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

Februar 2022 Ausgabe Nr. 102

Liebe Leserinnen und Leser,

wir hoffen, Sie sind gut ins neue Jahr gestartet.

Wir möchten Sie wie gewohnt, aber im neuen Design, über Neuigkeiten und Änderungen in den Bereichen Datenschutz und Informationssicherheit informieren.

1. Datenschutzbehörde erklärt Einsatz von Google Analytics für unzulässig

Max Schrems hat mit seiner Datenschutz-NGO NOYB einen Bescheid gegen ein Medienunternehmen erwirkt, in dem der Einsatz von Google Analytics für die Erhebung und Verarbeitung von Nutzerstatistiken für unzulässig erklärt wurde.

Hierzu ist durch die Datenschutzbehörde die Entscheidung ergangen, dass dieser Einsatz gegen die Rechtsprechung des EuGH bzw. die geltende Rechtslage nach Kapitel V (Internationaler Datentransfer) verstößt. Dies liegt vor allem an der fehlenden Anonymisierung der IP-Adressen und dem fehlenden Hinweis zur entsprechenden Übermittlungsgrundlage.

Es ist anzumerken, dass es sich um den erstinstanzlichen Teilbescheid zu einem Sachverhalt aus dem Jahr 2020 handelt, der möglicherweise noch im verwaltungsgerichtlichen Weg aufgehoben wird. Mit einer Erkenntnis des Bundesverwaltungsgerichts ist jedoch erst in ca. 6 bis 12 Monaten zu rechnen. Daher wird die Datenschutzbehörde in Österreich wohl in ähnlich gelagerten Fällen zunächst bei dieser Linie bleiben.

Offen bleibt der zweite Teilbescheid der DSB, der angeben soll, welche Rolle Google in diesem Konstrukt einnimmt und ob es ein Auftragsverarbeiter oder gemeinsamer Verantwortlicher mit Eigeninteresse ist. Dieser Bescheid wird wahrscheinlich wesentlich mehr Verwaltungsaufwand auslösen.

Bei dieser Thematik ist zur Zeit einiges in Bewegung. Insbesondere sind das Cookiebot-Urteil des VG Wiesbaden zu erwähnen, welches eine einstweilige Verfügung ausgesprochen hat, und die Entscheidung der französischen Datenschutzbehörde CNIL, Google und Facebook auf Grundlage der e-Privacy-RL Millionenbußgelder aufzuerlegen. Und auch die niederländische Behörde hat im Dezember 2021 den Einsatz von Google Analytics für unzulässig erklärt.

Zusätzlich hat die CNIL in einer Stellungnahme weitere „Anordnungen (Orders to Comply)“ an französische Websitebetreiber versendet, nach denen die weitere Nutzung von Google Analytics aufgrund des internationalen Datentransfers als unzulässig erachtet wird. Die Behörde

vertritt die Ansicht, dass aus europäischer Sicht die Nutzung von Google Analytics illegal ist.

Wir raten gegenwärtig davon ab, Google Analytics einzusetzen und empfehlen eine Deaktivierung des Dienstes. Als alternatives Tool empfehlen wir beispielweise die Lösung von Matomo/Piwik, die sich datenschutzfreundlich auf der eigenen Website implementieren lässt, und zwar weiterhin einwilligungsbedürftig ist, allerdings keine Drittlandübermittlung darstellt. Selbstverständlich sind auch andere Webanalyseanbieter problemlos zulässig, sofern sie aus einem Land mit angemessenem Datenschutzniveau stammen und keine US-Auftragsverarbeiter einsetzen.

Sollte es gegenwärtig zu einem Verfahren vor der Datenschutzbehörde kommen, ist mit keinem anderweitigen Ergebnis zu rechnen als dass die Nutzung von US-Diensten zur statistischen Analyse oder Werbung nicht mit dem EuGH-Urteil in der RS Schrems-II in Einklang steht.

Für den weiteren Google Analytics-Einsatz wäre es aus Compliance-Sicht notwendig, zusätzliche Maßnahmen wie den Abschluss der neuen SCCs (seit 09/2021 in Geltung) sowie den Einsatz technischer Verschlüsselungsoptionen und Anonymisierungstechniken vorzunehmen. Bei Google ist dokumentiert anzufragen, welche Maßnahmen im Rahmen eines TIA (Transfer Impact Assessment) als geeignete Garantien angeführt werden können, um den Anforderungen an den internationalen Datenverkehr zu entsprechen.

Sie können das Erkenntnis im Original auf der Website von NOYB nachlesen.

2. Belgische Behörde straft Werbe-Organisation IAB Europe

Der Einsatz von Cookies und Trackern folgt dem Schema „notwendige Cookies“, „Werbe-Cookies“ und anderweitige Tracker. Die Organisation IAB Europe fungiert als Schnittstelle zur Einteilung dieser Cookies, die entweder als einwilligungsfrei oder einwilligungsbedürftig anzusehen sind, und bietet das sogenannte Real-Time-Advertising für das Ausspielen von Werbeanzeigen auf Websites an.

Die belgische Datenschutzbehörde APD hat IAB Europe nun für den Betrieb seines „Transparency & Consent Framework (TCF)“ mit einem Bußgeld von EUR 250.000 belegt. Begründet wird dies mit mangelnder Transparenz und damit einhergehend der Unfähigkeit, für den Cookie-Einsatz eine informierte Einwilligung einzuholen. Die Bußgeld-Entscheidung erging nach dem „One-Stop-Shop“-Prinzip und gilt daher für die gesamte EU (anders als beispielsweise das Erkenntnis der DSB oder der CNIL).

Der Grund für das Bußgeld liegt in der intransparenten Vorgehensweise von IAB Europe: Sobald ein Cookie-Banner erscheint und ein Nutzer auf „Akzeptieren“ klickt, wird ein sog. „TC-String“ erstellt und an die teilnehmenden Partner von IAB Europe geschickt. Diese Partner sind Teil eines Open-RTB-Netzwerks (real time bidding), das in Echtzeit Werbeplatzauktionen ermöglicht und somit Nutzern gezielt interessenbasierte Werbung anzeigen kann.

Die belgische Behörde kritisiert diese Vorgehensweise als nicht datenschutzkonform. Die Nutzer wüssten nicht, dass mit ihren auf diese Weise erzeugten Werbe-IDs Datenhandel betrieben wird. Das Einholen einer Werbeeinwilligung sei bereits für die eigene Website durch die vagen Kategorien intransparent und damit ungültig. Die Verwendung dieser Nutzerprofile zur Auktion und Ausspielung von personalisierter Werbung sei nicht mit der erteilten Einwilligung in Einklang zu bringen und daher unrechtmäßig.

Die Entscheidung ist nicht rechtskräftig und IAB Europe hat bereits Rechtsmittel dagegen erhoben. Auch hier gilt, dass von der weiteren Nutzung dieses „Transparency & Consent

Frameworks“ als Käufer oder Verkäufer von Werbeplätzen derzeit abzuraten ist. Aufgrund des Charakters der Datenerhebung und Weiterverwendung nimmt die belgische Behörde eine gemeinsame Verantwortung gem. Art. 26 DSGVO an, die auch den einzelnen Websitebetreiber für die Verstöße von IAB Europe und seinen Partnern haftbar machen kann.

IAB Europe hat nun 6 Monate Zeit, seine Vorgaben in Einklang mit der Rechtslage zu bringen sowie die zusätzlichen Pflichtverletzungen wie unzureichende TOM, das Fehler eines Verarbeitungsverzeichnisses, einer Datenschutz-Folgenabschätzung und einer Art. 26-Vereinbarung zu beheben.

3. DSB: Kooperationsverpflichtung verletzt

In diesem Erkenntnis belegte die Behörde ein Unternehmen mit einem Bußgeld für die fehlende Kooperation in gleich drei Beschwerdeverfahren. Das Unternehmen beteiligte sich an zwei Beschwerdeverfahren gar nicht, am dritten erst verspätet.

Aufgrund der in Art. 31 DSGVO normierten Kooperationsverpflichtung sind Verantwortliche und Auftragsverarbeiter berufen, an Beschwerde- oder Ermittlungsverfahren mitzuwirken. Gem. § 22 Abs. 1 DSG kann die Datenschutzbehörde vom Verantwortlichen oder Auftragsverarbeiter der überprüften Datenverarbeitung insbesondere alle notwendigen Aufklärungen verlangen sowie Einschau in die Datenverarbeitung und diesbezügliche Unterlagen begehren. Darüber hinaus ist die Behörde amtswegig verpflichtet, den maßgeblichen Sachverhalt im Ermittlungsverfahren zu untersuchen. Kommt ein Unternehmen seiner Verpflichtung wie im gegenwärtigen Verfahren durch die Unterlassung des Geschäftsführers nicht nach, ist die Behörde berechtigt, eine Strafe auszusprechen.

Weigert sich ein vertretungsbefugtes Organ, dieser Aufforderung nachzukommen, liegt ein objektiv sorgfaltswidriges Verhalten im Verschuldensgrad der Fahrlässigkeit vor. Das rechtswidrige und schuldhafte Verhalten einer natürlichen Person, im vorliegenden Fall des Geschäftsführers, kann gem. § 30 Abs. 2 DSG dem Unternehmen als juristischer Person zugerechnet werden. Es liegt daher ein Verstoß gem. Art. 83 Abs. 4 lit. a DSGVO vor.

Aus dem Erkenntnis lässt sich für die Aufforderung zur Stellungnahme durch die Behörde folgende Feststellung treffen: „Die Pflicht zur Zusammenarbeit ist auch daraus ableitbar, dass einer Aufsichtsbehörde nicht von vornherein unterstellt werden kann, sinnlose Anfragen zu stellen, die in keinem Zusammenhang mit ihrer Vollzugstätigkeit stehen.“

Sollten Sie also mit einer Aufforderung zur Stellungnahme durch die Datenschutzbehörde konfrontiert sein, ist es ratsam, binnen offener Frist zu antworten. Eine Stellungnahme sollte auch dann erfolgen, wenn man der Ansicht ist, keine weiteren Erkenntnisse für das Verfahren bereitstellen zu können.

4. Jö Bonus Club erneut gestraft

Das Thema Datenhandel betrifft nicht nur den Online-Markt. Auch im stationären Handel gibt es verschiedene Kundenbindungsprogramme, die das Einkaufs- und Nutzerverhalten von Kunden genau analysieren. Im Sommer 2021 wurde der jö Bonus Club bereits zu einer Strafe von EUR 2 Mio. verurteilt, da die Einholung der Einwilligung zum Profiling als intransparent erachtet wurde.

Nun wurde bekannt, dass es einen weiteren Bußgeldbescheid gegen das Kundenbindungsprogramm gibt, der mit EUR 8 Mio. beziffert ist, jedoch gegen die Konzernmutter REWE verhängt wurde. Es geht hierbei um die Datenströme im Konzern und die Frage der Bestrafung von Konzernunternehmen für die etwaigen Verstöße ihrer Tochtergesellschaften.

Der Bescheid wird von der REWE-Gruppe bekämpft und es bleibt abzuwarten, wie sich die datenschutzrechtliche Sicht auf Verarbeitungen im analogen Kundenbindungsbereich entwickeln wird.

5. Datenschutzbehörde ermittelt gegen Austrian Airlines

Ausgangspunkt dieses Ermittlungsverfahrens ist die Beschwerde einer Mitarbeiterin der Austrian Airlines, die sich gegen die Speicherung und Vervielfältigung ihres Impfnachweises in den Systemen der AUA zur Wehr setzt. Seitens der AUA sollen das Datum der Impfungen, der verwendete Impfstoff, die Verabreichung privat oder im Unternehmen, der Genesenenstatus, die Erforderlichkeit von Folgeimpfungen (Booster) sowie die Ablehnung der Datenverarbeitung gespeichert werden.

Das Flugunternehmen will die „2G-Regelungen“ für Personal konsequent umsetzen und stellt die Entgeltfortzahlung für ungeimpftes Personal per 1. März 2022 ein. Hierzu ist die Einholung und Speicherung des 2G-Nachweises notwendig, für die das Unternehmen laut Medienberichten eine Betriebsvereinbarung abgeschlossen hat.

Der Prozess beinhaltet jedoch die Einholung einer Einwilligung zum Speichern dieser Gesundheitsdaten, die gemäß der 6. COVID-19-Schutzmaßnahmenverordnung unter keinen Umständen gespeichert oder vervielfältigt werden dürfen. Die Ablehnung dieser Speicherung führt zur Einstellung der Entgeltfortzahlung. Aus datenschutz- und arbeitsrechtlicher Sicht kann eine Betriebsvereinbarung nicht eine Verordnung oder ein Gesetz zulasten des Einzelnen aushebeln. Darüber hinaus ist die Einwilligung im Arbeitsverhältnis im Allgemeinen unter Betrachtung der Unter- und Überordnung im Unternehmen als untaugliche Rechtsgrundlage anzusehen, da in der Regel keine Freiwilligkeit vorliegt.

Die Ablehnung führt im gegenständlichen Fall zu wirtschaftlich negativen Konsequenzen, sodass davon ausgegangen werden kann, dass die Einwilligung nicht freiwillig erfolgt. Darüber hinaus ist hier noch der Aspekt der besonderen Datenkategorien zu betrachten, der einen wesentlich höheren Maßstab an die Verarbeitung von Gesundheitsdaten iSd Art. 9 DSGVO anlegt.

Die Behörde hat der AUA 14 Tage zur Stellungnahme gegeben und es bleibt abzuwarten, wie sich dieses Verfahren entwickelt. Wir empfehlen Ihnen, keine Daten zur Impfung oder Genesung Ihrer Mitarbeiter ohne entsprechende gesetzliche Ermächtigung zu erheben oder zu speichern.

6. EuGH-Vorlage zu BVT-U-Ausschuss

Nicht nur politisch haben U-Ausschüsse in Österreich wesentliche Konsequenzen. Nun legt der Verwaltungsgerichtshof nach einer Revision der Datenschutzbehörde dem EuGH die Vorlagefrage vor, ob parlamentarische Untersuchungsausschüsse generell der DSGVO unterliegen. Das Verfahren ist anhängig unter der RS C-33/22 und betrifft im Wesentlichen die Frage, ob die DSGVO bei innerstaatlichen Kontrollakten im Rahmen der parlamentarischen Kontrolle anwendbar ist oder ob diese Verarbeitung außerhalb des Anwendungsbereichs der DSGVO gem. Art. 2 Abs. 1 lit. a DSGVO liegt.

7. EDSA beschließt Leitlinien zum Auskunftsrecht

Der Europäische Datenschutzausschuss hat am 18. Jänner 2022 Leitlinien zum Auskunftsrecht beschlossen. Das Thema ist von großer Bedeutung, da das Auskunftsrecht statistisch eines der am häufigsten geltend gemachten Betroffenenrechte ist und Unternehmen oftmals in kritische Abwägungsfragen drängt, wie viel der betroffenen Person mitzuteilen ist.

In seinen Leitlinien legt der EDSA fest, in welcher Form die Übermittlung der Auskunft, die Identifizierung und auch die Ablehnung einer Beauskunftung erfolgen kann. Insbesondere im Arbeitsrecht spielt die Erfüllung von Auskunftsbegehren eine wesentliche Rolle. Die Leitlinien unterliegen einem öffentlichen Konsultationsverfahren, dem man sich noch bis 11. März 2022 anschließen kann.

Darüber hinaus sind derzeit auch Verfahren vor dem EuGH anhängig, die sich mit dem Umfang der Auskunftserteilung auseinandersetzen. Darunter unter anderem ein Verfahren[1] aus Österreich, zu dem die Frage zu behandeln ist, ob es ausreicht, nur „Kategorien" von Empfängern mitzuteilen, oder ob jeder einzelne Datenempfänger in der Datenauskunft zu nennen ist.

Ein weiteres Verfahren[2] beschäftigt sich mit der Qualität der Auskunftserteilung: Der EuGH hat die Frage zu beantworten, was unter dem Begriff „Kopie" zu verstehen ist und ob zur Erfüllung des Auskunftsrechts eine elektronische Kopie bereitzustellen ist oder auch eine Abschrift/Duplikat ausreicht.

8. Internationale Erkenntnisse in Kürze

Unrechtmäßige Verwendung von Mitarbeiterfotos

Die spanische Datenschutzbehörde verhängte eine Geldstrafe gegen ein Unternehmen wegen der Verwendung von Mitarbeiterfotos ohne Einwilligung und der anschließenden Nichtbeachtung eines Löschbegehrens. Ein Angestellter hatte bei der Behörde eine Beschwerde gegen das Unternehmen wegen der unrechtmäßigen Verwendung seines Fotos eingereicht. Educando Juntos SL hatte Fotos seiner Mitarbeiter für die Website sowie die Social Media-Präsenz verwendet, ohne zuvor die Einwilligung der betroffenen Personen einzuholen.

Der Beschwerdeführer hatte das Unternehmen mehrfach aufgefordert, seine Fotos zu entfer-

[1] C-154/21 (Österreichische Post)

[2] C-487/21 (Österreichische Datenschutzbehörde and CRIF)

nen, doch die Aufforderungen wurden vom Verantwortlichen ignoriert. In diesem Zusammenhang sprach die Behörde daher ein Bußgeld aus, das sich aus dem Verstoß gegen die Rechtmäßigkeit der Datenverarbeitung und der Nichtbeachtung des Löschbegehrens ergibt. Die Geldbuße setzt sich anteilig zusammen aus EUR 6.000 für einen Verstoß gegen Art. 6 Abs. 1 DSGVO und EUR 3.000 wegen des Verstoßes gegen Art. 17 DSGVO.

Die Verarbeitung von Mitarbeiterfotos bedarf einer genauen Abwägung zwischen berechtigten Interessen, beispielweise bei Außendienstmitarbeitern und Repräsentationskräften, rein interner Veröffentlichung an einen geschlossenen Kreis, zB Firmenfeiern mit Bildern im Intranet, und der Einwilligung mit Widerrufsmöglichkeit bei der Veröffentlichung auf Website und Social Media. Im letzteren Fall ist darauf zu achten, einen Model-Release-Vertrag abzuschließen, in dem die Nutzungsrechte geregelt sind.

Auf die Veröffentlichung von Kinderfotos sollte grundsätzlich verzichtet werden. Falls sie unumgänglich ist, muss auf die genaue Dokumentation der Erlaubnis durch die Erziehungsberechtigen geachtet werden.

Unzulässige Übermittlung von Daten in die USA

Die spanische Logistik-Tochter von Amazon wurde auf Grundlage einer Beschwerde der Gewerkschaft mit einem Bußgeld von EUR 2 Mio. belegt, da sie die Daten ihrer angestellten Fahrer an die Konzernmutter in den USA ohne gültige Rechtsgrundlage übermittelte.

Strafregisterauszüge und andere Ausweis- und Sozialversicherungsdokumenten waren durch die Tochtergesellschaft eingeholt und in die USA übermittelt worden. Dies geschah auf Basis einer Pauschaleinwilligung, die nicht gültig eingeholt wurde.

Darüber hinaus berief sich das Unternehmen für die Übermittlung dieser Daten auf das Privacy Shield-Abkommen, das seit 16. Juli 2020 nicht mehr in Geltung ist, und konnte daher keine gültige Rechtsgrundlage für den internationalen Datentransfer vorweisen.