Secur-Data Betriebsberatungsges.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

# DSG-Info-Service

August 2018 Ausgabe Nr. 89

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

*Drei Monate sind seit der unmittelbaren Geltung der EU-Datenschutzgrundverordnung vergangen. Mit diesem Datenschutz-Info möchten wir Sie auf die aktuellen Neuerungen im österreichischen Datenschutz sowie auf die aktuelle Rechtsprechung hinweisen.*

*Folgende Themen haben wir für Sie vorbereitet:*

1. *Letzte Änderungen im Datenschutzgesetz (DSG) durch das Datenschutz-Deregulierungsgesetz*
2. *Präsentation der sog. „White List" der Datenschutzbehörde*
3. *Vorstellung des Entwurfs der sog. „Black List" der Datenschutzbehörde*
4. *Updates zur EU E-Privacy Verordnung*
5. *Erstes Erkenntnis der Datenschutzbehörde nach neuer Rechtslage*
6. *EuGH-Urteil der Zeugen Jehovas zum „Dateibegriff"*
7. *BGH-Urteil zum „Digitalen Nachlass" – Datenschutz nach dem Tod?*

## 1. Letzte Änderungen im Datenschutzgesetz

Es wurde viel über das Datenschutz-Deregulierungsgesetz 2018 (BGBl. I Nr. 24/2018), das noch einen Monat vor der unmittelbaren Geltung der DSGVO im Nationalrat beschlossen wurde, diskutiert.

Von den in den Medien dargestellten „Entschärfungen" ist allerdings nur vorsichtigerweise die Rede. Die wesentlichen Punkte des Datenschutz-Deregulierungsgesetzes betreffen die Vorgangsweise der Datenschutzbehörde im Rahmen ihrer Strafbefugnis, Erleichterungen bei der Datenverarbeitung für Medienunternehmen und Journalisten, den Schutz für Geschäfts- und Betriebsgeheimnisse, sowie Einschränkungen für Datenschutz-NGOs.

### *„Beraten statt strafen" (§ 11 DSG)*

Das Prinzip der Verhältnismäßigkeit ist bereits in der DSGVO verankert und spielt dort eine tragende Rolle bei der Strafbemessung. Der österreichische Gesetzgeber hat im neueingefügten § 11 DSG dieses Prinzip nochmals gesetzlich verankert und legt damit ausdrücklich fest, dass vor einer Verhängung der hohen

Strafen der DSGVO eine Prüfung der Verhältnismäßigkeit und Angemessenheit im Einzelfall erfolgen soll. Dies ist in Art. 83 Abs. 2 DSGVO ohnehin schon vorgesehen und wird somit nur nochmals verdeutlicht.

Im Umkehrschluss heißt das natürlich nicht, dass die Datenschutzbehörde alle ihr gemeldeten Verstöße zunächst nur abmahnen wird, sondern, dass eine Einzelfallprüfung erfolgt. Es kann also bereits beim ersten groben Verstoß gegen die DSGVO zur Verhängung von einer hohen Strafe kommen. Es steht der Datenschutzbehörde frei, als unabhängige Behörde zu entscheiden, ob eine Strafe zu verhängen ist und ob diese angemessen und verhältnismäßig ist. Keinesfalls kann man davon ausgehen, dass sämtliche Verstöße der DSGVO nur mit einer Abmahnung getadelt werden. Es ist daher Vorsicht geboten, davon auszugehen, dass man erst als „Wiederholungstäter" den hohen Strafen der DSGVO ausgesetzt ist.

### *Keine Doppelbestrafung (§ 30 Abs. 2 DSG, § 69 DSG)*

Eine tatsächliche Erleichterung hat das Datenschutz-Deregulierungsgesetz im Bereich der verwaltungsrechtlichen Doppelbestrafung gebracht. Zum einen wird nach dem Grundsatz „ne bis in idem" (nicht zweimal in derselben [Sache]) eine Doppelbestrafung durch die Datenschutzbehörde verhindert, wenn bereits eine andere Verwaltungsbehörde in derselben Sache eine Strafe verhängt hat.

Zum anderen werden die sog. verantwortlichen Beauftragten des § 9 VStG (Verwaltungsstrafgesetz) nicht zusätzlich zur juristischen Person für denselben Verstoß bestraft. Dies ist insofern eine begrüßenswerte Klarstellung, da dieser für verwaltungsstrafrechtliche Verstöße zur Verantwortung gezogen wird, worunter auch Strafen nach der DSGVO fallen.

Zusätzlich wird in § 69 DSG ausdrücklich das „Günstigkeitsprinzip" festgelegt, das besagt, dass Verstöße, die vor dem 25. Mai 2018 begangen wurden, nach der Rechtslage beurteilt werden, die für den Verursacher günstiger sind.

### *Medienunternehmen und Journalisten wird Datenverarbeitung erleichtert (§ 9 Abs. 1 DSG)*

Werden Daten zu journalistischen Zwecken durch Medienunternehmen oder Mediendienste verarbeitet, finden ein Großteil der Normen des Datenschutzgesetzes sowie der DSGVO keine Anwendung. Die Datenschutzbehörde hat dabei das Redaktionsgeheimnis zu beachten und im Zweifel der Meinungs- und Informationsfreiheit Vorrang vor dem Recht auf Datenschutz zu gewähren. Dies ist eine bemerkenswerte Ausnahme, die sich auch in anderen Materiengesetzen wiederfindet, hier allerdings explizit Eingang in das neue Datenschutzgesetz gefunden hat.

### *Geschäfts- und Betriebsgeheimnisse hindern Auskunftsrecht (§ 4 Abs. 5 DSG)*

Betroffenen kann das in Art. 15 DSGVO verankerte kostenlose Auskunftsrecht verweigert werden, wenn der Verantwortliche oder Dritte dadurch Geschäfts-bzw. Betriebsgeheimnisse offenbaren müsste bzw. diese durch die Auskunftserteilung an eine betroffene Person gefährdet würden. Der österreichische Gesetzgeber nutzt damit die Öffnungsklausel des Art. 23 DSGVO und schränkt das Betroffenenrecht insoweit ein, als der Verantwortliche begründen muss, wieso hier Geschäfts- oder Betriebsgeheimnisse von sich oder einem Dritten gefährdet werden.

### *Keine Abtretung von Schadenersatzansprüche an Datenschutz-NGOs (§ 28 DSG)*

Datenschutzorganisationen ohne Gewinnerzielungsabsicht können im Namen betroffener Personen keine Schadenersatzansprüche mehr geltend machen. Organisationen wie beispielsweise von Max Schrems gegründeten NGO „*NOYB*" wird somit die Möglichkeit genommen die kollektive Geltendmachung von Ansprüchen auf Schadenersatz gegen Verant-

wortliche und Auftragsverarbeiter wahrzunehmen. Dies ist insoweit bemerkenswert, da diesen Organisationen weiterhin offensteht, Beschwerde an die Datenschutzbehörde sowie das Bundesverwaltungsgericht im Namen von betroffenen Personen einzureichen. Schadenersatzklagen wurde durch das Datenschutz-Deregulierungsgesetz jedoch explizit die Möglichkeit von Gemeinschaftsklagen ausgeschlossen.

## 2. Datenschutzbehörde veröffentlicht „White List“ als Verordnung über Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)

Die DSGVO sieht vor, dass bei einer Form der Datenverarbeitung, die nach Art, Umfang, Umständen und Zwecken ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, eine sogenannte „Datenschutz-Folgenabschätzung“ (DSFA) durchzuführen ist. Die nationalen Datenschutzbehörden sind ermächtigt, Listen von Verarbeitungsvorgängen zu erstellen, für die eine Datenschutz-Folgenabschätzung jedenfalls durchzuführen ist („*Black List*“), oder nicht erforderlich ist („*White List*“).

Die Österreichische Datenschutzbehörde hat pünktlich zum Geltungstag der Datenschutzgrundverordnung die sog. *„White List“* veröffentlicht, die als Datenschutz-Folgenabschätzung-Ausnahme-Verordnung (DSFA-AV, BGBl. II Nr. 108/2018) gestaltet wurde. Die darin umfassten Datenverarbeitungsvorgänge sind gem. Art. 35 Abs. 1 und 5 DSGVO von einer Datenschutz-Folgenabschätzung ausgenommen.

Großteils orientiert sich die White List an der ehemaligen Standard- und Musterverordnung (StMV 2004), die bereits eine Vielzahl an Datenanwendungen enthielt, für die keine bzw. eine stark vereinfachte Meldepflicht an das Datenverarbeitungsregister (DVR) bestand.

Nachdem das Datenverarbeitungsregister aufgelassen wurde und keine Meldepflichten mehr bestehen, ist es Aufgabe des Verantwortlichen zu entscheiden, ob eine Folgenabschätzung notwendig ist und diese gegebenenfalls auch durchzuführen. Das Fehlen einer Datenschutz-Folgenabschätzung bzw. einer angemessenen Begründung, weshalb auf die Durchführung einer DSFA verzichtet werden kann, kann ebenfalls Strafen der Datenschutzbehörde auslösen.

Anders als bei der Standard- und Musterverordnung nennt die *White List* keine konkreten Datenkategorien (wie *Name, Adresse, Kontodaten*), sondern beschreibt die Datenverarbeitungsvorgänge ihrem Zweck nach.

Weiters bleiben Datenanwendungen von einer Datenschutz-Folgenabschätzung ausgenommen, die von der Datenschutzbehörde im Rahmen eines Vorabkontrollverfahrens im ehemaligen Datenverarbeitungsregister (DVR) genehmigt wurden sowie jene, die bereits vor dem 24. Mai 2018 gem. § 17 Abs. 2 Z 6 DSG 2000 nicht meldepflichtig waren.

Wir haben für Sie die Datenverarbeitungsvorgänge der neuen Datenschutz-Folgenabschätzung-Ausnahme-Verordnung (DSFA-AV) der ehemaligen Standard- und Musterverordnung gegenübergestellt, damit Sie sich orientieren können, ob Ihre Datenverarbeitung einer Ausnahme unterliegt.

Sollten Sie sich nicht sicher sein, ob Ihre Datenwendung sich unter den angeführten Verarbeitungstätigkeiten wiederfindet, beraten wir Sie gerne.

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| **DSFA-A01** | **Kundenverwaltung, Rechnungswesen, Logistik, Buchführung**<br>Verarbeitung personenbezogener Daten im Rahmen jeglicher Geschäftsbeziehung mit Kunden und Lieferanten samt systematischer Aufzeichnung aller die Einnahmen und Ausgaben betreffenden Geschäftsvorgänge.<br>Verarbeitungstätigkeiten von Unternehmen, die Daten über Dritte verarbeiten (keine Kunden des Verantwortlichen), mit denen die Unternehmen in keiner Geschäftsbeziehung stehen (etwa Detektivbüros, Inkassobüros oder Kreditauskunfteien), sind von dieser Ausnahme nicht umfasst. | Ehemalige SA001 |
| **DSFA-A02** | **Personalverwaltung**<br>Verarbeitung und Evidenthaltung personenbezogener Daten für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist;<br>Verarbeitung und Evidenthaltung dienstrechtlicher, besoldungsrechtlicher, ausbildungsbezogener und sonstiger mit dem Beschäftigungsverhältnis in unmittelbarem Zusammenhang stehender personenbezogener Daten von öffentlich Bediensteten und sonstigen von Verantwortlichen des öffentlichen Bereichs besoldeten Personen (wie zB von Beamten, Vertragsbediensteten, Personen in Ausbildung, Aushilfskräften, aber auch von Abgeordneten und Funktionären) sowie von Volontären und Zivildienern (jeweils ohne Entgeltbezug) durch die Dienstbehörden und Personalstellen zum Zweck von Einzelpersonalmaßnahmen und statistischer Auswertungen;<br>Verarbeitung und Evidenthaltung personenbezogener Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden.<br>Eine Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 und eine Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO im Rahmen dieser Ausnahme sind ausschließlich aufgrund einer gesetzlichen Ermächtigung oder aufgrund rechtlicher Verpflichtungen zulässig. | Ehemalige SA002 |
| **DSFA-A03** | **Mitgliederverwaltung**<br>Führung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen und Personengemeinschaften sowie Betreuung von Mitgliedern und Förderern. | Ehemalige SA003 |

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| **DSFA-A04** | **Kundenbetreuung und Marketing für eigene Zwecke**<br>Verarbeitung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot sowie zur Durchführung von Werbemaßnahmen und Newsletter-Versand. | Ehemalige SA022 |
| **DSFA-A05** | **Sach- und Inventarverwaltung**<br>Inventarverwaltung (Führung von Inventaraufzeichnungen), Unterstützung des Sachgüteraustausches und der Betriebsabrechnung, mit der Inventarverwaltung in Zusammenhang stehende Neben- und Hilfsaufzeichnungen über Lieferanten, Anschaffungskosten sowie Verwaltung der Zuteilung von Hard- und Software an EDV-Systembenutzer. | Ehemalige SA014 (für öffent. Auftraggeber) |
| **DSFA-A06** | **Register, Evidenzen, Bücher**<br>Verarbeitung personenbezogener Daten im Rahmen von durch Unions-, Bundes- oder Landesrecht eingerichteten Registern, Evidenzen oder Büchern, sofern keine personenbezogenen Daten im Sinne der Art. 9 und 10 DSGVO verarbeitet werden. | Ehemalige SA008ff bis SA012 |
| **DSFA-A07** | **Zugriffsverwaltung für EDV-Systeme**<br>Verwaltung von Benutzernamen und Passwörtern sowie Systemzugriffsprotokollierung. | Ehemalige SA007 |
| **DSFA-A08** | **Zutrittskontrollsysteme**<br>Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt verarbeiten, wobei keine biometrischen Daten von Betroffenen verarbeitet werden. Die bloße Echtzeitwiedergabe von Gesichtsbildern ist von dieser Ausnahme umfasst. | Ehemalige MA002 |
| **DSFA-A09** | **Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)**<br>1. Allgemeine Voraussetzungen für die nachfolgenden Ausnahmen:<br>a) Räumlicher Erfassungsbereich<br>Örtlichkeiten, über welche der Verantwortliche verfügungsbefugt ist. Die Videoüberwachung darf räumlich nicht über die Liegenschaft hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter gemessen von der Grundstücksgrenze des überwachten Objekts. Die Video- | Ehemalige SA032 |

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| | überwachung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.<br><br>b) Speicherdauer<br><br>Aufgenommene personenbezogene Daten sind vom Verantwortlichen spätestens nach 72 Stunden zu löschen, es sei denn eine längere Speicherdauer wurde in einem Gesetz, durch einen behördlichen Rechtsakt, in einer Betriebsvereinbarung oder mit Zustimmung der Personalvertretung ausdrücklich festgelegt.<br><br>c) Kennzeichnung<br><br>Voraussetzung für die Ausnahme ist die geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.<br><br>2. Zweck der Datenverarbeitung:<br><br>A. Einfamilienhaus samt Grundstück, eigene Wohnung<br><br>Bild- und Akustikverarbeitungen, welche dem vorbeugenden Schutz von Personen oder Sachen auf privaten, zu Wohnzwecken dienenden Liegenschaften, die ausschließlich vom Verantwortlichen und von allen im gemeinsamen Haushalt lebenden Nutzungsberechtigten genutzt werden, dienen. Voraussetzung ist die Einwilligung aller Nutzungsberechtigten.<br><br>B. Allgemein zugängliche Örtlichkeiten, die dem Hausrecht des Verantwortlichen unterliegen<br><br>Bild- und Akustikverarbeitungen, welche für den vorbeugenden Schutz von Personen oder Sachen an allgemein zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich sind und kein gelinderes geeignetes Mittel zur Verfügung steht. In Fällen, in denen Arbeitnehmervertretungen zu bilden sind, ist das Vorliegen einer gültigen Betriebsvereinbarung oder einer gültigen Zustimmung der Personalvertretung, welche die Durchführung der Videoüberwachung regeln, Voraussetzung.<br><br>Keine Anwendung findet diese Ausnahme auf Örtlichkeiten, welche aufgrund eines bestehenden Kontrahierungszwanges oder aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen. | |
| **DSFA-A10** | **Bild- und Akustikdatenverarbeitung in Echtzeit**<br><br>1. Allgemeine Voraussetzungen für die nachfolgende Ausnahme:<br><br>a) Räumlicher Erfassungsbereich | |

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| | Örtlichkeiten, über welche der Verantwortliche verfügungsbefugt ist. Die Bilddatenverarbeitung darf räumlich nicht darüber hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter. Die Bild- und Akustikdatenverarbeitung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen.<br>b) Kennzeichnung<br>Voraussetzung für die Ausnahme ist die geeignete Kennzeichnung der Bildverarbeitung durch den Verantwortlichen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen.<br>2. Zweck der Datenverarbeitung:<br>Bild- und Akustikübertragungen ohne Aufzeichnung. | |
| **DSFA-A11** | **Bild- und Akustikverarbeitungen zu Dokumentationszwecken**<br>Bild- und Akustikverarbeitungen, welche ausschließlich ein Dokumentationsinteresse verfolgen, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist. Strafrechtliche, verwaltungsstrafrechtliche oder zivilrechtliche Zwecke dürfen im Rahmen dieser Ausnahme nicht verfolgt werden. | |
| **DSFA-A12** | **Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken**<br>Patientenverwaltung und Honorarabrechnung von einzelnen Ärzten, Zahnärzten und Dentisten sowie Patienten-/Klientenverwaltung und Honorarabrechnung anderer freiberuflich oder gewerblich einzeln tätiger Gesundheitsdiensteanbieter und Apotheken. | Ehemalige SA024 |
| **DSFA-A13** | **Rechts- und Beratungsberufe**<br>Datenverarbeitung von rechtsberatenden und unternehmensberatenden Berufen, wie einzelne Rechtsanwälte, Notare, Patentanwälte, Wirtschaftstreuhänder, Steuerberater und Unternehmensberater im Rahmen ihrer Berufsausübung. | NEU |

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| **DSFA-A14** | **Archivierung, wissenschaftliche Forschung und Statistik**<br>Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke aufgrund besonderer gesetzlicher Vorschriften oder mit Einwilligung der betroffenen Person. | NEU |
| **DSFA-A15** | **Unterstützungsbekundungen**<br>Verarbeitung personenbezogener Daten im Rahmen von Bürgerinitiativen, Petitionslisten oder Unterschriftensammlungen durch die Organisatoren. | Ehemalige SA034 |
| **DSFA-A16** | **Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts**<br>Erstellung von Voranschlägen, Finanzbuchführung, Zahlungsverkehr, Erstellung von Berichten, Betriebsabrechnungen, Neben- und Hilfsbuchführungen und Auswertung der Daten zur Budgetkontrolle, zu strategischem Controlling und zur Liquiditätssteuerung, Abschlussrechnungen, Jahresabschlüsse sowie Abschlussprüfungen und Rechnungsprüfungen. | Ehemalige SA005 |
| **DSFA-A17** | **Öffentliche Abgabenverwaltung**<br>Vorschreibung, Einhebung und Abrechnung von öffentlich-rechtlich geregelten Abgaben und Gebühren durch Bund, Länder, Gemeinden, Gemeindeverbände und sonstige Körperschaften des öffentlichen Rechts sowie deren Kontrolle. | Ehemalige SA004 |
| **DSFA-A18** | **Förderverwaltung**<br>Verarbeitung personenbezogener Daten durch Fördergeber und auszahlende Stellen im Rahmen der Abwicklung öffentlicher Förderungen, sofern keine personenbezogenen Daten im Sinne der Art. 9 und 10 DSGVO verarbeitet werden. | NEU |
| **DSFA-A19** | **Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate**<br>Verarbeitung von Daten Anfragender im Rahmen des Auskunftspflichtgesetzes, der Öffentlichkeitsarbeit und Informationstätigkeit, einschließlich automationsunterstützt erstellter und aufbewahrter Textdokumente in diesen Angelegenheiten;<br>Verarbeitung von Daten zu informierender Personen, sofern aufgrund einer Vielzahl von Anfragen zu einem bestimmten Thema ein allgemeines Bedürfnis an Informationen besteht. | Ehemalige SA030 |

| Nr. | Bezeichnung und Zweck | Entspricht StMV 2004 |
|---|---|---|
| **DSFA-A20** | **Aktenverwaltung (Büroautomation) und Verfahrensführung**<br>Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit angefallenen Dokumente, Abrechnung von Gebühren, Organisation von Großverfahren). | Ehemalige SA029 |
| **DSFA-A21** | **Organisation von Veranstaltungen**<br>Datenverarbeitung zur Abhaltung von Veranstaltungen im öffentlichen und privaten Bereich, wie Einladung und Registrierung der Teilnehmer, Organisation von Reisen und Aufenthalten, Versorgung der Teilnehmer und Kommunikation vor und nach der Veranstaltung, Abrechnung von Geldleistungen (Honorare, Ersatz für Reisekosten), Abwicklung von Kulturprogrammen, Übermittlung von Unterlagen sowie Anfertigung von im Zusammenhang mit der Veranstaltung stehenden Bild- und Akkustikaufnahmen. | NEU |
| **DSFA-A22** | **Preise und Ehrungen**<br>Datenverarbeitung zur Verleihung von Preisen und Ehrenzeichen oder ähnlicher Auszeichnungen, einschließlich der damit verbundenen Vorprüfungen. | NEU |

## 3. „Black List“ in Begutachtung

Wie bereits erwähnt, müssen die nationalen Datenschutzbehörden auch eine Liste jener Datenverarbeitungsvorgänge erstellen, für die in jedem Fall eine Datenschutz-Folgenabschätzung durchzuführen ist. Es gibt bereits einen Entwurf der sog. *„Black List“*, der sich aktuell noch in Begutachtung befindet. Aufgrund des verpflichtend anzuwendenden Kohärenzverfahrens, das besagt, dass die nationalen Aufsichtsbehörden miteinander im Rahmen des Datenschutz-Ausschusses gemeinsam abgestimmte Listen festlegen, ist noch nicht abzusehen, welche Veränderungen der Entwurf erhalten wird. Für einen ersten Einblick dürfen wir Sie auf die in Deutschland bereits erlassenen „Black Lists“ verweisen.

Das Kohärenzverfahren besagt, dass die nationalen Aufsichtsbehörden gemeinsam abstimmen sollen, welche Datenverarbeitungsvorgänge in die *„Black List“* fallen und somit ein einheitliches Datenschutzniveau gewährleistet ist. Dieses Verfahren findet jedoch im Datenschutz-Ausschuss statt, der abseits der Öffentlichkeit tagt. Zudem haben noch nicht alle Aufsichtsbehörden eine solche *„Black List“* vorgelegt.

**Landesdatenschutzbehörde Nordrhein-Westfalen:**
https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSFA-Muss-Liste-1_0.pdf

**Landesdatenschutzbehörde Baden-Württemberg:** https://www.baden-

wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf

**Landesdatenschutzbehörde Brandenburg:**
https://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss_Liste_allgemein_180710.pdf

Sobald die Verordnung durch die österreichische Datenschutzbehörde erlassen wurde, informieren wir Sie selbstverständlich auch über deren Inhalt.

# 4. Updates zur E-Privacy Verordnung

Das nächste große europäische Projekt auf legislativer Ebene ist die sog. E-Privacy Verordnung, die wie die DSGVO in allen Mitgliedsstaaten unmittelbare Geltung erhalten soll. Sie soll die Richtlinie 2002/58/EG (Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)) sowie die ergänzende Richtlinie 2009/136/EG ablösen.

Sie soll als sog. „lex specialis", also Spezialverordnung zur Datenschutzgrundverordnung gelten, behandelt das Setzen von Cookies und Trackern sowie die Datenverarbeitung zu Werbezwecken und enthält außerdem Regelungen für die Telekommunikationsbranche. Ziel ist unter anderem, den Betroffenen eine explizite Opt-In Möglichkeit zu geben, um der Datenverarbeitung zuzustimmen. Das stellt nicht nur Unternehmen vor neue Herausforderungen, sondern auch die Betroffenen, die über das neue Regulativ erneut informiert werden müssen und nun aktiv handeln sollen.

Die bisherige Aktenlage lässt sich als „*lebendes Dokument*" in Form eines Arbeitspapieres beschreiben, da sich der Entwurf erst im Europäischen Trilog-Verfahren befindet. Dennoch wird der Vorschlag ebenso kontrovers diskutiert wie seinerzeit die DSGVO. Ob es noch während der Österreichischen Ratspräsidentschaft (1. Juli bis 31. Dezember 2018) zu einer finalen Lösung kommen wird, bleibt weiterhin offen, ist allerdings zu bezweifeln.

Wir möchten Ihnen den vorläufigen Zwischenstand der bisherigen Verhandlungen vorstellen, der in Form einer Stellungnahme am 10. Juli 2018 (10.07.2018 [2017/0003 (COD)], Austrian Presidency Council Document 10975/18[1]) ergangen ist.

### *I. Art. 6 E-Privacy Verordnung*

Zum einen soll Artikel 6 E-Privacy Verordnung, dessen Inhalt die erlaubte Verarbeitung elektronischer Kommunikationsdaten behandelt, geändert werden. Mit Kommunikationsdaten sind sowohl jene Daten gemeint, die elektronische Kommunikationsnetz-Betreiber- und Diensteanbieter generieren, als auch Kommunikationsmetadaten, also wer, wann, wo mit wem elektronisch kommuniziert hat. Von der erlaubten Verarbeitung weiters umfasst wären auch Kommunikationsinhalte, d.h. welche Bilder, Musik, Sprachnachrichten etc. elektronisch versendet und empfangen werden.

Aus dem Vorschlag vom 10. Juli 2018 geht hervor, dass Anbietern von Kommunikationsdiensten erlaubt werden soll, Metadaten auch ohne Einwilligung der Betroffenen zu sammeln. Der Zweckbindungsgrundsatz soll dahingehend durchbrochen werden, dass die Verarbeitung auch für andere Zwecke als die ursprünglich vorgesehenen stattfinden darf.

[1] http://data.consilium.europa.eu/doc/document/ST-10975-2018-INIT/en/pdf

Netzbetreiber wie A1, Telekom, UPC und andere, aber auch elektronische Kommunikationsdiensteanbieter wie WhatsApp, Facebook-Messenger und Skype, könnten damit weitgehende Analysen des Kommunikationsverhaltens ihrer Nutzer zu Werbezwecken rechtfertigen. Voraussetzung dafür soll sein, dass der neue Verwendungszweck „kompatibel" mit dem ursprünglichen Zweck ist, und dass die Daten pseudonymisiert werden (siehe Art. 6 Abs. 2a (neu)).

*2a. Where the processing for a **purpose other than that for which the electronic communications metadata have been collected is not based on the end-user's consent** or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11**, the provider shall,** in order to ascertain whether processing for another purpose is **compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:***

*(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;*

*(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;*

*(c) the nature of the electronic communications metadata, in particular where such data could reveal categories of data, pursuant to Article 9 of Regulation (EU) 2016/679;*

*(d) the possible consequences of the intended further processing for end-users;*

*(e) the existence of appropriate safeguards.*

*Such processing, **if considered compatible, may only take place, provided that:***

- *the processing **could not be carried out** by processing information **that is made anonymous,** and electronic communications metadata **is erased or made anonymous** as soon as it is no longer needed to fulfil the purpose, **and***
- *the processing is limited **to electronic communications metadata that is pseudonymised,***
- *the electronic communications metadata **is not used** to **determine the nature or characteristics** of an **end-user or to build a profile of an end-user**.*

### *II. Art. 8 E-Privacy Verordnung*

Im aktuellen Vorschlag wird zudem eine Klarstellung zum Verhältnis des Artikel 8 zu Erwägungsgrund 20 der EU E-Privacy Verordnung vorgeschlagen. Inhaltlich behandelt dieser Artikel die Erlaubnistatbestände der Verarbeitung von Informationen aus Endeinrichtungen wie Browsern und Mobilgeräten (Hardware und Software), sowie die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, um mit anderen Geräten oder Netzanlagen zu kommunizieren. Damit gemeint sind Cookies und (Retargeting)-Tracker in den Endgeräten. Grundsätzlich ist das Verwenden der Verarbeitungs- und Speicherfunktionen in Endeinrichtungen untersagt. Als Erlaubnistatbestände werden weiterhin die Nutzung für Übertragungs- und Sicherheitszwecke sowie die Messung des Web-Publikums genannt, aber auch die Einwilligung des Endnutzers. Sofern eine Verarbeitung auf der Einwilligung des Endnutzers beruht, ist sie jederzeit widerrufbar. Die EU E-Privacy-Verordnung verweist zudem auf die Informationspflichten des Art. 13 DSGVO, die technischen und organisatorischen Sicherheitsmaßnahmen des Art. 32 sowie das jederzeitige Widerrufsrecht des Art. 7 Abs. 3 DSGVO.

Allerdings besagt Erwägungsgrund 20 der EU E-Privacy-Verordnung, dass es zulässig sein

kann, den Zugang zu einer Website von der Einwilligung des Endnutzers zum Setzen von Cookies für zusätzliche Zwecke abhängig zu machen. Dies gilt insbesondere dann, wenn er einem kostenlosen Angebot wählen kann, das seine Einwilligung zu zusätzlichen Cookies beinhaltet, und einem gleichwertigen (aber bezahlpflichtigen) Angebot desselben Betreibers, bei dem keine weiteren Cookies gesetzt werden. Dies steht im Widerspruch zum Koppelungsverbot und der freien, informierten Einwilligung des Endnutzers gem. Art. 7 Abs. 4 DSGVO.

Die Änderung des Erwägungsgrund 20 würde lauten:

*„Not all cookies are needed in relation to the purpose of the provision of the website service. Some are used to provide for additional benefits for the website operator. Making access to the website content provided without direct monetary payment conditional to the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate in particular if the end-user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other hand. Conversely, in some cases, making access to website content conditional to consent to the use of such cookies may be considered to be disproportionate. This would normally be the case for websites providing certain services, such as those provided by public authorities, where the user could be seen as having few or no other options but to use the service, and thus having no real choice as to the usage of cookies."*

### *III. Art. 10 E-Privacy Verordnung*

Die gewünschte Streichung des Artikel 10 EU E-Privacy Verordnung *„Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre"* hat nun Eingang in den Vorschlag der Österreichischen Ratspräsidentschaft gefunden. Inhaltlich geht es um Browsereinstellungen, die bereits bei der Installation die Einwilligung des Nutzers zu Cookies, Trackern und anderen Identifiern abfragen sollen. Die ursprüngliche Intention des Art. 10 EU E-Privacy Verordnung war die Eindämmung der sog. „Cookie-Banner" und die Durchsetzung von datenschutzfreundlichen Voreinsteillungen *„Privacy by default"*, wie sie auch in Art. 25 DSGVO zu finden sind.

Im aktuellen Arbeitspapier wird dieser Mechanismus allerdings aus der Verordnung gestrichen. Als Hauptgründe dafür werden die technischen Umsetzungsprobleme für Browser- und App-Hersteller genannt, sowie ein verzerrtes Wettbewerbsverhältnis zu Lasten des europäischen Marktes durch voraussichtliche Wettbewerbsnachteile. Weiters stellt sich die Österreichische Ratspräsidentschaft die Frage, wie eine Nicht-Einhaltung zu sanktionieren ist und welche Auswirkungen solche Voreinstellungen auf die Endnutzer haben werden, da diesfalls von deren Seite ein aktives Handeln (Opt-in) verlangt wird. Die Ratspräsidentschaft spricht dabei von einer *„Einwilligungs-Müdigkeit"* (*consent fatigue)* der Endnutzer, für die dieser Mechanismus keine nennenswerte Verbesserung bewirken würde. Aus Industrie-Sicht könnte damit ein Artikel gestrichen werden, der schon seit Beginn des Verordnungs-Vorschlags im Zentrum der Kritik stand.

Folgender Text des Art. 10 EU E-Privacy Verordnung soll gestrichen werden:

(1) *In Verkehr gebrachte Software, die eine elektronische Kommunikation erlaubt, darunter auch das Abrufen und Darstellen von Informationen aus dem Internet, muss die Möglichkeit bieten zu verhindern, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endein-*

*richtung gespeicherte Informationen verarbeiten.*

(2) *Bei der Installation muss die Software den Endnutzer über die Einstellungsmöglichkeiten zur Privatsphäre informieren und zur Fortsetzung der Installation vom Endnutzer die Einwilligung zu einer Einstellung verlangen.*

(3) *Bei Software, die am 25. Mai 2018 bereits installiert ist, müssen die Anforderungen der Absätze 1 und 2 zum Zeitpunkt der ersten Aktualisierung der Software, jedoch spätestens ab dem 25. August 2018 erfüllt werden.*

## 5. Erstes Erkenntnis der Datenschutzbehörde nach DSGVO

Die Datenschutzbehörde hat am 21. Juni 2018 ihr erstes Erkenntnis (GZ: DSB-D122.844/0006-DSB/2018) nach neuer Rechtslage getroffen. Der Sachverhalt war noch nach den Bestimmungen des DSG 2000 anhängig gemacht worden, wurde allerdings gem. § 69 Abs. 4 DSG nach DSGVO entschieden.

Inhaltlich ging es um einen Bankkunden, der von seiner Bank die Zusendung von Kontoauszügen aus den Jahren 2013 bis 2018 begehrte, da innerhalb seines Online-Bankings, sein individueller Zugriff nur auf ein Jahr zurückdatieren konnte, ohne dass er die gewünschten Zeiträume angezeigt bekam.

Nachdem er zunächst eine Anfrage an die Bank geschickt hatte, verwies diese ihn auf eine Vergebührung für Entgeltnachweise, die über ein Jahr hinausgehen. Daraufhin stellte der Beschwerdeführer ein Auskunftsbegehren nach den Bestimmungen des damaligen DSG 2000, das die Bank unbeantwortet ließ. Nach Ablauf der Frist wandte sich der Beschwerdeführer an die Datenschutzbehörde, um seinen Auskunftsanspruch gem. § 26 DSG 2000 (nun Art. 15 DSGVO) geltend zu machen. Die Bank berief sich im Verfahren auf die bereits zur Verfügung gestellten Kontoauszüge gem. Zahlungsdienstegesetz, die in Umsetzung der Zahlungsdienste-Richtlinie erfolgt seien.

Kern dieser Entscheidung ist die Frage, ob eine Bank sich auf ein anderes Gesetz stützen kann, dass die datenschutzrechtlichen Betroffenenrechte in den Hintergrund stellt.

Die Datenschutzbehörde stellte fest, dass der Grundsatz, dass eine speziellere materielle Regelung nach dem Rechtsgrundsatz „lex specialis derogat legis generalis“, der allgemeinen durchaus vorgehen kann. Im gegenständlichen Fall seien allerdings die Bestimmungen des Zahlungsdienstegesetzes (ZaDig 2018) nicht als speziellere materielle Regelungen verfasst, sondern verweisen explizit auf die Bestimmungen der damals noch geltenden Datenschutz-Richtlinie, die nun auch für die Datenschutzgrundverordnung gelten.

Dem Einwand, dass die Betroffenenrechte somit bereits erfüllt seien und der Beschwerdeführer seine Rechte schikanös ausübe, konnte demnach stattgegeben werden. Vielmehr sei durch das nicht fristgerechte Erteilen des Auskunftsanspruches ein Verstoß gegen Art. 15 DSGVO erfolgt, den die Bank nun erfüllen muss.

Das Erkenntnis zeigt zwei wesentliche Aspekte auf. Zum einen wurde bestätigt, dass einfachgesetzliche Regelungen, sofern sie ein Betroffenenrecht spezieller, also erweiternd regeln, den Bestimmungen der DSGVO vorgestellt werden können. Zum anderen zeigte sich, dass bei Fehlen solche Regelungen das Datenschutzrecht als legitimes Mittel verwendet werden kann, um ggf. auch kostenpflichtige Dienstleistungen hinsichtlich eines Auskunftsanspruches ohne Entgelt wahrzunehmen.

## 6. Private Notizen der Zeugen Jehovas unterliegen der DSGVO

Die Notizen, die sich „Verkünder“ der Zeugen Jehovas bei Hausbesuchen machen, unterliegen den Regelungen des Datenschutzes. Dies ist das Ergebnis eines EuGH-Verfahrens, bei dem die finnische Datenschutzbehörde die Erhebung und Verarbeitung dieser Daten zunächst untersagt hatte. Zu beachten ist, dass die Richter in Luxemburg nicht nach der DSGVO entschieden, sondern noch auf Grundlage der alten Datenschutz-Richtlinie (95/46/EG), die auch in Finnland umgesetzt wurde.

Kernthema der Entscheidung (EuGH 10.07.2018, C-25/17) ist der sog. „Dateibegriff, den der EuGH als „Daten [die] nach bestimmten Kriterien so strukturiert sind, dass sie in der Praxis zur späteren Verwendung leicht wiederauffindbar sind“, definiert. Darunter können also gesammelte Visitenkarten, Notizzettel aus Personalgesprächen oder andere gesammelte personenbezogene Daten fallen, die wenngleich nicht automatisiert, strukturiert und leicht zu finden sind. Damit wird der Dateibegriff im analogen Bereich erheblich erweitert, sodass jede Art von Datenverarbeitung umfasst ist, denen eine Sortier-Systematik zu Grunde liegt.

Die Richter stellten fest, dass die Erhebung und Verarbeitung nicht unter die Ausnahmebestimmungen der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten fällt, selbst dann, wenn es sich um persönliche Notizen der jeweiligen „Verkünder“ in ihren eigenen Büchern handelt, die auch nicht mit der Gemeinschaft geteilt werden.

Vielmehr sei die Religionsgemeinschaft als Verantwortlicher iSd der Datenschutz-Richtlinie anzusehen, auch wenn diese „keinerlei Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat“.

Abschließend lässt sich das Erkenntnis als erneute Erweiterung des Dateibegriffs sehen, die auch die nicht automatisierte Verarbeitung umfasst. Sofern Daten auf strukturierte Art erhoben und verarbeitet werden, ist die Information und Einwilligung der Betroffenen notwendig, um als rechtmäßig zu gelten.

## 7. BGH-Urteil zum „Digitalen Nachlass“ – Datenschutz nach dem Tod?

In Deutschland ist ein junges Mädchen im Alter von 15 Jahren verstorben und die Hintergründe ihres Todes lassen Fragen offen. Aus diesem Grund wollten die Eltern der Verstorbenen, insbesondere wegen des Verdachts auf Suizid wegen Mobbings, Zugriff auf das Facebook-Konto erhalten, um mögliche Hintergründe des Todes in Erfahrung zu bringen.

Dies wurde allerdings von Facebook mit dem Argument verwehrt, dass es sich bei dem Nutzungsvertrag zu dem Sozial Netzwerk um ein „höchstpersönlichen Vertrag“ handle, der nach dem Tod des Nutzers Dritten, sei es auch den unmittelbaren Erben, verwehrt bleibe. Dagegen klagten die Eltern (BGH 12.07.2018 - III ZR 183/17) der Verstorbenen, die argumentierten, dass der analoge Nachlass (in Form

von Tagebüchern, Briefen und anderen teils höchstpersönlichen Dokumenten) an die Erben übergeben werden könne, was auch für den sog. „digitalen Nachlass“ gelten müsste.

Es galt also zunächst zu erklären, welche Art von Vertrag zwischen einem Facebook-Nutzer und dem Sozialen Netzwerk geschlossen wird und wie dieser zu qualifizieren sei.

Facebook geht davon aus, dass es sich bei den Inhalten um höchstpersönliche, der Erbmasse vorenthaltene, Güter handle, die auch den Eltern als Erben keinen Zugriff erlauben. Als weiteres Argument wurden datenschutzrechtliche Aspekte vorgebracht, da auch Korrespondenz mit Dritten stattgefunden habe und das Fernmeldegeheimnis als Briefschutz für die Erblasserin und andere gelte.

Rein zivilrechtlich lässt sich davon ausgehen, dass der Nutzungsvertrag zwischen der Verstorbenen und Facebook auf die Erben in Form einer Gesamtrechtsnachfolge übergeht, sofern die Vererblichkeit nicht ausdrücklich ausgeschlossen ist. Danach können also die Erben den Account grundsätzlich auch weiterbetreiben, Facebook schaltet diesen nach Bekanntgabe des Todes eines Nutzers aber in den sog. „Gedenkzustand“, sodass ein Zugriff prinzipiell nicht mehr möglich ist.

Der sog. „Gedenkzustand“ wurde vom Deutschen BGH im Rahmen einer AGB-Kontrolle (§ 307 BGB) als „gröblich benachteiligend“ iSd § 879 Abs. 3 ABGB eingestuft und ist somit auch für den Nutzungsvertrag nichtig. Zur Frage der „höchstpersönlichen Natur“ der Inhalte befand der BGH, dass die Integrität der versendeten Nachrichten und Beiträge nicht personen-, sondern kontobezogen seien und daher auch mit Missbrauch des Zugangs durch Dritte zu rechnen ist, wenn beispielsweise das Passwort „gehackt“ wird. Von einem höchstpersönlichen Charakter, der an die Person des Nutzers gebunden ist, könnte somit keine Rede sein, sondern nur einem kontobezogenen Zugang, der auch – ob zulässig oder unzulässig – durch Dritte erfolgen kann.

Durch die zivilrechtliche Gesamtrechtsnachfolge, also das Eintreten in sämtliche Rechte und Pflichten des Erblassers, besteht auch aus Sicht des Fernmeldegeheimnisses kein Hindernis für einen Zugang zum Facebook-Konto, da die Erben in die gleiche Rechtsposition eintreten und somit nicht als Dritte bezeichnet werden können.

Der datenschutzrechtliche Aspekt ist insofern kein Novum, als für Verstorbene grundsätzlich kein Datenschutz gilt. Verstorbene werden durch das sog. „postmortale Persönlichkeitsrecht“ geschützt, das seine Wurzel jedoch im allgemeinen Zivilrecht hat. In der DSGVO ist der Schutz lebender natürlicher Personen vorgesehen, dem die DSGVO jedoch nationalstaatliche Öffnungsklauseln zur Verfügung stellt. Diese wurden aber weder in Deutschland noch Österreich genutzt, um den Anwendungsbereich auch auf Verstorbene zu erweitern.

Zusammenfassend ist daher der digitale Nachlass insoweit wie der analoge Nachlass zu behandeln. Die deutsche Entscheidung lässt sich hinsichtlich der Bestimmungen für das Erbrecht auf Österreich übertragen, auch aus Sicht des Telekommunikationsgesetzes und der DSGVO stehen dem keine Hindernisse entgegen.

••••

**Rainer Knyrim**

## Der DatKomm Grundwerk

**Praxiskommentar zum Datenschutzrecht, DSGVO und DSG Kommentar in Faszikeln**

Der neue DatKomm – Praxiskommentar zum Datenschutzrecht (DSGVO und DSG) stellt sich den wirklich schwierigen Fragen, die im Zusammenhang mit dem neuen Datenschutzregime auftauchen.

Dem Aufbau der DSGVO folgend werden die jeweils passenden Bestimmungen des österreichischen DSG gleich „mitgenommen". Die Kommentierung bezieht sich auf beide Normen und behandelt inhaltlich sinnvoll verschränkt und tiefgehend die wesentlichen Auslegungsschritte, wichtige Literatur und Judikatur – auch zu bisher geltendem Recht – inklusive.

Anhänge mit Checklisten, Guidelines und Beschlüssen des Datenschutzausschusses, wichtigen Bestimmungen aus Nebennormen, wie zB der RL über Polizei und Strafjustiz, runden den Praxiskommentar ab.


Erarbeitet wird diese fundierte Rechtsinformation von einem 33-köpfigen Autorenteam.

| | |
|---|---|
| **ISBN:** | 978-3-214-17236-7 |
| **Reihe:** | Manz Großkommentare |
| **Verlag:** | MANZ Verlag Wien |
| **Format:** | Sonstige Buchform |
| | 1000 Seiten, Kpl, 2018 |
| **Preis:** | Ca. EUR 198,00 |

Das Werk erscheint im Oktober, die Möglichkeit zur Direktbestellung finden Sie unter www.manz.at

Unser nächstes Seminar

„**DSGVO – Grundlagen und Praxis**"

findet am 19. November 2018 statt.

Es referiert der Mitautor des Standardwerkes zum österreichischen DSG, **Prof. KommR Hans-Jürgen Pollirer** sowie Frau **Mag. Judith Leschanz**.

Außerdem veranstalten wir am 19. und 20. November 2018 den Lehrgang

**„Ausbildung zum internen Datenschutzbeauftragten"**

In diesem Lehrgang werden praxisnah und im kleinen Kreis die Grundlagen für alle wesentlichen Aufgaben des Datenschutzbeauftragten vermittelt.

Anmeldung unter www.secur-data.at oder telefonisch unter (01) 533 42 07-0.