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

DSG-Info-Service

September 2019 Ausgabe Nr. 92

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Der Sommer ist vorbei und von einem datenschutzrechtlichen Sommerloch kann nun gar nicht die Rede gewesen sein. Seit der letzten Ausgabe ist viel im nationalen und internationalen Datenschutz passiert. Neben neuen Erkenntnissen der Datenschutzbehörden in Deutschland und Österreich meldet sich der EuGH nun auch zu Wort und macht die ohnehin schon komplizierte Rechtslage zwischen Telekommunikationsrecht und Datenschutz noch ein Stück komplexer. Das Landesgericht Feldkirch hat (nicht rechtskräftig) das erste Urteil über einen immateriellen Schadenersatz durch einen DSGVO-Verstoß verhängt und die Europäische Kommission hat sich ambitionierte Ziele gesetzt. Unter der aktuellen finnischen Ratspräsidentschaft wurde energisch verkündet: Die e-Privacy-Verordnung ist nicht tot – es wird weiter diskutiert.

Diese Ausgabe widmet sich also der Zusammenfassung der wichtigsten Ereignisse im Sommer. Zudem möchten wir Sie auf unser Seminar im Oktober hinweisen und Ihnen unser neues Produkt „DSGVO-Löschkonzept“ vorstellen.

Viel Spaß beim Lesen!

1. Judikaturübersicht

I. *Erster immaterieller Schadenersatz für Datenschutzverstoß in Österreich*

Das Landesgericht Feldkirch (Gz. 57 Cg 30/19b) entschied, dass die Verarbeitung von besonderen Datenkategorien ohne gültige Rechtsgrundlage und Information geeignet ist, einen immateriellen Schaden zu begründen. Der Sachverhalt ist vielfach durch die Medien gegangen: Die österreichische Post hat auf Grundlage von Marketinganalyseverfahren eine statistische Zugehörigkeit bzw. Affinität zu einer politischen Partei errechnet und Datensätze betroffener Personen den jeweiligen Kunden für Werbezwecke bereitgestellt.

Das Gericht ist der Ansicht, dass das Errechnen einer möglichen Affinität zu einer politischen Partei geeignet ist, ein besonderes personenbezogenes Datum darzustellen. Aus diesem Grund greifen die Rechtsgrundlagen des Art. 9 Abs. 2 DSGVO, wonach unter anderem die ausdrückliche Einwilligung der Betroffenen für diese Verarbeitung notwendig ist.

Wenngleich nicht rechtskräftig, zeigt das Erkenntnis, dass eine rechtswidrige Datenverar-

beitung auch zu einem (immateriellen) Schadenersatz führen kann. Dieser kann unabhängig von einem verwaltungsrechtlichen Bußgeld in einem Gerichtsverfahren erstritten werden. Die Höhe von EUR 800,00 mag in der individuellen Betrachtung noch marginal erscheinen, doch bei einer größeren Anzahl von Betroffenen kann diese Summe durchaus zum finanziellen Ruin führen.

II. *UK: Rekordstrafen für Marriott-Hotelgruppe und British Airways angekündigt*

Verstöße gegen die IT-Sicherheit sind auch Datenschutzverstöße, und die Strafen drakonisch: Die Hotelgruppe Marriott soll EUR 110 Mio Strafe zahlen, bei British Airways sind es stolze EUR 204 Mio, ca. 1,5 % des Jahresumsatzes.

Die britische Datenschutzbehörde (ICO) hat Rekordstrafen für einen Hack der Hotelgruppe Marriott und eine gravierende Sicherheitslücke bei der Fluglinie British Airways angekündigt. Beide Fälle haben ihren Ursprung bereits im Jahr 2018 und werden mit wesentlichen Nachlässigkeiten im IT-Sicherheitsbereich begründet. Während es bei Marriott ein Hack war, der dazu führte, dass die Kundendatenbank der Hotelkette mit 339 Mio Datensätzen kompromittiert wurde, war es bei British Airways eine interne Sicherheitslücke, da die Buchungsseite auf eine Phishing-Seite führte und so die Kundendaten abgriff. Das Resultat ist jedoch in beiden Fällen gleich.

IT-Sicherheitslücken, die zu Data Breaches führen, gehören zu den teuersten Verstößen gegen die DSGVO. Mit den zwei Strafen löst die britische Datenschutzbehörde die frz. CNIL mit ihren EUR 50 Mio Bußgeld gegen Google ab. Freilich sind diese Bußgelder noch nicht bestätigt und es bleibt offen, wie hoch die tatsächlichen Strafen schließlich ausfallen.

III. *EuGH zu Social Plugins von Facebook, Google etc. – Websitebetreiber sind mitverantwortlich*

Wenn ein sog. Social-Plugin auf Ihrer Website implementiert ist, das Daten an Facebook, Google oder Instagram weitergibt, so sind Sie für diese Datenverarbeitung mitverantwortlich. Das ist jedenfalls dem Erkenntnis des EuGH in der Rechtssache C-40/17[1] (*Fashion ID*) vom 29. Juli 2019 zu entnehmen. Die maßgeblichen Fragen waren dabei jene der Verantwortung zwischen Website- und Plattformbetreiber sowie der gültigen Rechtsgrundlage für die Verarbeitung. Strittig war das „berechtigte Interesse“ im Gegensatz zur „Einwilligung“ für das Setzen dieser Plugins unter Berücksichtigung der ehem. Datenschutz- und e-Privacy-Richtlinie. Die Entscheidung fällt somit unter die alte Rechtslage, lässt sich jedoch auf die neue Situation übertragen.

Der EuGH hat seine Judikatur fortgesetzt[2] und bestätigt erneut die gemeinsame Verantwortung von Plattform- und Websitebetreibern bei Verwendung von Plattform-Dienstleistungen und -Produkten. Als Beispiel sei der „*Gefällt-Mir*“-Button auf einer Website genannt, der vielfach am Fuße eines Artikels oder Produkts einer Website zu finden ist. Dieser *Gefällt-Mir*-Button kommuniziert unmittelbar zwischen dem Endgerät des Nutzers und Facebook, das Gleiche gilt für Plugins anderer Betreiber. Diese Kommunikation erfolgt jedoch ohne vorherige Information des Nutzers bzw. Möglichkeit der Unterbindung.

Die datenschutzrechtliche Verantwortlichkeit endet ab dem Zeitpunkt, in der nur noch der Plattformbetreiber die Datenverarbeitung übernimmt. Bis dahin muss der Websitebetreiber die Information zur Datenweitergabe an Facebook etc. erteilen und eine gültige Einwilligung einholen. Tut er das nicht, findet eine

[1] https://kurzelinks.de/88dv

[2] *EuGH vom 05.07.2018, C-210/16 – Facebook Fanpages* https://kurzelinks.de/nqz5

unzulässige Datenübermittlung statt und es liegt ein Verstoß gegen Datenschutz- und Telekommunikationsrecht vor.

Fazit: Beim Einsatz von Plugins sollten Verfahren wie Embetty[3] oder Shariff[4] angewandt werden, die eine automatische Datenübermittlung verhindern. Es handelt sich dabei um 1- oder 2-Klicklösungen, die erst beim aktiven Betätigen des Buttons durch den Nutzer den Kommunikationskanal in Richtung des Plugin-Betreibers öffnen. Weiters sollten Sie in Ihrer Art. 13-Information auf die Social-Plugins hinweisen und erläutern, wie die Daten an die jeweiligen Betreiber übermittelt werden.

IV. *PwC erhält sechsstellige Strafe für DSGVO-Verstoß*

Vor einer Strafe ist selbst das renommierte Wirtschaftsprüfungs- und Steuerberatungsunternehmen PricewaterhouseCoopers (PwC) nicht gefeit. Die griechische Niederlassung wurde nach einer Beschwerde von der dortigen Datenschutzbehörde überprüft, die einen Verstoß gegen die Rechtmäßigkeit der Datenverarbeitung feststellte. Es wurde eine Strafe in Höhe von EUR 150.000[5] ausgesprochen, da von den Mitarbeitern für die Verarbeitung ihrer Personaldaten Einwilligungen eingeholt wurden. Die griechische Behörde wertete dies als Verstoß gegen die Grundsätze der Datenverarbeitung, da Mitarbeitern das Gefühl vermittelt wurde, dass sie in die Datenverarbeitung einwilligen müssten, was jedoch nicht der Fall war.

Mitarbeiterdaten werden überwiegend auf Grundlage rechtlicher Pflichten sowie des Arbeitsvertrags verarbeitet. In Sonderfällen greift das berechtigte Interesse des Arbeitgebers. Die Einwilligung ist im Arbeitsverhältnis stets kritisch zu betrachten, da aufgrund des hierarchischen Verhältnisses zwischen Arbeitgeber und Arbeitnehmer selten von echter Freiwilligkeit ausgegangen werden kann. Dass PwC für diese Datenverarbeitung Einwilligungserklärungen unterschreiben ließ, sah die griechische Datenschutzbehörde als Verstoß gegen die Rechtmäßigkeit der Datenverarbeitung und trug auf, die korrekten Rechtsgrundlagen zu wählen und dies den Mitarbeitern auch mitzuteilen.

Fazit: Die Wahl der korrekten Rechtsgrundlage für die Datenverarbeitung ist für die Einhaltung der Grundsätze von größter Bedeutung. Insbesondere im arbeitsrechtlichen Kontext ist eine Einwilligung nur selten eine taugliche Rechtsgrundlage iSd Art. 6 oder Art. 9 DSGVO.

V. *Schweden: Behörde straft Schule für automatische Gesichtserkennung*

Mit einem Bußgeld von umgerechnet rund EUR 18.000 beendete eine schwedische Schule in Skellefteå ein Pilotprojekt, in dem sie die Anwesenheit von Schülerinnen und Schülern mittels Gesichtserkennung testete. Statt eines üblichen Anwesenheitsbuches wurden 22 Schülerinnen und Schüler über den Zeitraum von 3 Wochen mittels Gesichtserkennung im Unterricht überwacht. Hierfür holte die Schule auch die Einwilligung der Betroffenen ein. Allerdings sei dies unzulässig, wie die schwedische Datenschutzbehörde[6] entschied.

Wie im PwC-Fall sei eine Einwilligung in einem hierarchischen Verhältnis kaum haltbar, die Freiwilligkeit wird in Zweifel gezogen. Zudem handelt es sich bei der Datenverarbeitung um biometrische Daten, weshalb die ausdrückliche Einwilligung eingeholt werden muss, da es sich

[3] https://www.heise.de/newsticker/meldung/Embetty-Social-Media-Inhalte-datenschutzgerecht-einbinden-4060362.html

[4] https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html

[5] https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF

[6] https://www.datainspektionen.se/nyheter/facial-recognition-in-school-renders-swedens-first-gdpr-fine/

um besonders schutzwürdige Daten handelt. Unter Berücksichtigung des Abhängigkeitsverhältnisses und der Tatsache, dass für die Überprüfung der Anwesenheit auch andere, gelindere Mittel als die biometrische Erfassung der Gesichter angewendet können, sind sowohl die Datenanwendung als auch die Einwilligung die falsche Wahl. Anders als in Österreich ist es in Schweden möglich, Bußgelder gegen öffentliche Stellen zu verhängen, sodass eine Strafe von SEK 200.000 ausgesprochen wurde.

2. Nachrichten

I. *Deutsche Datenschutzkommission beschließt Berechnungsmodell für Bußgelder – Vorbildwirkung für ganz Europa?*

Bei der bisherigen Bußgeld-Praxis der europäischen Datenschutzbehörden ist von Kohärenz keine Rede. Die Höhen der Strafen unterscheiden sich im Ausmaß einiger Hundert Euro für Verstöße beim Einsatz von Videoüberwachungsanlagen über Millionen-Bußgelder bei internationalen Konzernen für Informations- und Sicherheitsverstöße. Selbst innerhalb von Deutschland ist die Bußgeldpraxis im Einklang mit dem dort herrschenden Datenschutz-Föderalismus alles andere als vorhersehbar. Aus diesem Grund hat sich die deutsche Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)[7] auf ein gemeinsames Konzept zur Berechnung von Bußgeldern verständigt. (Quelle: Juve[8])

Datenschutzverstoß gem. Art. 83 DSGVO
(z.B. Data Breach, Verstoß gegen Datenschutzgrundsätze etc.)

Bemessungsgrundlage: $\frac{\text{Vorjahresumsatz}}{\text{365 Tage}} =$ **Tagsatz**	
−	+
Ausmaß des Schadens Getroffene Maßnahmen Kooperation mit Behörde Unbewusst/Leichte Fahrlässigkeit	Art der Verletzung Anzahl der Betroffenen Dauer des Verstoßes Frühere Verstöße Vorsatz/Absicht
Schweregrad: Faktor 1 bis 14,4	

[7] https://datenschutzkonferenz-online.de/index.html

[8] https://www.juve.de/nachrichten/namenundnachrichten/2019/09/dsgvo-datenschutzbehoerden-berechnen-bussgelder-nach-neuem-modell

(Siehe auch https://www.juve.de/nachrichten/namenundnachrichten/2019/09/dsgvo-datenschutzkonferenz-nimmt-stellung-zum-bussgeldmodell

Die Eckpfeiler der Berechnung lassen sich folgendermaßen skizzieren:

- Die Bemessungsgrundlage ergibt sich aus dem Unternehmensumsatz des letzten Geschäftsjahres, geteilt durch 365 Tage. Somit gelangt der Tagsatz zur weiteren Berechnung.
- Dazu kommt je nach Schwere des Verstoßes ein Multiplikator, der von *Faktor 1* (leichter Verstoß) bis hin zu *Faktor 14,4* bei sehr schweren Verstößen reichen kann.

  Leichter Verstoß: Faktor 1 bis 4,
  Mittlerer Verstoß: Faktor 4 bis 8,
  Schwerer Verstoß: Faktor 8 bis 12,
  Sehr schwerer Verstoß mit Höchstfaktor: Faktor 12 bis 14,4,
  Sehr schwerer Verstoß ohne Höchstfaktor: Faktor ab 12.
- Der Schweregrad bemisst sich nach Art und Dauer des Vorfalls sowie der Anzahl der betroffenen Personen. Einberechnet werden außerdem das Ausmaß des Schadens, die getroffenen Maßnahmen zur Schadensminderung und die Zusammenarbeit mit der jeweiligen Behörde.

Schließlich kommen noch verschiedene Zu- und Abschläge hinzu: Abhängig vom Grad des Verschuldens werden -25 % für leichte oder unbewusste Fahrlässigkeit, +25 % für Wissen und bewusste Inkaufnahme und +50 % für Absicht ab- bzw. zugeschlagen. Für wiederholte Verstöße kommen ebenfalls Zuschläge zur Anwendung: +50 % (ein vorhergehender Verstoß), +150 % (zwei Verstöße), +300 % (drei oder mehr erneute Verstöße).

Die Arbeit der DSK wurde auch der Arbeitsgruppe des EDBP (European Data Protection Board) unterbreitet und wird in der „*Taskforce Finings*“ diskutiert. Sie könnte sich zum Berechnungsmodell für alle anderen europäischen Datenschutzbehörden entwickeln.

II. *Wichtige Nachricht für Ihre Dokumentationspflichten*

Viele Unternehmen führen noch immer ihre DVR-Nummer aus dem ehemaligen „*Datenverarbeitungsregister*“ der Datenschutzbehörde. Dieses wurde jedoch seit Inkrafttreten der DSGVO nur mehr zu Archivzwecken geführt und bleibt nur noch begrenzt öffentlich einsehbar.

Wir möchten Sie darauf hinweisen, dass dieses Datenverarbeitungsregister mit Ablauf des Jahres nicht mehr abrufbar sein wird. Wir empfehlen, dass Sie Ihre dort veröffentlichten und ggf. dem Vorabkontrollverfahren unterzogenen Datenanwendungen herunterladen und in Ihrer Dokumentation berücksichtigen (s. Information der DSB unter https://www.dsb.gv.at/fragen-und-antworten#Was_geschieht_mit_dem_Datenverarbeitungsregister_).

Sie erreichen das DVR unter:

https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx

Unsere nächsten Seminartermine

„DSGVO – Rechtsentwicklung und Best Practices“

findet am 22. Oktober 2019 statt.

Es referieren **Prof. KommR Hans-Jürgen Pollirer** sowie **Mag. Judith Leschanz** und **Mag. Katja Wyrobek**.

Außerdem veranstalten wir am 23. Oktober 2019 das Praxisseminar

„Praxisnahe Updates zu Datenschutz und IT-Sicherheit“

mit Schwerpunkt auf IT-Security, technischen Anforderungen und einem Update für Datenschutzbeauftragte und -Koordinatoren.

Nähere Informationen finden Sie unter www.secur-data.at.

Neues Produkt: DSGVO-Löschkonzept

Die **Speicherbegrenzung** ist ein verbindlicher Grundsatz der DSGVO. Personenbezogene Daten dürfen nicht länger gespeichert werden, als für den jeweiligen Verarbeitungszweck wirklich nötig ist. Danach müssen die Daten gelöscht oder zuverlässig anonymisiert werden.

Für Unternehmen ergeben sich daraus **verschiedene Fragen**: Welche Speicherdauer ist für welche Verarbeitung und Datenkategorie notwendig oder zulässig? Wann dürfen Daten überhaupt gelöscht werden und wann ist dies verpflichtend? Soll das Löschen vollautomatisch erfolgen oder muss es von einem Mitarbeiter freigegeben werden? Wo ist eine Anonymisierung die richtige Strategie und wie kann der Löschprozess dokumentiert werden?

Um diese Probleme aufwandsparend und effizient zu lösen, haben wir unser **DSGVO-Löschkonzept** entwickelt. Es bildet die Brücke zwischen der Entwicklung angemessener Aufbewahrungsfristen und ihrer technischen oder organisatorischen Umsetzung im Unternehmen. Die Fristen werden übersichtlich dargestellt und gegebenenfalls individuell auf das Unternehmen abgestimmt. Alle für die Löschung oder Anonymisierung relevanten Parameter werden abgebildet. Das DSGVO-Löschkonzept enthält außerdem die **rechtlichen Bestimmungen und Verpflichtungen**, die bei Löschbegehren von Betroffenen zu berücksichtigen sind, welche aufgrund des wachsenden Datenschutzbewusstseins immer mehr zunehmen.

Das DSGVO-Löschkonzept dient als **Übersichtsdokument** zur Vorlage an die Geschäftsführung, an interne und externe Auditoren und bei Bedarf auch an die Datenschutzbehörde. Die enthaltenen Regelungen können bei **Entwicklungsvorhaben und Beschaffungsvorgängen** in das Pflichtenheft aufgenommen werden. Es kann auch genutzt werden, um Mitarbeiterinnen und Mitarbeiter auf ihre **Mitwirkungspflichten** wie z.B. das Vernichten von Papierakten oder eigenen Aufzeichnungen hinzuweisen und zu sensibilisieren. Das DSGVO-Löschkonzept ist ein wichtiger Schritt zum **Nachweis der Einhaltung der DSGVO** und vereinfacht die Umsetzung der neuen Regelungen entscheidend.

Für eine unverbindliche Beratung können Sie uns unter office@secur-data.at kontaktieren oder unsere Website www.secur-data.at besuchen.