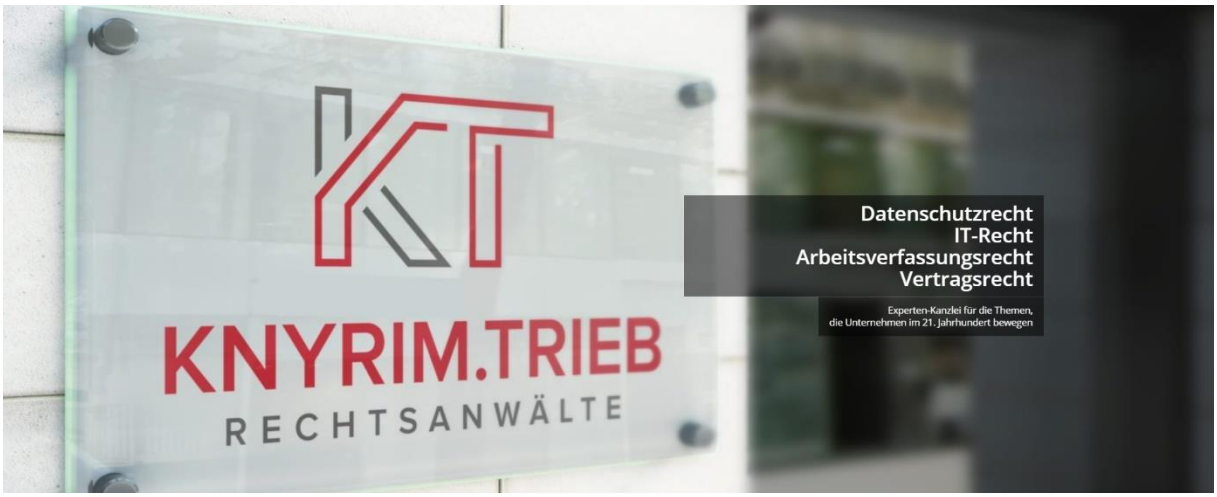

Newsletter 03.2020
Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Die rasante Ausbreitung des Coronavirus stellt das Gesundheitssystem vor große Herausforderungen und verändert aufgrund gesundheitsbehördlich angeordneter Verbote auch das Arbeitsleben. Wir haben unseren Kanzleibetrieb auf Telearbeit umgestellt, alle Mitarbeiter arbeiten von zu Hause weiter. Sie erreichen uns nicht nur per E-Mail, sondern auch über unsere normale Telefonnummer +43 1 9093070, die auf unser Kanzleihandy umgeleitet wird. Auch Videokonferenzen können wir jederzeit einrichten.

Das Arbeiten der Dienstnehmer von zu Hause bringt verschiedene datenschutzrechtliche Fragen mit sich. Gemeinsam mit Alexander Höller, LL.M., seit 1. März Rechtsanwalt in unserer Kanzlei (siehe https://www.kt.at/team) gebe ich nachstehend einen kurzen Überblick über ausgewählte Fragen dazu:

Datenschutzrechtliche Aspekte der Covid-19 Epidemie im Dienstverhältnis

Beitrag verfasst von RA Dr. Rainer Knyrim und RA Alexander Höller, LL.M. am 16.03.2020 – KTR-Newsletter März 2020

Darf der Dienstgeber den Dienstnehmer im Fall von (drohenden) Epidemien über private Reisen in Risikogebiete sowie den Gesundheitszustand befragen?

Grundsätzlich gestatten Art 9 Abs 2 lit g und i DSGVO den Mitgliedstaaten, spezifische Regelungen vorzusehen, um die Verarbeitung (auch sensibler) Daten aus Gründen erheblicher öffentlicher Interessen, insbes. im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, durchzuführen, wobei die **Vermeidung von Epidemien** ein solches erhebliches öffentliches Interesse darstellt (siehe Erwägungsgründe 46 und 52 der DSGVO). Die Zulässigkeit der Verarbeitung erfordert eine gesetzliche Grundlage im Recht des Mitgliedstaates oder der Union.

Eine solche ausreichend determinierte **Bestimmung fehlt im österreichischen Recht** jedoch. § 10 Abs 2 DSG normiert bloß die Berechtigung zur Weitergabe zuvor rechtmäßig erhobener Daten, nicht jedoch die Erhebung der Daten selbst. Dasselbe gilt für die Verpflichtung zur Auskunftserteilung an die Gesundheitsbehörden gemäß § 5 Epidemiegesetz; eine Ermächtigung zur (proaktiven) Erhebung der Daten durch den Dienstgeber wird dadurch nicht normiert.

In arbeitsrechtlicher Hinsicht ist der Dienstnehmer aufgrund der ihn treffenden **Treuepflicht** sowie § 15 Abs 5 **ArbeitnehmerInnenschutzgesetz** jedoch verpflichtet, dem Dienstgeber ernste Gefahren für die Gesundheit – zB. eine Infektion mit dem Coronavirus bzw. eine besondere Erhöhung des Risikos einer solchen Infektion aufgrund einer Reise in ein Risikogebiet – zu melden. Aufgrund der **Fürsorgepflicht des Dienstgebers** gegenüber seinen (anderen) Dienstnehmern lässt sich argumentieren, dass der Dienstgeber auch verpflichtet ist, solche Informationen durch Befragung pro-aktiv zu erheben. Über diesen Umweg des Arbeitsrechts ist der Dienstgeber in datenschutzrechtlicher Hinsicht berechtigt, für die Erfüllung dieser Pflichten notwendige Daten zu erheben und zu verarbeiten; dies entspricht auch der Argumentation des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz. Die datenschutzrechtliche Rechtsgrundlage für diese Verarbeitung ist das berechtigte Interesse nach Art 6 Abs 1 lit f DSGVO, die Verarbeitung ist nach Art 9 Abs 2 lit b) DSGVO (Erfüllung arbeitsrechtlicher (Fürsorge-)Pflichten erlaubt).

Insgesamt wäre jedoch wünschenswert, dass der österreichische Gesetzgeber entsprechend legistisch tätig wird und eine ausdrückliche Ermächtigung zur Verarbeitung solcher Daten normiert (zB. im Epidemiegesetz oder in § 10 DSG).

Einige Datenschutzbehörden in Europa haben schon Statements zum Thema Datensammlung wegen Coronavirus veröffentlicht, ua die französische (https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles), die irische (https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19) und die italienische (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117). Einen Überblick über die Meinungen gibt dieser Beitrag: https://fpf.org/2020/03/10/eu-dpas-issue-green-and-red-lights-for-processing-health-data-during-the-covid-19-epidemic.

Der deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat heute ebenfalls Informationen zum Thema online gestellt (https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html) laut denen *„nach Ansicht der unabhängigen Datenschutzaufsichtsbehörden die angemessene Reaktion auf die epidemische bzw. inzwischen pandemische Verbreitung einer meldepflichtigen Krankheit“* zulässig ist. *„Diese Maßnahmen müssen dabei natürlich immer auch verhältnismäßig sein. Die Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks (regelmäßig also spätestens dem Ende der Pandemie) müssen die erhobenen Daten unverzüglich gelöscht werden.“*

Zusammengefasst stehen die Behörden einer systematischen und allgemeinen Datensammlung teils sehr kritisch gegenüber (wie etwa die italienische Datenschutzbehörde), lassen aber eingeschränkt Datenverarbeitung im Hinblick auf die oben angesprochenen Treuepflichten zu, insbesondere bei infizierten Personen und bei Gästen und Besuchern.

Seitens der österreichischen Datenschutzbehörde gibt es keine inhaltlichen Informationen zum Umgang mit der Corona-Epidemie, aber den Hinweis auf deren Webseite, dass der Parteienverkehr vorerst bis zum 13. April ausgesetzt ist und der Dienstbetrieb eingeschränkt möglich ist.

Update 17. März: Die Datenschutzbehörde hat nun ebenfalls Informationen zu Datenschutz & Coronavirus direkt auf ihre Startseite online gestellt, die die Handlungsvorschläge unseres Newsletters bestätigen: https://www.dsb.gv.at/

Darf der Dienstgeber Notfallkontakte (zB. Ehepartner, Eltern) seiner Mitarbeiter verarbeiten?

Die Verarbeitung von **Notfallkontakten** dient der Kontaktierung von (nahen) Angehörigen im Fall eines Notfalls. Die betroffene Person ist in diesen Fällen nicht der betroffene Mitarbeiter selbst, sondern die von ihm genannte Kontaktperson; eine Einwilligung (durch den Mitarbeiter) scheidet daher mangels Bevollmächtigung üblicherweise aus. Die Datenschutzbehörde hat schon vor der DSGVO solche Notfallkontaktdatenbanken unter der Bindung zugelassen, dass die Mitarbeiter gegenüber dem Arbeitgeber bestätigen müssen, dass sie die Kontaktperson über die Bekanntgabe ihrer Kontaktdaten informiert haben. (siehe https://www.ris.bka.gv.at/).

Eine **Verpflichtung** der Mitarbeiter, Notfallkontakte bereitzustellen, besteht hingegen **nicht**.

Was ist bei Teleworking auf Zeit in datenschutzrechtlicher Hinsicht zu beachten?

Arbeit von zu Hause bringt für die Eindämmung von Epidemien große Vorteile. In datenschutzrechtlicher Hinsicht birgt dies jedoch einige Risiken.

Der Dienstgeber bleibt auch bei der Arbeit von zu Hause Verantwortlicher der von seinen Mitarbeitern vorgenommen (betrieblichen) Datenverarbeitungen. Daher ist der Dienstgeber insbesondere verpflichtet, **technische und organisatorische Maßnahmen zur Datensicherheit** gemäß Art 32 DSGVO zu ergreifen.

Der physische Schutz vor unberechtigten Zugriffen auf Daten, der sich bei der Arbeit in der Betriebsstätte des Dienstgebers durch entsprechende Zutrittskontrollen und Schließkonzepte leicht(er) umsetzen lässt, entzieht sich bei der Arbeit zu Hause faktisch der Kontrolle des Dienstgebers. Dasselbe gilt für den Einsatz von privatem IT-Equipment des Dienstnehmers, auf dessen technischen Schutz der Dienstgeber keinen Einfluss hat.

Dienstgeber sollten ihren Dienstnehmern daher jedenfalls **klare und verbindliche Anweisungen** zum Umgang mit personenbezogenen Daten bei der Arbeit zu Hause geben und – soweit möglich – **betriebseigenes IT-Equipment** zur Verfügung stellen. Betriebseigenes IT-Equipment wie PCs oder Laptops sollten unbedingt mittels BitLocker gesichert werden, damit der Zugang zu den auf den Geräten gespeicherten Daten geschützt ist. Ein normales Windows-Passwort ist kein ausreichender Schutz der Daten bei Verlust oder Diebstahl des Laptops und es könnte dann schon allein wegen fehlender Datensicherheitsmaßnahmen ein Data Breach vorliegen.

Soweit kein betriebseigenes Equipment zur Verfügung steht, sollten entsprechende Maßnahmen getroffen werden, insbesondere:

- Die Mitarbeiter sollten, sofern sie nicht direkt online auf Cloud-Lösungen zugreifen können, nur über einen VPN-Tunnel auf den Server oder ihren PC in der Arbeit arbeiten und keinesfalls zB lokale Postfächer auf ihrem privaten Rechner installieren.
- Mittels VPN-Tunnel kann eine gesicherte, verschlüsselte Verbindung aufgebaut werden und der Mitarbeiter hat dann denselben Desktop, wie wenn er im Büro säße zur Verfügung und sämtliche Daten bleiben auf den betrieblichen Arbeitsgeräten.
- Es sollte den Mitarbeitern untersagt werden, Daten auf ihren privaten Rechner herunterzuladen. Ausdrucke von Arbeitsunterlagen sollten entweder generell unterbunden werden oder wenn, dann nur im Ausnahmefall und unter der Bedingung gestattet werden, dass die Ausdrucke später in der Arbeit ordnungsgemäß geschreddert werden und keinesfalls im Hausmüll entsorgt werden.
- Berufliche Passwörter und das VPN-Passwort dürfen nicht auf dem privaten Rechner gespeichert werden.
- Es sollten keine privaten Kommunikationsmedien für die berufliche Kommunikation benutzt werden, wie zB. WhatsApp oder private Social Media–Konten. Die Kommunikation

kann über den VPN-Tunnel über die normalen E-Mail-Zugänge oder dienstliche Kommunikationsprogramme durchgeführt werden.

Bei Fragen zur Datenverarbeitung im Zusammenhang mit der Coronavirus-Epidemie stehen wir Ihnen gerne unter kt@kt.at zur Verfügung!

Der Corona-Virus als Fortbildungs-Chance

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Wir planen seit längerem gemeinsam mit Microsoft ein Training Event. Dieses sollte am 23. März von 9.00 bis 14.00 Uhr bei Microsoft Österreich stattfinden und nur eine sehr begrenzte Teilnehmerzahl zulassen. Aufgrund der aktuellen Situation hat Mircrosoft beschlossen, das Event nur Online stattfinden zu lassen, was Ihnen die Möglichkeit bietet, online daran teilzunehmen. Nachstehend finden Sie die Einladung. Entgegen dem Text wird die Veranstaltung aber nicht bei Microsoft stattfinden, sondern ausschließlich online, auf ca. 2 Stunden verkürzt stattfinden. Gerne können Sie sich zu diesem kostenlosen Online-Event anmelden!

Immer mehr Unternehmen lagern ihre IT in die Cloud aus oder nutzen hybride Umgebungen. Eine große Herausforderung für SicherheitsexpertInnen und Compliance Manager, denn natürlich müssen gleichzeitig alle Unternehmensdaten geschützt und wichtige Verhaltensregeln eingehalten werden.

Ich möchte Sie auf diesem Wege herzlich zu unserem **Microsoft 365 Training Day: Meeting Organizational Compliance Requirements** einladen. Melden Sie sich heute noch an und lernen Sie die neuesten Lösungen und Tools im Compliance-Bereich kennen.

Der Training Day findet am **23. März 2020 Online** statt und richtet sich vorrangig an **IT-ExpertInnen, Rechts- und Compliance-Manager oder -Implementierer, sowie an CISOs und Sicherheitsbeauftragte**.

Folgende thematische Schwerpunkte werden im Rahmen der Veranstaltung behandelt:

- Erfahren Sie Ihre Möglichkeiten zur Vereinfachung und Automatisierung Ihrer Compliance mit Microsoft 365
- Verstehen Sie Ihre eigene Datenlandschaft und wie die neusten Microsoft Information Protection-Lösungen zum Schutz Ihrer vertraulichen Daten beitragen.
- Erfahren Sie, wie Ihr Unternehmen Kosten und Risiken reduzieren und gleichzeitig regelkonform arbeiten kann.

Zum Event anmelden:
https://www.microsoftevents.com/profile/form/index.cfm?PKformID=0x10138971abcd

---

(Kein) Ideeller Schadenersatz für Datenschutzverstöße

Beitrag verfasst von RA Alexander Höller, LL.M. am 16.03.2020 – KTR-Newsletter März 2020

Das Oberlandesgericht Innsbruck hat die vielbeachtete Entscheidung des Landesgerichts Feldkirch, in der einem Kläger aufgrund der DSGVO-widrigen Datenverarbeitung durch die **Österreichische Post** der Ersatz (vermeintlich) erlittener ideeller Schäden in Höhe von EUR 800,- zugesprochen wurde, nunmehr dahingehend abgeändert, dass der **Schadenersatzanspruch abgewiesen** wurde (13.2.2020, 1 R 182/19b; Entscheidung im Volltext bei addendum.org).

Die bedeutet jedoch keinesfalls, dass für Verletzungen der datenschutzrechtlichen Bestimmungen überhaupt kein ideeller Schadenersatz zustehen kann. Das Oberlandesgericht Innsbruck hat vielmehr ausdrücklich festgehalten, dass Art 82 Abs 1 DSGVO den Ersatz **tatsächlich eingetretener materieller und ideeller Schäden** anordnet und der Ersatz ideeller Schäden **keine schwere Verletzung des Persönlichkeitsrechts** voraussetzt (vgl hingegen RIS-Justiz RS0115189 zum Erfordernis des groben Verschuldens beim Ersatz von Trauerschäden). Der Eintritt eines ersatzfähigen ideellen Schadens setzte jedoch eine „*tatsächliche Beeinträchtigung in der Gefühlswelt des Geschädigten*“ voraus. Der bloße Umstand der Verletzung datenschutzrechtlicher Bestimmungen per se stellt keinen solchen ersatzfähigen Nachteil dar. Zu ersatzfähigen ideellen Schäden könne es beispielsweise kommen, wenn

- jemand einem Zustand der **Angst** ausgesetzt wird,
- das **Ansehen**, die **Würde** oder die **Ehre** verletzt werden,
- die **Integrität** einer Person in Zweifel gestellt werden,
- man einen **Schock** erleidet oder
- man **frustriert**, **unzufrieden** und **unsicher** ist.

Die Abweisung des Schadenersatzanspruches resultiere aus dem Umstand, dass ein solcher ersatzfähiger Schaden vom Kläger weder vorgebracht noch bewiesen wurde. Der Kläger begründete seinen vermeintlichen Ersatzanspruch (nach Verbesserung der unschlüssigen Klage) lediglich mit dem „*Ungemach, das durch den rechtswidrigen und geradezu sorglosen Umgang der [Post] mit […] teilweise sensiblen Daten […] ausgelöst wurde*“. Dieses Ungemach stelle jedoch **keinen Schaden im Sinne des Schadenersatzrechts** dar.

Die Entscheidung steht unseres Erachtens in **Einklang mit der schadenersatzrechtlichen Judikatur** des EuGH und der nationalen Gerichte. Der Ersatz von Schäden setzt den tatsächlichen Eintritt eines Schadens voraus. Das Vorliegen einer rechtswidrigen Datenverarbeitung alleine führt nicht zu einem Schadenersatzanspruch; dies entspreche vielmehr dem angloamerikanischen Konzept von *punitive damages*.

Topaktuelle Datenschutznews: Neues Datenschutz-Infoservice

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Wenn Sie laufend Zusammenfassungen von Entscheidungen wie die vorangegangene direkt in ihr Mail-Postfach haben möchten, bietet ihnen Knyrim Trieb Rechtsanwälte seit Ende letzten Jahres mit einem Abonnement des Datenschutz-Infoservices stets topaktuelle Neuigkeiten aus dem Bereich des Datenschutzrechts.

Wir fassen Ihnen ausgewählte Entscheidungen der Datenschutzbehörde und Gerichte, Richtlinien des Europäischen Datenschutzausschusses, des Europäischen Datenschutzbeauftragten und ausgewählter

Datenschutzbehörden anderer Mitgliedstaaten, legistische Neuerungen und sonstiges aktuell Wissenswertes zum Datenschutzrecht zusammen. Unsere Zusammenfassungen nimmt Ihnen die Lesearbeit ab und erleichtert das Aktuell-Halten des Datenschutzwissens. Sie müssen weder selbst nach aktuellen, wichtigen Entscheidungen suchen, noch diese in voller Länge suchen. Wir schicken Ihnen zeitnah und in qualitativ hochwertiger Form relevante Informationen „in kleinen Häppchen" direkt in ihr Postfach. Damit Sie diese gleich lesen und informiert sind. Mit dem Abonnement des Datenschutz-Infoservices erhalten Sie zumeist etwa ein bis zwei topaktuelle News pro Woche und müssen sich

Dieses exklusive Service richtet sich ausschließlich an Unternehmen und öffentliche Einrichtungen. Wenn Sie Interesse an diesem haben, kontaktieren Sie mich gerne per Email mit dem Stichwort Datenschutz-Infoservice unter kt@kt.at.

DSGVO-Strafen in Österreich und der EU

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Kaum ein Tag vergeht ohne ein neues DSGVO-Bußgeld in Europa. Aus diesem Grund finden Sie hier einen Überblick über einige Geldbußen der letzten Wochen und Monate:

Unzureichendes Authentifizierungsverfahren bei telefonischer Kundenauskunft:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat gegen den Telekommunikationsdienstleister 1&1 eine Geldstrafe iHv **EUR 9.550.000** verhängt. Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass **Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können**. Konkret wurde bemängelt, dass Anrufer bei der Kundenbetreuung des Unternehmens allein schon durch Angabe des Namens und Geburtsdatums eines Kunden weitreichende Informationen zu weiteren personenbezogenen Kundendaten erhalten konnten. In einem solch (laschen) Authentifizierungsverfahren bestehe ein Verstoß gegen Art 32 DSGVO. Dieser Artikel ist derzeit Gegenstand vieler Bußgeldverfahren, wohl nicht zuletzt wegen seinem weiten Anwendungsbereich und der offenen Formulierung.

1&1 hat bereits angekündigt, dagegen vorzugehen und gegen den Strafbescheid „zu klagen", da es die Geldstrafe für absolut unverhältnismäßig hält. „Die neue Bußgeldregelung, nach der die Summe berechnet wurde und die für die gesamte deutsche Wirtschaft gilt, wurde am 14. Oktober 2019 veröffentlicht und orientiert sich am jährlichen Konzern-Umsatz. So können bereits kleinste Abweichungen riesige Geldbußen zur Folge haben. In der Datenschutz-Grundverordnung (DSGVO) ist der Umsatz allerdings nicht als Kriterium für die Bemessung der Bußgeldhöhe vorgesehen. Darüber hinaus verstößt die neue Bußgeldlogik gegen das Grundgesetz, insbesondere die Grundsätze der Gleichbehandlung und der Verhältnismäßigkeit." Das Unternehmen führt in seiner Stellungnahme aus, dass der fragliche Fall (Abfrage der Handynummer des ehemaligen Lebenspartners) bereits im Jahr 2018 geschehen sei und „zu diesem Zeitpunkt eine Zwei-Faktor-Authentifizierung üblich [war]". Einen einheitlichen Marktstandard für höhere Sicherheitsanforderungen hätte es nicht gegeben. Nunmehr setze das Unternehmen laut eigenen Angaben eine dreistufige Authentifizierung mit einem persönlichen Service-PIN ein.

Unzulässige Telefonwerbung und sensible Daten im CRM-System:

Die französische Datenschutzbehörde CNIL verfügte eine Geldstrafe in der Höhe von EUR 500.000 (etwa 2,5% des Jahresumsatzes) gegen ein Unternehmen wegen Verstößen gegen die Informationspflichten, das Widerspruchsrecht und die allgemeinen Grundsätze der Datenübermittlung. Ebenso wurde die Pflicht zur Zusammenarbeit mit der Datenschutzbehörde verletzt. Eine Beschwerde über unzulässige Telefonwerbung machte die Behörde auf das Unternehmen aufmerksam, sodass es dieses einer Prüfung unterzog. Dabei wurde klar, dass das Unternehmen **keinen Mechanismus für den Widerspruch gegen die Telefonwerbung** vorsah und die **Gespräche ohne das Wissen der Betroffenen aufgezeichnet** wurden. Zusätzlich wurden **in dem verwendeten CRM-System sensible Informationen über den Gesundheitszustand** der angerufenen Personen gespeichert.

Fehlende Schutzmaßnahmen bei Online-Portal:

Potentiell bis zu EUR 900.000 verhängte die niederländische Datenschutzbehörde bereits Ende Oktober über die Agentur für Personalversicherungen (UWV). Grund **waren unzureichende Sicherheitsmaßnahmen (Art 32 DSGVO) bei deren Online-Portal**. Da die UWV **bei der Gewährung des Zugangs zum Portal keine Multi-Faktor-Authentifizierung (MFA) verwendete**, konnten Arbeitgeber und Behörden in einem Abwesenheitssystem Fehlzeiten von Arbeitnehmern erfassen und einsehen. Solche **Abwesenheitszeiten wurden als Gesundheitsdaten gewertet**, welche besonders hohen Schutzanforderungen unterliegen. Die UWV hat nun (nach einmaliger Fristverlängerung) bis zum 1. März 2020 Zeit, die von der Behörde geforderten Sicherheitsmaßnahmen zu implementieren und so der Geldstrafe zu entgehen.

Rechtswidriges Cookie Management:

Die spanische Datenschutzbehörde sanktionierte die Billigfluggesellschaft Vueling mit EUR 30.000 wegen Verstößen im Zusammenhang mit deren Cookie-Einsatz. Bei der Verwaltung von Cookies weist das Unternehmen lediglich darauf hin, dass der Browser so konfiguriert werden kann, dass er entweder standardmäßig alle Cookies akzeptiert oder ablehnt oder dass Benachrichtigungen über den Empfang jedes einzelnen Cookies auf dem Bildschirm angezeigt werden und der User dann über die Implementierung entscheidet. Weiters wird auf die Möglichkeit von Tracking-Cookie-Blocker verwiesen. **Die Behörde bemängelte, dass kein Managementsystem oder ein Cookie-Konfigurationspanel zur Verfügung gestellt wird, welches dem Benutzer ermöglicht, auf granulare Art und Weise einzelne Cookies zu löschen.** Daher war laut Behörde ein Verstoß gegen spanisches (Telekommunikations-)Recht erfolgt.

Keine Einwilligung und Information beim Cookie-Setzen:

Wie im Fall von Vueling wurde auch über IKEA Ibérica von der spanischen Behörde ein fünfstelliges Bußgeld verhängt, weil auf unzulässige Art und Weise Cookies gesetzt wurden. EUR 10.000 musste der spanische Ableger des Möbelhauses bezahlen, **weil dem Webseiten-Besucher keine Möglichkeit gegeben wurde, die direkt bei Aufruf der Seite gesetzten Cookies abzulehnen.** Es wurde auch **keine klare Information über die Datenverarbeitung erteilt**, sondern lediglich festgehalten, dass die Cookies eine „bessere User-Erfahrung“ bereiten würden. Verwiesen wurde auf eine mögliche Browser-Einstellung für das Blocken der Cookies, welche jedoch eine Benützung der Webseite de facto unmöglich machte, da bei dieser Einstellung auch „notwendige“ Cookies (etwa der Warenkorb) erfasst wurden.

Unzureichende TOM bei der Verarbeitung von Gesundheitsdaten:

Die norwegische Datenschutzbehörde hat gegen die Stadt Oslo eine Geldbuße in Höhe von 49.300 EUR verhängt, weil sie von 2007 bis November 2018 in den Pflegeheimen/Gesundheitszentren der Stadt Oslo **Patientendaten außerhalb des elektronischen Patientendatensystems gespeichert** hat, indem Arbeitsblätter benutzt wurden, die Informationen über die Bewohner enthalten, die ihre täglichen Bedürfnisse und Pflegeabläufe detailliert beschreiben. Die Bewohner wurden durch ihren vollen Namen und ihre nationalen Identitätsnummern, Initialen oder Zimmernummern eindeutig identifiziert. Die Behörde beurteilte die Praxis der Speicherung identifizierbarer Patientendaten außerhalb des elektronischen Patientendatensystems als **Verstoß gegen die Anforderungen an technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO**. Bei der Berechnung der Höhe des Bußgeldes berücksichtigte die schwedische Datenschutzbehörde, dass die Stadt den Verstoß von sich aus der Datenschutzbehörde gemeldet und rasch Maßnahmen zur Löschung der Daten ergriffen hat. Außerdem wurde berücksichtigt, dass der Verstoß in erster Linie vor dem Inkrafttreten der DSGVO erfolgt sind. Nach der Rechtslage vor Inkrafttreten der waren die Geldbußen auf etwa 100 000 EUR begrenzt. Daher wurde in diesem besonderen Fall eine Geldbuße von 49 300 EUR für angemessen erachtet.

Verkauf von personenbezogenen (Mitglieder-)Daten zu Werbezwecken:

Die niederländische Datenschutzbehörde verhängte am 20. Dezember 2019 gegen den Tennisverband KNLTB eine Geldbuße in Höhe von EUR 525.000 wegen des **Verkaufs von personenbezogenen Daten** seiner (mehrerer hunderttausend) Mitglieder an zwei Sponsoren. Diese erhielten etwa Name, Geschlecht und Adresse, damit **sie per Telefon und Post den Betroffenen tennisbezogene, aber auch andere Werbung bzw. Angebote übermitteln** konnten. Die Behörde vertrat die Meinung, dass der Verkauf von personenbezogenen Daten ohne die Zustimmung der betroffenen Person generell verboten sei. Der Tennisverband hingegen war der Ansicht, dass sie ein überwiegendes berechtigtes Interesse am Verkauf der Daten habe und sich auch auf dieses stützen könne, was die niederländische Datenschutzbehörde verneinte. KNLTB legte ein Rechtsmittel ein, sodass die Strafe noch nicht rechtskräftig ist.

Massives Ausmaß unzulässiger Werbeanrufe:

Der britische ICO hat ein Bußgeld von GBP 500.000 (EUR 574.675) über das schottische Unternehmen CRDNN Limited wegen **unerlaubter Telefonanrufe in massivem Ausmaß** verhängt. Die Datenschutzbehörde stellte ernsthafte Verstöße gegen das Gesetz, welches zur nationalen Umsetzung der ePrivacy-Richtlinie erlassen wurde, fest. Eine Untersuchung des ICO ergab, dass das Unternehmen zwischen dem 1. Juni und dem 1. Oktober 2018 **täglich etwa 1,6 Millionen (automatisierte) Anrufe** getätigt hat, um Dienstleistungen (zB. Fensterverschrottung, Schuldenmanagement) und den Verkauf von Fenstern, Wintergärten und Heizkesseln anzubieten. 63.615.075 Anrufe wurden insgesamt verbunden, wobei der ICO von einer weit höheren Anzahl an Anrufen ausgeht, die von CRDNN getätigt wurden. **Etwa 3.000 Beschwerden** über die Anrufe gingen bei dem ICO ein, wobei die **Anrufe über so genannte „Spoof-Nummern" erfolgten**, sodass die Herkunft der Anrufe zunächst unbekannt war. Erst durch eine umfangreiche Untersuchung des ICO konnte CRDNN Limited als Verantwortlicher identifiziert werden. Das Unternehmen holte für die Anrufe keine Einwilligung von den Betroffenen ein und stellte auch keine funktionierende Opt-Out-Möglichkeit zur Verfügung. Die Bemessung der Geldbuße erfolgte gemäß Artikel 95 DSGVO.

Freier Zugang zu Dokumenten mit Gesundheitsdaten:

Die britische Datenschutzbehörde ICO hat (soweit bekannt) am 17.12.2019 ihr erstes direkt wirksames Bußgeld verhängt. Die Geldbuße in Höhe von etwa 320.000 EUR richtete sich gegen ein

Pharmaunternehmen, welches rund 500.000 Dokumente mit Stammdaten aber auch Gesundheitsdaten unsachgemäß verwahrte und den Informationspflichten der Artikel 13 und 14 DSGVO nicht in rechtskonformer Weise entsprach. Im Zuge einer Hausdurchsuchung (aus anderem Anlass) wurden in einem Hinterhof 47 unverschlossene Kisten, zwei Beutel und ein Karton voller Dokumente mit personenbezogenen Daten entdeckt. Der Zugang zu den rund 500.000 Dokumenten war für Hausbewohner uneingeschränkt möglich; keines der Dokumente war als vertraulich markiert und einige stark durchnässt. Enthalten waren Namen, Adressen, Geburtsdaten, Krankenversicherungsnummern, medizinische Informationen und Rezepte. Der ICO erblicke in diesem Verhalten Verstöße gegen die Art 5 lit f, 24 Abs 1 und 32 DSGVO.

Die meisten Geldstrafen wurden bis jetzt übrigens in Spanien verhängt (gefolgt von Deutschland). In Österreich sind derzeit 38 Geldbußen bekannt, wobei mehrere noch nicht rechtskräftig sind. Durch die zwei betragsmäßig größten Individualstrafen (Achtung: derzeit jeweils nur „intentions to fine“) liegt Großbritannien mit großem Abstand an der Spitze der verteilten Gesamtstrafsummen (etwa EUR 315 Mio.). Frankreich belegt „dank“ der EUR 50 Mio. Strafe für Google Platz zwei.

Gemeinsame Verantwortlichkeit bei Social Media

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Der baden-württembergische Landesdatenschutzbeauftragte hat unlängst mitgeteilt, seinen Twitter-Account aufgrund der Entscheidungen des EuGH (5. 6. 2018, C-210/16) und des deutschen BVerwG (11.09.2019, 6 C 15.18) zur **gemeinsamen Verantwortlichkeit** des Facebook-Seitenbetreibers und Facebook einzustellen. Wenngleich die gemeinsame Verantwortlichkeit – soweit ersichtlich – für Twitter bislang nicht gerichtlich geklärt wurde und es Argumente gegen eine gemeinsame Verantwortlichkeit bei Twitter gibt, ist die Frage für Facebook und Instagram zwischenzeitlich geklärt.

Wir empfehlen daher eindringlich, die **eigene Datenschutzerklärung für den Betrieb der Social Media Seiten (Facebook und Instagram)** in Hinblick auf die rechtsrichtige Aufklärung der gemeinsamen Verantwortlichkeit zu **überprüfen und gegebenenfalls zeitnah zu aktualisieren**. Wir beraten Sie in diesem Zusammenhang gerne und stellen auch entsprechende Musterbausteine zur Verfügung.

IAPP-Ausbildung in Österreich

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Die IAPP (International Association of Privacy Professionals) ist die weltweit größte Community zum Thema Datenschutz. Die branchenweit anerkannten Zertifizierungen zum Certified Information Privacy Technologist (CIPT) mit über 50.000 Mitgliedern, zum Certified Information Privacy Manager (CIPM) sowie spezifische Zertifizierungen zum Certified Information Privacy Professional (CIPP) für Asien, Kanada, Europa und die USA bescheinigen höchste Kompetenz in Bezug auf die technischen, planerischen/organisatorischen und rechtlichen Beratung zu den Themen der Datensicherheit und des Datenschutzes.

Die mit uns kooperierende eyecoon GmbH wurde von der IAPP nunmehr als erstes und einziges österreichisches Unternehmen als **offizielles IAPP-Schulungszentrum** anerkannt.

Die nächsten **Kurstermine**:

- Certified Information Privacy Professional/Europe (CIPP/E): 05. bis 06. Mai 2020, Wien
- Certified Information Privacy Manager (CIPM): 22. bis 23. April 2020, Wien
- Certified Information Privacy Technologist (CIPT): 01. bis 02. April 2020, Wien
- Certified Information Privacy Technologist (CIPT): 14. bis 15. Mai 2020, Wien

Nähere Informationen finden Sie auf der Website der eyecoon GmbH. Über uns erhalten Sie Ermäßigungen für die Kurse.

Neue Verbraucherschutzvorschriften der Union

Beitrag verfasst von Dr. Claudia Gabauer, LL.M am 16.03.2020 – KTR-Newsletter März 2020

Wir möchte auf die kürzlich in Kraft getretene RL (EU) 2019/2161 „**zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union**" aufmerksam machen, mit der u.a. die RL (EU) 2011/83 („Verbraucherrechte-RL") und die RL 2005/29/EG (unlautere Geschäftspraktiken) geändert werden.

Bei den Sanktionen hat man sich an der DSGVO orientiert und diese sogar noch verschärft. Der Höchstbetrag der zu verhängenden Geldbuße beträgt **mindestens (!) 4 % des Jahresumsatzes des Unternehmens**. Sofern keine Informationen über den Jahresumsatz des Unternehmens verfügbar sind, sind Geldbußen mit einem Höchstbetrag von **mindestens (!) 2 Mio. EUR** vorzusehen.

Auf folgende Änderungen möchten wir besonders hinweisen:

Verbot von Geschäftspraktiken, durch die Verbrauchern Informationen in Form von **Suchergebnissen aufgrund einer Online-Suchanfrage** des Verbrauchers bereitgestellt werden, ohne dass etwaige **bezahlte Werbung oder Zahlungen**, die speziell dazu dienen, ein höheres Ranking der jeweiligen Produkte im Rahmen der Suchergebnisse zu erreichen, **eindeutig offengelegt** werden. Wenn ein Gewerbetreibender den Anbieter einer Online-Suchfunktion unmittelbar oder mittelbar dafür bezahlt hat, dass ein Produkt im Rahmen der Suchergebnisse ein höheres Ranking erhält, sollte der Anbieter der Online-Suchfunktion die Verbraucher über diese Tatsache in kurzer, einfach zugänglicher und verständlicher Weise informieren.

Wenn Gewerbetreibende **Verbraucherbewertungen** von Produkten zugänglich machen, sollten sie Verbraucher darüber informieren, **ob Prozesse oder Verfahren angewandt** werden, um sicherzustellen, dass die **veröffentlichten Bewertungen tatsächlich von Verbrauchern verfasst** wurden, die die Produkte tatsächlich verwendet oder erworben haben. Wenn solche Prozesse oder Verfahren angewandt werden, sollten Gewerbetreibende Informationen darüber bereitstellen, wie die entsprechenden Prüfungen ablaufen, und den Verbrauchern eindeutige Informationen darüber zur Verfügung stellen, wie mit Bewertungen umgegangen wird, etwa ob alle Bewertungen — positive wie negative — veröffentlicht werden oder ob diese Bewertungen im Wege eines Vertragsverhältnisses mit einem Gewerbetreibenden gesponsert oder beeinflusst wurden. Zudem sollte es deshalb als unlautere Geschäftspraktik zur Irreführung der Verbraucher angesehen werden, wenn behauptet wird, dass Bewertungen eines Produkts von Verbrauchern stammen, die das Produkt tatsächlich verwendet oder erworben haben, ohne dass zumutbare und angemessene Schritte unternommen wurden, um sicherzustellen, dass die Bewertungen wirklich von solchen Verbrauchern stammen. Solche Schritte wären etwa technische Mittel zur Überprüfung der Glaubwürdigkeit einer Person, die eine Bewertung veröffentlicht, beispielsweise indem die Informationen zur Überprüfung, ob ein Verbraucher das Produkt tatsächlich verwendet oder erworben hat, angefordert wird.

Die Verbraucherrechte-RL soll auch dann gelten, wenn der Unternehmer dem Verbraucher **digitale Inhalte**, die **nicht auf einem körperlichen Datenträger geliefert** werden, **bereitstellt** oder deren Bereitstellung zusagt oder für den Verbraucher digitale Dienstleistungen bereitstellt oder deren Bereitstellung zusagt und der **Verbraucher dem Unternehmer personenbezogene Daten bereitstellt** oder deren Bereitstellung zusagt, außer in Fällen, in denen die vom Verbraucher bereitgestellten personenbezogenen Daten durch den Unternehmer ausschließlich zur Bereitstellung digitaler Inhalte, die nicht auf einem körperlichen Datenträger geliefert werden, oder digitaler Dienstleistungen im Einklang mit dieser Richtlinie oder zur Erfüllung von vom Unternehmer einzuhaltenden rechtlichen Anforderungen verarbeitet werden, und der Unternehmer diese Daten zu keinen anderen Zwecken verarbeitet.

Die RL ist bis zum **28.11.2021** in nationales Recht umzusetzen und das nationale Recht ab dem **28.5.2022** anzuwenden.

Evaluierung der DSGVO durch den Europäischen Datenschutzausschuss und die Datenschutzbehörde

Beitrag verfasst von RA Dr. Rainer Knyrim am 16.03.2020 – KTR-Newsletter März 2020

Der **Europäischen Datenschutzausschusses** (EDSA) hat seine Stellungnahme zur DSGVO-Evaluierung herausgegeben, in der er folgendes festhält:

- Der EDSA stellte fest, dass die Datenschutzbehörden bei der Umsetzung des **Kooperations- und Kohärenzmechanismus** Herausforderungen identifiziert haben. Dies ist vor allem auf Unterschiede bei den Verfahren zur Bearbeitung von Beschwerden, der Stellung der Parteien im Verfahren, den Zulässigkeitskriterien, der Dauer der Verfahren, den Fristen usw. zurückzuführen. Der EDSA prüft mögliche Lösungen zur Bewältigung dieser Herausforderungen und zur Gewährleistung einer gemeinsamen Anwendung der DSGVO.
- Der EDSA begrüßt das Interesse von Drittländern an einer Zusammenarbeit mit der EU im Rahmen der **Angemessenheitsentscheidung**. Der EDSA wird sich an der Bewertung der gegenwärtigen Angemessenheitsentscheidungen und der Annahme künftiger Entscheidungen beteiligen, wobei er betont, dass ihm alle relevanten Dokumente rechtzeitig vorliegen müssen, um eine gründliche Bewertung zu ermöglichen.
- Der EDSA ist der Ansicht, dass es für die Europäische Kommission dringend erforderlich ist, die bestehenden **Standardvertragsklauseln** mit der DSGVO in Einklang zu bringen und zusätzliche Standardvertragsklauseln zu entwerfen.
- Seit Inkrafttreten der DSGVO hat der EDSA drei positive Stellungnahmen zu nationalen Entscheidungen zur Genehmigung von **Binding Corporate Rules** (BCR) angenommen, während mehr als 40 BCR zur Genehmigung anstehen, von denen die Hälfte bis Ende 2020 genehmigt werden dürfte.
- Was **Verhaltensregeln und Zertifizierungen** betrifft, so bereitet der EDSA derzeit Richtlinien für Interessensgruppen vor, die voraussichtlich bis Ende 2020 für eine erste Annahme vor ihrer Vorlage zur öffentlichen Konsultation fertig gestellt werden.
- Was schließlich **Verwaltungsvereinbarungen** betrifft, so bereitet der EDSA auch Leitlinien für Behörden und Einrichtungen vor, die personenbezogene Daten an öffentliche Einrichtungen außerhalb des EWR übermitteln wollen. Diese Leitlinien wurden angenommen und werden vor ihrer endgültigen Verabschiedung zur öffentlichen Konsultation veröffentlicht.
- Bisher konnte der EDSA alle Stellungnahmen innerhalb der gesetzlichen Frist abgeben. Die Praxis zeigt jedoch, dass die in der DSGVO vorgesehenen Fristen (8 + möglicherweise 6 Wochen) relativ kurz sein können, um eine Einigung zwischen allen Mitgliedern zu erzielen.

Zusammenfassend erklärt der EDSA, dass er insgesamt eine positive Haltung gegenüber der Umsetzung der DSGVO hat und eine Überarbeitung für verfrüht hält. Anstatt die DSGVO zu überarbeiten, sollten die Bemühungen um die Annahme der ePrivacy-VO intensiviert werden.

Die österreichische **Datenschutzbehörde** (DSB) hat in Zusammenhang mit der Evaluierung des EDSA in ihrer Stellungnahme folgendes festgehalten:

- Bezüglich des **Kooperationsmechanismus** nach Art 60 DSGVO empfand die DSB die verschiedenen nationalen Verwaltungsverfahrensgesetze und die Dauer der Verfahren als problematisch. Es wird daher versucht auf informellen Weg mit den Ländern eine Lösung zu finden. Die DSB würde sich aber Unterstützung der EU – zB. durch Kollisionsnormen – wünschen.
- Die DSB klagt über zu wenig Ressourcen (aus personeller, finanzieller und technischer Sicht).
- Im Zeitraum vom 25. Mai 2018 bis 30. November 2019 wurden **2.807 Beschwerden** eingereicht und 1.142 Beschwerden sind über das IMI eingelangt (bloße Anfragen sind hier nicht enthalten).
- Es wurden **38 Bußgelder** verhängt (zwischen 200,- EUR und 18.000.000,- EUR). Die meisten Bußgelder wurden wegen unrechtmäßiger Videoüberwachung verhängt.
    - Als **mildernde Umstände** wurden Integrität, einmaliges Fehlverhalten, nachträgliche Beseitigung oder Wiederherstellung der rechtmäßigen Verhältnisse, Maßnahmen zur künftigen Vermeidung eines Verstoßes, Mitwirkung am Verfahren sowie Geständnisse berücksichtigt.
    - Als **erschwerende Umstände** wurden höchst unrechtmäßiges Verhalten, systematische Verletzung, hohe Anzahl betroffener Personen, lange Dauer der durchgeführten Verletzung, Kategorie der betroffenen Personen (Angestellte, nackte Frauen unter der Dusche), schwerwiegende Folgen der Verletzung (geistige Behinderung mit Krankheitswert), große Anzahl von Empfängern (Veröffentlichung in sozialen Netzwerken), nicht ergriffene Maßnahmen zur Schadensbegrenzung, einschlägige Strafregister, keine Mitarbeit im Verfahren, vorsätzliches Verhalten, Grad der Verantwortung sowie ein hoher wirtschaftlicher Nutzen aus der Verletzung berücksichtigt.

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, W: www.kt.at

FN 462250f, HG Wien