Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

# DSG-Info-Service

März 2021 Ausgabe Nr. 98

*Sehr geehrter DSG-Paket-Kunde!*
*Sehr geehrter Leser!*

*Wir freuen uns, Sie im neuen Jahr wie gewohnt mit einer DSG-Info begrüßen zu können. Die Behörden und Gerichte werken auch während der Pandemie und schaffen neue Erkenntnisse zum Datenschutz.*

*Von großer Bedeutung sind mittlerweile die Instanzgerichte, die die teils hohen Strafen der Datenschutzbehörden beträchtlich mindern oder aufheben. Wir präsentieren Ihnen die aktuellsten Rechtsmittelverfahren.*

*Der österreichische Gesetzgeber ist ebenfalls tätig geworden und hat mehrere Vorhaben angekündigt, die eine notwendige Anpassung des TKG 2003 betreffen und auch neue gesetzliche **Home-Office-Regelungen** umfassen.*

*Zudem ist im Rahmen der portugiesischen Ratspräsidentschaft ein neuer Entwurf der E-Privacy-Verordnung veröffentlicht worden.*

*Wir wünschen viel Vergnügen beim Lesen!*

## 1. Rechtsmittelgerichte vs. Datenschutzbehörden

Die Erkenntnisse der Datenschutzbehörde werden überwiegend im RIS veröffentlicht. Veröffentlichte Entscheidungen dienen vor allem dazu, die Anwendung der DSGVO und des DSG zu konkretisieren und die Rechtssicherheit zu stärken. Neue Entscheidungen werden auch im DSB-Newsletter publiziert, wo insbesondere Besprechungen von noch nicht rechtskräftig abgeschlossenen Verfahren kommuniziert und vorgestellt werden.

Das Bundesverwaltungsgericht – als Instanzgericht für Beschwerde- und Bußgeldverfahren – hatte bereits die Gelegenheit, in einer Vielzahl von Verfahren Entscheidungen zu treffen und die Liste an Erkenntnissen, die bestätigt oder komplett aufgehoben wurden, wird immer länger.

**Prof. KommR Pollirer** ist selbst als fachkundiger Laienrichter am BVwG tätig und hat eine Vielzahl von Entscheidungen inhaltlich begleitet.

Die bekanntesten den Datenschutz betreffenden Rechtsmittelerkenntnisse in Österreich drehen sich allesamt um ein österreichisches Direktmarketingunternehmen. Sowohl der Anspruch auf immateriellen Schadenersatz[1] für

[1] OLG Innsbruck - 13.02.2020, 1 R 182/19b.

unrechtmäßiges Profiling als auch die amtswegigen Bußgeldverfahren[2] wegen Verstößen gegen die DSGVO wurden in den jeweiligen Instanzen aufgehoben.

**Deutsche Rechtsmittelentscheidungen**

Ein ähnliches Schicksal trifft auch die Erkenntnisse der deutschen Datenschutzbehörden.

In der Sache „**1&1**" ging es um ein unzureichendes Sicherheitskonzept für die Identifikation von Kunden im Kundenservice und die Erteilung von Auskünften. Der Fall einer missbräuchlichen Datenübermittlung an eine unberechtigte Person wurde angezeigt und führte zu einem Bußgeld von EUR 9 Mio. Das Landesgericht Bonn hat als Rechtsmittelgericht befunden, dass das Erkenntnis dem Grunde nach gerechtfertigt sei, die Höhe jedoch nicht angemessen war. Es beschloss daher eine Herabsetzung des Bußgelds auf 10 % der ursprünglichen Strafe, d.h. EUR 900.000.

Das Bußgeld der **Deutschen Wohnen SE** wurde durch das Landgerichts Berlin[3] hingegen vollständig aufgehoben. Die Grundlage dieser Entscheidung war ähnlich gelagert wie im österreichischen Fall des Direktmarketing-Unternehmens: Das strafbare Verhalten konnte von der Aufsichtsbehörde keiner handelnden natürlichen Person vorgeworfen werden, die der juristischen Person zuzurechnen ist.

Auch das deutsche „Ordnungswidrigkeitenrecht" kennt keine Haftung juristischer Personen ohne Zurechnung eines rechtswidrigen Verhaltens natürlicher Personen. DSGVO-Verstöße müssen durch menschliches Fehlverhalten von Mitarbeitern, Führungskräften oder der Geschäftsführung veranlasst werden, damit dieses der juristischen Person zurechenbar ist.

Offen bleibt die Einordnung dieser Verantwortlichkeiten im Bereich der gemäß § 9 VStG bestellten Personen. Eine Klärung durch den Europäischen Gerichtshof wäre diesbezüglich begrüßenswert, um hohe Bußgelder bzw. Rechtsunsicherheit zu vermeiden und organisatorische Prozesse besser zu gestalten.

**Schadenersatz-Frage vor EuGH**

Aus Deutschland ist nun auch ein interessantes **EuGH-Verfahren** anhängig, in der es um die Erheblichkeitsschwelle von immateriellen Schäden geht. Das Amtsgericht Goslar entschied, dass es sich bei einer unzulässigen Werbe-E-Mail **nicht** um eine Beeinträchtigung handle, die einen immateriellen Schadenersatz auslöst. Dies geschah, ohne die Auslegung von Art. 82 DSGVO und die fehlende Rechtsprechung des EuGH zu berücksichtigen.

Der Kläger ging mit einer Verfassungsbeschwerde vor das Bundesverfassungsgericht und erhielt Recht. Das BVerfG entschied per Beschluss[4], dass die Frage, ob es eine Erheblichkeitsschwelle für immateriellen Schadenersatz gibt, durch den EuGH ausgelegt werden müsse. So heißt es im Urteil: „*dieser Geldentschädigungsanspruch ist in der Rechtsprechung des Gerichtshofs der Europäischen Union weder erschöpfend geklärt noch kann er in seinen einzelnen, für die Beurteilung des im Ausgangsverfahrens vorgetragenen Sachverhalts notwendigen Voraussetzungen unmittelbar aus der DSGVO bestimmt werden*".

Wir verfolgen den Verlauf des Verfahrens und werden Sie weiter über aktuelle Entwicklungen in dieser Rechtssache informieren.

[2] BVwG 26.11.2020 - W258 2227269-1 und W258 2217446-1

[3] LG Berlin, Beschluss vom 18.02.2021, Az. (526 OWi LG) 212 Js-OWi 1/20 (1/20).

[4] Beschluss vom 14. Januar 2021, 1 BvR 2853/19

# 2. Home-Office-Gesetzespaket

Seit letztem Jahr sind Home-Office und Telearbeit nicht mehr aus der Arbeitswelt wegzudenken. Damit einhergehend sollen nun Gesetzesänderungen folgen, die ihre rechtssichere Einführung oder Fortführung sowie die Rechtslage klarstellen sollen.

**Kein Anspruch, keine Pflicht zu Home-Office**

Es besteht weiterhin kein Anspruch auf Home-Office oder die einseitig durch den Arbeitgeber auferlegte Pflicht, von zuhause zu arbeiten. Damit bleibt die Notwendigkeit der Einzelvereinbarung mit den Mitarbeitern erhalten, die nach dem Gesetzesentwurf nun explizit schriftlich erfolgen muss. Der Gesetzgeber lässt es Arbeitnehmer und Arbeitgeber offen, ob die Tätigkeiten vollständig oder teilweise von zuhause verrichtet werden müssen. Eine Kündigung muss im Einvernehmen oder einseitig aus wichtigem Grund (zB Einschränkung der Wohnungsnutzung) erfolgen.

**Betriebsmittel**

Klargestellt wird, dass der Arbeitgeber verpflichtet ist, dem Arbeitnehmer die „erforderlichen digitalen Arbeitsmittel“ zur Verfügung zu stellen. Darunter werden PC/Laptop, Telefon und Datenverbindung (Internet) verstanden.

Bereitgestellte Arbeitsmittel durch den Arbeitgeber lösen jedoch keine Abgabenpflicht aus und sind somit nicht als Sachbezug zu werten.

**Home-Office-Betriebsvereinbarung**

Der Gesetzgeber plant mit § 97 Abs. 1 Z 27 ArbVG die Festlegung von Rahmenbedingungen für Arbeit im Home-Office als fakultative (freiwillige) Betriebsvereinbarung. Diese soll unabhängig von bestehenden kollektivvertraglichen Regelungen für sämtliche Branchen gelten.

Es ist weiterhin zwar notwendig, eine Einzelvereinbarung mit dem Mitarbeiter abzuschließen, da die Einführung von Home-Office keine kollektive Maßnahme ist. Dennoch schafft der neue BV-Tatbestand eine Rechtsgrundlage, um betriebliche Rahmenbedingungen (wie pauschaler Kostenersatz, Bereitstellung von digitalen Arbeitsmitteln, technische Ausfälle etc.) festzulegen.

Das Thema Datenschutz unterliegt grundsätzlich anderen BV-Tatbeständen (vgl. insb. § 96 und § 96a ArbVG) und bedarf daher einer weiteren gesonderten Betriebsvereinbarung.

**26 Tage-Frist für Werbungskosten**

Mitarbeiter, die die Anschaffung von Material und Mobiliar als Werbungskosten geltend machen wollen, müssen nachweislich 26 Tage von zuhause arbeiten. Dies ist auch durch den Arbeitgeber im Lohnkonto zu verzeichnen. Diese Frist wurde von den ursprünglich geforderten 42 Tagen herabgesetzt. Als zusätzliche Werbungskosten können in der Arbeitnehmerveranlagung EUR 300 für Einrichtung oder Ausgaben für das Home-Office angegeben werden, falls kein eigenes Arbeitszimmer steuerlich geltend gemacht wird.

**Änderung Dienstnehmerhaftpflichtgesetz**

Das Dienstnehmerhaftpflichtgesetz regelt Haftungsfragen und -höhe, wenn Schäden, etwa an Betriebsmitteln oder Arbeitsergebnissen, durch den Dienstnehmer verursacht wurden. Die Novelle des DHG nimmt nun auch Haushaltsangehörige und Haustiere in den Anwendungsbereich haftungsmildernder Umstände bei Schadenverursachung im Home-Office auf, da diese bei Schäden dem Dienstnehmer zugerechnet werden.

**Unfallschutz**

Der Unfallversicherungsschutz im Home-Office wurde bereits durch das 3. COVID-19-Gesetz geregelt. Unfälle können als Arbeitsunfälle qualifiziert werden, wenn sie sich in zeitlichem

und ursächlichem Zusammenhang mit der beruflichen Tätigkeit im Home-Office ereignen.

**Arbeitszeit**

Sämtliche Bestimmungen des AZG bleiben unverändert. Mitarbeiter haben ihre Zeiterfassung auch von zuhause aus zu führen und die gesetzliche Maximalarbeitszeit gilt auch für die Tätigkeit im Home-Office.

**Keine konkreten Datenschutzbestimmungen**

Aus den Gesetzesmaterialien ist erkennbar, dass keine näheren Regelungen zum Beschäftigtendatenschutz geplant sind, obwohl die DSGVO hier eine ausdrückliche Öffnungsklausel für den nationalen Gesetzgeber vorsieht. Die digitale Überwachung von Mitarbeitern im Home-Office ist allerdings bereits jetzt unzulässig.

## 3. Angemessenheitsbeschluss zum internationalen Datenverkehr mit Großbritannien

Seit 1. Jänner 2021 hat das Vereinte Königreich die EU verlassen und damit die Frage der Anwendbarkeit der Regelungen für den internationalen Datenverkehr in der Datenschutzgrund-Verordnung ausgelöst. Statt der EU-DSGVO gilt in Großbritannien die „UK-GDPR", die im Wesentlichen die gleichen Grundsätze und Regelungen wie die bisherige DSGVO enthält, allerdings national beschränkt bleibt. Der bisherige Data Protection Act sowie die Privacy and Electronic Communications Regulation (PECR) bleiben in Geltung.

Nun wurden **zwei** Entwürfe für **Angemessenheitsbeschlüsse der Kommission** über die Datenübermittlung an ein Nicht-EU-Land für den Datenverkehr mit Großbritannien sowie zur Richtlinie 2016/680 zum Datenschutz bei der Strafverfolgung veröffentlicht. Aktuell wären Datenübermittlungen in das Vereinte Königreich wie jene in Drittländer zu behandeln, doch es besteht noch eine Übergangsregelung bis **30. Juni 2021**. Der Datenaustausch von EU-Unternehmen mit Großbritannien darf daher noch zu den gleichen Bedingungen wie vor dem Brexit stattfinden.

Für die Datenübermittlung aus Großbritannien in die EU hat sich nichts geändert, da hier die DSGVO territorial und sachlich anwendbar bleibt. Im nächsten Schritt wird der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme abgeben. Auch die Mitgliedstaaten müssen noch im sogenannten Ausschussverfahren ihre Zustimmung geben.

Anschließend könnte die Kommission die endgültigen Angemessenheitsbeschlüsse annehmen. Mit deren Annahme stellt die EU ein ausreichendes Datenschutzniveau für Großbritannien fest und ermöglicht den Datentransfer ohne zusätzliche Bedingungen (zB Abschluss von **Standardvertragsklauseln** oder **Binding Corporate Rules**). Eine Re-Evaluierung ist dann in vier Jahren geplant.

## 4. Internationale Erkenntnisse

**1) Gastbeitrag zu Clubhouse – RECHT Aktuell**

Der Hype um die neue Social-Media App erreicht immer mehr den Mainstream: **Clubhouse** dient als soziales Netzwerk zur Übertragung von Audio-Unterhaltungen, die in großer Runde oder privatem Rahmen stattfinden können und die auch als Live-Podcasts genutzt werden.

Die App wird wegen des Zugriffs auf Kontakte und Speicherns von Gesprächsinhalten heftig für ihren Umgang mit Daten kritisiert.

Frau **Mag. Wyrobek** hat für die MANZ-Zeitschrift **RECHT Aktuell** einen Gastbeitrag zur datenschutzrechtlichen Einschätzung von Clubhouse verfasst.

In Deutschland erwägt die Verbraucherzentrale bereits eine Klage vor dem Landgericht Berlin und auch der Hamburger Landesbeauftragte für Datenschutz hat bereits eine Stellungnahme verfasst.

**2) NL: Unzureichende Sicherheit für Patientendaten: Bußgeld für Krankenhaus**

Der Schutz von Patientendaten der Krankenhäuser gehört zu den wichtigsten Aufgaben der IT- und Benutzerverwaltung. Die niederländische Datenschutzbehörde hat das Amsterdamer Krankenhaus OLVG mit einem Bußgeld von EUR 440.000 belegt, da es unzureichende Zugriffsmaßnahmen für das Krankenhauspersonal implementiert hatte. Über einen Zeitraum von zwei Jahren war es ohne eine Zwei-Faktor-Authentifizierung, die das Personal und dessen Berechtigungen prüft, möglich, Patientendaten einschließlich Krankengeschichte, SV-Nummer sowie Stammdaten ohne entsprechende Berechtigung abzufragen und einzusehen.

**3) NL: Verwarnung für niederländischen Supermarkt wegen des Einsatzes von Gesichtserkennungssoftware**

Einem Supermarkt in den Niederladen wurde untersagt, Gesichtserkennungstechnologie für die Prävention von Diebstählen zu verwenden.

Beim Eingang des Supermarktes wurden die Gesichter der Kunden und Mitarbeiter gescannt und mit einer Liste derjenigen Personen abgeglichen, gegen die bereits ein Hausverbot wegen Diebstahls besteht. Die biometrischen Daten von Personen, bei denen kein Treffer erzielt werden konnte, wurden wenige Sekunden nach dem Abgleich gelöscht.

Die niederländische Behörde befand, dass die strengen Voraussetzungen für den Einsatz von Gesichtserkennung, d.h. Verarbeitung biometrischer Daten, nicht erfüllt wären und untersagte die Datenverarbeitung, ohne ein Bußgeld zu verhängen.

**4) Norwegen straft Dating-App Grindr mit EUR 10 Mio**

Die Dating-App Grindr wurde für ihren unzulässigen Umgang mit personenbezogenen Daten, insbesondere aus besonderen Datenkategorien gestraft. Das Unternehmen betreibt eine Plattform, auf der sich LGBTQ-Personen treffen und miteinander Kontakt aufnehmen können. Angesichts der Verarbeitung von Daten zur sexuellen Orientierung besteht dafür besonderer Schutzbedarf. Dabei wurden die Nutzer weder richtig informiert noch wurde von ihnen die Einwilligung erteilt, dass ihre Daten mit Werbeunternehmen geteilt werden. Es musste der gesamten Datenschutzerklärung zugestimmt werden, ohne separate Opt-In Möglichkeiten oder ausreichende Informationen.

Die norwegische Datenschutzbehörde argumentierte in ihrem Urteil, dass die angebliche „Einwilligung", auf die sich Grindr berief, ungültig sei. Zudem habe etwa Werbung nicht spezifisch aktiviert oder deaktiviert werden können. Fünf Adtech-Unternehmen hätten über die App personenbezogene Daten der Nutzer erhalten. Jedes Mal, wenn ein Nutzer Grindr öffne, würden Informationen wie dessen aktueller Standort oder ID an Werbetreibende übermittelt. Diese Informationen seien auch verwendet worden, um umfassende Nutzerprofile für gezielte Werbung zu erstellen, was ohne ausdrückliche Einwilligung im Kontext der sensiblen Daten nicht zulässig ist.

**5) TikTok im Visier der Behörden nach Tod eines Kindes**

Die Videoplattform TikTok kommt nicht aus der Kritik. Neben der Französischen Datenschutzbehörde und Europäischen Kommission gerät das Unternehmen jetzt auch in den Fokus der Italienischen Datenschutzbehörde, nachdem ein 10-jähriges Mädchen bei einer *„TikTok-Challenge"* ums Leben gekommen ist.

Die italienische Behörde hat eine Anordnung zum sofortigen Stopp der Datenverarbeitung für minderjährige Nutzer, deren Alter TikTok nicht ausdrücklich bekannt ist, erlassen.

Diese Anordnung spiegelt wider, dass es TikTok noch immer nicht gelungen ist, einen adäquaten Verifizierungsprozess für Minderjährige einzurichten bzw. ausreichende Datensicherheitsmaßnahmen zu treffen, um dieser zu schützenden Gruppe den angemessenen datenschutzrechtlichen Schutzbedarf zuzuweisen. Der Einsatz der Videoplattform aus B2B-Sicht ist jedenfalls kritisch zu hinterfragen, da angesichts der Rechtsprechung zu sog. Joint Controllerships (RS Fashion ID) eine gemeinsame Verantwortlichkeit zwischen TikTok und dem Unternehmen entsteht, sobald es eine Insight-Funktion gibt. Dies ist bei gewerblichen Konten regelmäßig der Fall, sodass Vorsicht geboten ist.

**6) Millionenstrafe gegen notebooksbilliger.de wegen unzulässiger Videoüberwachung**

Erneut schlägt das Thema Mitarbeiterüberwachung große Wellen bei den deutschen Datenschutzbehörden. Nachdem bereits H&M mit einer Strafe für unzulässige Mitarbeiterüberwachung belegt wurde, hat die Behörde aus Niedersachen den Online-Shop „notebooksbilliger“ mit EUR 10,4 Mio bestraft.

Zwei Jahre lang wurden Beschäftigte per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorgelegen sei. Die eingesetzten Kameras haben unzulässigerweise unter anderem Arbeitsplätze, Lager und Aufenthaltsbereiche der Mitarbeiter erfasst. Die Aufnahmen wurden darüber hinaus bis zu 60 Tage lang aufbewahrt, was nicht mit dem Grundsatz der Verhältnismäßigkeit in Einklang zu bringen ist. In diesem Zusammenhang verweisen wir auf die „**Checkliste Videoüberwachung nach der EDPB-Leitlinie 3/2019“ von Prof. KommR Pollirer (hier für Sie abrufbar**).

**7) BE: Pink Box verkaufte Daten von Kunden**

Die belgische Behörde strafte das Unternehmen Family Services für den unrechtmäßigen Verkauf von Daten. Das Unternehmen, das u.a. „Mutter-Kind Boxen“ an werdende Eltern verschickt, verkaufte die Daten von Kunden an sog. Data Broker für zielgruppenorientierte Werbung.

Das Unternehmen knüpfte den Erhalt der Gratis-Waren an die stillschweigende Einwilligung zur Datenübermittlung an Dritte. Die erhobenen Daten wurden dann Adressverlagen zur Verfügung gestellt. Aufgrund der fehlenden Informationen zur Datenverarbeitung und der unzureichenden Einwilligung wurde das Unternehmen in Belgien mit einem Bußgeld iHv. EUR 50.000 belegt.

**8) Illegaler Handel mit COVID-19 Daten**

In den Niederlanden ermittelt die Polizei in Fällen, bei denen Daten, die aus den durch die Gesundheitsbehörden bereitgestellten Systemen zur COVID-19-Verwaltung stammen, im Internet angeboten worden sind. Zwei Männer sind bereits festgenommen worden. Bei den Datensätzen handelt es sich um Millionen privater Datensätze von Niederländern, die einen Corona-Test durchgeführt haben, aus dem Contact-Tracing-System.

## 5. E-Privacy-VO im Trilog-Verfahren

Die portugiesische Ratspräsidentschaft hat einen entscheidenden Fortschritt in den Verhandlungen um die neue E-Privacy-Verordnung erreicht. Mittlerweile befindet sich der Verordnungsentwurf im sog. Trilog-Verfahren und wird auch inhaltlich durch das europäische Parlament behandelt.

Die Themen bleiben unverändert und betreffen elektronische Kommunikationsdaten, Metadaten, IOT-Dienste, die Einbindung von

sog. OTT-Diensten wie WhatsApp und Telegram sowie den Einsatz von Cookies. Umfasst sind natürliche Personen und juristische Personen. Damit wird der Anwendungsbereich im Vergleich zur DSGVO erweitert.

Bei den Fragen rund um Cookies soll Endnutzern eine echte Wahl angeboten werden, Cookies oder ähnliche Kennungen zu akzeptieren, ohne aus einer Ablehnung Nachteile zu erfahren. Das betrifft im Wesentlichen die Opt-In-Pflicht, die ohnehin schon großteils gelebte Praxis im Wirtschaftsleben geworden ist.

Unter Kommunikationsdaten werden die Daten zusammengefasst, die bei der Nutzung von Online-Diensten generiert und übermittelt werden. Davon betroffen sind zB Nachrichten über WhatsApp oder Videoanrufe auf Skype. Ziel der E-Privacy-Verordnung ist eine technologieneutrale Regelung für elektronische Kommunikationsanbieter, sodass auch neue Player und Kommunikationsformen berücksichtigt werden. Die Analyse und Verfolgung des Online-Verhaltens von Nutzern soll reguliert werden und geht damit in Richtung des Schutzes von Nutzerdaten.

## 6. Whistleblowing

Der Countdown läuft: Bis 17. Dezember 2021 muss der österreichische Gesetzgeber die Umsetzung der Whistleblowing-RL veranlassen. Der Anwendungsbereich umfasst eine Vielzahl von privaten Unternehmen sowie vor allem öffentliche Stellen und Behörden.

Die Stadt Wien geht mit einer Whistleblower-Plattform in den Betrieb und reiht sich bereits in die Riege von öffentlichen Stellen (wie beispielsweise die FMA) oder auch Privatunternehmen (zB Uniqa) ein.

Die Implementierung eines Whistleblowing-Systems bedarf der Eingliederung in den Bereichen Arbeitsrecht, Datenschutz und IKT. Von besonderer Bedeutung ist die Gewährleistung der Anonymität und Schutz der Hinweisgeber bei gleichzeitigem Ermöglichen der Bekämpfung und Verhinderung von Missständen und Wirtschaftskriminalität.

## 7. Publikationen 2021

Die Publikationsliste von **Prof. KommR Pollirer** zum Datenschutz begleitet Praktiker in Österreich seit Jahrzehnten. Neben den **Fachkommentaren** zum **DSG** und der **DSGVO** ist er auch als Autor des einschlägigen Groß-Kommentars „**DatKomm**“ für den Artikel 32 DSGVO (technische und organisatorische Sicherheitsmaßnahmen) verantwortlich. Darüber hinaus veröffentlicht er regelmäßig seine **Datenschutz-Checklisten**, die auf Fragen des Datenschutzes und der Informationssicherheit praxisnahe Antworten geben.

Wir dürfen Sie daher auf die aktuelle Ausgabe der Zeitschrift „*Datenschutz konkret*“ hinweisen, in der **Prof. Pollirer** eine Checkliste zum Thema „Checkliste Videoüberwachung nach der EDPB-Leitlinie 3/2019**“** verfasst hat.

Wir freuen uns zudem, dass auch Frau **Mag. Wyrobek** ein Kapitel im „**DatKomm**“, und zwar zu Artikel 26 DSGVO (Joint Controllership) geschrieben hat.

Darüber hinaus hat sie das Kapitel zur „*Einwilligung*“ im **Praxishandbuch Datenschutz** (4. Auflage, 2020) verfasst.

••••

## Website-Check – Ihre Online-Compliance

Die EuGH-Rechtsprechung zu Cookies und Tracking hat zu einer wesentlichen Änderung der Marketing-Strategie vieler Unternehmen geführt. Auch das Thema Social Media und Social Plugins hat rechtliche Verschärfungen gebracht.

Überprüfen Sie, ob Ihre Website mit der Rechtslage im Einklang ist! Wir bieten Ihnen hierzu den Secur-Data Website-Check an, der Ihre Online-Präsenz auf die gesetzlichen Grundlagen überprüft und Sie bei Schwachstellen oder Optimierungen unterstützt. Der Website-Check behandelt materielle **datenschutz- und telekommunikationsrechtliche Fragestellungen** des Website-Betriebs.

Wir prüfen Ihre Website auf sicherheitsrelevante Themen, die von Verschlüsselung über Zertifikatsprüfung reichen und auch die Prüfung von **Auftragsverarbeitungsvereinbarungen** und **Joint Controllerships** beinhalten. Die inhaltliche Betrachtung der Website reicht von der Schutzbedarfseinschätzung des angesprochenen Publikums (Kinder, Forum, journalistische Medien) bis hin zur korrekten Implementierung des Cookie-Banners, den Opt-In-Mechanismen und der passenden Datenschutzerklärung. Dazu kommt eine Durchschau Ihrer Einwilligungserklärung sowie etwaiger Newsletter-Masken, die wir für Sie in eine transparente und verständliche Formulierung bringen.

Sie erhalten die Ergebnisse nach Untersuchungsbereichen getrennt. Sofern notwendig, führen wir zu den einzelnen Bereichen spezifische Maßnahmenempfehlungen an, die für die vollständige datenschutzrechtliche Online Compliance erforderlich sind.

Für eine unverbindliche Beratung können Sie uns unter office@secur-data.at kontaktieren oder unsere Website www.secur-data.at besuchen.

••••

Schweren Herzens müssen wir unser für April 2021 geplantes Seminar absagen. Angesichts der laufenden Entwicklung ist es uns nicht möglich, die reibungslose Durchführung des Seminars zu gewährleisten.

Wir werden Sie informieren, sobald es einen Ersatztermin gibt. In der Zwischenzeit stehen wir jederzeit für eine Inhouse-Schulung vor Ort oder per Videokonferenz zur Verfügung.

••••