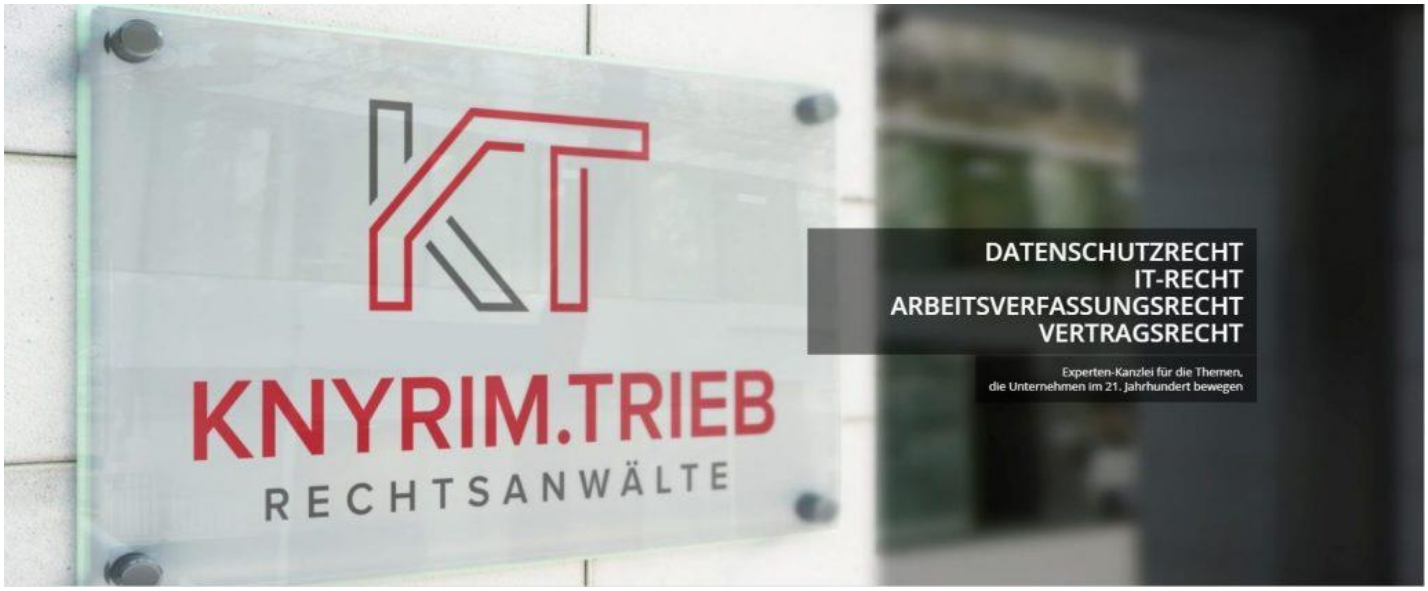

Newsletter August 2021

Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!

Liebe Datenschutzinteressierte!

Im aktuellen Newsletter berichten wir Ihnen über das von uns gemeinsam mit Secur-Data gegründete Zertifizierungsunternehmen KT & SD DSGVO ZERT GmbH und haben für Sie gleich mehrere Beiträge zum Thema internationaler Datentransfers vorbereitet. Weitere Themen sind die datenschutzrechtlichen Dauerbrenner „Cookie-Banner“ und „Facebook-Fanpages“ sowie eine ebenso nützliche wie umfassende Liste mit Materialien der deutschen Datenschutzaufsichtsbehörden.

Wir wünschen Ihnen einen angenehmen restlichen Sommer. Bleiben Sie gesund!

Knyrim Trieb und Secur-Data gründen gemeinsame Zertifizierungs-GmbH

Beitrag verfasst von Dr. Gerald Trieb, LL.M. – KTR-Newsletter August 2021

Im Juni 2021 haben wir gemeinsam mit Frau Mag. Judith Leschanz und Herrn Prof. Hans-Jürgen Pollirer von Secur-Data Betriebsberatungs GmbH die **KT & SD DSGVO ZERT GmbH** gegründet. Die Gründung verfolgt den Zweck, die Voraussetzungen für die Akkreditierung dieser Gesellschaft als Zertifizierungsstelle nach Art 43 DSGVO durch die Datenschutzbehörde zu erlangen, da für die Akkreditierung neben juristischem Fachwissen auch technische Expertise erforderlich ist; die Zertifizierungsstelle muss in der Lage sein, nicht nur die rechtliche, sondern auch die technische Konformität eines Zertifizierungsgegenstandes mit bestimmten Zertifizierungskriterien attestieren zu können. Neben der Schaffung aller Voraussetzungen für die Akkreditierung sind wir gerade dabei, solche datenschutzrechtlichen Zertifizierungskriterien nach Art 42 DSGVO vorzubereiten. Je nach Zertifizierungsgegenstand werden diese Zertifizierungskriterien dafür Sorge tragen, dass das zu zertifizierende Produkt bzw. die zu zertifizierende Dienstleistung den Vorgaben der DSGVO entspricht.

Die Zertifizierung durch eine akkreditierte Zertifizierungsstelle nach Art 43 DSGVO auf Basis von der Datenschutzbehörde gebilligter Zertifizierungskriterien nach Art 42 DSGVO verschafft dem zertifizierten Unternehmen – anders als andere Datenschutzzertifikate, die nicht durch eine entsprechend akkreditierte Stelle bzw. auf Basis entsprechend gebilligter Kriterien erteilt wird – besondere Privilegien nach der DSGVO: So hilft es dem Verantwortlichen dabei, die Anwendung angemessener technischer und organisatorischer Maßnahmen sowie auch allgemein die Rechenschaftspflicht nachzuweisen; auch kann die Einhaltung entsprechend genehmigter Zertifizierungskriterien bei der Frage, ob und in welcher Höhe eine Geldbuße für eine allfällige Verletzung verhängt wird, als mildernd durch die Datenschutzbehörde gewertet werden. Nicht zuletzt kann auch die Zertifizierung von Verarbeitungstätigkeiten als Auftragsverarbeitung dem Verantwortlichen den Nachweis erleichtern, sich eines geeigneten Auftragsverarbeiters für die Datenverarbeitung zu bedienen und somit gleichzeitig Auftragsverarbeitern zu einem Wettbewerbsvorteil verhelfen.

Wir rechnen damit, dass wir in der zweiten Jahreshälfte zur Zertifizierungsstelle akkreditiert werden sowie auch die von uns vorbereiteten Zertifizierungskriterien von der Datenschutzbehörde gebilligt erhalten, sodass wir mit Ende 2021/Anfang 2022 datenschutzrechtliche Zertifizierungen nach DSGVO anbieten können sollten. Für alle

Fragen dazu stehen wir Ihnen gerne zur Verfügung. Die Vorbereitung auf entsprechende Zertifikate kann schon jetzt beginnen!

Neue Standarddatenschutzklauseln (I)

Beitrag verfasst von Dr. Rainer Knyrim, Dr. Gerald Trieb, LL.M. und Denise Stahleder, LL.B. – KTR-Newsletter August 2021

Am 4. Juni 2021 hat die Europäische Kommission (Publications Office (europa.eu) neue Standarddatenschutzklauseln (im Text der Kommission entgegen der Bezeichnung in Art 46 Abs 2 lit c DSGVO allerdings Standardvertragsklauseln genannt) angenommen, die im Fall von Datentransfers in Drittländer angewendet werden können. Um mehr Rechtssicherheit zu schaffen, wurden die neuen Anforderungen der DSGVO und die Vorgaben aus dem Schrems II-Urteil einbezogen.

Die neuen Standarddatenschutzklauseln sehen einen modularen Ansatz vor: Neben der Anwendung zwischen (1) Verantwortlichem und Verantwortlichem und (2) Verantwortlichem und Auftragsverarbeiter können die neuen Standarddatenschutzklauseln nun auch zwischen (3) Auftragsverarbeiter und Unterauftragsverarbeiter sowie zwischen (4) Auftragsverarbeiter und Verantwortlichem angewendet werden. Während es sich bei den alten Standardvertragsklauseln um zwei separate, vollständige Vertragsmuster für die beiden geregelten Szenarien von Datenübermittlungen gehandelt hat, enthalten die neuen Klauseln einerseits Inhalte, die für alle Übermittlungsszenarien gelten, andererseits modulare Inhalte, die nur auf bestimmte Arten der vier Datentransferszenarien anwendbar sind. Es müssen daher entweder aus dem Entwurf der Kommission zunächst die für das im konkreten Fall jeweils vorliegende Szenario anwendbaren Passagen ausgewählt und zusammengefügt werden (was einen erheblichen Aufwand und hohe Aufmerksamkeit erfordert) oder muss festgehalten werden, für welches Szenario die Klauseln abgeschlossen werden sollen. Zudem muss an mehreren Stellen eine Auswahl zwischen verschiedenen Textoptionen getroffen werden. Für die Praxis besonders relevant ist das neue Modul 3 für die Übermittlung von einem innerhalb der EU ansässigen Auftragsverarbeiter an einen Unterauftragsverarbeiter im Drittland; die bisherige „Hilfskonstruktion“ für den Fall, dass der Auftragsverarbeiter innerhalb der EU sitzt, Standardvertragsklauseln zwischen dem Verantwortlichen und dem Unterauftragsverarbeiter abzuschließen, ist nun nicht mehr nötig. Die neuen Standarddatenschutzklauseln lösen dieses Problem nun, im Unterschied zu den alten Standardvertragsklauseln, durch Abschluss des entsprechenden Moduls der neuen Klauseln.

Im Gegensatz zu den alten Klauseln können die neuen auch von Verantwortlichen oder Auftragsverarbeitern verwendet werden, die nicht im EWR ansässig sind, sofern deren Verarbeitung unter die DSGVO fällt und auch diese folglich geeignete Garantien für internationale Datentransfers vorsehen müssen. Ein weiterer Unterschied zu den alten Klauseln besteht darin, dass nach dem Wortlaut der Entscheidung der Kommission jedenfalls zwischen Verantwortlichem und Auftragsverarbeiter bzw. zwischen Auftragsverarbeiter und Unterauftragsverarbeiter kein separater Auftragsverarbeitervertrag abgeschlossen werden muss, da die neuen Klauseln den Anforderungen an einen Auftragsverarbeitungsvertrag nach Art 28 Abs 3 lit f DSGVO entsprechen. Nur so lässt sich auch erklären, dass die Kommission ihre Entscheidung nicht nur auf Art 46 Abs 1 lit c, sondern auch auf Art 28 Abs 7 DSGVO stützt, nach denen sie zur Erlassung von – richtig – Standarddatenschutzklauseln (Art 46) und Standardvertragsklauseln (Art 28) ermächtigt ist.

Sehr praktisch ist, dass die neuen Standarddatenschutzklauseln auch den Beitritt Dritter erlauben und damit auch nach Erstabschluss später von zusätzlichen Parteien mitgenutzt werden können.

Im Zusammenhang mit der Umsetzungsfrist ist zwischen Neu- und Altverträgen zu unterscheiden: Die alten Standardvertragsklauseln können nur noch bis 27. September 2021 verwendet werden; für danach neu geschlossene Verträge sind die neuen Klauseln anzuwenden. Die alten Standardvertragsklauseln müssen aber bei Änderung des Verarbeitungsvorgangs und jedenfalls binnen 18 Monaten durch die neuen ersetzt werden. Die Übergangsfrist endet am 27. Dezember 2022. Bitte beachten Sie aber, dass ein Drittlandstransfer auch aktuell schon durch die alten Standardvertragsklauseln nur gerechtfertigt werden kann, wenn diese – allenfalls durch zusätzliche, ergänzende Maßnahmen – unter Berücksichtigung des Rechts des Drittlandes und des konkreten Verarbeitungsvorgangs auch tatsächlich geeignete Garantien gewährleisten. Eine dokumentierte „Datentransfer-Folgenabschätzung“ wird in den neuen Klauseln beiden Vertragsparteien verpflichtend vorgeschrieben. Ein unterschiedsloser, gleichförmiger Abschluss ist daher in Zukunft schon nach dem Wortlaut der Klauseln nicht möglich, vielmehr muss die Erforderlichkeit von auf die konkrete Verarbeitungssituation und das Recht im Drittland abstellenden zusätzlichen, ergänzenden Maßnahmen zumindest geprüft und diese allenfalls dementsprechend vereinbart werden. In ihrer Entscheidung hält die Kommission ausdrücklich fest, dass ergänzende Vertragsklauseln erwünscht und zulässig sind, sofern sie den im Entwurf enthaltenen Klauseln nicht widersprechen; letztere gehen diesen jedenfalls vor.

Letztlich ist in Bezug auf die weiterhin auszufüllenden Anhänge zu den Klauseln zu beachten, dass in Annex II nicht nur jedenfalls konkrete technische und organisatorische Maßnahmen zu vereinbaren sind, sondern auch solche, die speziell auf die allfällige Verarbeitung sensibler Daten (einschließlich Art 10 DSGVO-Daten) Anwendung finden und die Einhaltung der Rechte der betroffenen Personen wahren. Auch ist eine Liste von Unterauftragsverarbeitern anzuschließen, um die Transparenz der Verarbeitungskette zu sicherzustellen. Diese und noch weitere Anforderungen an den Abschluss der neuen Klauseln – deren Besprechung den Rahmen einer Ausgabe unserer Datenschutz-Info sprengen würde – sorgen dafür, dass die neuen Klauseln vor Abschluss an den Einzelfall angepasst werden müssen, um je nach konkreter Verarbeitungssituation auch tatsächlich geeignete Garantien für den Datentransfer gewährleisten zu können. Das bereitet im Vergleich zu den bislang in Verwendung stehenden Klauseln einen erheblichen Mehraufwand und bietet Raum für Risikoabschätzungen, rechtliche Evaluierungen und nicht zuletzt auch für Verhandlungen zwischen den Vertragsparteien.

Wir haben aus der Kommissionsentscheidung bereits vier separate Texte für die vier neuen Übermittlungsszenarien erstellt, die wir Ihnen auf Anfrage gerne zusenden; weiters erarbeiten wir gerade ein Muster für eine Datentransfer-Folgenabschätzung und begleitende Klauseln.

Neue Standarddatenschutzklauseln (II)

Beitrag verfasst von Dr. Rainer Knyrim – KTR-Newsletter August 2021

Am 4. Juni 2021 hat die EU-Kommission ein **neues Set an Standarddatenschutzklauseln für den internationalen Datentransfer** veröffentlicht (Publications Office (europa.eu)). Die neuen Standarddatenschutzklauseln sind **seit 27. Juni 2021 in Kraft und können seither angewandt werden**.

Im Folgenden informieren wir Sie kurz über die wesentlichen Regelungsinhalte und Neuerungen:

- Wer die neuen C2P oder P2P Standarddatenschutzklauseln vereinbart, benötigt **keinen zusätzlichen Auftragsverarbeitervertrag**. Die Europäische Kommission hat nämlich von ihrer Ermächtigung Gebrauch gemacht und die entsprechenden Mindestinhalte für Auftragsverarbeiterverträge in die Standarddatenschutzklauseln aufgenommen. Wir raten Ihnen dennoch zur Vereinbarung zusätzlicher

Themenbereiche! Denn nur weil etwas gesetzlich nicht verlangt ist, heißt das nicht, dass es nicht wirtschaftlich sinnvoll wäre.

- Den Verantwortlichen oder Auftragsverarbeiter im EWR (Datenexporteur) trifft (nun auch offiziell) eine **umfassende Vorabprüfungs- und Rechenschaftspflicht**. So haben alle Parteien die Einhaltung der Standarddatenschutzklauseln durch eine geeignete Dokumentation nachweisen zu können. Für den Datenexporteur kommt hinzu, dass er die Einhaltung der Standarddatenschutzklauseln durch den Verantwortlichen oder Auftragsverarbeiter im Drittland (Datenimporteur) garantiert. Auch das mittlerweile übliche Auditrecht ist in Zukunft ein fixer Bestandteil.

- Ein Anknüpfungspunkt zum *Schrems II* Urteil des EuGH findet sich in Zukunft bei detaillierten Vorgaben, wie mit **Geheimhaltungs- und Vertraulichkeitsverletzungen** durch einen Data Breach oder durch staatliche Stellen im Drittland umzugehen ist.

- Änderungen und Erweiterungen der Vertragsparteien können in Zukunft durch eine großzügige **Docking Klausel** effizient erledigt werden. Hierfür bedarf es bloß einiger kleiner Ergänzungen in den bestehenden Anhängen zu den vereinbarten Standarddatenschutzklauseln und einer Unterschrift; gerade in Zeiten einer vermehrten Austauschbarkeit von Lieferanten eine sinnvolle Arbeitserleichterung.

Zusammenfassend lässt sich sagen, dass der internationale Datentransfer mit Standarddatenschutzklauseln ab sofort ein strenges Prüf-, Notifikations- und Überwachungskonzept verlangt. Im Gegenzug erhält man einen Formblattcharakter, der die tägliche Arbeit erleichtert. Dienstleister im EWR-Ausland sind vorab genau unter die Lupe zu nehmen; immerhin garantieren Sie die Eignung und Wahrung des angemessenen Schutzniveaus beim Datenimporteur. Auch haben Sie sich regelmäßig durch Überwachungen und Prüfungen von der Einhaltung und fortdauernden Eignung zu überzeugen und letztlich umgehend die Notbremse zu ziehen, sollten Sie die Information oder den Verdacht haben, dass Ihr Datenimporteur den vereinbarten Schutzrahmen nicht einhält bzw. aufgrund äußerer Umstände (bspw. Gesetze im Drittland) nicht einhalten kann. Gerade mit Blick auf die vereinbarten technischen und organisatorischen Maßnahmen sollte das Lieferantenmanagement entsprechend angepasst werden, denn Standarddatenschutzklauseln weisen auch eine **Drittbegünstigtenklausel** auf. Diese kann für den Datenexporteur sehr unangenehm werden: Vorgesehen ist, dass Sie betroffenen Personen – mit einigen wenigen Ausnahmen – für die Einhaltung der Standarddatenschutzklauseln haften.

Welche die entscheidenden Punkte bei der Implementierung der zusätzlichen Maßnahmen aus Sicht der Datenschutzbehörden sind erfahren Sie aus der **finalen Version der Empfehlungen 1/2020 des Europäischen Datenschutzausschusses**, die am 19. Juni 2021 publiziert wurden: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu).

EDSA-Empfehlungen für Prüfschritte bei Drittlandstransfers

Beitrag verfasst von Dr. Rainer Knyrim – KTR-Newsletter August 2021

Der Europäische Datenschutzausschuss (EDSA) hat nach öffentlicher Konsultation am 18. Juni 2021 die endgültige Fassung der **„Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“** beschlossen (die englische Version können Sie hier herunterladen). Diese Empfehlungen können und sollen bei Datentransfers in Drittländer für die – jedenfalls seit dem EuGH-Urteil Schrems II (Rs. C-311/18) erforderliche – Prüfung der Rechtslage im Drittland und der Erforderlichkeit sowie der Festsetzung ergänzender Maßnahmen herangezogen werden.

Die von der EU-Kommission beschlossenen neuen Standarddatenschutzklauseln (siehe Beiträge in diesem Newsletter) regeln die aus der Rechtsprechung des EuGH zu Schrems II folgenden Anforderungen nun ausdrücklich (Klausel 14) und können weiterhin als Rechtsgrundlage für eine Übermittlung personenbezogener Daten in ein Drittland herangezogen werden. Die EU-Kommission und der EDSA haben die neuen Standarddatenschutzklauseln und die Empfehlungen 01/2021 bewusst aufeinander abgestimmt – dies bedeutet, dass auch bei Verwendung der neuen Standarddatenschutzklauseln die Verantwortlichen oder Auftragsverarbeiter als Datenexporteure eine umfassende Prüfpflicht hinsichtlich der Rechtslage und der Praxis im Drittland trifft, durch die sichergestellt werden soll, dass das durch die Standarddatenschutzklauseln gewährleistete Schutzniveau erhalten bleibt.

In der endgültigen Fassung der Empfehlungen beschreibt der EDSA die wesentlichen Schritte, die Datenexporteure vor dem Hintergrund der umfassenden Rechenschaftspflicht Unternehmen sollten. Allerdings enthält die überarbeitete Fassung im Vergleich zur Vorversion einige wichtige Änderungen und Ergänzungen, die bei der Bewertung internationaler Datentransfers zu berücksichtigen sind.

- Ein verstärkter Fokus wird auf die **Behördenpraxis** im Drittland gelegt (Rz 43). Fehlt relevante Gesetzgebung im Drittland völlig, ist die jeweilige Behördenpraxis die einzige Grundlage für die datenschutzrechtliche Bewertung. Gibt es entsprechende Bestimmungen im Drittland, die den Datenzugriff durch staatliche Behörden regeln, ist die tatsächliche Behördenpraxis in die Prüfung als weiterer Faktor miteinzubeziehen, die sich negativ oder positiv auf die Zulässigkeit des

Datentransfers auswirken kann. Negativ wirkt sich aus, wenn die formelle Rechtslage im Drittland zwar den Europäischen Standards entspricht, die tatsächliche Behördenpraxis den rechtlichen Standards aber nicht folgt und zu befürchten ist, dass die in den Übermittlungsinstrumenten vorgesehenen Garantien (Art 46 DSGVO) beeinträchtigt werden. Positiv wirkt sich die Behördenpraxis aus, wenn formell zwar eine „problematische Rechtslage" im Drittland besteht, die Behördenpraxis aber dazu führt, dass eine Beeinträchtigung der in den Übermittlungsinstrumenten vorgesehenen Garantien dennoch faktisch nicht zu befürchten ist.

- Insgesamt wird nun ein **„risikobasierter Ansatz"** unter Berücksichtigung der (Behörden)Praxis im Drittland verfolgt. Ein Datentransfer in ein Drittland kann im Ergebnis selbst dann ohne ergänzende Maßnahmen zulässig sein, wenn in diesem Drittland zwar eine „problematischer Rechtslage" besteht, der Datenexporteur nach sorgfältiger und im Detail dokumentierter Prüfung jedoch zur Auffassung gelangt, dass die „problematischen" Gesetze des Drittlandes so interpretiert oder in der Praxis angewendet werden, dass sie im konkreten Fall auf die übermittelten Daten und auf den Datenimporteur nicht angewendet werden (Rz 43.3). Andererseits kann dieser „risikobasierte Ansatz" allerdings auch dazu führen, den Datentransfer einstellen zu müssen, wenn dieser zwar „am Papier" zulässig erscheint, die tatsächliche Behördenpraxis im Drittland jedoch inkompatibel mit Europäischen Datenschutzstandards ist. Zu beachten ist jedoch, dass demgegenüber ein solcher risikobasierter Ansatz in der bisherigen Rechtsprechung der österreichischen Datenschutzbehörde und auch des EuGH nicht ersichtlich ist und erst abgewartet werden muss, ob sich Gerichte und Behörden der Sichtweise des EDSA anschließen.

Die Publikation der endgültigen Fassung der Empfehlungen 01/2020 sowie der neuen Standarddatenschutzklauseln läuten jedenfalls eine neue Ära des Datentransfers in Drittländer ein. Ausgangspunkt jeder Datenübermittlung in sogenannte „unsichere" Drittländer ist eine umfassende, detaillierte und dokumentierte Datentransfer-Folgenabschätzung unter besonderer Berücksichtigung der Behördenpraxis im Drittland. Ein entsprechendes Muster arbeiten wir gerade aus und stellen wir Ihnen gerne zur Verfügung.

Datenschutzkonformer Betrieb einer Facebook-Fanpage unmöglich

Beitrag verfasst von Dr. Gerald Trieb, LL.M. – KTR-Newsletter August 2021

In seinem Rundschreiben vom 16. Juni 2021 nimmt der Bundesbeauftragte für den Datenschutzschutz und die Informationsfreiheit Deutschlands, Prof. Ulrich Kelber, auf sein Rundschreiben vom 20. Mai 2019 Bezug, in dem er schon darauf hingewiesen hatte, dass ein datenschutzkonformer Betrieb einer Facebook-Fanpage gegenwärtig nicht möglich sei. Dies deswegen, weil es erforderlich wäre, dass öffentliche Stellen als Fanpage-Betreiber eine Vereinbarung mit Facebook zur gemeinsamen Verantwortung schließen, die den Anforderungen von Art 26 DSGVO entspricht. Da der Bundesdatenschutzbeauftragte in Beantwortung seines Schreibens von vielen Dienststellen den Hinweis bekam, dass Facebook-Fanpages ein wesentlicher Teil deren Öffentlichkeitsarbeit seien, hat – wohl in seinem Auftrag – das Presse- und Informationsamt der Bundesregierung (BPA) versucht, mit Facebook – vergebens – eine Lösung zu erzielen. Facebook sei zu keinen Änderungen an seiner Datenverarbeitung bereit.

Der Bundesdatenschutzbeauftragte weist nochmals darauf hin, dass jene Dienststellen, die Fanpages betreiben, weiterhin ihrer Rechenschaftspflicht nach Art 5 Abs 2 DSGVO nicht nachkommen können, weil es insbesondere auch nicht ausreichend sei, die Nutzer in Bezug auf Informationen zur Verarbeitung ihrer personenbezogenen Daten im Rahmen einer Facebook-Fanpage alle pauschal auf Facebook zu verweisen. Da er nun – nachdem er zunächst noch im Sinne der Verhältnismäßigkeit von Abhilfemaßnahmen abgesehen hatte – nicht weiter zuwarten könne, kündigt Prof. Kelber an, von den Abhilfemaßnahmen ab Jänner 2022 Gebrauch zu machen, sollten bis zum 31.12.2021 die Facebook-Fanpages nicht eingestellt worden sein.

Da die rechtliche Situation für alle Fanpage-Betreiber, ob öffentliche Dienststelle oder privatwirtschaftlich tätiges Unternehmen, gleich ist, muss erneut überdacht werden, ob Facebook-Fanpages weiterhin Teil des Öffentlichkeitsauftrittes sein sollen. Da schon das deutsche Presseamt daran gescheitert sein dürfte, Verbesserungen bei der Verarbeitung personenbezogener Daten bzw. der datenschutzrechtlichen Dokumentation durch Facebook zu erreichen, ist nicht zu erwarten, dass sich daran bis Jahresende etwas ändern wird. Es ist durchaus zu befürchten, dass sich auch die Landesdatenschutzbeauftragten in Deutschland bzw. Datenschutz-Aufsichtsbehörden in anderen Mitgliedstaaten, wie die österreichische

Datenschutzbehörde, der Vorgehensweise des Bundesdatenschutzbeauftragten anschließen und entsprechend von ihren Abhilfemaßnahmen Gebrauch machen werden.

Die von uns schon im Jahr 2018 erstellte „Datenschutzinformation-Facebook“ kann zumindest verhindern, dass sich Fanpage-Betreiber damit begnügen müssen, auf die – in der Tat – spärlichen Informationen von Facebook über die Verarbeitung personenbezogener Daten über Facebook-Fanpages zu "vertrauen". Vielmehr können Sie mit deren Hilfe immerhin eine transparente Information bereitstellen. Offene Themen bleiben natürlich die unzureichenden Artikel 26-Vereinbarung, wie sie Facebook zur Verfügung stellt, wie auch eine der nunmehr sich festigenden Judikatur zum Cookie-Einsatz genügende Einwilligungserklärung durch die Nutzer. Doch kann das verantwortliche Unternehmen mit einer eigenen "Datenschutzinformation-Facebook" zumindest dem Kernkritikpunkt des Datenschutzbeauftragten begegnen und über die erfolgte Information der Nutzer über die Verarbeitung personenbezogener Daten Rechenschaft leisten.

Vor dem Hintergrund, dass angesichts der Warnung des Bundesdatenschutzbeauftragten Facebook-Fanpages nur noch begrenzte Laufzeit haben könnten, bieten wir unsere "Datenschutzinformation–Facebook" Abonnenten unseres Newsletters zum reduzierten Pauschalpreis von netto EUR 300,00 an. Bitte kontaktieren Sie uns bei Interesse!

Deutsche Datenschutzkonferenz veröffentlicht Übersichtsliste über Publikationen

Beitrag verfasst von Dr. Gerald Trieb, LL.M. und Antonia Kühbauer – KTR-Newsletter August 2021

Die deutsche Datenschutzkonferenz (DSK) hat vor kurzem eine **Übersichtsliste über ihre Publikationen** veröffentlicht. Die Liste illustriert die Fülle an behördlichem Informationsmaterial in Bezug auf Datenschutz, die allein die Landes- und Bundesdatenschutzbehörden des größten EU-Mitgliedslandes veröffentlicht haben. Aufgrund ihres Umfanges ist diese nur schwer zu überblicken, doch sind die Informationsmaterialien deutscher Behörden traditionell und naheliegenderweise für den österreichischen Rechtsanwender von hoher Bedeutung; dies gerade dann, wenn das Recht – wie im Datenschutz – durch eine direkt anwendbare Verordnung der EU harmonisiert ist.

Das Dokument ist seit April 2021 hier online abrufbar. Die Liste bietet einen detaillierten Überblick darüber, wann und wo sich eine Behörde in Deutschland bereits zu datenschutzrechtlichen Themen und Fragestellungen geäußert hat. Die Gliederung der Liste ist in Informationsmaterialien des Bundes und der einzelnen Länder unterteilt, wobei zuerst Publikationen auf Bundesebene und dann jene der einzelnen Länder gelistet sind. Von links nach rechts finden Sie die zugrundeliegende Norm, daneben die entsprechende Beitragsbezeichnung und zuletzt die Fundstelle per Link. Neben generellen Informationen zu datenschutzrechtlichen Begriffen und Erläuterungen zur DSGVO sind auch Beiträge zu spezielleren Themen erfasst, wie beispielsweise zum Datenschutz im Zusammenhang mit Führerscheinkontrollen. Darüber hinaus beinhaltet die Liste auch zahlreiche Ratgeber, Broschüren, Orientierungshilfen, FAQs und Muster(-verträge).

Es ist jedoch darauf hinzuweisen, dass in dieser Übersicht alle Materialien ungefiltert dargestellt werden und dieselbe infolge sehr umfangreich ist. Mithilfe unseres Abo-Services „Datenschutz-Info“ erhalten Sie hingegen ausgewählte Informationen, die für Sie übersichtlich zusammengefasst aufbereitet werden; in unsere Themenauswahl beziehen wir neben Entscheidungen aus Österreich und der EU auch Publikationen des EDSA, der CNIL wie auch der ICO ein.

In Summe lässt sich sagen, dass die Übersicht der deutschen Datenschutzkonferenz durchaus hilfreich sein kann, um eine schnelle Auflistung aller datenschutzrechtlichen Publikationen der Aufsichtsbehörden zu erhalten und recht rasch Detailinformationen zu bestimmten datenschutzrechtlichen Fragen zu erhalten.

Beschwerdewelle gegen Cookie-Banner

Beitrag verfasst von Dr. Rainer Knyrim – KTR-Newsletter August 2021

Die Datenschutz-NGO noyb (gegründet von Max Schrems) hat **422 (!) formale Beschwerden** gegen Unternehmen wegen deren Cookie-Bannern angekündigt - wie z.B. Die Presse berichtete. Davon betreffen über 200 Österreich. Innerhalb eines Jahres sollen laut Schrems darüber hinaus noch über 10.000 Webseiten überprüft und wenn nötig Abmahnungen erteilt werden. Zur Vermeidung solcher Risiken sollten Sie Ihren Cookie-Banner anhand der folgenden Punkte prüfen, wobei wir gerne behilflich sind.

Anforderungen an Consent-Layer und Cookie-Banner

Viele Webseiten verwenden Cookies oder Dienste von Drittdienstanbietern, die eine Einwilligung erfordern. Mittlerweile werden vermehrt aufwändigere Consent-Banner genutzt, die konkrete Informationen über den Einsatz von Cookies und die Einbindung von Drittdiensten liefern und Entscheidungs- und Wahlmöglichkeiten bieten. Ein DSGVO-konformes Consent-Management erfordert die Verarbeitung von Nutzerdaten in einer Weise, die der abgegebenen oder verweigerten Einwilligung sowie den getroffenen Einstellungen entspricht. Den Websitebetreiber trifft dabei die Darlegungs- und Beweislast für die datenschutzrechtskonforme Gestaltung der Website. Eine Einwilligung muss nach Art 4 Z 11 DSGVO freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben werden und kann in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung bestehen. Für den bestimmten Fall abgegeben ist eine Einwilligung dabei dann, wenn Inhalt, Zweck und Tragweite der Erklärung konkretisiert sind.

Zeitpunkt der Einwilligung

Die Einwilligung muss vor der Datenverarbeitung erteilt werden. Wird eine Website zum ersten Mal abgerufen, dürfen die einwilligungsbedürftigen Cookies erst gesetzt werden, wenn diesen im Consent-Tool zugestimmt wurde.

Informiertheit bei der Einwilligung

Vor Abgabe der Einwilligung müssen der betroffenen Person Mindestinformationen erteilt werden, und zwar die Identität des Verantwortlichen, die Verarbeitungszwecke, die verarbeiteten Daten, die Absicht einer ausschließlich automatisierten Entscheidung sowie die Absicht einer Datenübermittlung in Drittländer. Beim Einsatz eines Nutzertrackings durch Drittdienste sind die Verarbeitungszwecke detailliert zu erläutern. Außerdem ist darüber zu informieren, wenn Profile erstellt werden und diese mit Daten anderer Websites angereichert werden. Eine informierte Einwilligung erfordert auch den Hinweis auf das Widerrufsrecht der Einwilligung, das bereits aus der ersten Ebene des Consent-Fensters hervorgehen muss.

Eindeutig bestätigende Handlung

Auf einer Webseite werden Einwilligungen in Form einer eindeutig bestätigenden Handlung erteilt. Dazu sind vor allem die Bezeichnung und Darstellung der Schaltfläche im Vergleich zur Schaltfläche, durch die die Einwilligung verweigert wird, maßgeblich. Außerdem stellt sich die Frage, ob dem Mausklick ein eindeutiger Erklärungsinhalt zukommt. Geht aus dem Informationstext nicht eindeutig hervor, wozu die Einwilligung erteilt wird, liegt eine solche

nicht vor. Unklarheiten ergeben sich auch dann, wenn Schieberegler und Schaltflächen nicht miteinander verknüpft sind und nicht automatisch aktiviert werden, wenn alle Cookies akzeptiert werden.

Freiwilligkeit der Einwilligung

Eine Einwilligung ist nur dann freiwillig, wenn kein Druck oder Zwang ausgeübt wird. Unzulässig sind Cookie-Walls, die den Inhalt der Webseite nicht oder nur eingeschränkt erkennbar machen, wenn der Nutzer den Einsatz von Cookies nicht akzeptiert hat und die Inhalte ausschließlich dann sichtbar werden, wenn eine Einwilligung erfolgt. Wird aber die Alternative angeboten, die Inhalte durch Bezahlung sichtbar zu machen, spricht dies nicht gegen die Freiwilligkeit.

Nudging

Mithilfe von Nudging wird das Verhalten der Nutzer beeinflusst. Die Zustimmung wird im Rahmen des Consent-Layers oft auffälliger gestaltet als die Ablehnung. Außerdem wird der Ablehnungsprozess oft kompliziert ausgestaltet, indem auf der ersten Ebene des Consent-Tools zwar die Einwilligung erteilt werden kann, die Ablehnung aber die Öffnung der Cookie-Einstellungen und Deaktivierung vorangekreuzter Häkchen erfordert. Auch das LG Rostock führte zur Rechtswidrigkeit von Cookie-Bannern aus, dass die Opt-Out-Variante zur Einholung einer wirksamen Einwilligung nicht geeignet ist. Den Aufwand der Abwahl von Cookies würde regelmäßig gescheut werden und die Cookies ohne Information bestätigt, wodurch dem Verbraucher die Tragweite seiner Erklärung nicht bewusst sei. Dass die Möglichkeit bestand, die Einwilligung auf technisch notwendige Cookies zu beschränken, ändere an der Beurteilung nichts. Außerdem sei die Abwahl der Cookies als nicht anklickbare Schaltfläche zu erkennen gewesen. Neben dem grün unterlegten „Cookie zulassen“-Button trete die Ablehnung in den Hintergrund und könne gar nicht als gleichwertige Einwilligungsmöglichkeit wahrgenommen werden. Unter Nudging fällt auch die wiederholte Frage nach der Einwilligung, sodass der Nutzer die Einwilligung erteilt, um nicht mehr belästigt zu werden. Solche verhaltensmanipulierenden Ausgestaltungen können wie im Fall vor dem LG Rostock zur Unwirksamkeit der Einwilligung führen.

Widerruf der Einwilligung

Der Widerruf einer Einwilligung muss so einfach wie ihre Erteilung sein. Wird die Einwilligung im Rahmen der Nutzung der Webseite erteilt, muss auch der Widerruf über diese möglich sein. Wird ein Consent-Fenster eingesetzt, ist dem Nutzer die Möglichkeit zu geben, dieses wieder zu öffnen und seine Einstellungen ändern zu können.

Erfahren Sie mehr zu aktuellen Veranstaltungen auf unserer Webseite:
www.kt.at/termine

Vergangene Newsletter finden Sie in unserem Archiv zum Nachlesen:
www.kt.at/newsletter

Datenschutzinformation

Die Verarbeitung der Daten zu diesem Newsletter 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: https://www.kt.at/datenschutzinformation/

Knyrim Trieb Rechtsanwälte OG
Mariahilfer Straße 89a, A-1060 Wien, T: +43 1 909 30 70, F: +43 1 909 36 39
FB: knyrimtrieb E: kt@kt.at, W: www.kt.at

FN 462250f, HG Wien
