

DSG-Info-Service

Digitaler Geburtstag: 2 Jahre DSGVO

Mai 2020

Ausgabe Nr. 95

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

Die DSGVO feiert ihren zweiten Geburtstag und die Schonfrist hat damit nun endgültig ein Ende

gefunden. Wir fassen die Neuigkeiten, Erkenntnisse und Gesetzesvorhaben für Sie zusammen und informieren Sie zu den aktuellen Themen im Datenschutz.

1. Neuigkeiten aus Europa

I. **EDSA Guideline zur Einwilligung veröffentlicht**

Der Europäische Datenschutzausschuss (EDSA) hat sich in einer neuen [Leitlinie](#) dem Thema Einwilligung gewidmet. Darin werden wesentliche Punkte, die bereits von der Rechtsprechung der österreichischen Datenschutzbehörde, dem Obersten Gerichtshof und dem EuGH thematisiert wurden, durch die Rechtsmeinung des EDSA weiter konkretisiert.

Wir haben für Sie die wesentlichen Punkte mit Angabe der Randnummer im Dokument kommentiert und zusammengefasst.

1. Strenges Kopplungsverbot

In der Datenschutzgrundverordnung wird ausdrücklich normiert, dass eine Einwilligung zur Datenverarbeitung für eine vertragsunabhängige Leistung nicht zur Bedingung des Vertrages gemacht werden darf (vgl. Art. 7 Abs. 4 DSGVO) (Rn. 30 ff.). Damit wird ausdrücklich festgehalten, dass die Koppelung der Einwilligung an den Vertrag nicht zulässig ist.

Aus den einschlägigen Rechtsgrundlagen wird Art. 6 Abs. 1 lit. b DSGVO als relevante Rechtsgrundlage empfohlen. Die Beweislast, dass keine Koppelung der Einwilligung an die Vertragserfüllung vorliegt, trägt der Verantwortliche (Rn. 36).

2. Zulässigkeit „entgeltlicher Alternativzugänge“

In der Medienlandschaft wurde ein neues Modell eingeführt, das den Betroffenen die Wahl ermöglicht, in die Datenverarbeitung einzuwilligen, um Werbung auszuspielen oder gegen Zahlung eines periodischen Betrages von Werbung und Trackern ausgenommen zu sein. Der EDSA stellt in seiner Rechtsmeinung fest, dass bei grundsätzlich kostenlosen Angeboten ein „entgeltlicher Alternativzugang“ ausdrücklich erlaubt ist (Rn. 37). Damit wird das „Standard.at-Modell“, das auch einem [Beschwerdeverfahren](#) vor der Datenschutzbehörde standgehalten hat, nunmehr ausdrücklich legitimiert. Die Grenze ist bei der Höhe des Entgelts zu setzen, dieses darf keine

Wucherpreise erreichen. Angebote anderer Anbieter iS einer Marktstellung dürfen nicht als Argument für das Vorhandensein eines „entgeltlichen Alternativzugangs“ herangezogen werden (Rn. 38).

3. Informiertheit der Einwilligung setzt nicht Vollinformation voraus

Um eine gültige Einwilligung abzugeben, ist eine aktive, eindeutige, freiwillige und vor allem informierte Handlung zu setzen. Der EDSA berücksichtigt jedoch, dass es nicht immer möglich ist, die Informationspflichten in bestimmten Verarbeitungssituationen voll zu erfüllen. Eine „Vollinformation“ iSd Art. 13 oder Art. 14 DSGVO ist nicht zur Gültigkeit der Einwilligung notwendig (Rn. 64). Zu beachten ist jedoch, dass in weiterer Folge auch die restlichen Art. 13/14-Informationen nachgereicht werden müssen. Über gemeinsame Verantwortliche iSd Art. 26 DSGVO oder Übermittlungen an Dritte muss vor der Einwilligung informiert werden, über Auftragsverarbeiter dagegen erst nachträglich (Rn. 65).

4. Kein Medienbruch bei Widerruf

Der Nutzer darf bei Ausübung seines Widerrufsrechts nicht zu einem Medienbruch genötigt werden. Das bedeutet, dass die Erteilung der Einwilligung und deren Widerruf grundsätzlich genauso einfach und über dasselbe Medium zu erfolgen haben. Es ist also nach Meinung des EDSA unzulässig, eine Einwilligung über E-Mail erteilen, aber nur über Telefon, SMS oder postalisch widerrufen zu können (Rn. 114). Dies deckt sich mit den aktuellen OGH-Entscheidungen (vgl. auch [OGH 23.09.2019, 9 Ob 38/19g – Pay-TV](#)).

5. Kein Wechsel zwischen mehreren Rechtsgrundlagen

Es obliegt dem Verantwortlichen, noch vor der Datenverarbeitung eine taugliche Rechtsgrundlage zu wählen. Entscheidet er sich dabei für die Einwilligung, so muss er an dieser als einziger Rechtsgrundlage festhalten. Bei einem Widerruf oder fehlender Gültigkeit der

Einwilligung kann nicht ersatzweise eine andere Rechtsgrundlage (zB Erfüllung des Vertrages oder überwiegendes berechtigtes Interesse) herangezogen werden. Damit erteilt der EDSA in seiner Rechtsmeinung (Rn. 121ff) sog. „Pro-Forma Einwilligungen“ eine Absage.

6. Altersverifikation für alle elektronische Dienste oder Services an Kinder erforderlich

Bietet der Verantwortliche elektronische Dienste oder Services an, die sich nicht ausschließlich an Erwachsene richten, so hat immer eine Altersverifikation zu erfolgen (Rn. 130, 133). Dies konkretisiert die Pflicht, die sich bereits aus Art. 8 DSGVO ableitet. Bedauerlicherweise gibt der EDSA keine deutliche Abgrenzung zum Aufwand oder den technischen Vorrichtungen für die Altersverifikation an. Das Ergebnis einer unzureichenden Altersüberprüfung bzw. der fehlenden Einholung der Einwilligung durch Vertretungsbefugte ist aber mit der Unrechtmäßigkeit der Datenverarbeitung behaftet, sodass beim Angebot von Diensten der Informationsgesellschaft an Minderjährige „angemessene“ Vorkehrungen getroffen werden müssen.

II. 725.000 Euro Bußgeld für Verarbeitung von Fingerabdrücken

Die niederländische Datenschutzbehörde hat das bis dato höchste nationale Bußgeld für die unrechtmäßige Verarbeitung von [Fingerabdrücken als Zutrittskontrollmaßnahme](#) verhängt.

Ein Unternehmen hatte die Fingerabdrücke von rund 300 Mitarbeitern erhoben und aus ihnen Templates generiert, die den Zutritt zum Betriebsgelände gewähren. Hierbei hat die Behörde allerdings Mängel bei den Grundsätzen der Datenverarbeitung (Art. 5 DSGVO), den Informationspflichten (Art. 13 DSGVO) und den Rechtsgrundlagen (Art. 9 Abs. 2 DSGVO) erkannt.

Fingerabdrücke unterliegen gem. Art. 4 Z 14 DSGVO als biometrische Daten einem höheren Schutzniveau, da sie sensible Daten darstellen.

Aus diesem Grund gilt für sie ein grundsätzliches Verarbeitungsverbot mit dem eingeschränkten Ermächtigungskatalog des Art. 9 Abs. 2 DSGVO.

Die Mitarbeiter wurden nicht über die Datenverarbeitung informiert bzw. wurde ihnen mitgeteilt, dass diese Datenverarbeitung Teil des Arbeitsvertrages sei. Einige gaben offenbar mündliche Einwilligungen; diese erfüllen jedoch nicht die in Art. 9 Abs. 2 lit. a DSGVO normierte Anforderung der ausdrücklichen Einwilligung. Zudem ist die Einwilligung im Arbeitsverhältnis stets einer strengeren Prüfung der Freiwilligkeit unterzogen und unterliegt aufgrund des Unterordnungsverhältnisses der Mitarbeiter oftmals in dieser Prüfung.

Daher war die Datenverarbeitung als unrechtmäßig einzustufen und verletzte die Grundsätze der Rechtmäßigkeit und Transparenz.

III. **Belgische Datenschutzbehörde straft Unternehmen für Datenschutzbeauftragten mit Interessenkonflikt**

Die belgische Behörde hat den [Telekommunikationsanbieter Proximus SA](#) mit einem

Bußgeld von 50.000 Euro versehen, da dieser einen Datenschutzbeauftragten eingesetzt hatte, der darüber hinaus drei weitere Funktionen innehatte. Neben der Rolle als Datenschutzbeauftragter war dieser als Leiter der Internen Revision sowie der Abteilung für Risikomanagement und Compliance tätig. Diese Kumulierung mit der Funktion des Datenschutzbeauftragten stellte für die Behörde einen Interessenkonflikt dar, da keine unabhängige Kontrolle der jeweiligen Abteilungen mit deren Leitungsaufgaben gewährleistet war. Das Unternehmen argumentierte mit dem beratenden Charakter sämtlicher Funktionen, die Behörde sah aber die weisungsfreie und unabhängige Tätigkeit, die Voraussetzung für die Arbeit des Datenschutzbeauftragten ist, nicht als gewährleistet an und stellte einen Verstoß gegen Art. 38 Abs. 6 DSGVO fest.

Der interne DSBA darf gem. Art. 38 Abs. 6 DSGVO auch in anderen Abteilungen tätig sein. Dies darf jedoch nicht zu einem Interessenkonflikt mit seiner Funktion führen, die seine Tätigkeit als unabhängiger und weisungsfreier Berater und Überwacher der DSGVO im Unternehmen beeinträchtigt.

2. Judikaturübersicht

I. **DSB: Double-Opt-In-Verfahren als Stand der Technik**

Diese [Entscheidung](#) (DSB-D130.073/0008-DSB/2019 vom 9.10.2019) befasst sich mit der Frage, welche technischen und organisatorischen Maßnahmen ein Unternehmen treffen muss, um personenbezogene Daten vor Missbrauch zu schützen.

Der Ausgangsfall betraf die E-Mail-Adresse eines Minderjährigen, die zur Anmeldung auf einem „Dating-Portal“ verwendet wurde. Das Unternehmen hatte kein Double-Opt-In-Verfahren vorgesehen, bei dem die E-Mail-Adresse

durch den Besitzer des Mail-Accounts verifiziert wird. Das führte dazu, dass dem Minderjährigen eindeutige Angebote und Werbung des Unternehmens zugesandt wurde, ohne dass er hierzu eingewilligt hatte.

Die Thematik betrifft also die notwendigen technischen und organisatorischen Maßnahmen (TOM) für die Daten von Betroffenen bzw. die Verhinderung von Missbrauch.

Die DSB führte dazu aus, dass das Unternehmen keine ausreichenden entsprechenden Datensicherheitsmaßnahmen iSd Art. 32 DSGVO gesetzt hatte. Daher war es möglich,

dass die Daten eines Minderjährigen unrechtmäßig verarbeitet wurden. Sie stellte eine Verletzung des Grundrechts auf Geheimhaltung nach § 1 Abs. 1 DSG fest.

Der Bescheid ist rechtskräftig und konkretisiert das Double-Opt-In-Verfahren als Stand der Technik. Das BVwG hat hierzu bereits eine Reihe von Erkenntnissen publiziert. Das neueste ([BVwG W219 2190019-1](#)) befasst sich mit der Frage von Direktwerbung und Single-Opt-In-Verfahren bei E-Mail-Werbung. Das BVwG stellt darin fest, dass ein Verantwortlicher „ohne jede Überprüfung der Zustimmung durch jene Person, die über die E-Mail-Adresse Verfügungsbefugt ist [...] das viel größere und strukturelle Risiko [eingeht], dass es – bei Nichtvorliegen einer Zustimmung – zur Begehung einer Vielzahl von Deliktshandlungen kommt“.

Zusammenfassend schützt also der Einsatz von Double-Opt-In-Verfahren Betroffene vor Missbrauch und unbefugter Nutzung ihrer Daten sowie Verantwortliche vor der missbräuchlichen Verwendung ihrer Dienste.

II. **OGH: Koppelungsverbot weiter bestätigt**

Eine Verbandsklage gegen einen Vermittler von Hotelgutscheinen (Midnight Deal) führte zur Prüfung verschiedener Klauseln, die unter anderem das datenschutzrechtliche Koppelungsverbot betrafen. Der Senat bestätigte damit die in der ausführlichen Auseinandersetzung der SimpliTV-Entscheidung (OGH 31.8.2018, 6 Ob 140/18h) festgelegten, strengen Voraussetzungen an die Freiwilligkeit der Einwilligung.

Im vorliegenden Fall lag erneut eine Koppelung von vertragsunabhängiger Datenverarbeitung an den Vertragsabschluss durch die Bündelung von Einwilligung und AGB ohne separate Auswahlmöglichkeit vor. Der beklagte Gutscheinvertreiber stritt nicht ab, dass er nicht bereit wäre, ein Vertragsangebot der Kunden

anzunehmen, wenn die Klausel vorab durch den Konsumenten ausgeschlossen würde. Der Senat ließ das Argument, man könne seine Einwilligung nachträglich ohnehin widerrufen, nicht zu, da es keine Schlüsse auf die geforderte Freiwilligkeit zulässt.

Damit bestätigt der OGH erneut die strengen Anforderungen an die Freiwilligkeit, die an eine Einwilligung geknüpft sind und schafft einen Rechtsatz für die ständige Rechtsprechung (*stRsp*): „Bei der Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsabschluss ist grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen.“ (6 Ob 140/18h = [RS0132251](#)).

III. **Schlussanträge-EuGH: Konkretisierung des Koppelungsverbots**

Der EuGH beschäftigt sich in der [RS C-61/19 – Orange România SA](#) mit der Frage der Koppelung des Vertragsabschlusses eines Mobilfunkvertrages an die Bereitstellung und Aufbewahrung von Ausweiskopien des Kunden. Generalanwalt Szpunar stellt fest, dass die Beweislast für die Existenz einer Einwilligung (Rechenschaftspflicht) und darüber hinaus auch die Umstände ihres wirksamen Zustandekommens beim Verantwortlichen liegt.

Die aktive, eindeutige, freiwillige Einwilligungshandlung wird im Schlussantrag auch anhand der bereits bestehenden Judikatur der Planet49-Entscheidung konkretisiert; Opt-Out-Lösungen werden endgültig für unzulässig erklärt. Die Bereitstellung einer Ausweiskopie darf nicht den Anschein erwecken, dass sie Teil des Vertrages ist, wenn sie tatsächlich auf einer Einwilligung beruht (Unzulässigkeit der Proforma-Einwilligung).

3. Datenschutzbericht der DSB

Die Datenschutzbehörde hat ihren jährlichen [Datenschutzbericht für das Jahr 2019](#) veröffentlicht. Daraus sind die jeweils geführten Verfahren und die Rechtsmeinung der Behörde ersichtlich. Äußerst spannend erscheint jedoch die rechtliche Beurteilung der aktuellen Gesetzeslage und der Bedarf nach Verbesserungen des Datenschutzgesetzes (DSG).

Anbei einige Auszüge aus dem Bericht:

I. **Unklare sachliche Zuständigkeit für (sonstige) zivilrechtliche Klagen auf Basis der DSGVO**

„So hielt der OGH in seiner Entscheidung vom 23. Mai 2019, 6 Ob 91/19d, fest, dass aus Art. 79 DSGVO ein unmittelbarer Zugang zu einem Zivilgericht abgeleitet werden kann. Das DSG regelt bis dato nur die gerichtliche Zuständigkeit für Schadenersatzklagen (§ 29 DSG). Die Zuständigkeit für (sonstige) zivilrechtliche Klagen auf Basis der DSGVO ist – anders als noch in § 32 DSG 2000 – nicht geregelt. Die genannte Entscheidung des OGH führt nunmehr dazu, dass ein Betroffener sich zur Geltendmachung datenschutzrechtlicher Ansprüche (mit Ausnahme des Schadenersatzes) wahlweise an die DSB (Beschwerde gemäß Art. 77 DSGVO iVm § 24 DSG) oder an ein Zivilgericht (Klage gemäß Art. 79 DSGVO) wenden kann. Um einander widersprechende Entscheidungen zu vermeiden, ist es daher erforderlich, im DSG flankierende Verfahrensbestimmungen vorzusehen (bspw. wechselseitige Aussetzungspflichten der DSB und der Zivilgerichte).“

Fazit: Eine Partei kann die Verletzung ihrer Rechte aus der DSGVO vor der DSB in einem **Beschwerdeverfahren feststellen** lassen. Darüber hinaus ist es möglich, die Verletzung der Rechte aus der DSGVO auch in Form einer **Klage vor Gericht** geltend zu machen. Es handelt sich dabei nur um die **Feststellung der**

Verletzung, ohne parallel einen Schadenersatzanspruch zu begehren.

Dabei ist jedoch nach aktueller Rechtslage offen, vor welchem Gericht zu klagen ist. Eine solche Feststellungsklage kann vor einem Bezirksgericht oder Landesgericht am Wohn- oder Firmensitz des Beklagten (natürliche oder juristische Person) eingebracht werden. Die DSB betont in ihrem Bericht, dass nicht klar ist, ob dabei die Höhe des geltend gemachten Anspruches (sog. Wertzuständigkeit) entscheidend ist oder eine im Gesetz festgelegte Eigenzuständigkeit der Landesgerichte (wie bei Schadenersatzklagen, vgl. § 29 Abs. 2 DSG) zur Anwendung kommt. Dies ist bis dato in keinem nationalen Verfahrensgesetz oder dem DSG geregelt, allerdings ausdrücklich in Art. 79 DSGVO vorgesehen.

II. **2. Unionsrechtswidrigkeit der §§ 12 und 13 DSG**

*„Das BVwG wiederum hat in zwei rezenten Entscheidungen die Gültigkeit von §§ 12 und 13 DSG (Bildverarbeitung) im Lichte der DSGVO in Zweifel gezogen und ausgesprochen, dass – in den konkreten Fällen – für § 13 DSG sowie § 12 Abs. 4 Z 1 DSG keine Öffnungsklausel besteht und diese Bestimmungen daher nicht anzuwenden sind (siehe dazu BVwG, Beschluss vom 20.11.2019, W256 2214855-1, und BVwG, Erkenntnis vom 25.11.2019, W211 2210458-1). Diese Entscheidungen haben weitreichende Auswirkungen. So wird die **DSB, sofern im Einzelfall nicht besondere Gründe dafürsprechen, die §§ 12 und 13 DSG nicht mehr anwenden, sondern Bildverarbeitungen ausschließlich auf Basis der Art. 5 und 6 DSGVO prüfen. Dass eine Bildverarbeitung (in einem Mehrparteienhaus) auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann, hat der EuGH in einem rezenten Urteil (zur Rechtslage nach der Richtlinie 95/46/EG)***

bestätigt (EuGH, Urteil vom 11.12.2019, C-708/18).

Eine Bildverarbeitung entspricht demgemäß nur dann der DSGVO, wenn sie zumindest auf einen Tatbestand gemäß Art. 6 Abs. 1 DSGVO (im Regelfall wird nur lit. f in Betracht kommen) gestützt werden kann und alle Vorgaben gemäß Art. 5 Abs. 1 DSGVO erfüllt sind. Dies wird im Rahmen einer Einzelfallbeurteilung zu prüfen sein.“

Fazit: Die bereits bestehenden Kennzeichnungen, die auf die §§ 12 f DSG verweisen, können

aktuell noch beibehalten werden, allerdings bedarf es stets einer Rechtsgrundlage aus dem Katalog des Art. 6 DSGVO. Besteht bereits ein Hinweis auf Art. 6 Abs. 1 lit. f mit einer Erörterung des überwiegenden berechtigten Interesses, gibt es keinen unmittelbaren weiteren Handlungsbedarf. Dies ist auch im Verarbeitungsverzeichnis gem. Art. 30 DSGVO zu berücksichtigen.

Die rechtliche Unsicherheit, die aus dem Wegfall der Bestimmungen resultiert, ist jedoch beträchtlich.

4. Zertifizierungsstellen-Akkreditierungs-VO

Die Datenschutzbehörde hat den Entwurf zur „Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (**Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V**) vorgelegt. Dieser ist unter diesem [Link](#) abrufbar. Das Begutachtungsverfahren ist noch bis 26. Juni 2020 offen. Inhaltlich befasst sich die Verordnung mit dem Aufbau und der Einführung von Zertifizierungsstellen in Österreich. Zurzeit gibt es noch kein Europäisches Datenschutzzertifikat, das die Compliance mit der DSGVO bestätigt.

International bewährt hat sich das [EuroPriSe Datenschutzsiegel](#), bei dem Prof. KommR Pollner sowie drei weitere unserer Mitarbeiter als juristische und technische Gutachter zertifiziert sind. Es wurde bereits an mehrere österreichische Unternehmen vergeben und ist eines der aussichtsreichsten DSGVO-Gütesiegel mit einer europaweiten Zertifizierung.

Nicht mit der ZeStAkk-V zu verwechseln ist die bereits geltende [Überwachungsstellenakkreditierungs-Verordnung \(ÜStAkk-V\)](#), BGBl. II Nr. 264/2019 idgF, die regelt, wie abgeschlossene „Codes of Conduct“ (Branchen-Verhaltensregeln) zu überwachen sind.

Bereits bekannte Codes of Conduct in Österreich gibt es unter anderem seitens der Internet Service Provider, Direktmarketingunternehmen und Garagenbetreiber. Die Arbeit an einem Code of Conduct kann datenverarbeitenden Branchen helfen, gemeinsame Lösungen zu finden und eine einheitliche Vorgehensweise zu schaffen. Aktuell besteht in vielen Branchen noch Rechtsunsicherheit aufgrund individueller Lösungen, die erst im Rahmen der Rechtsprechung der Datenschutzbehörde oder der Gerichte überprüft werden müssen. Ein verbindlicher Code of Conduct bringt wesentliche Vorteile für das gemeinsame Vorgehen und eine unmittelbare Legitimation durch die Datenschutzbehörde.

5. Corona-Update

Die Corona-Krise hat eine große Welle an Herausforderungen, allerdings auch Chancen in vielen Unternehmen ausgelöst. Das Potenzial von Home-Office für einen Großteil der Mitarbeiter hat viele Prozesse intern sowie extern digitalisiert.

I. *To-Dos*

Die Erweiterung der Datenverarbeitung durch den Einsatz von Home-Office-Tools bedingt organisatorische Maßnahmen im Rahmen der Datenschutz-Dokumentation. Neben der Adaption der Verarbeitungsverzeichnisse um zusätzlich verarbeitete personenbezogene Daten von Mitarbeitern ist auch die Art. 13- bzw. Art. 14-Erklärung zu ergänzen, sofern diese nicht schon vorher berücksichtigt wurden.

Der Einsatz neuer Dienste erfordert zudem den Abschluss von Auftragsverarbeitungsvereinbarungen bzw. bei Auftragsverarbeitern aus Drittstaaten den Abschluss von EU-Standardvertragsklauseln.

Bereits bestehende Prozesse sollten in jedem Datenschutz-Management stetig evaluiert und Änderungen berücksichtigt werden.

II. *Checkliste Home-Office*

Prof. KommR Pollirer hat in der nächsten Ausgabe der Zeitschrift *Datenschutz konkret* (Dako) eine Checkliste für Home-Office im Unternehmen veröffentlicht.

Eine Bestellmöglichkeit finden Sie hier: <https://www.manz.at/Zeitschriften/2313-5409/2020/02.html>

6. DSGVO Praxisseminare finden im September statt

Die Corona-Krise hat deutlich gemacht, dass Datenschutz weiterhin von größter Wichtigkeit ist, sodass wir auch dieses Jahr unsere bewährten [Praxisseminare](#) anbieten möchten. Das Seminar „Rechtsentwicklung und Best Practices“ mit dem rechtlichen Schwerpunkt findet am **23. September 2020** statt.

Das Praxisseminar „Praxisnahe Updates zu Datenschutz und IT-Sicherheit“ mit Schwerpunkt auf technischen Umsetzungsmaßnahmen, Erläuterungen zu TOM und offenen Fragen der Informationssicherheit findet nun am **24. September 2020** statt.

Bestehende Anmeldungen gelten auch für die neuen Termine weiter und es sind noch Plätze verfügbar. Der Veranstaltungsort wird ausreichend Platz für den einzuhaltenden Sicherheitsabstand bieten.

Sollten Sie eine Inhouse-Schulung wünschen, können Sie sich jederzeit an uns wenden. Zudem bieten wir auch Schulungen für Führungskräfte und Mitarbeiter im Umgang mit Datensicherheit an, um richtig auf Datenschutzvorfälle reagieren zu können und bei Datenschutzfragen eine Antwort parat zu haben.

7. Immer auf dem Laufenden bleiben

- **BGH Urteil Planet49**

Im Herbst 2019 hat der EuGH mit der Entscheidung in der RS Planet49 zu einer Zäsur in der Welt der Online-Tracker und digitalen Marketingtools geführt. Für viele Websites und Datenschutzerklärungen gab es aufgrund des EuGH-Urteils Nachbesserungsbedarf; Konzepte zu Cookies und Trackern mussten an die Rechtsprechung angepasst werden. Die [Urteilsverkündung](#) im Ausgangsverfahren ist für den 28. Mai 2020 geplant.

- **Max Schrems gegen Google**

Der Datenschutzaktivist Max Schrems ist bereits für seine Verfahren in den RS Schrems/Facebook I und II bekannt, die zum Fall des Safe-Harbor Abkommens geführt

haben. Als Geschäftsführer der Datenschutz-NGO „NOYB.eu“ hat er nun die Beschwerde gegen Google veröffentlicht, in der er die Zuweisung einer „Android Advertising ID“ an jeden Android-Nutzer als rechtswidrig einstuft. Es geht insb. um die Frage, auf welcher Rechtsgrundlage diese sog. „AAID“ vergeben wird und wie ein Widerruf/Widerspruch ausgeübt werden kann. Das Verfahren wird in Österreich geführt und könnte zu einer nationalen Entscheidung führen, wenn die Österreichische DSB als federführende Behörde das Beschwerdeverfahren übernimmt.

https://noyb.eu/sites/default/files/2020-05/complaint_aaid_redacted.pdf

8. Neuauflage Praxishandbuch Datenschutzrecht mit Secur-Data-Beteiligung

Wir dürfen Sie über das im Sommer erscheinende Praxishandbuch Datenschutzrecht informieren, zu dem Prof. KommR Pollirer und Frau Mag. Wyrobek insgesamt gleich drei Kapitel beitragen.

Das Praxishandbuch erscheint in der nunmehr 4. Auflage, wurde passend zur DSGVO vollständig überarbeitet und größtenteils neu verfasst.

Es enthält ua:

- Prüfschema zur Zulässigkeit von Datenverarbeitungen,
- Flussdiagramm für Schwellenwertprüfung bei der DSFA
- Praxisanleitungen für die Betroffenenrechte inkl. Checkliste
- Analyse der aktuellen Judikatur zu Einwilligungen inkl. Musterklausel
- Informationssicherheit
- Bilddatenverarbeitung
- Werbemaßnahmen
- Rechtsschutz und Sanktionen
- Arbeitnehmerdatenverarbeitung inkl. Covid-19-Maßnahmen

