Newsletter der Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren! Liebe Datenschutzinteressierte!

Seit Mai 2018 ist nun bald ein Jahr vergangen. Im Stress rund um die Einführung der Datenschutz-Grundverordnung haben viele Unternehmen versucht, in kürzester Zeit die datenschutzrechtlichen Anforderungen „irgendwie“ hinzubekommen. Ohne sich eingehender mit der Materie auseinanderzusetzen, wurden Informationstexte für die eigenen Homepages und Einwilligungen für Kunden nach zirkulierenden Texten erstellt, Informationen und Muster der eigenen Kammern unreflektiert übernommen und vermeintliche „Patentlösungen“ eingeführt. Die Braut wurde für den 25. Mai herausgeputzt, oftmals ohne dass viel dahinter stand. Was dabei herauskommt, zeigt ein **Bescheid der Datenschutzbehörde, der vor zwei Woche im Rechtsinformationssystem veröffentlicht wurde:** Der Datenschutz-Koordinator eines Allergie-Tageszentrums meldete bei der Behörde zweimal (verpflichtend) Sicherheitsverletzungen ein; der Behörde fiel offensichtlich auf, dass laut der Datenschutzinformation auf der Homepage des Allergiezentrums aber ein Datenschutzbeauftragter bestellt war, den es anscheinend aber nicht gab. Darauf leitete die Datenschutzbehörde ein amtswegiges Prüfverfahren gegen das Allergiezentrum ein.

Die Datenschutzbehörde sah sich daraufhin die Datenschutzinformationen auf der Webseite an, ebenso die Einwilligungserklärung der Patienten. Sie stellte einige Fragen, ließ sich das Verarbeitungsverzeichnis schicken und konnte dadurch zahlreiche Unverträglichkeiten mit dem Datenschutzrecht feststellen. **Das Ergebnis war ein Bescheid, der nicht weniger als vierzehn (!) einzelne Mängel auflistet.**

Eine Zusammenfassung dieser 14 Mängel sowie ein Beitrag von mir über diesen wurden im „Rechtspanorama“ der „Presse“ vom 18. März publiziert - **ZUM BEITRAG - www.kt.at**

Den Bescheid selbst finden Sie im Volltext hier, ihn genau zu studieren kann ich nur dringlich empfehlen - **ZUM VOLLTEXT - www.ris.bka.gv.at**

Auch die **polnische Aufsichtsbehörde** hat für Aufsehen gesorgt: Für die **Verletzung der Informationspflicht nach Art 14 DSGVO** verhängte diese eine Geldbuße in Höhe von umgerechnet **EUR 220.000,-**. Das gegenständliche Unternehmen teilte die nach Art 14 DSGVO erforderlichen Informationen lediglich jenen betroffenen Personen mit, von denen sie über eine E-Mail-Adresse verfügte. Hinsichtlich der übrigen – 6 Millionen – betroffenen Personen beschränkte sich das Unternehmen auf eine Informationserteilung über die Webseite, obwohl dem Unternehmen Postanschriften und Telefonnummern dieser Personen bekannt waren. **Nach Ansicht der polnischen Aufsichtsbehörde war die Veröffentlichung auf der Webseite jedoch unzureichend, da das Unternehmen die Informationen den betroffenen Personen postalisch oder telefonisch bereitstellen hätte können.** Den Einwand des Unternehmens, dass die persönliche Informationserteilung zu teuer sei, verwarf die polnische Aufsichtsbehörde mit dem Hinweis, dass die Information nicht per Einschreiben erfolgen müsse.

Unternehmen sollten daher in sich gehen und überlegen, ob sie betroffene Personen in geeigneter Form informiert haben oder sich hierfür zusätzlich anderer Kanäle bedienen sollten.

Die Begründung der polnischen Aufsichtsbehörde kann in der Pressemitteilung des Europäischen Datenschutzausschusses nachgelesen werden - **ZUR PRESSEMITTEILUNG - edpb.europa.eu**

Österreichischer DSGVO-Song von deutscher Datenschutzbehörde verfilmt

Im Mai 2018 hat die Singer-Songwriterin Flickentanz auf Youtube ein Spaß-Anleitungslied über die Datenschutzgrundverordnung veröffentlicht. Der mit der Ukulele begleitete Song traf den Nerv der Zeit und erreichte über die Sozialen Medien auch bald unsere Kanzlei, wo er zu einer Art „Kanzleihymne“ wurde.
Wir luden Frau Flickentanz in unsere Kanzlei ein und sie gab den Song live zum Besten. Teile des witzigen Songtextes wurden in der Zeitschrift „Datenschutz konkret“ abgedruckt und Frau Flickentanz heizte bei der Party der Privacy und Security Konferenz PriSec von BusinessCircle im November in Rust mit diesem Song und weiteren selbstgeschriebenen Songs die Stimmung so an, dass behauptet wird, der Moderator der Konferenz und ein bekannter Datenschutzrechtsanwalt wären gegen Mitternacht beim Headbangen gesichtet worden (dies, obwohl sie nicht über ausreichend Haarpracht für diese Bewegungsform haben). Namen werden nicht genannt, es ist aber durch Zeugenaussagen belegt, dass die Datenschutzbeauftrage von Chanel aus Paris, die einen Vortrag auf der Konferenz hielt, von der Stimmung so angetan war, dass sie Wochen später bei einer Datenschutzkonferenz in Deutschland die PriSec als die Datenschutzkonferenz mit der besten Stimmung bezeichnet hatte.

Das Talent von Frau Flickentanz, die juristischen Kernelemente der DSGVO humorvoll in Liedform zu verpacken, hat nun auch eine deutsche Datenschutzbehörde erkannt. Im Februar wurde Frau Flickentanz für einen Videodreh vom Landesbeauftragten für

Datenschutz Baden-Württemberg eingeladen. Am 26.3.19 wurde das Video im Rahmen einer Vorlesung in der Hochschule der Medien mit Bundesjustizministerin Dr. Katarina Barley und dem Landesbeauftragten für Datenschutz und Informationssicherheit Dr. Stefan Brink erstmalig gezeigt - **ZUM VIDEO - www.youtube.com**

Man beachte die Szene bei Minute 3:55, wo der Landesdatenschutzbeauftragte Dr. Brink verkleinert vor Frau Flickentanz auf dem Tisch tanzt. Das ist kultig und lässt erahnen, dass an der Geschichte mit dem Headbangen etwas Wahres dran sein könnte…

Übrigens: Die PriSec gibt es auch heuer wieder, und zwar am 12./13. November - **ZUR VERANSTALTUNG - www.businesscircle.at**

Die datenschutzrechtlichen Folgen des Brexit

Da das Chaos um den Brexit immer größer wird, der Brexit aber immer realer wird, hat Frau Dr. Claudia Gabauer, LL.M., Rechtsanwaltsanwärterin in unserer Kanzlei, für Sie die nachfolgenden Informationen über die datenschutzrechtlichen Folgen und Handlungserfordernisse bei Austritt des Vereinigten Königreichs (UK) aus der EU („Brexit“) zusammengestellt.

Grundsätzlich bestehen zwei mögliche Szenarien, wobei angesichts der aktuellen politischen Entwicklungen ein ungeregelter Austritt (sogenannter „No-Deal-Brexit“) wahrscheinlich ist.

Im Fall eines No-Deal-Brexit sollten Sie kurz zusammengefasst:
1. alle relevanten Datenverarbeitungen feststellen,
2. geeignete Datentransfer-Instrumente festlegen und bis zum tatsächlichen Austrittstermin umsetzen,
3. Ihre Datenschutzinformation aktualisieren,
4. Ihre interne Dokumentation (insb. das Verfahrensverzeichnis) aktualisieren und
5. die Erforderlichkeit der Benennung eines Vertreters evaluieren.

Sowohl der **Europäische Datenschutzausschuss** („EDSA“) als auch die deutsche **Konferenz der unabhängigen Datenschutzaufsichtsbehörden** („DSK“) haben Informationen zur Übermittlung von Daten nach UK im Fall eines No-Deal-Brexit veröffentlicht, die in der nachstehenden, aufführlicheren Information berücksichtigt werden.

I. Ungeregelter Austritt („No-Deal-Brexit“)

Für den Fall, dass keine Einigung zwischen der EU und UK erzielt werden sollte („No-Deal-Brexit“), wird UK ab dem Austritt zu einem „Drittland“ iSd DSGVO. Verantwortliche, die personenbezogene Daten ab dem Austritt an UK übermitteln möchten, müssen die Datenübermittlungen mit besonderen Maßnahmen iSd Kapitels zu den Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen (Kapitel V der DSGVO) absichern. Ohne Absicherung der Datenübermittlung kann die zuständige Aufsichtsbehörde die Aussetzung der Übermittlung von Daten an einen Empfänger in UK

anordnen (vgl. Art 58 Abs 2 lit j DSGVO) und/oder Geldbußen in Höhe von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängen (vgl. Art 83 Abs 5 lit c DSGVO). Sofern Sie personenbezogene Daten ab dem Austrittsdatum nach UK übermitteln möchten, sollten Sie daher folgende Maßnahmen umsetzen:

1. Feststellung der relevanten Datenverarbeitungen

Stellen Sie fest, ob und welche Verarbeitungen eine Übermittlung personenbezogener Daten in das Drittland UK mit sich bringen. Sensibilisieren Sie die Mitarbeiter Ihrer Organisation für den Brexit und beziehen Sie Schlüsselpersonen Ihrer Organisation in diesen Prozess ein.

2. Festlegung eines geeigneten Datentransfer-Instruments und Umsetzung bis zum Austritt

In Ermangelung eines Angemessenheitsbeschlusses der Europäischen Kommission zum Zeitpunkt des Brexit (Art 45 DSGVO), stehen folgende Transferinstrumente zur Verfügung:

a) Ausnahmeregelungen gemäß Art 49 DSGVO

Unter bestimmten Voraussetzungen legitimieren die Ausnahmeregelungen des Art 49 DSGVO die Datenübermittlung in ein Drittland auch ohne Angemessenheitsbeschluss der Europäischen Kommission oder Setzung von angemessenen Garantien. Die Ausnahmeregelungen sind jedoch sehr restriktiv auszulegen und beziehen sich nach Auffassung des EDSA hauptsächlich auf gelegentliche und sich nicht wiederholende Verarbeitungen.

b) Standard-Datenschutzklauseln

Sie können die Datenübermittlung auf folgende – von der Europäischen Kommission – genehmigte Standarddatenschutzklauseln stützen:
- Im Fall der Übermittlung von Daten eines Verantwortlichen im EWR an einen Verantwortlichen im Drittland (z.B. UK) auf **2001/497/EG** oder **2004/915/EG**.
- Für die Übermittlung von Daten eines Verantwortlichen im EWR an einen Auftragsverarbeiter in einem Drittland (z.B. UK) auf **2010/87/EU**.

Bitte beachten Sie, dass die Standarddatenschutzklauseln nicht geändert werden dürfen und so unterzeichnet werden müssen, wie sie von der Europäischen Kommission zur Verfügung gestellt wurden. Eine Aufnahme in einen umfassenderen Vertrag oder zusätzliche Klauseln sind insoweit zulässig, als diese nicht im unmittelbaren oder mittelbaren Widerspruch zu den von der Europäischen Kommission verabschiedeten Standarddatenschutzklauseln stehen. Angesichts des zeitlich beschränkten Umsetzungsspielraums bieten die Standarddatenschutzklauseln den Vorteil der raschen Einsatzbereitschaft. Es sind lediglich die Anhänge auszufüllen und die Unterschriften der Zeichnungsberechtigten einzuholen.

c) Ad-hoc-Datenschutzklauseln

Jede weitere Änderung der Standarddatenschutzklauseln führt dazu, dass diese Klauseln als Ad-Hoc-Vertragsklauseln gelten, welche vor einer Datenübermittlung von der zuständigen nationalen Aufsichtsbehörde genehmigt werden müssen, nachdem der Europäische Datenschutzausschuss dazu Stellung genommen hat.

d) Verbindliche interne Datenschutzvorschriften gemäß Art 47 DSGVO („Binding Corporate Rules“ – „BCRs“)

Binding Corporate Rules sind Richtlinien zum Schutz personenbezogener Daten, die von Unternehmensgruppen befolgt werden, um angemessene Garantien für die Übermittlung personenbezogener Daten innerhalb der Gruppe auch außerhalb des EWR zu gewährleisten. Organisationen können sich weiterhin auf die unter der Datenschutz-Richtlinie 95/46/EG genehmigten BCRs stützen, sofern diese im Einklang mit den Bestimmungen der DSGVO aktualisiert wurden (vgl. Art 46 Abs 5 DSGVO). Sofern Sie neue BCRs erstellen möchten, müssen diese von der zuständigen nationalen Aufsichtsbehörde genehmigt werden, nachdem der Europäische Datenschutzausschuss dazu Stellung genommen hat.

Ad-hoc-Datenschutzklauseln und BCRs bieten also keine schnelle Abhilfe. Ähnlich ist das leider auch bei Verhaltensregeln (Art 40 f DSGVO) und Zertifizierungsmechanismen (Art 42 DSGVO) der Fall. Grundsätzlich können auch Verhaltensregeln und Zertifizierungsmechanismen unter bestimmten Voraussetzungen eine angemessene Garantie für die Übermittlung personenbezogener Daten in eine Drittland sein, sofern diese Instrumente rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters in einem Drittland zugunsten der betroffenen Personen normieren. Damit Verhaltensregeln eine Datenübermittlung in ein Drittland legitimieren können, müssen auch sie durch die zuständige Aufsichtsbehörde genehmigt sowie von der Europäischen Kommission für allgemein gültig erklärt werden. Die ebenfalls unter einem Genehmigungsvorbehalt der zuständigen Aufsichtsbehörden stehenden Zertifizierungsmechanismen kommen aktuell mangels akkreditierter Zertifizierungsstellen als Rechtsgrundlage für eine Drittlandsübermittlung nicht in Betracht.

3. Aktualisierung der Datenschutzinformation

Aktualisieren Sie Ihre Datenschutzinformation und informieren Sie betroffene Personen über die Datenübermittlung in ein Drittland (UK) und über die verwendeten geeigneten Datenschutzgarantien (siehe Art 13 Abs 1 lit f und Art 14 Abs 1 lit f DSGVO).

4. Interne Dokumentation

Dokumentieren Sie Datenübermittlungen in ein Drittland (UK) sowie die von Ihnen getroffenen geeigneten Garantien in Ihrem Verarbeitungsverzeichnis (siehe Art 30 Abs 1 lit d, lit e und Art 30 Abs 2 lit c DSGVO). Sofern eine betroffene Person von ihrem Auskunftsrecht nach Art 15 DSGVO Gebrauch macht, müssen Sie die betroffene Person über die Datenübermittlung in ein Drittland sowie über die geeigneten Garantien unterrichten (siehe Art 15 Abs 1 lit c und Abs 2 DSGVO).

5. Benennung eines Vertreters in der Union gemäß Art 27 DSGVO

Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der Union müssen schriftlich einen Vertreter benennen, wenn sie Waren oder Dienstleistungen an betroffene Personen in der Union anbieten oder das Verhalten von betroffenen Personen in der Union beobachten. Dieser „Art 27-Vertreter“ fungiert als lokaler Vertreter gegenüber den betroffenen Personen und den Aufsichtsbehörden innerhalb des EWR.

Eine Ausnahme zur Benennung des Vertreters für nicht öffentliche Stellen oder Behörden besteht nur, wenn die Verarbeitung nur gelegentlich erfolgt, keine umfangreiche Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art 9 Abs 1 DSGVO oder strafrechtsbezogene Daten nach Art 10 DSGVO vorliegt und die Verarbeitung voraussichtlich nicht zu einem Risiko für die betroffene Person führt.

II. Geregelter Austritt („Deal-Brexit“)

Für den Fall eines geregelten Austritts sieht der Entwurf eines Austrittsabkommens zwischen der EU und UK einen Übergangszeitraum vom Austritt bis Ende 2020 vor. Das bedeutet, dass während dieses Zeitraumes das EU-Recht – und damit auch die DSGVO – nach wie vor auch in UK anzuwenden ist (vgl. Art 126 und 127 Austrittsabkommen, ABl C 2019/66, I). Eine Verlängerung des Übergangszeitraums um ein oder zwei Jahre ist einmalig und vor dem 1. Juli 2020 möglich (vgl. Art 132 Austrittsabkommen). Im Fall eines geregelten Austritts dürfen personenbezogene Daten während des Übergangszeitraumes in UK unter denselben Voraussetzungen wie bisher übermittelt werden.

III. Datenübermittlungen aus UK an EWR-Mitglieder

Die britische Regierung hat eine **Leitlinie zur Verwendung von personenbezogenen Daten nach dem Brexit** veröffentlicht (Stand 6.2.2019), die auch den **6-Punkte-Plan** des Information Commissioner’s Office (ICO) berücksichtigt. Nach Angabe der britischen Regierung soll es im Fall eines No-Deal-Brexit keine sofortige Änderung der britischen Datenschutzstandards geben. Die DSGVO werde in britisches Recht umgesetzt und das ICO weiterhin als unabhängige britische Aufsichtsbehörde für Datenschutz bleiben. Angesichts der Angleichung zwischen den Datenschutzsystemen von UK und des EWR verweist die britische Regierung auf das zum Zeitpunkt des Austritts ausreichende Datenschutzniveau. Auch wenn UK einen Angemessenheitsbeschluss anstrebt, so wird dieser nicht bis zum Austritt getroffen werden können.

Gerne stehen wir Ihnen für Fragen zur Verfügung und unterstützen Sie bei der Umsetzung von Maßnahmen für den Fall eines No-Deal-Brexit.

Aktuelle Seminare

6.-8. 5. 2019 - Lehrgang zum zertifizierten Datenschutzbeauftragten

Wien, Business Circle - Referenten: RA Dr. Rainer Knyrim, Dr. Maximilian Wellner, DI Michael Löffler, Mag. Manfred Spanner MSc.

Mehr zur Veranstaltung und zur Online-Buchung

7. 5. 2019: Datenschutz-Compliance / Datenschutzgrundverordnung

Wien, Business Circle - Referent: RA Dr. Gerald Trieb, LL.M. im Rahmen des Praxislehrgangs Non Financial Risk Management – Compliance Officer in Banken

Mehr zur Veranstaltung und zur Online-Buchung

16. 5. 2019: HR-Daten, Erlaubtes & Verbotenes

Wien, Business Circle - Referent: RA Dr. Rainer Knyrim, RA Dr. Barbara Bartlmä

Mehr zur Veranstaltung und zur Online-Buchung

21. 5. 2019: Jahrestagung Datenschutzrecht 2019

Wien, Manz Rechtsakademie - Tagungsleitung: RA Dr. Gerald Trieb

Mehr zur Veranstaltung und zur Online-Buchung

22. 5. 2019: Der erfolgreiche Einkaufsleiter

Wien, imh - Referent ua: Dr. Tobias Tretzmüller,LL.M.

Mehr zur Veranstaltung und zur Online-Buchung

22. 5. 2019: Qualitätsmanagement 4.0.

Wien, imh - Referent ua: Dr. Tobias Tretzmüller,LL.M.

Mehr zur Veranstaltung und zur Online-Buchung

23.-24. 5. 2019: IT-Rechtstag Forschungsverein

Wien, Infolaw - Referenten ua: Prof. Dr. Eva Souhrada-Kirchmayer, Mag. Andreas Zavadil, Dr. Natalie Ségur-Cabanac, Dr. Rainer Knyrim

Mehr zur Veranstaltung und zur Online-Buchung

Verhaltensregeln nach DSGVO

Maximilian Kröpfl, Juristischer Mitarbeiter in unserer Kanzlei

Es ist aktuelles Thema vieler Branchentreffen: Datenschutzrechtliche Verhaltensregeln. Der Verband der österreichischen Internet Service Provider (ISPA) hat letzten November seine Verhaltensregeln der Öffentlichkeit präsentiert. Zahlreiche Verbände und Interessenvertretungen befinden sich im Finale des Genehmigungsprozesses bei der DSB. Knyrim Trieb unterstützt unter anderem den Verband der österreichischen Energiewirtschaft dabei.

Die mit einem solchen Regelwerk verbundene Gestaltungsmöglichkeiten sind mannigfaltig. Die wesentlichsten Eckpunkt von Verhaltensregeln für Sie zusammengefasst: In Verhaltensregeln werden gängige Anwendungsfälle und

Arbeitsweisen der Datenverarbeitung oder Produktionsabläufe der Branche konkretisiert und die Transparenz hinsichtlich dem, was üblich und erforderlich ist, gesichert. Es geht um „Good Practice“. Der Europäische Datenschutzausschuss hebt insbesondere die Wirkung als Nachweis der „state-of-the-art“-Compliance hervor.

Durch den Charakter der Selbstverpflichtung wirken die eigenen Verbände auf wichtige Datenschutzfragen im Interesse der Branche ein. Die bescheidmäßige Genehmigung sichert die behördliche Vermutung eines rechtskonformen Vorgehens. Für all jene, die Partner in Drittstaaten haben, können auch Verhaltensregeln als geeignete Garantien für den internationalen Datentransfer vorgesehen werden.

Der Weg hin zu genehmigten Verhaltensregeln

Am Anfang steht die oft lange Diskussion der Branchenvertreter über Geltungsbereich, Inhalt und Umfang von Verhaltensregeln. Die Regelwerke können sich national oder europäisch ausrichten und jeden beliebigen Inhalt vorsehen. Wichtig ist nur, dass der Regelungsinhalt spezifisch, in sich konsistent und realistisch erfüllbar ist sowie regelmäßig aktualisiert wird. Verhaltensregeln müssen einen nennenswerten Mehrwert zum Datenschutz in der Branche schaffen. Zusätzlich dazu müssen Verhaltensregeln noch Bestimmungen vorsehen, die es einer Überwachungsstelle ermöglichen, ihren Überwachungs- und Prüfpflichten nachzukommen.

Der fertige Entwurf ist der Datenschutzbehörde zu übermitteln, welche diesen auf formelle und materielle Mängel prüft und bescheidmäßig genehmigt. Sollte eine Geltung über Österreich hinaus geplant sein, so setzt die Datenschutzbehörde die weiteren Schritte im Europäischen Datenschutzausschuss.

Überwachungsstelle statt Datenschutzbehörde

Die Einhaltung genehmigte Verhaltensregeln werden nicht unmittelbar von der Datenschutzbehörde, sondern von einer privaten Überwachungsstelle geprüft. Nach dem Gedanken der DSGVO sollen Verantwortliche und Auftragsverarbeiter frei aus einer Mehrzahl dieser Stellen wählen können.

Um eine gleichbleibende Qualität zu garantieren, sind diese Stellen von der Datenschutzbehörde zu akkreditieren. Voraussetzungen dafür sind nach der DSGVO und dem aktuellen Entwurf der Überwachungsstellenakkreditierungs-Verordnung (ÜStAkk-V) eine entsprechende Unabhängigkeit gegenüber den sich unterstellenden Unternehmen und Fachwissen hinsichtlich der konkreten Regelungsinhalte.

Jede akkreditierte Überwachungsstelle hat drei generelle Aufgaben: Einerseits stellt sie die Konformitätsbescheinigung aus, die nachweist, dass sich unterstellende Unternehmen die konkreten Verhaltensregeln erfüllen können. Andererseits kommen ihr Prüf- und Überwachungsfunktionen zu. Das bedeutet, dass Überwachungsstellen die Einhaltung der Verhaltensregeln grundsätzlich überwachen und im Einzelfall überprüfen müssen. Eine solche Prüfung kann sich insbesondere aufgrund einer Betroffenenbeschwerde an die dafür bestellte Überwachungsstelle ergeben.

Trotzdem auch der Überwachungsstelle ein gewisses Sanktionsrecht eingeräumt wird, ist es mit jenem der Datenschutzbehörde in Umfang und Wirkung nicht vergleichbar. Die schärfste Sanktion besteht im Ausschluss von den Verhaltensregeln.

Datentransfer mit genehmigten Verhaltensregeln

Unsere Wirtschaft wird digitaler und damit internationaler. Produktion und Dienstleistung findet nicht mehr notwendiger Weise im eigenen Unternehmen statt. Neben den offensichtlichen Vorteilen bleiben jedoch auch immer Risiken bei der Verarbeitung von personenbezogenen Daten. Richtig gestaltet, können Verhaltensregeln diese Risiken minimieren: Auftragsverarbeiter und Dritte in Drittstaaten können sich dem Regelwerk unterstellen und sich somit dem europäischen Branchenstandard verpflichten.

Gemeinsame Verantwortung bei Facebook-Fanpages

Dr. Claudia Gabauer, LL.M., Rechtsanwaltsanwärterin in unserer Kanzlei

EuGH 5. 6. 2018, C-210/16 – Teil II

Frau Dr. Claudia Gabauer, LL.M. hat für den letzten und diesen Newsletter eine Zusammenfassung der Facebook-Fanpage-Problematik erstellt, hier ist nun Teil II:

Facebook-Fanpages – Seiten-Insights-Ergänzung

Im letzten Newsletter wurde die Entscheidung des EuGH zur Gemeinsamen Verantwortlichkeit von Fanpage-Betreibern und Facebook skizziert (vgl. EuGH 5.6.2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig Holstein GmbH). Als Reaktion auf dieses Urteil veröffentlichte Facebook Ireland („Facebook“) das sogenannte „Page Insights Controller Addendum“ bzw. „**Seiten-Insights-Ergänzung**“, mit der dem Erfordernis einer „Joint Controller“-Vereinbarung nach Art 26 DSGVO entsprochen werden soll.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit äußerte im November 2018 Bedenken, dass die bisher von Facebook zur Verfügung gestellten Informationen und die Seiten-Insights-Ergänzung ausreichen würden, um Rechenschaft über die Rechtmäßigkeit der Verarbeitung von Daten von Fanpage-Besuchern ablegen zu können. Gleichzeitig kündigte die Berliner Beauftragte für Datenschutz und Informationsfreiheit umfassende Prüfungen des Betriebs von Facebook-Fanpages bei Unternehmen und Organisationen an und veröffentlichte jenen **Fragenkatalog**, der auch im Anhörungsverfahren Anwendung findet und den jeder Betreiber einer Facebook-Fanpage – ungeachtet einer Prüfung durch die zuständige Aufsichtsbehörde – beantworten können sollte.

Seiten-Insights-Ergänzung als wirksame Art 26-Vereinbarung?

Zunächst ist klarzustellen, dass sich die Seiten-Insights-Ergänzung ausschließlich auf die Verarbeitung von sogenannten „Insights-Daten“ der Fanpage bezieht, nicht hingegen auf

jegliche Datenverarbeitung im Zusammenhang mit der Fanpage. Während für die Verarbeitung von Insights-Daten eine gemeinsame Verantwortung von Facebook und den Fanpage-Betreiber vorliegt, ist der Fanpage-Betreiber für die Verarbeitung anderer Daten auf seiner Fanpage grundsätzlich allein Verantwortlicher.

Die Seiten-Insights-Ergänzung verpflichtet den Fanpage-Betreiber zuzustimmen, „dass nur Facebook Ireland Entscheidungen hinsichtlich der Verarbeitung von Insights-Daten treffen und umsetzen kann“. Darüber hinaus entscheidet Facebook „nach seinem alleinigen Ermessen, wie es seine Pflichten gemäß dieser Seiten-Insights-Ergänzung erfüllt“. Nach der Legaldefinition gemäß Art 4 Z 7 DSGVO ist Verantwortlicher, wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Die gemeinsame Verantwortlichkeit setzt daher eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung voraus. Daran vermag auch der Umstand nichts zu ändern, dass der EuGH in seiner Entscheidung zu Facebook-Fanpages klargestellt hat, dass nicht jeder Verantwortliche Zugang zu den betreffenden personenbezogenen Daten haben muss. Ob die gemeinsame Entscheidungsbefugnis durch eine Joint-Controller-Vereinbarung nach Art 26 DSGVO abbedungen werden kann, ist kritisch zu hinterfragen. Im Ergebnis ist es daher zweifelhaft, ob eine alleinige Entscheidungshoheit von Facebook über die Verarbeitung der Insights-Daten mit der Konzeption der gemeinsamen Verantwortlichkeit nach der DSGVO vereinbar ist.

Rechtmäßigkeit der Verarbeitung von sogenannten „Insights-Daten“?

Facebook verpflichtet den Fanpage-Betreiber sicherzustellen, dass dieser über eine Rechtsgrundlage für die Verarbeitung von Insights-Daten verfügt, den Verantwortlichen benennt und jedwede sonstigen geltenden rechtlichen Verpflichtungen erfüllt. Fanpage-Betreiber müssen daher sowohl in ihrer verpflichtenden Datenschutzinformation als auch gegenüber der Datenschutzbehörde eine Rechtsgrundlage für die Verarbeitung von Insights-Daten benennen können. Als Rechtsgrundlage kommt faktisch nur eine Einwilligung der betroffenen Personen in Betracht, da berechtigte Interessen iSd Art 6 Abs 1 lit f DSGVO nach herrschender Meinung bei der Verarbeitung von personenbezogenen Daten durch Cookies – die auch im Fall der Verarbeitung von Insights-Daten eingesetzt werden – nicht ins Treffen geführt werden können. Das Erfordernis einer wirksamen Einwilligung ist wohl nach der aktuellen Ausgestaltung von Fanpages nicht erfüllt:

a) Registrierte Facebook-Nutzer

Der Verein „NOYB – Europäisches Zentrum für digitale Rechte“ reichte Beschwerde gegen Facebook ein, da die Einwilligung in die Nutzungsbedingungen von Facebook gegen die Anforderungen gemäß Art 4 Z 11, Art 6 Abs 1 lit a, Art 7 und/oder Art 9 Abs 2 lit a DSGVO verstoßen würden (zur Beschwerde siehe **hier**). Ob die Einwilligung von registrierten Facebook-Nutzern die Verarbeitung von Insights-Daten legitimiert, sollte daher bis zum Ausgang des Verfahrens kritisch betrachtet werden.

b) Nicht registrierte Fanpage-Besucher

Der EuGH betonte, dass auch personenbezogene Daten von Fanpage-Besuchern, die über kein Facebook-Benutzerkonto verfügen, verarbeitet werden und dass bereits das

bloße Aufrufen der Fanpage automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst (vgl. EuGH 5.6.2018, C-210/16, Rz 41). Auch die deutsche Datenschutzkonferenz differenziert zwischen registrierten Facebook-Nutzern und Nicht-Mitgliedern von Facebook und fordert in ihrem Anhang zum Beschluss vom 5. September 2018 betreffend „Facebook-Fanpages“ sowohl Facebook als auch Fanpage-Betreiber explizit auf, die für die Legitimierung der Verarbeitung von personenbezogenen Daten von Nicht-Mitgliedern erforderliche Rechtsgrundlage zu benennen (zum Beschluss siehe **hier**).

Eine Einwilligung könnte etwa durch einen Cookie-Banner eingeholt werden, der auch technisch gewährleistet, dass erst nach wirksamer Einwilligung durch den Fanpage-Besucher Cookies gesetzt und personenbezogene Daten verarbeitet werden. Der Umstand, dass Facebook die Implementierung eines Cookie-Banners technisch nicht oder nur eingeschränkt ermöglicht, ändert nichts an der gesetzlichen Verpflichtung der Fanpage-Betreiber. Auch das Landesverwaltungsgericht Niederösterreich verwarf kürzlich den Einwand eines Seiten-Administrators, dass Facebook die Schaltung eines Impressums technisch nicht zulasse und hielt ausdrücklich fest, dass die faktischen Gegebenheiten nichts an der gesetzlichen Verpflichtung ändern und daher nicht von der Offenlegungsverpflichtung nach § 25 Mediengesetz befreien (vgl. LVwG NÖ 13.12.2018, LVwG-S-1598/001-2018).

Conclusio

Mit der Seiten-Insights-Ergänzung soll nunmehr die nach Art 26 DSGVO zwingend erforderliche Vereinbarung zwischen Facebook und den Fanpage-Betreibern als gemeinsam Verantwortliche geschaffen werden. Diese Vereinbarung weist jedoch einige Rechtsunsicherheiten sowie nachteilige Klauseln zulasten des Fanpage-Betreibers auf. Die Seiten-Insights-Ergänzung kann auch nicht das Defizit beseitigen, dass für die Verarbeitung von Insights-Daten mit Hilfe von Cookies mangels wirksamer Einwilligungserklärung keine Rechtsgrundlage existiert.

Sofern Betreiber von Facebook-Fanpages etwa aus unternehmerischen Gründen nicht auf ihre Fanpage verzichten möchten, sollten diese zumindest folgende risikominimierende Maßnahmen treffen:

- Die Fanpage-Betreiber müssen ungeachtet der Seiten-Insights-Ergänzung eine Datenschutzinformation auf ihrer Fanpage bereitstellen, die unter dem Menüpunkt „Info“ als „Datenrichtlinie“ oder im Impressum als Link implementiert werden kann. Die Datenschutzinformation sollte insbesondere auch jene Informationen nach Art 13 und Art 14 DSGVO bereitstellen, die Facebook nicht oder nur unvollständig offenlegt.

- Fanpage-Betreiber sind verpflichtet, die Verarbeitung von personenbezogenen Daten im Rahmen ihrer Fanpage in ihr Verarbeitungsverzeichnis nach Art 30 DSGVO aufzunehmen.

- Fanpage-Betreiber sollten in der Lage sein, den aus 15 Fragen bestehenden Fragenkatalog der Berliner Datenschutzbeauftragten beantworten zu können. Dieser Fragenkatalog beschäftigt sich u.a. mit der rechtlichen Qualifikation der Seiten-Insights-Ergänzung, dem Zweck und der Rechtsgrundlage für die Verarbeitung von sogenannten „Insights-Daten“, der Speicherdauer von Cookies sowie dem Umgang mit Betroffenenrechte durch Facebook und den Fanpage-Betreiber. Weiters sollte der

Fanpage-Betreiber eine Definition und eine abschließende Auflistung der sogenannten „Insights-Daten“ bereitstellen können. Der ausgefüllte Fragebogen kann als Maßnahme zur Dokumentation der eigenen Rechenschaftspflicht für den Betrieb der Facebook-Fanpage herangezogen werden.

Auch wenn Mark Zuckerberg kürzlich eine auf „Datenschutz ausgerichtete Vision für Social Networking“ proklamiert hat (siehe **hier**), sollten Fanpage-Betreiber sich Ihrer datenschutzrechtlichen Verantwortlichkeit und des Risikos für Facebook-Fanpages bewusst sein und risikominimierende Maßnahmen treffen. Bei Bedarf können wir Sie bei der Umsetzung dieser Maßnahmen gerne unterstützen. Wir haben schon entsprechende Vorlagen entwickelt.

Facebook Custom Audience
Neben Facebook-Fanpages stehen auch andere Facebook-Tools im Fokus der datenschutzrechtlichen Rechtsprechung: Der Bayerische Verwaltungsgerichtshof hat den Einsatz des Marketing-Tools „Facebook Custom Audience“ ohne Einwilligung der betroffenen Personen für unzulässig erklärt (Beschluss VGH München, 26.9.2018, 5 CS 18.1157). Bei dieser Funktion können Unternehmen Kundendaten an Facebook übermitteln, um diese Daten mit Facebook-Nutzern abgleichen und im Anschluss zielgruppenspezifische Werbeanzeigen für die registrierten Kunden schalten zu können. Unternehmen, die Facebook Custom Audience nutzen, müssen daher eine Einwilligung der betroffenen Personen nachweisen können.

Aktuelle Entscheidungen

Zum Abschluss möchten wir Sie noch über zwei weitere Entscheidungen der Datenschutzbehörde informieren, die von Frau Dr. Claudia Gabauer, LL.M. für Sie zusammengefasst wurden:

1. Ausstattung von Firmenfahrzeugen mit GPS-System

Die DSB überprüfte ihm Rahmen eines amtswegigen Prüfverfahrens die Wirksamkeit der datenschutzrechtlichen Einwilligung von Mitarbeitern zur Ausstattung von Firmenfahrzeugen mit einem GPS-System (DSB 8.8.2018, DSB-D213.658/0002-DSB/2018).

Die DSB hielt zunächst unter Verweis auf § 10 AVRAG fest, dass die Freiwilligkeit einer Einwilligung im Beschäftigungskontext – trotz der typischerweise vorliegenden wirtschaftlichen Ungleichheit von Arbeitnehmer und Arbeitgeber – nicht grundsätzlich ausgeschlossen ist. Eine freiwillige Einwilligung könne etwa dann vorliegen, wenn ein bestimmter Verarbeitungsvorgang auch zum erkennbaren Vorteil des Arbeitnehmers gereicht. Die Freiwilligkeit wäre beispielweise gegeben, wenn die Erhebung und Speicherung der Wegzeiten erfolgt, weil Außendienstmitarbeiter diese Daten für ihre Einkommenssteuer benötigen und die Fahrtenbuchfunktion nach Belieben ein- und

abgestellt werden kann. Im konkreten Fall ist ein klarer Vorteil für den Arbeitnehmer durch den Einsatz des GPS-Systems nicht erkennbar. Die für die Dauer von 93 Tagen gespeicherten GPS-Daten ermöglichen es dem Arbeitgeber, genau zu protokollieren, wie pünktlich bzw. schnell ein Arbeitnehmer seine Leistung vollbringt. Das Unternehmen argumentierte zwar, dass das GPS-System nicht zur Mitarbeiterüberwachung, sondern zum Schutz und zur Sicherheit des Firmeneigentums, zur monatlichen Abrechnung mit der Leasingfirma, zur Routenplanung- und Optimierung, zur Disposition sowie als Fahrtenbuch eingesetzt werde. Nach Ansicht der DSB übersieht das Unternehmen jedoch, dass diese Faktoren zwar im Rahmen einer Interessenabwägung nach Art 6 Abs 1 lit f DSGVO berücksichtigt werden können, jedoch nicht im Rahmen der Beurteilung der Freiwilligkeit einer Einwilligung. Da das Unternehmen ihren gesamten betrieblichen Ablauf betreffend den Einsatz der Firmenfahrzeuge auf Grundlage des GPS-Systems plant und koordiniert, kann wohl nicht davon ausgegangen werden, dass einem Arbeitnehmer bzw. einem Fahrer tatsächlich die Wahl bleibt, seine Einwilligung nicht zu erteilen. Die wahrscheinliche Konsequenz wäre daher, dass ein Arbeitnehmer das Dienstverhältnis (als Fahrer) ohne Einwilligung nicht eingehen könne bzw. ein aufrechtes Dienstverhältnis ohne Einwilligung beendet werden würde. Im Ergebnis kann daher nicht von einer freiwilligen Abgabe einer Einwilligung ausgegangen werden.

2. Zweckwidrige Verwendung von allgemein verfügbaren Daten

Im gegenständlichen Fall wurde die auf einer Webseite eines psychologischen Hilfsverbands unter dem Profil des Beschwerdeführers kundgemachte Handynummer ohne Einwilligung zu Werbezwecken verwendet (DSB 31.10.2018, DSB-D123.076/0003-DSB/2018).

Die DSB hielt einleitend fest, dass Anrufe zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers („Unerbetene Nachrichtungen“) nach § 107 Abs 1 TKG 2003 zu beurteilen und eine entsprechende Verwaltungsstrafe gemäß § 109 Abs 4 Z 8 TKG 2003 ggf. von der zuständigen Fernmeldebehörde zu verhängen ist. Auch wenn eine Beurteilung der Rechtmäßigkeit der Verarbeitung iSd Art 6 DSGVO ausgeschlossen ist, kann durch einen Verstoß gegen das TKG 2003 gleichzeitig sehr wohl eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs 1 DSG und auch eine Verletzung jener Bestimmungen der DSGVO vorliegen, die dem Verantwortlichen gerade keine zusätzlichen Pflichten iSv Art 95 DSGVO auferlegen.

Die Handynummer wurde gerade nicht allgemein verfügbar gestellt, um Anrufe zu Werbezwecken zu erhalten, sondern diente vielmehr als „Beratungsnummer“ für bedürftige Personen. Die generelle Annahme des Nichtvorliegens einer Verletzung schutzwürdiger Geheimhaltungsinteressen für zulässigerweise veröffentlichte Daten ist mit den Bestimmungen der DSGVO nicht vereinbar. Diese Sichtweise ist auch in Einklang mit den Vorgaben von § 107 Abs 1 TKG 2003, wonach eine auf einer Homepage zur Verfügung gestellte Handynummer zu Beratungszwecken gerade nicht als Rechtsgrundlage für die Durchführung von Werbezwecken ausreicht, sondern ausdrücklich eine Einwilligung des Teilnehmers erforderlich ist. Die zweckwidrige Verwendung der Handynummer für Werbemaßnahmen stellt daher eine Verletzung im Recht auf Geheimhaltung dar. Da die

Handynummer als personenbezogenes Datum nicht bei der betroffenen Person erhoben wurde, muss der Verantwortliche spätestens einen Monat nach Erhebung der Daten die entsprechenden Informationen nach Art 14 DSGVO zur Verfügung stellen.

Mit freundlichen Grüßen

Dr. Rainer Knyrim

Datenschutzinformation

Die Verarbeitung der Daten erfolgt durch Knyrim Trieb Rechtsanwälte OG. Für den Versand bedienen wir uns eines Newsletter-Versandpartners, derzeit Mailjet.de, für die Speicherung Ihrer Daten eines Internet-Service-Providers, derzeit A1 Telekom Austria. Die Einwilligung kann durch Klicken des untenstehenden Links „Vom Newsletter anmelden“ jederzeit widerrufen werden.

Alle Informationen, welche Daten wir für den Newsletter verarbeiten finden Sie in unserer Datenschutzinformation.

Mit freundlichen Grüßen

Dr. Rainer Knyrim

Knyrim Trieb Rechtsanwälte OG

Mariahilfer Straße 89a, A-1060 Wien, T: +43 1 909 30 70, F: +43 1 909 36 39

FB: www.facebook.com/knyrimtrieb E: ky@kt.at, W: www.kt.at

FN 462250f, HG Wien, DVR 4017263