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

Jänner 2019 Ausgabe Nr. 90

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

Während im Jahr 2018 die Implementierung und Einschätzung der neuen Rechtslage nach der DSGVO im Vordergrund stand, wird es in diesem Jahr insbesondere um die Optimierung der getroffenen Maßnahmen gehen. Die österreichische Datenschutzbehörde hat seit dem 25. Mai 2018 bereits einige Erkenntnisse verfasst, die wir Ihnen präsentieren möchten, aber auch beim Bundesverwaltungsgericht sind schon Verfahren zur Datenschutzgrundverordnung anhängig. Mit jeder Entscheidung wird der regulative Rahmen klarer, dies zeigt sich vor allem in der rechtlichen Bewertung von Videoüberwachungsanlagen, die in dieser Ausgabe näher beleuchtet werden.

Der Gesetzgeber ist ebenfalls tätig geworden und hat in der Novelle des Telekommunikationsgesetzes (TKG 2003) u.a. die Schwelle von 50 Empfängern des § 107 Abs. 2 beseitigt.

Als „Spam-Paragraf" gegen Direktwerbung gilt gem. § 107 Abs. 2 TKG 2003 nach wie vor, dass zum Zwecke der Direktwerbung über elektronische Kommunikationsmedien (SMS, E-Mail etc.) die Einwilligung des Betroffenen vorliegen muss. Wenn E-Mail-Adressen oder Telefonnummern ohne Einwilligung der Betroffenen für Werbung oder Marketing genutzt werden, kann sowohl ein Verstoß gegen das Telekommunikations- als auch Datenschutzrecht vorliegen. Der Wegfall der im TKG 2003 willkürlich festgesetzten Schwelle von 50 Empfängern ändert nichts an der bisherigen Rechtslage, dass die Zusendung einer elektronischen Post zum Zweck der Direktwerbung nach wie vor nur mit vorheriger Einwilligung des Empfängers erlaubt ist. Die Zuständigkeit für Verstöße gegen das Telekommunikationsgesetz liegt nicht bei der Datenschutzbehörde, sondern bei der Fernmeldebehörde.

Als weiteres Sondergesetz im mittelbaren Datensicherheitsbereich wurde das Netz- und Informationssystemsicherheitsgesetz (NISG) am 28. Dezember 2018 kundgemacht und ist daher seit 29. Dezember 2018 in Kraft (BGBl. I Nr. 111/2018). Es betrifft Betreiber kritischer Infrastrukturen, die im Laufe des Frühjahres mittels Bescheid über ihre Eigenschaft als „wesentlicher Dienst" in Kenntnis gesetzt werden bzw. Anbieter digitaler Dienste für die eine ex lege Feststellung getroffen wird.

Das NISG setzt die EU-NIS-Richtlinie um und sieht Sicherheitsvorkehrungen und Meldepflichten bei relevanten Sicherheitsvorfällen vor. Das NISG steht in Konkurrenz zur DSGVO und dem TKG 2003, sodass Verstöße nach allen drei Rechtsmaterien geahndet werden können. Die Zuständigkeit für die Verhängung von

Verwaltungsstrafen nach dem NISG liegt wiederum bei den Bezirksverwaltungsbehörden.

Der Gesetzgeber hat allerdings auch legislative Maßnahmen getroffen, um Anonymität zu verhindern. Betroffen sind Erwerber von sog. Pre-Paid Wertkarten, die von Mobilfunkanbietern ausgestellt werden. Seit 1. Jänner 2019 gilt mit der Änderung zum Telekommunikationsgesetz (vgl. § 97 Abs. 1 a TKG 2003) eine Registrierungspflicht für Neukunden von SIM-Karten ohne Vertragsbindung. Für Bestandskunden mit bereits bestehenden Wertkarten gilt eine Übergangsfrist bis 1. September 2019.

Das Ziel des Gesetzgebers lag in der Prävention von organisierter Kriminalität und der Identifizierung der jeweiligen Wertkartenbesitzer. Die Maßnahme trifft Mobilfunk- und Telekommunikationsanbieter, die nun ihre Kunden verifizieren müssen.

1. Judikaturübersicht

Die Datenschutzbehörde hat seit der Geltung der Datenschutzgrundverordnung bereits eine Vielzahl von Erkenntnissen getroffen. Wir haben für Sie einige aufbereitet, die bereits in Rechtskraft erwachsen sind. Der Übersichtlichkeit halber haben wir jeder Entscheidung eine kurze Beschlagwortung vorangestellt.

Zu unterscheiden sind *Beschwerdeverfahren*, wonach eine betroffene Person wegen einer Verletzung des Datenschutzrechtes gegen einen Verantwortlichen tätig wird, und *Verwaltungsstrafverfahren*, wonach die Datenschutzbehörde gegen den Verantwortlichen direkt tätig wird und Bußgelder verhängt.

Bei den hier vorgestellten Entscheidungen handelt es sich um Beschwerdeverfahren vor der Datenschutzbehörde.

I. Speicherdauer von Kommunikationsdaten eines Gläubigerschutzverbandes DSB-D216.580/0002-DSB/2018 vom 28.05.2018 – rechtskräftig.

Recht auf Löschung, Rechtmäßigkeit der Verarbeitung, Speicherdauer, Gläubigerschutzverband, Kontaktdaten, Zweck der Verarbeitung

In der ersten veröffentlichten Entscheidung seit Geltung der DSGVO hatte die Datenschutzbehörde zu entscheiden, ob die Speicherdauer von Kontaktdaten, auch nach Erfüllung des ursprünglichen Erhebungszwecks, fortgesetzt werden kann.

Das Verfahren wurde bereits im November 2017 begonnen und schließlich am 28. Mai 2018 mit dem Erkenntnis beendet.

Der Beschwerdeführer bemängelte in einem Löschantrag, dass seine Daten weiterhin durch einen Gläubigerschutzverband verarbeitet würden, ohne dass hierfür eine Rechtsgrundlage oder seine Einwilligung vorliege. Die Beschwerdegegnerin wandte dagegen ein, dass die Daten zunächst gelöscht, allerdings dann für die weitere Kommunikation und zur Vermeidung einer Neuaufnahme der Kontaktdaten der Datensatz mit Vor- und Zunamen, Geburtsdatum sowie Adresse erneut gespeichert wurde. Im Wesentlichen berief sich die Beschwerdegegnerin demnach auf die weitere Speicherung der Daten zu Dokumentations- und Kommunikationszwecken und löschte die Daten daher nicht.

Die Datenschutzbehörde hatte zu entscheiden, ob ein Ausnahmetatbestand vom Recht auf Löschung gem. Art. 17 Abs. 3 DSGVO bestand. Die Beschwerdegegnerin verwies dabei auf „sicher amtsbekannte Gründe“ und konnte somit nicht ausreichend darlegen, weshalb die Daten weiterhin benötigt wurden.

Aus diesem Grund stellte die Datenschutzbehörde fest, dass der Antrag auf Löschung gem. Art. 17 Abs. 1 lit. a DSGVO berechtigt sei. Die Daten seien nicht mehr notwendig, insbesondere da eine „eventuell zukünftige Kontakt-

aufnahme“ aufgrund des Löschbegehrens nicht erfolgen würde. Weiters stelle die unbegrenzte Speicherdauer einen Verstoß gegen den Grundsatz der Speicherbegrenzung gem. Art. 5 Abs. 1 lit. e DSGVO dar.

Da die Beschwerdegegnerin keine weiteren Gründe für die fortgesetzte Speicherung der Daten angab, entschied die Datenschutzbehörde im Sinne des Beschwerdeführers und trug die unverzügliche, spätestens binnen zwei Wochen zu erfolgende Löschung der Daten und Bestätigung ebendessen auf.

Fazit: Neben der Zweckbindung sind bei der Datenverarbeitung auch Rechtmäßigkeit sowie Speicherbegrenzung von großer Bedeutung. Eine unbegrenzte Speicherdauer ohne ausreichende Rechtsgrundlage (beispielsweise die Einwilligung der betroffenen Person) steht daher im Widerspruch zur Datenschutzgrundverordnung.

II. Unrechtmäßiger Zugriff auf Gesundheitsdaten durch Mitarbeiter

DSB-D122.831/0003-DSB/2018
vom 04.06.2018 – rechtskräftig.
DSB-D122.829/0003-DSB/2018
vom 06.06.2018 – rechtskräftig.
(zusammenhängende Rechtssache)

Zugriff auf Patientenakte, Recht auf Geheimhaltung, Recht auf Auskunft, Protokollierung von Zugriffen, unberechtigter Zugriff durch Mitarbeiter

Es handelt sich bei diesen Entscheidungen um eine zusammenhängende Rechtssache. Inhaltlich wurden die Themen „Verletzung des Rechts auf Geheimhaltung“ sowie „Verletzung des Rechts auf Auskunft“ behandelt. Zum einen ging es um die Feststellung, dass das Recht auf Geheimhaltung einer Krankenhaus-Mitarbeiterin verletzt wurde, indem unberechtigte Zugriffe auf ihren elektronischen Gesundheitsakt durch andere Mitarbeiter des Krankenhauses vorgenommen wurden. Zum anderen um die Frage, in welchem Umfang das Auskunftsrecht besteht, wenn eine Datenverarbeitung unzulässigerweise durch die eigenen Mitarbeiter stattgefunden hat und dies intern dokumentiert wurde.

Die Entscheidung hat ihren Ursprung noch zur Rechtslage vor Geltung der DSGVO und bezog sich auf eine Mitarbeiterin eines Krankenhauses, die ein Auskunftsbegehren über die Zugriffe auf ihren elektronischen Gesundheitsakt geltend machte, nachdem sie dort vermehrt fremde Einsichtnahmen bemerkt hatte, die sie nicht zuordnen konnte.

Im Verfahren DSB-D122.831 gestand das Krankenhaus ein, dass „nicht-plausible Zugriffe auf den elektronischen Gesundheitsakt“ stattgefunden haben, da diese protokolliert werden und keine konkrete Zuordnung zu einem Behandlungsfall herstellbar war. Die Datenschutzbehörde stellte fest, dass es sich dabei um eine Verletzung des Rechts auf Geheimhaltung handelte. Dies war insbesondere nach dem Anerkenntnis des Krankenhauses auch unstrittig feststellbar.

Anschließend wollte die Beschwerdeführerin allerdings auch erfahren, wer konkret auf die Daten zugriffen hatte. Dies machte sie mit einem Auskunftsbegehren gegenüber dem Datenverantwortlichen des Krankenhauses geltend. Das Krankenhaus verwies noch mit Hinblick auf die alte Rechtslage auf die Bestimmung des § 14 Abs. 4 DSG 2000. Demnach sind Protokolldaten inhaltlich nicht zu beauskunften, wenn dies für andere Zwecke als die Kontrolle der Zulässigkeit der Verwendung der protokollierten Datenverarbeitung vorgesehen ist. Die Information, welcher Mitarbeiter wann Zugriff auf den Datenbestand hatte, unterläge daher nicht dem Auskunftsrecht.

Die Datenschutzbehörde verwies auf ein Erkenntnis des Bundesverwaltungsgerichts (GZ W214 2117640-1 vom 11. Juli 2017), wonach Abfragen (Anm. Zugriffe) von Mitarbeitern des Verantwortlichen, die sich innerhalb des ursprünglichen Aufgabengebietes bewegen, nicht der Auskunftspflicht unterliegen, solange sie keine Übermittlung darstellen. Dies

galt für die Rechtslage vor der DSGVO und lässt sich auch auf die neue Rechtslage übertragen.

Gem. Art. 15 Abs. 1 lit. c sind aber Empfänger, denen Daten offengelegt wurden, zu beauskunften. Die Datenschutzbehörde stellte im Anschluss fest, dass ein Empfänger jeder sein kann, unabhängig davon, ob es sich dabei um einen Dritten handelt oder nicht (vgl. Art. 4 Z 9 DSGVO).

Dadurch, dass Mitarbeiter ohne Zugriffsberechtigung auf die Daten der Beschwerdeführerin zugegriffen hatten, sind sie per Definition des Art. 4 Z 10 DSGVO Dritte. Dies wurde im Vorverfahren zur Geschäftszahl DSB-D122.831 festgestellt. Aus diesem Grund musste die Beschwerdegegnerin über die protokollierten Zugriffe Auskunft erteilen.

Fazit: Anders als § 14 Abs. 2 Z 7 DSG 2000 enthält die DSGVO keinerlei Hinweise auf eine Protokollierungspflicht von Änderungen, Abfragen und Übermittlungen. Im Sinne des in Art. 5 Abs. 1 lit. f DSGVO verankerten Grundsatzes der „Integrität und Vertraulichkeit" wird aber wohl eine Protokollierung – unter Berücksichtigung der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten – erforderlich sein. Sollten Sie einen Missbrauch feststellen, ist dies der betroffenen Person mitzuteilen und ggf. in einem anhängigen Auskunftsbegehren bekanntzugeben.

III. Speicherdauer von Daten in einer Bewerberdatenbank ohne Evidenzhaltung DSB-D123.085/0003-DSB/2018 vom 27.08.2018 – rechtskräftig.

Bewerberdatenbank, Recht auf Löschung, Aufbewahrungsfristen, Einwilligung zur Datenverarbeitung, Speicherdauer

Die Datenschutzbehörde hat im Beschwerdeverfahren zum Recht auf Löschung das Begehren des Beschwerdeführers abgewiesen. Es ging um die Frage, wie lange ein Verantwortlicher die für die Stellenbewerbung zur Verfügung gestellten Daten eines Bewerbers verarbeiten darf.

Der Beschwerdeführer hatte sich bei der Beschwerdegegnerin beworben und verlangte bereits kurze Zeit später die Löschung seiner Daten, da die Stelle nicht mehr ausgeschrieben war. Die Beschwerdegegnerin wies dieses Begehren mit der Begründung ab, dass sie aufgrund § 29 Abs. 1 GlBG (Gleichbehandlungsgesetz) eine Aufbewahrungsfrist von sieben Monaten beansprucht, um sich gegen Ansprüche aus dem Bewerbungsprozess verteidigen zu können. Berechnet wurde dies anhand der Frist von sechs Monaten nach Gleichbehandlungsgesetz zzgl. eines Monats für den Klagsweg.

Die Datenschutzbehörde hatte somit zu prüfen, ob eine unmittelbare Löschung vorzunehmen war bzw. wie lange die Datenverarbeitung einer Rechtsgrundlage im Gesetz unterliegt.

Als Ausnahme vom Recht auf Löschung wird gem. Art. 17 Abs. 3 lit. e DSGVO die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen genannt. In diesen Fällen muss einem Löschbegehren eines Betroffenen nicht entsprochen werden.

Die Voraussetzung ist jedoch, dass ein konkretes Verfahren entweder anhängig ist bzw. zukünftig anhängig sein könnte. Aus der Rechtsprechung des Verfassungsgerichtshofes gegenüber einem öffentlichen Verantwortlichen geht hervor, dass kein allgemeiner Ausnahmetatbestand für die „bloß abstrakte Möglichkeit rechtlicher Auseinandersetzungen" besteht, um dem Löschbegehren nicht zu entsprechen.

Im vorliegenden Verfahren wurde dem Beschwerdeführer die ehestmögliche Löschung zugesichert, sobald die Frist für die Geltendmachung von Ansprüchen nach dem Gleichbehandlungsgesetz abgelaufen ist. Der zusätzliche Monat für den Klagsweg (Einlangen bei Gericht, Schriftsatzvorbereitung etc.) wurde von der Datenschutzbehörde als „angemessen und nicht unverhältnismäßig lange" befunden.

Im Ergebnis ist daher einem Löschbegehren nach Abschluss eines Bewerbungsprozesses erst nach Ablauf der sechsmonatigen Aufbe-

wahrungsfrist zzgl. eines Monats für den etwaigen Klagsweg zu entsprechen.

Fazit: Vergessen Sie beim Bewerbungsprozess nicht, den Informationspflichten gem. Art. 13 DSGVO nachzukommen und informieren Sie die Bewerber über die gesetzlichen Aufbewahrungsfristen. Der einfachste Weg für eine längere Datenverarbeitung ist die Einholung einer Einwilligungserklärung zur Evidenzhaltung, die dann bis auf Widerruf gilt. Diese Einwilligungserklärung ersetzt nach Ablauf der sieben Monate die bestehende Rechtsgrundlage.

IV. Werbeanruf mit der Nummer aus dem Internet
DSB-D123.076/0003-DSB/2018
vom 31.10.2018 – rechtskräftig.

Cold Call, Recht auf Geheimhaltung, Informationspflichten, Art. 14 DSGVO

Die vorliegende Entscheidung betrifft das Thema „Cold Calling“, das seinen Anwendungsbereich eigentlich im Telekommunikationsgesetz (TKG 2003) hat. Dennoch kann auch eine Verletzung des Datenschutzes vorliegen, wenn Daten unrechtmäßig ermittelt und weiterverarbeitet werden.

Der Beschwerdeführer erhielt von der Beschwerdegegnerin einen Werbeanruf zum Vertrieb von Wasserspendern. Die hierfür genutzte Handynummer hatte die Beschwerdegegnerin auf einer öffentlich verfügbaren Website gefunden, auf der der Beschwerdeführer als Obmann eines psychologischen Hilfsverbandes angeführt wird.

Im vorliegenden Fall wurde diese Handynummer für Werbemaßnahmen genutzt, ohne vorherige Einwilligung oder ein geschäftliches Bestandsverhältnis zum Beschwerdeführer bzw. dem Hilfsverband. Die Datenschutzbehörde hatte die Frage zu behandeln, ob ein Betroffener in seinem Recht auf Geheimhaltung verletzt worden ist, wenn seine Handynummer zwar öffentlich auf einer Website verfügbar ist, jedoch ausschließlich für den Zweck der Kontaktaufnahme mit betroffenen Personen des Verbandes veröffentlicht wurde. Weiters ging es um die Frage, ob ein Telefonanruf nach Erhebung der Daten ohne Mitwirkung des Betroffenen die vollständigen Informationspflichten des Art. 14 DSGVO auslöst.

Die Prüfung der Rechtmäßigkeit der Verarbeitung obliegt der Fernmeldebehörde, denn Werbeanrufe unterliegen den Sonderbestimmungen des § 107 Abs. 1 TKG. Daher ist die Datenschutzbehörde nicht befugt, die Zulässigkeit des Anrufs bzw. die Rechtmäßigkeit der Verarbeitung gem. Art. 6 DSGVO selbst zu prüfen. Allerdings kann das Recht auf Geheimhaltung verletzt worden sein, sodass hier die Datenschutzbehörde ihre Zuständigkeit bejahte. Weiters prüfte die Datenschutzbehörde auch jene Bestimmungen, die keine zusätzlichen Pflichten in Bezug auf die Konkurrenz zur E-Privacy RL (RL 2002/58/EG) darstellen. Darunter fällt insbesondere die Informationspflicht gem. Art. 14 DSGVO.

Hinsichtlich der Verletzung des Rechts auf Geheimhaltung wies die Beschwerdegegnerin darauf hin, einen Vertragsabschluss mit dem Verband abschließen zu wollen, ohne die Handynummer des Beschwerdeführers verarbeiten zu wollen. Die Datenschutzbehörde stellte fest, dass es „nicht auf die Intention des Verantwortlichen ankommt, Daten in bestimmter Weise zu verwerten“. Ein Verschulden des Verantwortlichen spiele bei einer Verletzung von § 1 Abs. 1 DSG ebenfalls keine Rolle. Zweck der Veröffentlichung der Handynummer war die Kontaktaufnahme von Betroffenen psychologischer Hilfsleistungen und nicht die Ansprache durch Werbemaßnahmen. Aus diesem Grund stellte sie eine Verletzung des Rechts auf Geheimhaltung fest, da die Handynummer zweckwidrig für Werbemaßnahmen verwendet wurde. Dies steht auch im Einklang mit den Regelungen des TKG.

Bei der Beurteilung der Informationspflichten kommt es darauf an, wie personenbezogene Daten erhoben werden. Im gegenständlichen Fall wurde die Handynummer durch den

Beschwerdegegner nicht direkt beim Beschwerdeführer, sondern über eine Website erhoben. Dies löst grundsätzlich die Informationspflichten gem. Art. 14 DSGVO aus. Durch die Verweigerung dieser Angaben während des Telefonats verstieß die Beschwerdegegnerin gegen Art. 14 Abs. 3 lit. b DSGVO, da sie die Daten zur Kommunikation nutzte und der betroffenen Person die Informationen zum Zeitpunkt der ersten Mitteilung hätte bereitstellen müssen. Allgemein gilt, dass bei einer indirekten Erhebung „unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats“, die Informationen erteilt werden müssen.

Fazit: Sollten Sie Daten über eine Website für Kommunikationszwecke erheben, stellen Sie sicher, dass dies nicht zweckwidrig geschieht. Die Frist zur Erteilung der Informationen gem. Art. 14 DSGVO beträgt maximal einen Monat nach Erlangung der personenbezogenen Daten, bei direkter Kontaktaufnahme jedoch spätestens zum Zeitpunkt der ersten Mitteilung.

2. Videoüberwachung – erweiterte Informationspflichten

Wir nehmen den neuesten Newsletter der Datenschutzbehörde 1/2019 zum Anlass, Sie über die erweiterten Kennzeichnungs- und Informationspflichten bei der Videoüberwachung in Kenntnis zu setzen. Lt. Datenschutzbehörde sind derzeit 59 neue Verwaltungsstrafverfahren eingeleitet worden, u.a. auch deshalb, weil die Informationspflichten gem. Art. 13 und 14 DSGVO bei Videoüberwachung nicht wahrgenommen wurden.

Nach unserer Einschätzung ist aus § 13 Abs. 5 DSG abzuleiten, dass diese Kennzeichnung dann geeignet erfolgt, wenn jeder potenziell Betroffene, der sich einem überwachten Objekt nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen. Diese Kennzeichnung erfolgt am besten unter Verwendung des bereits bekannten Piktogramms nach DIN 33450, einschließlich der Bekanntgabe des Verantwortlichen sowie grundlegender Art. 13-Informationen. **Das bedeutet, dass das vormalige „Pickerl“ ohne Angaben zum Verantwortlichen nicht mehr ausreicht.**

Die Kennzeichnung muss zusätzlich um die vollständigen Informationen nach Art. 13 DSGVO ergänzt werden. Die notwendigen Inhalte sind die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten, die Zwecke und Rechtsgrundlagen der Verarbeitung sowie Speicherdauer und etwaige Empfänger. Weiters kommen noch die Betroffenenrechte und das Beschwerderecht an die Aufsichtsbehörde hinzu.

Es besteht die Wahl, entweder eine „Langfassung“ mit allen Informationen anzubringen oder am Ort der Videoüberwachung auf ein solches Dokument zu verweisen. Die Erteilung der vollständigen Art. 13-Information kann daher auch durch einen Hinweis auf die Datenschutzerklärung auf der Website (www.firma.at/datenschutz) oder den Verweis auf einen Aushang im Eingangsbereich (z.B. Rezeption/Foyer) erfolgen.

Dem Grunde nach ändert sich nichts für Sie als Verantwortlichen der Videoüberwachung. Zur Kennzeichnung treten lediglich weitere Informationspflichten hinzu.

Geeignete Muster für die Kennzeichnung sowie Informationserteilung können Sie unter http://kurzelinks.de/6pvu abrufen.

P.S.: Eine kostengünstige Quelle für Hinweisschilder in den verschiedensten Ausprägungen finden Sie unter http://kurzelinks.de/mp11.

••••

Unser nächstes Seminar

„DSGVO – Best Practice, Erfahrungen und Rechtsentwicklung“

findet am 8. April 2019 statt.

Es referieren **Prof. KommR Hans-Jürgen Pollirer** sowie **Mag. Judith Leschanz** und **Mag. Katja Wyrobek**.

Außerdem veranstalten wir am 9. April 2019 das Seminar

„Update für Datenschutzbeauftragte“

In diesem Seminar 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.

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
	1024 Seiten, Kpl, 2018
Preis:	Ca. EUR 198,00

Die Möglichkeit zur Direktbestellung finden Sie unter www.manz.at