



Newsletter 07.2020

Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Im aktuellen Newsletter finden Sie einen Beitrag zum Thema ISO-konforme Datenschutzinformation und Einwilligung im Onlinebereich. Weiters gehen wir auf das Thema Goodbye EU-US-Privacy Shield - Auswirkungen auf den Datentransfer in die USA ein und bieten Ihnen eine Übersicht über bevorstehende Veranstaltungen.

ISO-konforme Datenschutzinformation und Einwilligung im Onlinebereich

Beitrag verfasst von Mag. Maximilian Kröpfl – KTR-Newsletter Juli 2020

Die Welt der internationalen Normung ist einen ISO/IEC-Standard reicher. Vor Kurzem wurde für die Themenbereiche der Datenschutzinformation und der wirksamen Einwilligung im Onlinebereich der internationale Standard ISO/IEC 29184:2020 06 veröffentlicht. Dieser soll Verantwortliche durch festgelegte Kontrollanforderungen bei der Struktur und der inhaltlichen Gestaltung von Datenschutzinformationen sowie dem Aufbau eines Einwilligungsmanagements im Onlinebereich unterstützen.

Die Norm gliedert sich dementsprechend in den **Aufbau** (Pkt 5.2) und **Inhalt einer Datenschutzinformation** (Pkt 5.3), die Gestaltung eines Einwilligungsmanagements (Pkt 5.4) zur Sicherstellung einer fairen, nachweisbaren, transparenten, unzweifelhaften und widerrufbaren Erklärung und in Regelungen für den Fall, dass sich **Aspekte der Datenverarbeitung ändern**. Zusätzlich bietet die Norm in zwei Anhängen einerseits Beispiele für einen **Einwilligungsprozess für PC und Smartphone** (A.2) und andererseits einen Vorschlag zur Gestaltung des **Nachweises der erteilten Einwilligung** sowie des „**Consent receipt**“.

Eines ist gleich klar: Allein auf Basis der ISO/IEC 29184:2020 06 sind weder eine DSGVO-konforme Datenschutzinformation noch ein den Anforderungen der Cookie-Richtlinie (2009/139/EG) oder der DSGVO entsprechender Einwilligungsprozess umsetzbar. Dies ist aber nicht der Qualität der Norm, sondern ihrer Natur als internationaler Standard geschuldet. So werden beispielsweise an den Aufbau der Datenschutzinformation eher generelle Anforderungen wie die klare und einfache Sprache, der

Zeitpunkt der Bereitstellung oder Zugänglichkeit angesprochen, doch zieht sich ein konsistenter roter Faden mit „Controls“, also Kontrollanforderungen durch das Dokument. Mit Hilfe dieser insgesamt **32 Kontrollanforderungen** bietet der ISO/IEC-Standard jedenfalls eine strukturierte Arbeitserleichterung und Hilfestellung. Durch die konsequente Einhaltung der ISO-High-Level-Structure lassen sich die Kontrollanforderungen auch gut in bestehende (Datenschutz-) Managementsysteme integrieren. Das ist besonders für Prozessverantwortliche und die im Unternehmen technischen Verantwortlichen wichtig.

Um bei der guten datenschutzrechtlichen Praxis im Unternehmen unterstützen zu können, sollten Verantwortliche die Norm ISO/IEC 29184:2020 06 als Fundament der Umsetzung von Datenschutzinformationen und des Einwilligungsmanagements im Onlinebereich heranziehen und mit der europäischen Interpretation der zahlreichen wenig bestimmten Begriffe und Anforderungen der Norm ergänzen. Hierfür können Leitlinien des Europäischen Datenschutzausschusses, die Judikatur des Europäischen Gerichtshofs und der Datenschutzbehörde sowie die mittlerweile mannigfaltige Kommentar- und Zeitschriftenliteratur zum Datenschutz herangezogen werden.

Wir sind Ihnen gerne behilflich, Ihre **bestehenden Datenschutzinformationen und Einwilligungen an den neuen ISO-Standard anzupassen**.

Anfragen senden Sie bitte an: kt@kt.at.

Goodbye EU-US-Privacy Shield

Auswirkungen auf den Datentransfer in die USA

Beitrag verfasst von RA Alexander Höller, LL.M. – KTR-Newsletter Juli 2020

In seiner Entscheidung [C-311/18](#) vom 16.7.2020 hat der Europäische Gerichtshof (EuGH) das „EU-US-Privacy Shield“ – konkret den Angemessenheitsbeschluss der Europäischen Kommission ([Durchführungsbeschluss \[EU\] 2016/1250](#)) – ersatzlos aufgehoben. Die Aufhebung erfolgte als ein weiterer Höhepunkt in der seit Jahren andauernden Auseinandersetzung des Datenschutzaktivisten Max Schrems mit Facebook.

1. Was war das EU-US-Privacy Shield?

Die Datenschutz-Grundverordnung (DSGVO) normiert in Kapitel V (Art 44 ff) verschiedene Instrumente zur Übermittlung personenbezogener Daten in Drittländer. Bislang haben sich dazu die Übermittlung auf Basis eines Angemessenheitsbeschlusses (Art 45 DSGVO) sowie der Abschluss von Standardvertragsklauseln (Art 46 Abs 2 lit c und d DSGVO) etabliert.

Im Rahmen von **Angemessenheitsbeschlüssen** beurteilt die Europäische Kommission das datenschutzrechtliche Schutzniveau in verschiedenen Staaten und spricht aus, dass dieses jenem der Europäischen Union gleichwertig ist. Aktuell liegen Angemessenheitsbeschlüsse für folgende Drittländer vor: Andorra, Argentinien, Kanada, Färöer-Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz und Uruguay ([Liste](#) abrufbar bei der Europäischen Kommission).

Besonderheiten galten dabei für die USA: Aufgrund der US-Gesetzgebung und insbesondere der sicherheitsbehördlichen und geheimdienstlichen Befugnisse konnte die Europäische Kommission keinen umfassenden Angemessenheitsbeschluss erlassen. Im Rahmen eines politischen Deals haben die EU und USA daher eine freiwillige Möglichkeit der **Selbstverpflichtung von US-Unternehmen** geschaffen. Unternehmen, die sich den Regeln des

EU-US-Privacy Shields unterworfen hatten, galten als Empfänger mit angemessenem Schutzniveau. Überdies garantierte die US-Regierung, den Datenzugriff durch Behörden bei solchen Unternehmen zu beschränken. Nahezu alle großen IT-Unternehmen waren nach dem EU-US-Privacy Shield zertifiziert.

2. Was waren die Gründe für die Aufhebung?

Der EuGH beschäftigt sich in seiner Entscheidung ausführlich mit den **sicherheitsbehördlichen und geheimdienstlichen Befugnissen** und den hierzu geschaffenen Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte. Die Zusagen der US-Regierung, den Datenzugriff durch Behörden bei EU-US-Privacy Shield zertifizierten Unternehmen zu beschränken, seien zu unbestimmt und wage. Außerdem wurde der **nicht ausreichende Rechtsschutz** bei Verstößen gegen die Verpflichtungen des EU-US-Privacy Shields bemängelt. Im Ergebnis hat der EuGH dem Datenschutzniveau in den USA ein vernichtendes Urteil ausgestellt.

3. Sind Standardvertragsklauseln ein Ausweg?

Bei [Standardvertragsklauseln](#) handelt es sich um standardisierte Verträge, die von der Europäischen Kommission erlassen und in denen die datenschutzrechtlichen Pflichten der beteiligten Unternehmen festgelegt werden.

Aufgrund von Bedenken der irischen Aufsichtsbehörde hat der EuGH auch die Zulässigkeit der Standardvertragsklauseln geprüft und diese als grundsätzlich geeignetes Instrument zur Übermittlung von personenbezogenen Daten in Drittländer bestätigt. Dies darf jedoch keinesfalls derart verstanden werden, dass Standardvertragsklauseln jedwede Drittlandsübermittlung rechtfertigen können. Vielmehr ist das datenübermittelnde Unternehmen verstärkt in die Pflicht genommen: Während sich das Unternehmen bei Vorliegen eines Angemessenheitsbeschlusses auf die **Angemessenheit des Schutzniveaus** im Empfängerstaat verlassen darf, so muss es diese bei der Nutzung von Standardvertragsklauseln **selbst beurteilen** und den **Rechtsrahmen im Empfängerstaat laufend evaluieren** (vgl zB Punkt 4.b. und 5.b der Standardvertragsklauseln im [Beschluss \[EU\] 2010/87](#)). Dies gilt unabhängig von der Befugnis nationaler Aufsichtsbehörden, den Datentransfer im Einzelfall zu beschränken oder ganz zu untersagen.

Für die USA wurde der Rechtsrahmen bereits durch den EuGH beurteilt: Die unter Punkt 2. dargestellten Gründe, die zur Aufhebung des EU-US-Privacy Shields geführt haben, sind dieselben, die gegen die Zulässigkeit der Übermittlung auf Basis von Standardvertragsklauseln sprechen. Dies gilt zumindest für jene Empfänger, die den einschlägigen sicherheitsbehördlichen und geheimdienstlichen Befugnisgesetzen, wie dem Foreign Intelligence Surveillance Act (FISA) 702, das den Sicherheitsbehörden ohne richterlichen Beschluss Zugriff auf die Daten gewährt, unterliegen. Wenngleich dies im Einzelfall zu beurteilen ist, gilt als Faustregel: Telekommunikationsunternehmen sind jedenfalls von den Befugnisgesetzen betroffen; dies gilt auch für alle Unternehmen, die selbst wiederum Telekommunikationsunternehmen in Anspruch nehmen. Rein faktisch führt dies dazu, dass kaum Fälle denkbar sind, in denen die USA einen DSGVO-konformen Rechtsrahmen bieten, sodass es sich bei der Übermittlung personenbezogener Daten in die USA auf Basis von Standardvertragsklauseln mehr um eine theoretische Ausnahme als um eine praxistaugliche Vorgehensweise handelt.

Im Ergebnis sind Standardvertragsklauseln **typischerweise kein Ausweg**, um personenbezogene Daten (weiterhin) in die USA zu übermitteln.

4. Kann man trotzdem noch personenbezogene Daten in die USA übermitteln?

Ja, es gibt dennoch Möglichkeiten zur Übermittlung personenbezogener Daten in die USA.

Die gute Nachricht für die **private Nutzung** von IT-Services: Art 2 Abs 2 lit c DSGVO nimmt Verarbeitungen zu ausschließlich persönlicher oder familiärer Tätigkeit überhaupt vom sachlichen Anwendungsbereich der DSGVO aus. Für diese Zwecke bedürfen Drittlandsübermittlungen überhaupt keiner Rechtsfertigung gemäß Kapitel V der DSGVO.

Aber auch für die nicht private Nutzung gibt es weiterhin Möglichkeiten zur Übermittlung personenbezogener Daten in die USA: Der EuGH selbst geht davon aus, dass die Aufhebung des EU-US-Privacy Shields nicht zur Entstehung eines „*rechtlichen Vakuums*“ führe (C-311/18, Rn 202). Begründet wird dies durch den Ausnahmetatbestand des Art 49 DSGVO, der – ausweislich seiner Überschrift – eine „*Ausnahme für bestimmte Fälle*“ normiert. Demnach ist die Übermittlung weiterhin zulässig:

- auf Basis einer Einwilligung;
- aufgrund der Erforderlichkeit zur Erfüllung eines Vertrages;
- bei Vorliegen wichtiger Gründe des öffentlichen Interesses;
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;
- zum Schutz lebenswichtiger Interessen einer Person; und
- wenn es sich um eine Datenübermittlung aus einem Register, das zur Information der Öffentlichkeit bestimmt ist, handelt.

Wenngleich der EuGH zum Umfang dieses Ausnahmetatbestandes nicht Stellung genommen hat, ist dieser nach Ansicht des [Europäischen Datenschutzausschusses](#) dahingehend eingeschränkt, dass es sich dabei **bloß um eine gelegentliche und nicht wiederholte Übermittlung** handeln darf. Daher kommt diese Ausnahme nach Ansicht des Europäischen Datenschutzausschusses nicht für laufend in Anspruch genommene Dienstleister in Frage. In Hinblick auf die Einholung einer Einwilligung sind überdies die strengen Wirksamkeitsvoraussetzungen des Art 7 DSGVO, insbesondere die Freiwilligkeit und das Verbot der Koppelung, zu berücksichtigen.

Folgt man dieser Ansicht, können die Ausnahmen des Art 49 DSGVO zwar in ausgewählten Fällen die Übermittlung von personenbezogenen Daten in die USA rechtfertigen – eine Lösung für typische Übermittlungstätigkeiten bieten sie jedoch nicht (siehe dazu auch 5. d)).

Weitere Möglichkeiten der Rechtfertigung von Drittlandsübermittlungen sind die Einführung von Binding Corporate Rules (Art 47 DSGVO), die Genehmigung von Verhaltensregeln (Art 40 DSGVO) und die Zertifizierungen (Art 42 DSGVO). Aufgrund des damit verbundenen zeitlichen Aufwands bei der Erstellung und behördlichen Genehmigung, bietet dies jedoch keine zeitnahe Abhilfe.

Die Systematik der Rechtsgrundlagen bei Drittlandsübermittlungen stellt sich dar wie folgt (eingeschränkte Darstellung):



5. Was ist jetzt zu tun?

Bei der Vielzahl von global agierenden IT-Dienstleistern ist zu erwarten, dass kaum ein Unternehmen von der Aufhebung des EU-US-Privacy Shields nicht betroffen ist, weil auch nahezu jedes europäische Unternehmen auf solche zurückgreift. Um dadurch nicht in das datenschutzrechtliche Sanktionsregime zu fallen, sollten Unternehmen zumindest folgende Maßnahmen ergreifen:

- Prüfen Sie, ob und wenn ja im Rahmen welcher Datenverarbeitungen **personenbezogene Daten in die USA übermittelt** werden. Diese Informationen sollten (im Idealfall) aus dem Verzeichnis von Verarbeitungstätigkeiten ersichtlich sein.
- Gruppieren Sie die Datenverarbeitungen nach der **Rechtsgrundlage** für den Datentransfer:
 - a) Widmen Sie sich zuerst allen Übermittlungen auf Basis des **EU-US-Privacy Shields**: Für diese Gruppe von Drittlandsübermittlungen muss eine andere Rechtsgrundlage gefunden werden.
 - b) Bei Übermittlungen auf Basis der **Standardvertragsklauseln** prüfen Sie, ob der Empfänger oder einer seiner Dienstleister den sicherheitsbehördlichen und geheimdienstlichen Befugnisgesetzen unterliegt. Ist dies der Fall, kann die Drittlandsübermittlung unserer Ansicht nach nicht auf diesen Rechtsgrund gestützt werden.
 - c) Finden Drittlandsübermittlung **bloß gelegentlich und nicht wiederholt** statt, so ist zu prüfen, ob eine der Ausnahmen gemäß Art 49 DSGVO vorliegt.
 - d) Findet die Drittlandsübermittlung **nicht bloß gelegentlich** statt, könnte – auch wenn der Europäische Datenschutzausschuss dies anders sieht – versucht werden, die Übermittlung dennoch auf die Ausnahmetatbestände des Art 49 DSGVO zu stützen; in diesem Fall sollte argumentiert werden, dass der EuGH explizit auf diese besonderen Ausnahmen als Ausweg hinweist. Diese Rechtfertigung ist jedoch mit erheblichen rechtlichen Risiken verbunden.
- Kann die Drittlandsübermittlung auf keinen Rechtsgrund gestützt werden, ist die **Übermittlung auszusetzen** und nach alternativen Anbietern zu suchen. Alternativ ist in wirtschaftlicher Hinsicht zu beurteilen, ob das Risiko einer datenschutzrechtlichen Sanktionierung durch die Datenschutzbehörde eingegangen werden will.
- In weiterer Folge sollte beurteilt werden, ob die Einführung von **Binding Corporate Rules** (Art 47 DSGVO), die Genehmigung von **Verhaltensregeln** (Art 40 DSGVO) und die **Zertifizierungen** gemäß Art 42 DSGVO gangbare Wege sind; dies kann jedoch kaum kurzfristig umgesetzt werden.
- Schaffen Sie **standardisierte Verfahren**, um sicherzustellen, dass die Rechtsgrundlage für eine Übermittlung in Drittländer systematisch erhoben und das Vorliegen eines angemessenen Schutzniveaus bei Anwendung von Standardvertragsklauseln konsequent geprüft wird.

- Vergessen Sie nicht, Ihre **datenschutzrechtliche Dokumentation** (Datenschutzinformationen, Betriebsvereinbarungen, Einwilligungserklärungen, Verzeichnis von Verarbeitungstätigkeiten) sowie Ihre Prozesse zur Abwicklung der Betroffenenrechte zu **aktualisieren**.

Hinweis:

Einen aktuellen Artikel zum Thema finden Sie unter [diepresse.com](https://www.diepresse.com):

[Digitaler Lock-Down: Datentransfer in die USA \(weitgehend\) unzulässig](#)

Was die EuGH-Entscheidung Schrems II genau besagt und wie Unternehmen darauf reagieren sollten.

Veranstaltungen 2020

16. Sep. 2020 – PHARMIG WEBINAR – Datenschutzrecht & Praxis in der Pharmabranche

Praxisorientiertes sowie fundiertes Update zum Thema Datenschutz.

Sie erfahren sowohl, was in den letzten 2 Jahren seit Inkrafttreten der DSGVO auf lokaler sowie europäischer Ebene passiert ist als auch wie Datenschutz in der Praxis umgesetzt wird. Use Cases in unterschiedlichen Bereichen und ein Ausblick in die Zukunft runden das Seminar ab. Nicht zu vergessen ist die strategische Komponente, die für die Geschäftsentwicklung von erheblicher Bedeutung ist und das Thema Datenschutz interessant macht.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

17. / 24. September 2020 – Manz Jahrestagung Datenschutzrecht 2020 – Wien/Linz

Alles, was die Datenschutzbranche bewegt.

Themen: Aktuelle datenschutzrechtliche Entscheidungen, DSGVO meets ZPO – Der Datenschutz vor Gericht, Mitarbeiter, IT und Datenschutz, DSGVO-konform umgesetzt: Cookies für Webseitenanalyse und Marketing, Informationsrecht und Auskunftspflicht, das Datenschutzmanagement der Greiner AG (LINZ), das Datenschutz-Managementsystem in der Praxis und die Tücken bei der Umsetzung – wie man dem Löschkonzept und Co auf die Pelle rückt (WIEN)

[Weitere Informationen finden Sie auf unserer Webseite.](#)

21. – 23. Sep. 2020 – Lehrgang zum zertifizierten Datenschutzbeauftragten

Die Ausbildung garantiert ihr Wissens-Update mit allen aktuellen Neuerungen, die die Datenschutzregeln der EU an Unternehmen und Behörden in Österreich stellen.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

30. Sep. / 1. Okt. – Datenschutzrecht für die Energiewirtschaft

Datenschutz ist weiterhin in aller Munde und nimmt auch in der Energiewirtschaft eine stetig wachsende Bedeutung ein. Erfahren Sie an einem Tag die wichtigsten Grundsätze des Datenschutzrechts und wo und wie sie auf die Verarbeitung personenbezogener Daten in der Energiewirtschaft Anwendung finden. Insbesondere auch, welche Aktivitäten die Branche bereits gesetzt hat, um die mit der Datenverarbeitung einhergehenden Risiken bestmöglich zu minimieren. Lernen Sie dabei auch gleichzeitig, mit den Mitteln des Datenschutzrechts personenbezogene Daten rechtssicher zu verarbeiten, ohne dabei die Grenzen der zulässigen Datenverarbeitung zu verlassen.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

6. Okt. 2020 – Spezialtagung Datenschutz im Gesundheitsbereich

Tagungsleitung von RA Dr. Gerald Trieb, LL.M., Knyrim Trieb Rechtsanwälte OG

Themen: Datenschutz im Krankenhaus, Hat der Betroffene noch Rechte nach der DSGVO im Gesundheitsbereich?, Health data and genetic data on their way. Von der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten, Reichweite und Ausnahmen von berufsrechtlichen Verschwiegenheitspflichten, Rechtliche Rahmenbedingungen für die Forschung mit Gesundheitsdaten, Weitergabe der Patientendokumentation unter datenschutzrechtlichen Gesichtspunkten

[Weitere Informationen finden Sie auf unserer Webseite.](#)

Okt. 2020 – Datenschutz für Fortgeschrittene und Rezertifizierung als Datenschutzbeauftragter

(genauer Termin wird noch bekannt gegeben – 13., 14. oder 15. Oktober 2020)

Dieses Seminar richtet sich an Datenschutzbeauftragte, Datenschutzkoordinatoren und Datenschutzberater, die bereits Wissen und Praxiserfahrung im Datenschutzrecht haben. Das Seminar gilt gleichzeitig als Rezertifizierungsseminar für das Austrian Standard Personenzertifikat für Datenschutzbeauftragte, die ihre Zertifizierung wegen Ablauf der dreijährigen Gültigkeit erneuern müssen. Weitere Voraussetzung für die Rezertifizierung ist die Vorlage einer Tätigkeitsbeschreibung.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

19. Okt. 2020 – Update-Seminar – EU-Datenschutzreform & neues Datenschutzgesetz

Themen: Grundlagen der EU-Datenschutzreform, Die neuen Pflichten von Verantwortlichen und Auftragsverarbeitern, Was man künftig mit der Datenschutzbehörde zu tun hat, Datenvernetzung im Konzern, Genehmigungspflichten, Datenschutzbeauftragter

[Weitere Informationen finden Sie auf unserer Webseite.](#)

20. Okt. 2020 – Spezial-Seminar – DSGVO und Marketing

Themen: Datenschutz im Marketing nach der neuen Datenschutz-Grundverordnung, Aktuelles aus Sicht der Datenschutzbehörde, Die Umsetzung im Marketing-Alltag

[Weitere Informationen finden Sie auf unserer Webseite.](#)

2. – 4. Nov. 2020 – Corporate Compliance Officer, Module 4-6

Die Top-Ausbildung zum zertifizierten Compliance Officer in Corporates

Sie erlangen praxisrelevantes Fachwissen, erprobte Instrumente und Methoden zum Aufbau eines Compliance Management Systems und Weiterentwicklung Ihrer Compliance Kenntnisse.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

10./11. Nov. 2020 – PRISEC – Privacy & Security

Die PriSec vereint die Themen Sicherheit & Datenschutzrecht im Unternehmen: Dieses wachsende Spannungsfeld erfordert zukünftig eine noch intensivere Zusammenarbeit der Bereiche Datenschutz, Compliance und IT. Wenn die PriSec am 10. November 2020 startet, ist die Datenschutz-Grundverordnung seit über 2 Jahren in Kraft. „Was war, was kommt“ zieht Rainer Knyrim zum Auftakt eine Zwischenbilanz und gibt einen Ausblick auf die kommenden Herausforderungen.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

23. – 25. Nov. 2020 – Lehrgang zum zertifizierten Datenschutzbeauftragten

Die Ausbildung garantiert ihr Wissens-Update mit allen aktuellen Neuerungen, die die Datenschutzregeln der EU an Unternehmen und Behörden in Österreich stellen.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

25. – 26. Nov. 2020 – Oesterreichs Netzservice Forum 2020

Was bewegt die Netze der Zukunft?

Beim diesjährigen Netzservice Forum der Österreichs Energie Akademie trägt Dr. Gerald Trieb, LL.M. zum Thema „Datenschutzkonformes Verarbeiten von Smart-Meter-Verbrauchsdaten“ vor.

Themen: Das Stromnetz als Enabler der Energiewende, Die neuen gesetzlichen Vorgaben – was bedeuten sie für die Netzbetreiber?, Versorgungssicherheit in COVID19-Zeiten, Cyber-Bedrohung und wirksame Gegenstrategien, Digitalisierung und Datenmanagement im Netz, Netzintegration von E-Mobilität und Erneuerbaren Energien, innovative Instandhaltung

[Weitere Informationen finden Sie auf unserer Webseite.](#)

3. Dez. 2020 – HR-Daten, Erlaubtes & Verbotenes

Auf welche datenschutz- & arbeitsrechtlichen Aspekte Dienstgeber, -nehmer und Betriebsrat achten müssen, erfahren Sie in diesem Fachseminar. Sie profitieren von Themen wie Datenschutzrecht im Recruiting, im Personalakt, in der Mitarbeiterentwicklung, in der Archivierung uvm.

[Weitere Informationen finden Sie auf unserer Webseite.](#)

Weitere Newsletter finden Sie auf unserer Webseite: www.kt.at/newsletter

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

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

E: kt@kt.at, W: www.kt.at

FN 462250f, HG Wien

(c) Copyright - Knyrim Trieb Rechtsanwälte