



## Newsletter der Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!

Liebe Datenschutzinteressierte!

Seit unserem letzten Datenschutz-Newsletter hat sich viel getan. Insbesondere: Die Datenschutzbehörden in Europa – inkl. Österreich – verhängen mittlerweile teils sehr massive Strafen und ein österreichischer Rechtsanwalt hat eine Abmahnwelle wegen Cookies gestartet. Aber der Reihe nach:

### DSGVO-Strafen in Österreich und der EU

Einem [MEDIENBERICHT](#) (derstandard.at) zufolge hat die österreichische Datenschutzbehörde die höchste und die zweithöchste bisherige Strafe verhängt:

**Die zweithöchste Strafe** betraf laut diesem Bericht jenen Fußballtrainer aus dem Mostviertel, der sein Handy in der Damen-Umkleide platzierte und damit jahrelang Spielerinnen in der Dusche filmte. Die Datenschutzbehörde verhängte eine **Strafe von EUR 11.000,-** gegen diesen Trainer.

**Die bisher höchste verhängte Strafe von EUR 50.000,-** betraf ein Unternehmen „aus dem medizinischen Bereich“ wegen **Verstößen gegen die Meldepflichten und Nichtbestellung eines Datenschutzbeauftragten**. Wir tippen darauf, dass es sich dabei um die Allergie-Tagesklinik gehandelt hat, über die wir im letzten Newsbeitrag berichtet haben [ZUM BEITRAG](#) (kt.at) bei der die Datenschutzbehörde nicht weniger als 14 Einzelverstöße feststellte – siehe auch den Beitrag dazu in „report“ [ZUM BEITRAG](#) (kt.at) sowie die Rezension dazu in ecolex [ZUR REZENSION](#) (kt.at). Da laut der damals berichteten Entscheidung dieses Unternehmen ein relativ kleines ist (im Bereich 20-40 Mitarbeiter), kann vermutet werden, dass die Strafe im Bereich von 1-2% des Umsatzes liegen dürfte.

Im internationalen Vergleich sind diese Strafen in absoluten Zahlen immer noch niedrig, denn die Liste der bereits verhängten oder angekündigten „geschmalzenen“ Strafen der Datenschutzbehörden anderer Staaten wird immer länger und dramatischer:

- .) **England: EUR 204 Mio** gegen British Airways und **EUR 110 Mio** gegen Marriott wegen Datenverlust bei Hackerangriffen angekündigt
- .) **Frankreich: EUR 50 Mio** gegen Google wegen Verstoß gegen Informationspflichten und freiwillige, informierte Einwilligung
- .) **Deutschland: Millionen-Bußgeld** von Berliner Landesdatenschutzbeauftragten angekündigt
- .) **Niederlande: EUR 460.000** wegen unzulässigem Zugriff auf Patientendaten in Krankenhaus
- .) **Portugal: EUR 400.000** wegen fehlendem Zugriffsmanagement in Krankenhaus
- .) **Polen: EUR 220.000** wegen fehlender Datenschutzinformation
- .) **Griechenland: EUR 150.000** gegen PwC wegen unfreiwilliger „Einwilligung“ der Mitarbeiter

Mehr zu den Strafen erfahren sie im Editorial des nächsten Heftes von „Datenschutz konkret“ das noch im September erscheint.

**Die Schonzeit im Datenschutzrecht ist jedenfalls vorbei!**

## Österreichischer Anwalt startet DSGVO-Abmahnwelle

Bevor sich jemand vor den Datenschutzbehörden zu fürchten beginnt, auch ein österreichischer Anwalt sorgt seit dem Sommer für Erstarrungsmomente: Er hat eine Abmahnwelle gegen Unternehmen im Hinblick auf Cookies gestartet. Er vertritt – zumindest im von uns betreuten Fall – eine Mandantin, die sich auf der Webseite eines Unternehmens für dessen Produkte interessiert hat und nachher Cookies auf ihrem Rechner platziert fand und in der Folge Werbeeinschaltungen auf anderen Webseiten sah, die zum davor besuchten Unternehmen passte. Er fordert für diese dann EUR 1.000,- pro (!) aus seiner Sicht nicht rechtskonform gesetztem Werbe- oder Tracking-Cookie, was je nach Anzahl der Cookies exorbitante Schadenersatzforderungen von über EUR 10.000,- plus EUR 1.000 Anwaltskostenforderung plus Forderung nach Abgabe einer Unterlassungserklärung nach sich zieht. Die Presse berichtete bereits über diesen Fall [ZUM BEITRAG](#) (diepresse.com)

Die Geltendmachung von immateriellen Schadenersatzforderungen bei (vermeintlichen) Datenschutzverstößen scheint mittlerweile auch in Österreich an Popularität zu gewinnen. Am 16. August 2019 wurde eine Entscheidung des Landesgericht Feldkirch publik [ZUM BEITRAG](#) (addendum.org), wonach ein österreichischer Rechtsanwalt die Österreichische Post AG auf EUR 2.500,00 an immateriellem Schadenersatz geklagt hat, weil diese Angaben zu dessen „Parteiaffinitäten“ ohne dessen Einwilligung und Information ermittelt und gespeichert haben soll. **Ihm wurden immerhin EUR 800,00 zugesprochen** (nicht rechtskräftig). Das ich persönlich eine andere Meinung zum Post-Sachverhalt habe, können Sie im August-Heft des ecolex nachlesen [ZUM BEITRAG](#) (kt.at)

Diese **erste Entscheidung eines Gerichtes zu Schadenersatz unter der DSGVO** und die Abmahnschreiben lassen befürchten, dass in absehbarer Zeit mit einem signifikanten Anstieg an Schadenersatzforderungen im Zusammenhang mit behaupteten

Datenschutzverletzungen zu rechnen sein wird. Daher besteht hier für Unternehmen dringender Handlungsbedarf!

Wir haben daher als Service für Sie unseren ständigen Kooperationspartner RA Mag. Alexander Nessler, LL.M. gebeten, Ihnen eine Anleitung zum Überblick zum rechtskonformen Einsatz von Cookies zu geben:

### **Rechtskonformer Einsatz von Cookies**

Man findet sie mittlerweile auf einer großen Anzahl von Webseiten. Tracking und Retargeting-Cookies: Kleine Textdateien, die das Surfverhalten von Besuchern der eigenen Webseite über diese hinausgehend erfassen, sodass diese anschließend auf anderen Webseiten mit gezielter Werbung für das eigene oder auch ein fremdes Angebot wieder angesprochen werden können. Trotz der Beliebtheit des Einsatzes solcher Cookies, herrscht bei vielen Unternehmen jedoch nach wie vor Unsicherheit darüber, wie diese datenschutzkonform zu implementieren sind, insbesondere die dafür erforderliche Einwilligung rechtskonform einzuholen ist.

Die aktuell verwendeten Lösungen reichen von schlichten Cookie-Bannern (die meist am oberen oder unteren Bildschirmrand angezeigt werden) bis zum Einsatz von sogenannten Cookie-Walls (die erst einmal angeklickt werden müssen, um überhaupt zu den Webseiteninhalten zu gelangen).

**Problematisch ist oftmals, dass die jeweilige Lösung so implementiert ist, dass Banner und Wall zwar korrekt dargestellt werden, das Setzen von Tracking und Retargeting-Cookies dennoch bereits unabhängig einer etwaigen Einwilligung erfolgt. Ein weiteres verbreitetes Problem ist, dass Webseitenbesuchern oftmals gar keine Wahlmöglichkeit gegeben wird, Cookies zu akzeptieren oder abzulehnen, um eine Webseite nutzen zu können. Regelmäßig kommt es auch vor, dass dem Nutzer keine hinreichende Information darüber geboten wird, wofür bzw wogegen er sich letztlich entscheiden kann.**

Die nachstehenden Punkte sollen Ihnen eine unverbindliche Orientierungshilfe bieten, Fallstricke beim Einsatz von Cookies und deren Implementierung zu vermeiden:

#### **1. Nicht alle Cookies sind bedenkenlos genießbar.**

Cookies sind regelmäßiger Bestandteil von Webseiten. Groß diskutiert werden oft nur Tracking- und Retargeting-Cookies; tatsächlich werden bestimmte Cookies aber in vielen Fällen schlichtweg für den ordnungsgemäßen Betrieb von Webseiten benötigt. Cookies helfen bei der richtigen Darstellung von Webseiten, der effizienten Nutzung von Onlineshops und verhindern, dass Sprach- und Darstellungspräferenzen jedes Mal aufs Neue eingegeben werden müssen. Cookies sind praktisch, manche greifen gar nicht in die Privatsphäre des Webseitenbesuchers ein, andere schon.

Werden Cookies auf Ihrer Webseite verwendet, so gilt es – abseits der technischen Merkmale – zu unterscheiden, ob für den Betrieb der Webseite unabdingbare, (technisch) bedingte oder sonstige Cookies vorliegen. Die sonstigen Cookies unterteilen sich wiederum in jene, die zwar technisch nicht absolut notwendig sind, aber dennoch aufgrund eines berechtigten Interesses gemäß Art 6 Abs 1 lit f DSGVO vom Webseitenbetreiber verarbeitet

werden dürfen und jenen, die jedenfalls eine Einwilligung des Webseitenbesuchers gemäß Art 6 Abs 1 lit a DSGVO voraussetzen.

Deshalb sollte in einem ersten Schritt die Definition und Klassifizierung aller Cookies erfolgen, die auf der eigenen Webseite zum Einsatz kommen (sollen).

## **2. Privacy by Default; auch auf der Webseite.**

Ruft ein Kunde oder Interessent Ihre Webseite auf, dürfen automatisch nur jene Cookies gesetzt bzw ausgelesen werden, die für den Betrieb der Webseite technisch notwendig sind oder die aufgrund Ihres berechtigten Interesses verarbeitet werden. Hierüber ist die betroffene Person dennoch vorab im Rahmen der Datenschutzinformation aufzuklären; diese ist somit für alle Cookies erforderlich, die personenbezogene Daten über Webseitenbesucher verarbeiten.

Wir empfehlen, die korrekte Gestaltung Ihrer Webseite zu überprüfen und gegebenenfalls erforderliche Anpassungen vorzunehmen.

## **3. Informationsbereitstellung**

Wir kennen sie alle: Cookie-Banner und Cookie-Walls. Überall zu sehen, führt die Implementierung aus datenschutzrechtlicher Sicht oft nicht zu einer Zulässigkeit der Verwendung von Cookies, beispielsweise wenn dies intrasparent umgesetzt ist. Cookie-Banner und Cookie-Walls sollen den Webseitenbesucher darüber informieren, dass es zu einer Datenverarbeitung im Zuge des Besuchs der Webseite kommt. Diese Datenschutzinformation ist auf jeder Webseite mit Cookies bereitzustellen und darf dabei weder das Impressum, noch die Datenschutzinformation überdecken.

Der Webseitenbesucher muss dadurch die Möglichkeit erhalten zu erfahren wer welche Cookies zu welchem Zweck verarbeitet und ob dadurch Dritte Zugriff auf seine personenbezogene Daten erhalten. Die Datenverarbeitungen sind im Einzelnen darzulegen und alle Cookies, der jeweilige Anbieter und die konkrete Funktion sind aufzuführen. Art 13 DSGVO sieht darüber hinaus noch weitere – detailliertere – Anforderungen vor, die es dringend einzuhalten gilt. Eine aktuelle Entscheidung der österreichischen Datenschutzbehörde lässt den Schluss zu, dass der Webseitenbetreiber den Einwilligenden vor der Einwilligung umfassend alle für ihn diesbezüglich relevanten Informationen zu offenbaren hat. Inhaltlich sollte man sich an den Artikeln 12 ff DSGVO orientieren.

Eine umfassende Datenschutzinformation ist gerade in Bezug auf Cookies ein wesentlicher Eckpunkt außenwirksamer Datenschutz-Compliance. Wir empfehlen daher eine detaillierte Aufschlüsselung der zum Einsatz gelangenden Cookies.

## **4. Berechtigte Interessen zur Verwendung von Cookies**

Selbst Cookies, die für den Betrieb der Webseite nicht absolut notwendig sind, können ohne Einwilligung der betroffenen Person gesetzt und ausgelesen werden, wenn dies zur Wahrung von berechtigten Interessen des Webseitenbetreibers oder eines Dritten erforderlich ist. Ob eine Verarbeitung im berechtigten Interesse liegt, ist im Einzelfall zu beurteilen. Beispiele für Zwecke, die das Setzen und Auslesen von Cookies im Rahmen eines legitimen Interesses gegebenenfalls begründen könnten: Die Einbindung von

Drittinhalten oder Web Fonts aus Effizienz- und Kosteneinsparungserwägungen, die Sicherstellung der Integrität und Sicherheit der Webseite oder Betrugsprävention.

Wir empfehlen die genaue Überprüfung, ob im Einzelfall tatsächlich ein zulässiges berechtigtes Interesse vorliegt. Nehmen Sie sich ausreichend Zeit, das potentielle berechnete Interesse genau zu definieren, die Erforderlichkeit darzustellen und die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person Ihren Interessen gegenüberzustellen.

### **5. Aktive Einwilligung (Opt-in)**

Sind Cookies weder für den Betrieb einer Webseite unabdingbar und auch nicht aufgrund eines berechtigten Interesses des Webseitenbetreibers oder eines Dritten rechtfertigbar, so ist regelmäßig die Einwilligung des jeweiligen Webseitenbesuchers erforderlich. Gefordert ist eine aktive Einwilligung vor Setzen der jeweiligen Cookies durch Klicken auf den Banner bzw die Wall oder eine sonstige Schaltfläche. Dabei muss der Webseitenbesucher die Möglichkeit haben, die betreffenden Cookies einzeln zu aktivieren. Die pauschale Einwilligung oder ein schlichtes „OK“ auf dem Cookie-Banner ohne Alternativmöglichkeit sind nicht ausreichend.

Wir empfehlen den Einsatz einer professionellen Cookie-Banner-Lösung, welche die notwendige Textinformation enthält und es dem Webseitenbesucher zugleich ermöglicht, einwilligungspflichtige Cookies einzeln zu aktivieren (Opt-in).

### **Haftungsausschluss**

Bei dieser Hilfestellung handelt es sich um eine unverbindliche Serviceleistung unserer Kanzlei und um keine verbindliche anwaltliche Auskunft. Das Dokument erhebt keinen Anspruch auf Vollständigkeit. Für tieferegehende Auskünfte und individuelle rechtliche Beurteilungen stehen wir Ihnen sehr gerne unter [kt@kt.at](mailto:kt@kt.at) oder 01/9093070 zur Verfügung.

## **Rechtskonformer Einsatz von Social Plugins**

*Dr. Claudia Gabauer, LL.M., Rechtsanwaltsanwältin in unserer Kanzlei*

*EuGH 29.7.2019, C-40/17, Fashion ID GmbH & Co KG/Verbraucherzentrale NRW e.V.*

Da sich nicht nur die nationalen Gerichte mit Datenschutzrecht befassen, sondern auch der EuGH erneut mit einer Datenverarbeitung durch einen Facebook-Dienst in seinem Urteil [ZUM URTEIL](https://curia.europa.eu) ([curia.europa.eu](https://curia.europa.eu)) vom 29. Juli 2019 (Rechtssache C-40/17, Fashion ID GmbH & Co KG/Verbraucherzentrale NRW e.V.) und dort grundlegende Aussagen zu den Anforderungen an die datenschutzrechtskonforme Einbettung von sogenannten „Social Plugins“ auf Webseiten trifft, haben wir unsere Rechtsanwaltsanwältin Dr. Claudia Gabauer, LL.M. gebeten, dieses Urteil für Sie zu analysieren und Handlungsempfehlungen für dessen Umsetzung in der Praxis zu geben:

Ausgangsfall dieses Urteils ist die Einbindung von „**Gefällt mir**“-Buttons von Facebook Ireland („Facebook“) auf der Webseite des bekannten Modeunternehmens. Der EuGH stellt

fest, dass die Einbindung dieses Social Plugins zur Folge hat, dass bereits beim Aufruf der Fashion ID-Webseite die personenbezogenen Daten der Besucher an Facebook übermittelt werden. Offenbar erfolgt diese Übermittlung, ohne dass sich die Besucher dessen bewusst sind und unabhängig davon, ob sie Mitglieder des sozialen Netzwerks Facebook sind oder den „Gefällt mir“-Button angeklickt haben.

### **Zur gemeinsamen Verantwortlichkeit von Facebook und Webseiten-Betreiber**

Der EuGH hält fest, dass ein Webseiten-Betreiber, der den „Gefällt mir“-Button von Facebook auf seiner Webseite eingebunden hat, für die Vorgänge des Erhebens der personenbezogenen Daten der Besucher der Webseite (IP-Adresse des Rechners des Besuchers sowie technische Informationen des Browsers) und deren Weiterleitung durch Übermittlung an Facebook als **gemeinsam mit Facebook verantwortlich** iSd Art 2 lit d Datenschutz-Richtlinie 95/46/EG („Datenschutz-Richtlinie“) **angesehen werden kann**, da der Webseiten-Betreiber und Facebook gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dahingegen ist der Webseiten-Betreiber nicht verantwortlich für Vorgänge, die Facebook nach der Übermittlung dieser Daten vorgenommen hat, wenn der Webseiten-Betreiber nicht über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheidet.

### **Ist eine Einwilligung erforderlich?**

Der EuGH weist darauf hin, dass nach Art 5 Abs 3 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG („e-Privacy-RL“) die Mitgliedstaaten sicherstellen müssen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf Grundlage von klaren und umfassenden Informationen, die er gemäß der Datenschutz-Richtlinie u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. **Kann der Anbieter eines Social Plugins auf Informationen zugreifen, die im Endgerät des Besuchers der Webseite des Betreibers gespeichert sind, so bedarf es demnach einer Einwilligung des Besuchers.**

### **Wem gegenüber muss die Einwilligung erklärt werden?**

Der EuGH stellt klar, dass die Einwilligung gemäß Art 2 lit h und Art 7 lit a der Datenschutz-Richtlinie **vor dem Erheben der Daten der betroffenen Person und deren Weitergabe durch Übermittlung erklärt werden muss**. Daher obliegt es dem Betreiber der Webseite und nicht dem Anbieter des Social Plugins, diese Einwilligung einzuholen, da der Verarbeitungsprozess der personenbezogenen Daten dadurch ausgelöst wird, dass ein Besucher diese Webseite aufruft. Die Einwilligung, die dem Betreiber gegenüber zu erklären ist, betrifft jedoch nur jene Vorgänge der Verarbeitung personenbezogener Daten, für die er tatsächlich über die Zwecke und Mittel entscheidet.

### **Wen trifft die Informationspflicht?**

Das Gleiche gilt für die Informationspflicht nach Art 10 der Datenschutz-Richtlinie. Aus dem Wortlaut dieser Bestimmung ergibt sich, dass **der Verantwortliche – oder sein Vertreter – der Person, bei der die Daten erhoben werden, mindestens die in dieser Bestimmung genannten Informationen bereitstellen muss**. Es scheint somit, dass der Verantwortliche diese Information sofort zu geben hat, d.h. zum Zeitpunkt des Erhebens der Daten. Daraus

folgt für den vorliegenden Fall, dass **die Informationspflicht nach Art 10 der Datenschutz-Richtlinie den Webseiten-Betreiber trifft**, wobei dieser die betroffene Person jedoch nur in Bezug auf jene Datenverarbeitungsvorgänge informieren muss, für die dieser Betreiber tatsächlich über die Zwecke und Mittel entscheidet.

### **Auswirkungen der Entscheidung**

Obwohl sich das Urteil auf die Datenschutz-Richtlinie bezieht, lassen sich die vom EuGH gezogenen Schlüsse auch auf die Rechtslage nach der DSGVO übertragen, da die materielle Rechtslage im Vergleich zur Vorgängerbestimmung im Wesentlichen unverändert geblieben ist. Daher ist bei einer Einbindung von Social Plugins auf Webseiten von einer gemeinsamen Verantwortlichkeit gemäß Art 26 DSGVO des Webseiten-Betreibers und des Anbieters des Social Plugins auszugehen ist. Für die Frage der Einwilligungsbedürftigkeit von Social Plugins ist es ausschlaggebend, ob das Social Plugin Cookies platziert oder auf vorhandene Cookies zugreift. Nur wenn keine Cookies involviert sind, könnte eine andere Rechtsgrundlage für die Datenverarbeitung – wie z.B. berechnete Interessen gemäß Art 6 Abs 1 lit f DSGVO – unter Umständen in Betracht gezogen werden.

### **Handlungsempfehlungen**

#### ***Feststellung des Handlungsbedarfs***

Überprüfen Sie die Social Plugins sowie Plugins anderer Drittanbieter auf Ihrer Webseite und klären Sie ab, ob bereits mit dem Aufruf der Webseite personenbezogene Daten an den Drittanbieter übermittelt werden

#### ***Abschluss einer Vereinbarung nach Art 26 DSGVO***

Aufgrund der gemeinsamen Verantwortlichkeit des Webseiten-Betreibers und des Anbieters des Social Plugins ist der Abschluss einer Vereinbarung nach Art 26 DSGVO erforderlich

#### ***Anpassung der Datenschutzinformation***

Der Webseiten-Betreiber hat den Besuchern seiner Webseite nach Art 13 DSGVO Informationen über die Erhebung und die Übermittlung ihrer personenbezogenen Daten an den Anbieter des Social Plugins zur Verfügung zu stellen. Die Datenschutzinformation auf der Webseite sollte daher – sofern erforderlich – entsprechend adaptiert und ergänzt werden.

#### ***Einholen der Einwilligung***

Werden im Rahmen des Social Plugins Cookies gesetzt, ist hierfür eine Einwilligung der betroffenen Personen erforderlich, die gegenüber dem Webseiten-Betreiber erteilt werden muss. Eine Einwilligung gilt nicht bereits mit dem Aufruf der Webseite als erteilt, sondern muss unmissverständlich in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen (vgl. Art 4 Z 11 DSGVO). Es gibt verschiedene Optionen, wie die Einwilligung eingeholt werden kann. Eine Einwilligung kann z.B. durch den Einsatz von Cookie-Konsensmanagern erteilt werden, wobei hier auf die rechtskonforme Umsetzung geachtet werden sollte. Im Fall der sog. „Zwei-Klick-Lösung“ werden Daten erst mit Aktivierung und Anklicken des Social Plugins an den Anbieter des Social Plugins übermittelt. Eine datenschutzfreundliche Lösung bietet die sog. „Shariff-Lösung“, mit der der Nutzer über ein Bildsymbol direkt auf die Webseite des Social Media Anbieters weitergeleitet wird.

## Haftungsausschluss

Bei dieser Hilfestellung handelt es sich um eine unverbindliche Serviceleistung unserer Kanzlei und um keine verbindliche anwaltliche Auskunft. Das Dokument erhebt keinen Anspruch auf Vollständigkeit. Bei Bedarf können wir Sie gerne bei der Umsetzung dieser Maßnahmen unterstützen, wir haben Umsetzungspakete sowohl für Facebook Fanpages als auch der Gefällt-mit – Buttons, die wir anbieten können. – Anfragen bitte an [kt@kt.at](mailto:kt@kt.at) oder 01/9093070.

## Das DVR wird abgedreht – letzte Exportmöglichkeit von Altmeldungen bis Jahresende!

Das Datenverarbeitungsregister wird von der Datenschutzbehörde seit In-Geltungtreten der DSGVO weiterhin zu Archivzwecken fortgeführt. Diese Fortführung endet jedoch mit Ende dieses Jahres zum 31.12.2019. Mit diesem Datum entfällt auch die Möglichkeit, aus dem Datenverarbeitungsregister bis zum 24.5.2018 registrierte Datenanwendungen in Form von XML-Files zu exportieren und die so gewonnenen Informationen für das Verzeichnis von Verarbeitungstätigkeiten, das seit 25.5.2019 jeder Verantwortliche und Auftragsverarbeiter zu führen hat, zu verwerten. Ab dem 1.1.2020 sind die für die Registrierung von Datenanwendungen einst zusammengetragenen und weiterhin wertvollen Informationen wohl für immer verloren!

Auch wenn die nach Art 30 DSGVO in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmenden Informationen über Datenanwendungen/Verarbeitungstätigkeiten über jene Informationen hinausgehen, die nach den Bestimmungen des außer Kraft getretenen DSG 2000 in einer Meldung an das Datenverarbeitungsregister zwecks Registrierung bekanntgegeben werden mussten, stellen die der Registrierung zu entnehmenden Informationen den Kern der Informationen dar, die für jede Verarbeitungstätigkeit eines Verantwortlichen oder Auftragsverarbeiter in sein Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden müssen. Registrierte Datenanwendungen im DVR können somit die Basis für das Verzeichnis von Verarbeitungstätigkeiten bilden.

In der **von unserer Kanzlei entwickelten Online-Verarbeitungsverzeichnis „VVT-Online“**, das es Verantwortlichen wie Auftragsverarbeitern unter anderem ermöglicht, entsprechende DSGVO-konforme Verzeichnisse von Verarbeitungstätigkeiten zu führen und sie „behördengerecht“ zu exportieren, haben wir eine automatische Upload-Funktion implementiert, über die die oben angesprochenen XML-Files, die aus dem Datenverarbeitungsregister noch bis 31.12.2019 heruntergeladen werden können, automatisiert einspielt. Die Informationen aus dem Datenverarbeitungsregister werden so auf Knopfdruck strukturiert in das Verzeichnis von Verarbeitungstätigkeiten eingespielt, sodass nur noch jene Informationen zu ergänzen sind, die nach Art 30 DSGVO in einem entsprechenden Verzeichnis zusätzlich enthalten sein müssen. Auf diese Weise kann erheblich Zeit und Arbeitsaufwand gespart werden.



Es ist dabei übrigens nicht nur möglich, einzelne Datenanwendungen aus dem Datenverarbeitungsregister zu exportieren und in VVT-Online hochzuladen, sondern auch alle für einen Auftraggeber registrierten Datenanwendungen zu exportieren und in VVT-Online auf einmal einzuspeisen. **Wir unterstützen Sie sowohl beim Export der Informationen aus dem Datenverarbeitungsregister wie auch bei der Erstellung und Führung von Verzeichnissen von Verarbeitungstätigkeiten über unser VVT-Online**, in die wir auch gerne die Informationen aus DVR-Online über die beschriebene Funktion einspielen. **Das Online-VVT ermöglicht Ihnen zudem auch die Durchführung von Schwellenwertanalysen, Datenschutzfolgenabschätzungen und Schutzbedarfsanalysen, die Überprüfung der Datenschutz-Compliance mithilfe von Checklisten und vieles mehr.** Wenn Sie an dessen Nutzung Interesse haben, können sie es gerne testen. Bei allen Fragen wenden Sie sich gerne unter [kt@kt.at](mailto:kt@kt.at) oder 01/9093070 an uns!

## **What's App dreht sich selbst für Unternehmen ab – ab Dezember wird gegen kommerzielle Angebote vorgegangen!**

Sollten Sie die seit einigen Monaten kursierende Neuigkeit nicht schon aus einschlägigen Medien mitbekommen haben, dann dürfen wir Sie warnen: WhatsApp ist laut dessen Nutzungsbedingungen – immer schon - **nur für Privatpersonen und nicht für Unternehmen gedacht**. Insbesondere der Versand von kommerziellen Info-Angeboten und Werbenachrichten auf Whats App ist unzulässig und WhatsApp macht ernst und hat angekündigt, **ab 7. Dezember 2019 selbst gegen Anbieter von kommerziellen Info-Angeboten auf WhatsApp vorzugehen**. Das Vorgehen soll gemäß der Allgemeinen Geschäftsbedingungen sowohl rechtlich als auch technisch erfolgen [MEHR DAZU](https://faq.whatsapp.com) ([faq.whatsapp.com](https://faq.whatsapp.com))

**Sollten Sie daher Newsletter oder Informationsnachrichten als Unternehmen über WhatsApp versenden, so müssen Sie sich dringend um Alternativen umsehen!** Eine Alternative sind die offiziellen Business-Lösungen von WhatsApp selbst. WhatsApp selbst ermöglicht mittlerweile über die [BUSINESS API](https://www.whatsapp.com/business/api) ([whatsapp.com](https://www.whatsapp.com)) eine 1:1-Kommunikation zwischen Unternehmen und Kunden auch offiziell, zB für customer service oder Ticketing. Der Versand von Newslettern oder Werbenachrichten ist aber auch dort ausgeschlossen!

Die Nutzung von WhatsApp im Unternehmen ist aber nicht nur wegen der AGB von WhatsApp selbst höchst problematisch sondern aufgrund der folgenden zwei Gründe:

- Wenn man WhatsApp Zugriff auf sein Telefonbuch gibt, dann werden sofort alle Kontaktdaten zu WhatsApp in die USA gespielt, was zumindest von den deutschen Datenschutzbehörden für unzulässig erachtet wird, wenn man nicht von allen Kontakten vorher die Einwilligung dafür eingeholt hat.
- Was auch immer völlig übersehen wird: Unternehmen sind laut § 212 UGB verpflichtet, **ihre geschäftsrelevante Unternehmenskorrespondenz („Geschäftsbriefe“) 7 Jahre lang aufzubewahren**. In immer mehr österreichischen Unternehmen führen ganze Abteilungen ihre Unternehmenskorrespondenz nicht mehr in Papier oder per Email durch,

sondern per WhatsApp. Bestellungen, Anmeldungen zu Services, Gewährleistungen, Schadensabwicklungen, etc. etc. werden dadurch nicht mehr über den Email-Server oder die Poststelle des Unternehmens abgewickelt, sondern über den privaten (!) WhatsApp-Account von Mitarbeitern. Dass die Regel aus dem UGB sinnvoll ist, merkt das Unternehmen erst dann, wenn es zB wegen eines Gewährleistungs- oder Schadenersatzfalls vor Gericht gezerrt wird und die gesamte zugehörige Vorkorrespondenz mit dem Gegner auf dem privaten WhatsApp-Account des Mitarbeiters liegt, der leider letztes Jahr gekündigt wurde und der auf seinen früheren Arbeitgeber „pfeift“. Optimaler kann ein Prozess für den Gegner gar nicht beginnen, wenn er – aus WhatsApp - womöglich auch noch weiß, dass der Mitarbeiter weg ist und man völlig ohne Informationen dasteht...

Gerne unterstützen wir Sie bei der rechtlichen Beurteilung von WhatsApp-Alternativen und bei der rechtskonformen Umsetzung von Social Media im Unternehmen. Denn sogar WhatsApp selbst zeigt nun: Social Media ist kein rechtsfreier Raum.

## **IAPP-Trainings und Zertifizierungen jetzt auch in Österreich**

Sie wollen die Datenschutzkoordinatoren und Datenschutzbeauftragten Ihres Konzerns einer global einheitlichen Ausbildung und Prüfung unterziehen, um dokumentieren zu können, dass Sie auch im Datenschutzbereich in der Aus- und Fortbildung standardisierte Compliance-Maßnahmen im Sinne eines nachweislichen Datenschutzes-Managements geschaffen haben? Sie wollen sich selbst fortbilden und sehen, wie ihr Datenschutzniveau im internationalen Vergleich steht? Sie wollen dafür aber nicht um die halbe Welt reisen und machen es lieber auf Deutsch?

Dafür gibt es jetzt eine Antwort: **Die International Association of Privacy Practitioners (IAPP) bietet seit Sommer ihre Trainings und Zertifizierungsprüfungen auch in Österreich an, und zwar in deutscher Sprache.**

Die IAPP als größte globale Non-Profit-Organisation für Datenschutzbeauftragte und Datenschutzkoordinatoren mit weltweit über 50.000 Mitgliedern bietet den einzigen globalen Ausbildungs- und Prüfungsstandard an, der auch Nichtmitglieder offen steht. Die Trainings und Prüfungen können nun auch in Österreich über einen österreichischen Kooperationspartner durchgeführt werden, zusätzlich kann die Prüfung in weltweit über 6.000 Prüfzentren als Computertest abgelegt werden, ua in Wien und anderen österreichischen Städten. Angeboten werden derzeit auf Deutsch die Zertifizierungen als Certified Information Privacy Professional/Europe (CIPP/E) und Certified Information Privacy Manager (CIPM), jene zum Certified Information Privacy Technologist (CIPT) soll demnächst folgen.

Wir haben im Sommer in unserer Kanzlei die ersten jeweils zweitägigen österreichischen Trainings zum CIPP/E und CIPM, veranstaltet von Rudolf Periny (eyecoon GmbH) als offizieller Trainingspartner der IAPP, durchgeführt. Neben mehreren Juristen unserer Kanzlei – darunter unser neuer Mitarbeiter Herr Mag. Martin Sageder, BSc LL.M. – nahm der Datenschutzbeauftragte eines internationalen Versicherungskonzerns daran teil. Die danach in einem externen Prüfungscenter in Wien abzulegende Prüfung bestand für den

CIPP/E aus 90 Prüfungsfragen, die in maximal 150 Minuten zu lösen waren, wobei die Fragen zum Teil in kurze, aber komplexe Sachverhalte eingebettet waren. Die Prüfung war relativ herausfordernd, aber mit Vorkenntnissen, Studium der Unterlagen und dem Training zu schaffen.

Gerne geben wir unsere Erfahrung über die Ausbildung weiter – kontaktieren Sie uns einfach unter [kt@kt.at](mailto:kt@kt.at) oder 01/9093070.

## Aktuelle Veranstaltungen

### 8. Okt. 2019 – EU Datenschutzreform & neues Datenschutzgesetz

Ihr Update-Seminar für die Unternehmenspraxis. Die Mitwirkung der Datenschutzbehörde garantiert Wissen aus erster Hand!

**Vorträge von Dr. Knyrim:** "Grundlagen der EU-Datenschutzreform", "Die neuen Pflichten für öffentliche und private Datenverarbeiter"

### 9. Okt. 2019 – Datenschutzgrundverordnung im Marketing

Praxisseminar - erfolgreiche Marketingkampagnen

**Vortrag von Dr. Knyrim:** "Datenschutz im Marketing nach der neuen Datenschutz-Grundverordnung"

### 10. Okt. 2019 – Der GmbH-Geschäftsführer

Haftungsrisiken und Absicherungsmöglichkeiten

**Vortrag von Dr. Tretzmüller:** "Neue Risikofelder für den Geschäftsführer durch Digitalisierung"

### 15. Okt. 2019 – Forum IT: Cloud Migration

Warum? Wie? Wann? Was? Mit wem? Unternehmen erklären, welche Überlegungen sie bei der Migration in die Cloud anstellen.

**Vortrag von Dr. Tretzmüller:** "Rechtliche Grundlagen zu Cloud Entwicklungen"

### 17.-18. Okt. 2019 – Vergabeforum

Jahresforum für das öffentliche Auftragswesen

**Vortrag von Dr. Knyrim:** "Durch Datenschutz zu schwarzen Schaff"

### 22. Okt. 2019 – imh Spezialtag Datenschutz

Planen Sie noch oder schützen Sie schon?

**Vortrag von Dr. Tretzmüller:** "Auftragsverarbeitung: Verantwortlichkeiten, Verträge und Konsequenzen"

**Vortrag von Dr. Trieb:** "Das Löschen personenbezogener Daten: Aber bitte DSGVO konform!"

### 24. Okt. 2019 – 4. Oberösterreichischer Datenschutztag – Wels

DSGVO-Schonfrist – Wie lange noch

**Vortrag von Dr. Trieb:** "Rechtliche Herausforderungen der DSGVO in den ersten 18 Monaten"

### 5. Nov. 2019 – Antikorruption, Datenschutz, Security & Compliance

Erfahren Sie alles, was Sie als Compliance Officer zum Thema Antikorruption, Datenschutz,

Security & Compliance wissen müssen!

**Vortrag von Dr. Knyrim: "Datenschutz Compliance"**

Erfahren Sie mehr zu aktuellen Veranstaltungen auf unserer Webseite:

[VERANSTALTUNGEN](#) (kt.at)

#### **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](#)

---

#### **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: [ky@kt.at](mailto:ky@kt.at), W: [www.kt.at](http://www.kt.at)

FN 462250f, HG Wien

*(c) Copyright - Knyrim Trieb Rechtsanwälte*

---