihnen eine angenehme Lektüre.

1. Abmahnwelle: Für den Einsatz von Google-Diensten EUR 190,00

Im Hinblick auf die gegenwärtig grassierende Abmahnwelle des NÖ-Rechtsanwalts H. weisen wir darauf hin, dass die Einbindung von Google-Diensten wie Google Fonts, Google Analytics und Google Tag Manager seit dem EuGH-Erkenntnis der RS Schrems II sowie den Bescheiden der österreichischen DSB (Näheres dazu unter Punkt 3.) nicht mit den Regelungen zum Internationalen Datenverkehr vereinbar ist.

Sie müssen daher dafür sorgen, dass Ihre Websites nur Cookies und Dienste einsetzen, die keinen Bezug zum internationalen Datenverkehr aufweisen. Fonts oder Skript-Bibliotheken sollten, soweit möglich, lokal eingebunden werden.

Das in der Abmahnung enthaltene Auskunftsbegehren ist jedoch unbedingt zu beantworten, auch wenn es unter Umständen zu einer Nullauskunft führt. Das Anfordern von Vertretungsvollmacht und Ausweiskopien ist nicht zielführend, da diese bereits auf der Website des Abmahnanwalts veröffentlicht wurden. Sollten Sie ein solches Abmahnschreiben erhalten haben, muss genau geprüft werden, welche Ansprüche Ihnen gegenüber geltend gemacht werden und ob diese überhaupt berechtigt sind. Zur Beantwortung des Auskunftsbegehrens müssen u.a. die Webserver-Protokolle nach der IP-Adresse im Abmahnschreiben

durchsucht werden. In den meisten Fällen ist dazu die Unterstützung Ihres Hosting-Dienstleisters erforderlich.

Die österreichische **Datenschutzbehörde** hat sich bereits in einer Stellungnahme zur gegenwärtigen Abmahnwelle geäußert. Näheres dazu finden Sie **hier**.

2. Datensicherheit in Österreich

Das Thema Daten- und Informationssicherheit wird oftmals nachrangig behandelt, obwohl es mit dem Datenschutzgedanken Hand in Hand gehen sollte. Versäumnisse im Bereich der „TOM" (technische und organisatorische Sicherheitsmaßnahmen) führen oft zu unangenehmen Situationen. Besonders der öffentliche Bereich ist für Angreifer attraktiv, da mit diesen Daten nicht nur wirtschaftlicher Schaden verursacht, sondern auch politischer Missbrauch betrieben werden kann. In Österreich waren zuletzt gleich mehrere öffentliche Stellen von Data Breaches betroffen.

Zum einen die Stadt Baden, die 33.000 Adressdatensätze auf einem Webserver unzureichend geschützt und dadurch für Angreifer zugänglich gemacht hatte. Mangelhafte Sicherheitsvorkehrungen im Zusammenhang mit einer Stadt-App (*Baden Card*) machten es einem Investigativ-Team möglich, mit einfachen Mitteln Zugriff auf Stammdaten der Bewohner wie Name, Anschrift, Geschlecht, Geburtsdatum sowie Informationen über die Qualität des Wohnsitzes zu erhalten. Die Gemeinde wurde von diesem Umstand in Kenntnis gesetzt und meldete den Vorfall an die Datenschutzbehörde. Ob die Daten von Dritten abgegriffen wurden ist unklar.

Der Vorfall zeigt, dass auch kommunale Strukturen anfällig für Sicherheitslücken sind, wenn keine geeigneten Sicherheitsmaßnahmen gesetzt werden. **Webserver** sind besonders exponiert und sollten stets vor externen Zugriffen geschützt sein. Wenn eine große Anzahl personenbezogener Daten verarbeitet wird, ist eine **Sicherheitsüberprüfung** durch kompetentes Personal, im Idealfall durch externe Spezialisten, ein absolutes Muss.

Allerdings sind Data Breaches auch auf Landesebene kein Einzelfall: Das **Land Kärnten** wurde gezielt von einer „Hackergruppe" angegriffen, der es gelang, zehntausende Datensätze einzusehen und abzugreifen. Hierbei handelt es sich um einen Angriff, dessen Tragweite noch nicht vollständig geklärt wurde. Es handelt sich laut Medienberichten um über 250 Gigabyte an Daten, die neben Stammdaten auch andere Datensätze beinhalten.

Die Hintergründe wurden nicht im Detail veröffentlicht, es dürfte sich aber um eine erfolgreiche Phishing-Attacke gehandelt haben. Der „Unsicherheits-Faktor Mensch" lässt sich nie ausräumen, Sensibilisierungsmaßnahmen und Benutzerschulungen können das Sicherheitsrisiko aber zumindest reduzieren. Hier zeigt sich wieder, dass **technische Vorkehrungen** allein **nicht ausreichen**, sondern immer durch **organisatorische** Maßnahmen ergänzt werden müssen, um ein ausreichendes Sicherheitsniveau zu erzielen.

Bei einem Data Breach muss es sich aber nicht immer um unrechtmäßige Zugriffe von außen handeln: Bei der **Allgemeinen Unfallversicherungsanstalt (AUVA**) wurden 6.000 E-Mail-Postfächer der Mitarbeiter durchsucht, um einen potenziellen Whistleblower ausfindig zu machen. Diese Vorgehensweise widerspricht der kommenden Gesetzeslage zum **HinweisgeberInnenschutzgesetz (HSchG)** und stellt unter Umständen einen Verstoß gegen das Grundrecht auf Geheimhaltung der Daten der Mitarbeiter dar. Mehr dazu weiter unten.

3. Google Analytics-Entscheidungen

Wie eingangs erwähnt, gehen die Datenschutzbehörden verstärkt auf Grundlage des EuGH-Erkenntnisses in der RS Schrems II vor. Die Österreichische Datenschutzbehörde hat bereits **zwei Erkenntnisse** zum Einsatz von Google Analytics gefällt, in der sie die Rechtmäßigkeit des weiteren Einsatzes ablehnt.

In Österreich gibt es daher mittlerweile zwei erstinstanzliche Entscheidungen (von **12/2021** und **04/2022**) der DSB zum Thema Google Analytics. Der Tenor ist gleichlautend: Die Übermittlung personenbezogener Daten in die USA ist unter den gegenwärtigen rechtlichen Voraussetzungen unzulässig, da Google-IDs Personenbezug haben und die Standardvertragsklauseln nicht für die Übermittlung in die USA ausreichen. Im Unterschied zum ersten Bescheid besagt die mit 22. April 2022 datierte Entscheidung klar, dass die Risikoeinschätzung eines „potenziellen" Eingriffs durch die US-Behörden bei der Rechtmäßigkeitsbewertung keine Rolle spielt. Für die Datenschutzbehörde ist unerheblich, ob es **unwahrscheinlich** ist, dass die Daten unrechtmäßig offengelegt werden. Es reicht bereits die **Rechtschutzlücke** eines Zugriffs auf die bei Google gespeicherten Daten zur Feststellung des unzureichenden Schutzniveaus aus. Damit hat die DSB den „**risikobasierten Ansatz bei Drittlandsübermittlungen**" für **nicht anwendbar** erklärt.

Darüber hinaus enthält das Erkenntnis das wichtige Detail, dass Verstöße gegen Art. 44 DSGVO (Internationaler Datenverkehr) subjektive Rechte betroffener Personen begründen und daher den Beschwerdeweg eröffnen. Dies ist auch ein möglicher Auslöser für die aktuelle Abmahnwelle.

4. Kündigungsschutz für Datenschutzbeauftragte – EuGH-Entscheidung C-534/20

Bekanntermaßen ist die Position des internen Datenschutzbeauftragten durch die DSGVO besonders geschützt. Die Person muss weisungsfrei und mit ausreichend Ressourcen und Informationen versehen werden, um beraten, kontrollieren und schulen können. Dabei ist wichtig, dass kein Druck von Seiten der Geschäftsführung oder Kollegen ausgeübt wird, um die Aufgaben in Erfüllung der DSGVO gewissenhaft vollziehen zu können. Falls es dennoch zu einer Trennung zwischen internem Datenschutzbeauftragten und dem Unternehmen kommt, ist genau zu prüfen, wie die nationale Rechtslage den Kündigungsschutz vorsieht.

Während die DSGVO nur die Motivkündigung, also die Kündigung wegen der Erfüllung der Aufgaben, verbietet, sieht die deutsche Regelung des § 6 Abs. 4 BDSG vor, dass nur aus wichtigem Grund (d.h. unabhängig von der Tätigkeit) gekündigt werden dürfe. Nach dem Urteil des EuGH kann jeder EU-Mitgliedstaat frei entscheiden, strengere Regelungen hinsichtlich der Kündigung eines DSBA zu treffen, als sie die DSGVO enthält.

Fazit: Um Probleme zu vermeiden, ist es wichtig, die arbeitsrechtliche Position des Datenschutzbeauftragten festzulegen und genau zu prüfen. Der Arbeitgeber und Verantwortliche muss darauf achten, dass dem internen DSBA genug Freiraum zur Erfüllung seiner Aufgaben ohne Repressalien oder unsachlichem Druck zur Verfügung steht. Dennoch sollte man sich im Vorhinein ausreichend Gedanken zu potenziellen Trennungsmöglichkeiten (zB mittels Befristung) machen und diese vertraglich regeln, um dem weitreichenden Kündigungsschutz des DSBA nicht unverhältnismäßig viel Spielraum zu geben.

5. Verbandsklagen-Richtlinie

Bekanntlich hat es der österreichische Gesetzgeber verabsäumt, zum vorgesehenen Stichtag ein Gesetz zur Umsetzung der **Whistleblowing-Richtlinie** zu erlassen. Zum HinweisgeberInnenschutzgesetz kursiert bisher nur ein Entwurf, der bis dato noch kein Verlautbarungsdatum erhalten hat. Nun ist der Gesetzgeber erneut gefordert, bis Ende dieses Jahres ein Umsetzungsgesetz zu einem heiklen wirtschaftlichen Thema zu erlassen: Die Rede ist von der Umsetzung der **EU-Verbandsklagen-Richtlinie**, die bis Dezember 2022 erfolgen muss.

Der Inhalt der Verbandsklagen-RL kann weitreichende Folgen für Datenschutzverstöße haben, die eine Multiplikatorwirkung erzeugen. Personen mit gleichen Ansprüchen soll es ermöglicht werden, ihre Ansprüche gemeinsam gegenüber einem Verantwortlichen oder Auftragsverarbeiter geltend zu machen. Der geringe Streitwert mancher datenschutzrechtlichen Ansprüche kann derzeit noch viele Betroffene davon abhalten, Datenmissbrauch, Data Breaches oder die Verarbeitung ihrer Daten ohne gültige Rechtsgrundlage einzuklagen. Allerdings zeigt bereits die aktuelle Abmahnwelle, dass auch geringe Ansprüche erhebliche wirtschaftliche Folgen haben können.

Sollte der EuGH darüber hinaus entscheiden, dass auch geringwertige Verstöße Anspruch auf immateriellen Schadenersatz eröffnen, kann bereits ein Werbe-Newsletter, der ohne dokumentierte Einwilligung an eine größere Personenzahl versendet wurde, zu einem kollektiven Schadenersatzanspruch aufgrund des Verstoßes gegen Art. 6 DSGVO führen. Diese Tendenz, gepaart mit der Möglichkeit einer Verbandsklage, kann Unternehmen in signifikante finanzielle Bedrängnis bringen, zumal die Definition eines Verbandes dadurch erfüllt ist, dass eine NGO seit mehreren Jahren auf diesem Gebiet tätig ist. Damit wäre beispielsweise der Verein NYOB von Max Schrems als ein

solcher Verband anzusehen und (neben dem VKI und der AK) berechtigt, Ansprüche für Betroffene kollektiv geltend zu machen. Bisher hat der österreichische Gesetzgeber von der Möglichkeit abgesehen, dass NGOs Schadenersatzansprüche aus Datenschutzverletzungen geltend machen können. Mit der Umsetzung der Verbandsklagen-RL wäre dieses „Geschäftsfeld" aber gesetzlich eröffnet.

Weiters kann das Prozessrisiko durch sog. Prozessfinanzierer abgefedert werden, die bereits in Deutschland durch die steigende Anzahl an Schadenersatzverfahren an Beliebtheit gewonnen haben. Von ihnen werden insbesondere Auskunftsansprüche genutzt, um Beträge im vierstelligen Bereich einzuklagen.

Offen ist auch, wie der Gesetzgeber mit dem Thema „Sammelklage" umgehen wird, da diese keine Rechtstradition in Österreich besitzt und trotz der herannahenden Frist noch keine Bestrebungen für die Umsetzung vorliegen. Sollte – wie bei der Whistleblowing-Richtlinie – zum Stichtag noch kein Umsetzungsgesetz vorliegen, würden sich Ansprüche zugunsten der Verbraucher direkt aus der Richtlinie ableiten lassen.

6. Exkurs: USA und UK

Im Hinblick auf die Rechtsprechung zu Google-Diensten bleibt derzeit nur die Hoffnung auf das **EU-US-Vorhaben eines „Data Privacy Frameworks"**. Bereits im Frühjahr angekündigt, wird es wohl noch einige Zeit dauern, bis sich die Regierungsvertreter auf einen Text einigen, um die gekippten Abkommen „Safe Harbor" und „Privacy Shield" zu ersetzen.

Umso bemerkenswerter ist das Bestreben Großbritanniens, mit einem neuen Datenschutzgesetz die Abkehr von der DSGVO zu betreiben. Der bestehende Angemessenheitsbeschluss nach dem Brexit enthält einen Evaluierungsmechanismus, der zeigen wird, ob durch die Änderung des Gesetzes das bisherige Datenschutzniveau erhalten bleibt oder ein amerikanisches Schicksal droht.