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

Jänner 2023 Ausgabe Nr. 104

Liebe Leserinnen und Leser,

Vorab wünschen wir Ihnen Prosit 2023 und ein angenehmes und erfolgreiches Arbeitsjahr!

Stand 2022 datenschutzrechtlich vor allem im Zeichen der Diskussion um die rechtskonforme Nutzung von Google Online-Diensten und Google Analytics, so steht auch 2023 das Thema Internationaler Datenverkehr auf der Agenda ganz weit vorne. Ein erleichterter Datentransfer zeichnet sich jetzt immerhin beim „Sorgenkind" USA ab: Nach Joe Bidens Executive Order im Oktober 2022, die mehr Datenschutz gegenüber Überwachungsaktivitäten der US-Geheimdienste verspricht, wird für die nächsten Monate ein entsprechender Angemessenheitsbeschluss der EU-Kommission erwartet. Damit würden die USA wieder zum sicheren Drittland. Lesen Sie dazu unsere Analyse des aktuellen Status Quo.

Während die Verhandlungen zur E-Privacy-Verordnung weiterhin zäh verlaufen, gelten ab 2023 der DGS (Data Governance Act) und der DSA (Digital Services Act). Der DGS regelt die kommerzielle Weiternutzung von Daten des öffentlichen Sektors sowie die Tätigkeit von Daten-Treuhändern, das Gesetz über digitale Dienste enthält Regeln für vermittelnde Online-Dienste. Finden Sie auch dazu eine rechtliche Einschätzung unsererseits.

Wir wünschen angenehme Lektüre, gerne freuen wir uns über Ihr Feedback.

Mag. Judith Leschanz
Geschäftsführung

1. Data Governance Act (DGA) – Schritt in die richtige Richtung oder verpasste Gelegenheit?

Schon vor seinem Inkrafttreten am 23. Juni 2022 hat der Data Governance Act[1] (DGA) für intensive Diskussionen unter Datenschutzexperten und -expertinnen geführt. Geplant als Instrument, das darauf abzielt, geschützte Daten unter bestimmten Voraussetzungen zur Verfügung zu stellen und weiterverwenden zu dürfen, wird das ab 24. September 2023 geltende Gesetz von besorgten Datenschützern und Datenschützerinnen ebenso wie von Vertretern und Vertreterinnen eines liberalen Datenschutzes kritisiert. Neben den Bestim-

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0868&from=EN

mungen zur gemeinsamen Datennutzung bringt das neue Gesetz Regeln zu Datenvermittlungsdiensten und Datenaltruismus. Unsicherheit besteht auch hinsichtlich der Rechtsanwendung. In Art. 1 Abs. 3 DGA ist jedenfalls klar definiert: Die DSGVO sowie entsprechende nationale Regelungen gehen im Konfliktfall dem DGA vor.

Für ein rechtskonformes Data-Sharing gibt der DGA nunmehr einheitliche Rahmenbedingungen für personenbezogene Daten vor. Dazu zählen geeignete Sicherheitsmaßnahmen (etwa Anonymisierung oder Aggregation) und definierte Verfahren zur Bereitstellung (Art. 5 Abs. 3 DGA), das Verbot der Re-Identifizierung betroffener Personen sowie die Verpflichtung, im Zuge der Weiterverwendung adäquate TOM zu implementieren. Unterstützt werden soll die Weitervermittlung in jedem Mitgliedstaat durch eine „Zentrale Informationsstelle“, die den Zugriff auf Daten in öffentlicher Hand erleichtert (Art. 8 DGA).

Im Bereich der Datenvermittlungsdienste möchte der DGA Datenpools oder Marktplätze für Daten schaffen, mit folgenden wesentlichen Vorgaben: Der Vermittler darf die Daten nicht zu eigenen Zwecken nutzen (Art. 12 DGA), er muss faire Preise anbieten und er unterliegt einer Anmeldepflicht (Art. 11 Abs. 1 DGA).

Besonders in den Regelungen des DGA zum „Datenaltruismus“ sehen Anhänger und Anhängerinnen eines liberalen Datentransfers eine Tendenz zur Überregulierung: Um Daten für im allgemeinen Interesse liegende Ziele zur Verfügung gestellt zu bekommen, muss sich eine Einrichtung gem. Art. 18 DGA als datenaltruistische Organisation eintragen lassen. Bei der Datenverarbeitung treffen die Organisation hohe Transparenzanforderungen sowie umfassende Berichts- und Informationspflichten (Art. 20 Abs. 1 DGA).

2. Digital Markets Act (DMA) – Fairness für Nutzer und Nutzerinnen der großen Digitalkonzerne

Die bessere Absicherung von Nutzern und Nutzerinnen der Angebote großer Online-Plattformen („Gatekeeper“) sowie generell den fairen Wettbewerb hat das neue Gesetz über den digitalen Binnenmarkt (DMA)[2] zum Ziel. Im Sommer 2022 vom Europäischen Parlament verabschiedet, soll das neue Regelwerk ab 2. Mai 2023 gelten.

Relevant werden die neuen Gesetzesbestimmungen für Unternehmen mit mehr als 45 Millionen Nutzern und Nutzerinnen sowie einem Umsatz von mehr als EUR 7,5 Mrd., sofern sie einen „zentralen Plattformdienst" bereitstellen. Zu letzteren zählen u.a. Suchmaschinen, Soziale Netzwerke, Cloud-Computing-Dienste oder auch Betriebssysteme und Webbrowser. Für diese Unternehmen gelten mit dem neuen Gesetz bestimmte Verhaltensregeln (Gebote und Verbote), die durch umfangreiche Compliance-Pflichten ergänzt werden. Neben ausgedehnten Untersuchungsbefugnissen legitimiert der DMA die Europäische Kommission zur Verhängung von Geldbußen in der Höhe von bis zu 20 % des weltweiten Jahresumsatzes. Neben der alleinigen Zuständigkeit der Kommission für die Durchsetzung bietet das DMA auch Dritten Mitwirkungs- und Beschwerdemöglichkeiten, nicht zuletzt im Rahmen von Verbandsklagen.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R1925&from=EN

3. Digital Services Act (DSA) – Wer haftet künftig für die Verbreitung illegaler Inhalte?

Der DSA[3], quasi die Antwort der EU auf die Verbreitung von Fake News, politischer Desinformation und Hate Speech, schafft europaweit eine einheitliche Struktur für die Verantwortlichkeiten der Anbieter von digitalen Vermittlungsdiensten. Insbesondere in der Frage der Haftung für die Verbreitung von illegalen Inhalten „verlängert" der DSA die in der E-Commerce-Richtlinie gewährten Haftungsprivilegierungen der Provider. Neu ist ein europaweit einheitlicher für die Vermittlungsdienste verpflichtender Mechanismus, der Dritten das Melden vermuteter illegaler Inhalte ermöglicht. An diesen soll künftig die Haftung von Anbietern anknüpfen, die nach einer Meldung den Inhalt nicht zeitnah sperren oder entfernen (Notice and Take Down-Verfahren).

Als weitere Neuerung soll auch das freiwillige Screening von Nutzerinhalten nicht zum Ausschluss der Haftungsprivilegien führen, d.h. die Anbieter sollen Rechtssicherheit haben, wenn sie etwa Filtertechnologien einsetzen.

Das DSA-Regelwerk betrifft aber nicht nur Facebook & Co, sondern auch eine Vielzahl kleinerer europäischer Anbieter. Eine frühzeitige Anpassung kann saftige Geldbußen vermeiden. So müssen etwa bereits bis zum 17. Februar 2023 alle Online-Plattformen und Suchmaschinen die Anzahl aktiver Endnutzer und Endnutzerinnen ihrer Plattform veröffentlichen und an die EU-Kommission melden.

4. Wie steht es eigentlich um die Verordnung zur Regulierung der Künstlichen Intelligenz?

Künstliche Intelligenz (KI) ist eines der Zukunftsthemen, das uns datenschutzrechtlich in den nächsten Jahren vor große Herausforderungen stellen wird. Bereits im April 2021 hat die EU einen Entwurf einer Verordnung zur Regulierung der Nutzung von KI-Systemen[4] vorgelegt. Zur Sicherstellung von sicherer, transparenter, ethisch korrekter und grundrechtskonformer KI wurde im Vorschlag der Verordnung ein risikobasierter Ansatz gewählt. Vier Risikogruppen von KI-Systemen unterscheidet der rechtliche Entwurf: von Risikostufe 1 („Unzulässig", etwa Social Scoring) über „Hohes Risiko" (kritische Infrastrukturen, Strafverfolgung, Rechtspflege), „Begrenztes Risiko" (Chatbots) bis hin zu Stufe 4 „Minimales Risiko" (Spamfilter). Daneben sieht der Entwurf spezifische Transparenzpflichten sowie eine eigenständige, öffentlich zugängliche Datenbank mit Informationen über Hochrisiko-KI-Systeme vor.

Kritisiert wird der Entwurf von Seiten der Arbeiterkammer: Zwar sei es begrüßenswert, dass das zukunftsweisende Thema KI für eine einheitliche europäische Regelung aufgegriffen werde, auch den risikobasierten Ansatz sieht man positiv. Im Gegensatz zum ursprünglich präsentierten Weißbuch sei der Vorschlag aber viel zu technikbasiert; es fehlten wichtige Schutzmechanismen etwa im Arbeits- und Konsumentenschutzrecht, ebenso Möglichkeiten zur Mitbestimmung. Auch dass sich die Verord-

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065&from=en

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=DE

nung in konsumentenschutzrechtlichen Fragen auf die Regulierung hochriskanter KI konzentriert, wird moniert.

Aber auch die Wirtschaft sieht den geplanten AI-Act weit weg vom von Brüssel propagierten „Goldstandard“ und fürchtet im Gegenteil sogar „massive Einschränkungen“. So warnen etwa IT- Unternehmen und Verbände vor einer Überregulierung und befürchten Wettbewerbsnachteile durch eine zu starke Fokussierung auf Risiken.

Fazit: Für Unternehmen sind insbesondere Anwendungen bedeutsam, die als Hochrisiko-System eingestuft werden können. Ein wirksames Risikomanagementsystem sowie umfangreiche Dokumentationspflichten sind essenziell.

5. „Aus“ für Medienprivileg: VfGH kippt § 9 (1) DSG – Neuregelung bis Mitte 2024

§ 9 Abs. 1 DSG enthält das sogenannte „Medienprivileg“, nämlich die Regelung, dass das DSG sowie auch Teile der DSGVO auf journalistische Datenverarbeitungen durch Medieninhaber, Herausgeber sowie Mitarbeiter eines Medienunternehmens oder -dienstes nicht anzuwenden sind. Mit Entscheidung vom 14. Dezember 2022 hat der Verfassungsgerichtshof § 9 Abs. 1 DSG wegen Verstoßes gegen das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gemäß § 1 Abs. 1 DSG als verfassungswidrig aufgehoben. Es sei nur dann zulässig, gesetzlich in den Datenschutz einzugreifen, wenn dies zur Wahrung überwiegender berechtigter Interessen eines anderen notwendig sei. Es ist vom Gesetzgeber also eine Abwägung zwischen der Schutzwürdigkeit des Betroffenen und den berechtigten Interessen des Medienunternehmens oder -dienstleisters vorzunehmen.

In seiner Argumentation konzediert der Verfassungsgerichtshof, dass Medien als „public watchdog“ in einer demokratischen Gesellschaft eine zentrale Rolle im öffentlichen Interesse wahrnehmen. Diese begründe auch die (Sonder-)Regelung des Art. 85 Abs. 1 DSGVO, wonach der nationale Gesetzgeber Rechtsvorschriften zu erlassen hat, durch welche der Schutz personenbezogener Daten mit der Verarbeitung zu journalistischen Zwecken in Einklang gebracht werden soll. Das Grundrecht auf Datenschutz gemäß Art. 1 Abs. 1 DSG erlaube aber keine kategorische Privilegierung des Rechtes auf freie Meinungsäußerung und Informationsfreiheit gegenüber dem Grundrecht auf Datenschutz.

Wie die Entscheidung auf Medienseite aufgenommen wird, bleibt abzuwarten.

6. Umstrittenes OGH-Urteil zur Informationspflicht des Art. 13 DSGVO: Kenntnisnahme = Einwilligung

In einem Rechtsstreit zwischen einem Versicherungsunternehmen und einem Verbraucher hatte der OGH zunächst die Frage zu erörtern, ob die vom Versicherungsunternehmen verwendete Datenschutzerklärung Vertragserklärungscharakter (Rechtsfolgewille) hat oder als bloße Informationserteilung im Sinn der Art. 13 lit. f DSGVO dient. Das Versicherungsunternehmen ließ sich die Datenschutzerklärung mit der Klausel „zur Kenntnis genommen“ bestätigen. Der OGH sieht diese Kenntnisnahme im Ergebnis gleichwertig mit einer Einwilligung, sofern der Inhalt der Datenschutzhinweise Erklärungscharakter hat. Weil

dies im konkreten Fall zu bejahen war, folgte daraus, dass die Datenschutzerklärung Rechtsfolgecharakter hat und somit auch der Inhaltskontrolle durch § 879 Abs. 3 ABGB sowie dem Transparenzgebot nach § 6 Abs. 3 KSchG unterliegt (OGH in seiner Entscheidung: „Dies macht aber keinen relevanten Unterschied, weil die Zurkenntnisnahme auch die Zustimmung zu dessen Inhalt implizieren kann“).

Wie Sie eine auf Ihr Unternehmen optimierte und datenschutzrechtskonforme Datenschutzinformation erstellen, erfahren Sie in unserem Praxisseminar am 28. und 29. März 2023.

7. Top 5 DSGVO-Bußgelder im November 2022 – Aktuelle Prüfungsschwerpunkte und Sanktionspraxis der Behörden

1. 265 Millionen Euro Bußgeld für geleakte User-Daten bei Facebook

Für Datenscraping im Ausmaß von 533 Millionen geleakten Datensätzen mit persönlichen Informationen muss sich der Social Media-Konzern Facebook (Meta) verantworten. Personenbezogene Daten wie Namen, Telefonnummern, E-Mail-Adressen von Nutzern und Nutzerinnen wurden nach dem unbefugten Zugriff im Internet veröffentlicht.

Der Scraping-Vorfall wurde bereits im April 2021 publik, Ermittlungen wurden daraufhin von der irischen Datenschutzbehörde DPC (Data Protection Commission) eingeleitet. Nach Ansicht der Aufsichtsbehörde hatte es Facebook versäumt, angemessene Sicherheitsmaßnahmen an den relevanten Programmierschnittstellen (APIs) einzurichten. Dadurch konnten die Angreifer die Daten abgreifen, ohne sich in die Facebook-Systeme hacken zu müssen. Neben der Verpflichtung, seine TOM an die Vorgaben der DSGVO anzupassen, wurde Facebook zu einem Bußgeld in Höhe von EUR 365 Millionen verurteilt.

Fazit: Die Aufsichtsbehörden haben den Konzern weiterhin im Auge. Bereits in der Vergangenheit wurden Bußgelder in dreistelliger Millionenhöhe fällig (WhatsApp: 225 Millionen, Instagram: 405 Millionen). Die Implementierung geeigneter TOM ist essenziell.

2. Aufbewahrung von Kundendaten ohne Einwilligung bei Douglas Italia S.p.A.

Auch Douglas Italia S.p.A. geriet in datenschutzrechtliche Schieflage: Obwohl 3,2 Millionen Kunden ihre Treuekarten nicht verlängert hatten, bewahrte das Unternehmen die Daten weiter ohne Einwilligung oder sonstige Rechtsgrundlage auf. Außerdem befand die italienische Aufsichtsbehörde Garante die Cookie- und Datenschutzrichtlinien von Douglas Italia als mangelhaft. Es sei nicht möglich gewesen, eine freiwillige und für einzelne Verarbeitungstätigkeiten spezifische Einwilligung zu geben. Douglas Italia muss neben der Bußgeldzahlung i. H. v. EUR 1.400.000,00 seine TOM nachbessern und jene Daten löschen, die bereits vor zehn Jahren oder noch früher erfasst wurden.

Fazit: Bei Aufbewahrungsfristen ist auf das Auslaufdatum zu achten. Weiters sind zulässige und vollständige Cookie-Banner zu verwenden. Das Erteilen der Einwilligung muss getrennt für unterschiedliche Verarbeitungstätigkeiten erfolgen können.

3. Ungenügende Aufbewahrungsprozesse und unsichere Passwörter bei Discord

Immerhin EUR 800.000,00 Bußgeld musste der französische Online-Telekommunikationsanbieter Discord berappen. Die CNIL (Commission Nationale de l’Informatique et des Libertés) hatte das Fehlen von an den konkreten Verarbeitungszweck angepassten Aufbewahrungsfristen bemängelt – die Folge waren über zwei

Millionen inaktive Accounts in der Datenbank des Anbieters. Weiters stellte die CNIL einen Verstoß gegen Art. 25 Abs. 2 DSGVO (Privacy by Default) fest: An den Clients der User wurde der Dienst nicht geschlossen, sondern lediglich minimiert, wodurch diese glaubten, nicht mehr Teilnehmer einer Audio- und/oder Video-Unterhaltung zu sein. Außerdem war die Passwort-Policy des französischen Unternehmens unzureichend: Discord erlaubte die Generierung von einfachen Passwörtern mit nur sechs Zeichen.

Fazit: Auch hier sind Fristen der ordnungsgemäßen Aufbewahrung zu beachten. Das Erstellen sicherer Passwörter ist vom Verantwortlichen sicherzustellen und zu dokumentieren. Auch kleinere Verstöße gegen den Datenschutz können sich summieren und schließlich ein erhebliches Bußgeld nach sich ziehen.

4. Bankinter gibt Kunden fehlerhaft Zugriff auf fremde Konten

Auf Beschwerde einer Kundin der spanischen Bank Bankinter, die neben ihrem eigenen Konto auch fremde Konten einsehen konnte, überprüfte die AEPD den Vorfall und musste schließlich das Fehlen geeigneter TOM beim spanischen Finanzdienstleister feststellen. Diesen kostete der Data Breach ein Bußgeld in Höhe von EUR 80.000,00.

Fazit: Wiederum wurde versäumt, geeignete TOM zu implementieren. Schon verhältnismäßig kleine Nachlässigkeiten können zu einer Vielzahl von Datenschutzvorfällen und hohen Pönalen führen.

5. Callcenter-Marketing ohne Einwilligung bei Vodafone Italia

Vodafone Italia wurde für den nicht datenschutzkonformen Einsatz eines Callcenters zu Marketingzwecken mit einem Bußgeld in Höhe von EUR 500.000,00 belangt. Eine Kundin des italienischen Telekommunikationsunternehmen wurde angerufen und zu einem Vertragsabschluss gebracht – ohne Zustimmung der Kundin und ohne die Kundin über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Neben dem Bußgeld ordnete die italienische Behörde Vodafone an, die Arbeitsweise der eingesetzten Callcenter genauer zu überprüfen.

8. Datentransfer in die USA: Biden macht Weg frei für „neuen Privacy Shield“

Seit der EuGH im Juli 2020 das Privacy Shield gekippt hatte, war der Datenaustausch zwischen der EU und den USA problematisch. Mit seiner Executive Order vom 7. Oktober 2022[5] hat Präsident Joe Biden nun einen wichtigen Schritt für ein neues Datenschutzabkommen mit der EU gesetzt.

In seinem Urteil gegen das Privacy Shield hatte der EuGH vor allem die umfangreichen Zugriffsmöglichkeiten US-amerikanischer Geheimdienste auf europäische Daten als nicht EU-rechtskonform beurteilt. Gemäß dem neuen Erlass dürfen die US-Geheimdienste zwar nach wie vor Massenüberwachungen (bulk collections) durchführen, diese müssen in Zukunft jedoch eine Verhältnismäßigkeitsprüfung durchlaufen und genehmigt werden. Der Erlass benennt auch konkret sechs Bedrohungen, deren Verfolgung zulässig ist, darunter bösartige

[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities

Cyberaktivitäten und internationale Finanzdelikte.

Des Weiteren wird in dem neuen Erlass ein zweistufiges Beschwerdeverfahren definiert, mit dem sich EU-Bürger gegen das Datensammeln von US-Behörden wehren können. In einer ersten Stufe soll ein Civil Liberties Protection Officer (CLPO), also eine Art Bürgerrechtsbeauftragter, eine mögliche Datenschutzverletzung prüfen. Quasi als zweite Instanz sieht der Erlass die Einrichtung eines Data Protection Review Courts (DPRC) vor, der die Entscheidungen des CLPO überprüfen kann. Schließlich kann noch ein Privacy and Civil Liberties Oversight Board (PCLOB) die Aktivitäten der US-Geheimdienste auf die Einhaltung und Umsetzung der Vorgaben der beiden neuen Instanzen überprüfen.

Der Ball für den künftigen Datenaustausch zwischen EU und den USA liegt nunmehr bei der EU-Kommission, die ein weiteres Mal einen Angemessenheitsbeschluss fällen müsste – und damit die Entscheidung, dass in einem Drittstaat (USA) ein vergleichbares Datenschutzniveau wie in der EU existiert. Mit einer Entscheidung ist im Frühjahr 2023 zu rechnen.

9. Post-Datenskandal: Niederlage vor EuGH bei Vorlagefrage um Auskunftsrecht – Empfänger müssen bei Anfrage konkret genannt werden

Der Fall ging als „Post-Datenskandal“ durch alle Medien: Die österreichische Post hatte 2019 personenbezogene Daten zu Marketingzwecken an Geschäftskunden weitergegeben. Eine betroffene Person begehrte Auskunft gem. Art. 15 DSGVO, die Post weigerte sich aber, konkrete Empfänger*innen zu nennen. Die betroffene Person wählte den Rechtsweg, die Causa zog sich bis zum OGH und führte zu einem Vorabentscheidungsverfahren vor dem EuGH.

Die Datenschutzbehörde hatte zuvor bereits entschieden, dass das Verhalten der Post AG allein deswegen unzulässig war, da diese aufgrund von demographischen Daten betroffenen Personen (partei-)politische Präferenzen zugeordnet hatte. Das Bußgeld belief sich auf immerhin 9,5 Mio. EUR.

In seiner aktuellen Entscheidung[6] folgt der EuGH – wie häufig – dem Schlussantrag des Generalanwalts: Der Verantwortliche hat die Verpflichtung, der betroffenen Person die Identität der Empfänger mitzuteilen. Die Verpflichtung entfällt nur dann ausnahmsweise, wenn der Verantwortliche die konkreten Empfänger nicht identifizieren kann oder wenn die unbegründet oder exzessiv sind.

Fazit: Die aktuelle Entscheidung stärkt die Betroffenenrechte; für die Unternehmen empfiehlt sich im Anlassfall einmal mehr eine enge Koordination mit dem Datenschutzbeauftragten.

[6] https://curia.europa.eu/juris/document/document.jsf?text=&docid=269146&pageIndex=0&doclang=DE

10. In eigener Sache: Neu an Bord

Mit Sylvia Metenczuk holt sich Secur-Data mit Januar 2023 kräftige Unterstützung an Board. Frau Mag. Metenczuk hat als Juristin und Compliance Managerin in den letzten Jahren vor allem Projekte im Gesundheitsmanagement begleitet.

Datenschutz-Seminare 2023

Save the Date: 28. und 29. März 2023: Secur-Data Seminar – Update Datenschutz-Praxis

Auch 2023 bringt eine Reihe von spannenden Neuerungen und Entwicklungen im heimischen und internationalen Datenschutz. Lassen Sie sich im bewährt kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen für 2023 in Angelegenheiten der Informationssicherheit und Datenschutzpraxis informieren. Neben praxisnaher Wissensvermittlung steht Secur-Data für State-of-the-Art-Anwendungstipps sowie praxistaugliche Muster und Vorlagen. Auch heuer wieder wird Ihnen **Herr Mag. Andreas Rohner von der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

Profitieren Sie vom Frühbucherbonus: - 10 % bis 31. Jänner 2023

Hier geht's zur Anmeldung: https://www.secur-data.at oder telefonisch unter (01) 533 42 07-0

Wir freuen uns auf Ihren Anruf!

28. März 2023, 9:15 – 17:00 Uhr: „Rechtsentwicklung und Best Practices"
Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Sylvia Metenczuk, MAS
Gastreferent: Mag. Andreas Rohner (Datenschutzbehörde Österreich)

29. März 2023, 9:15 – 17:00 Uhr: „Praxis-Updates zu Datensicherheit & Informationssicherheit"
Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Jürgen Stöger

Ort: Hilton Vienna Plaza, Schottenring 11, 1010 Wien

Selbstverständlich stehen wir auch für Inhouse-Schulungen oder Seminare zu Spezialthemen zur Verfügung.

Weitere Informationen und Details finden Sie auf unserer Website https://www.secur-data.at.