NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 04/2023

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Wenn man sich mit der Frage beschäftigt, ob die Funktion eines Datenschutzbeauftragten (DSB) und eines IT-Sicherheitsbeauftragten (IT-SiBe) in einer einzelnen Person vereinbar ist, lassen sich sehr viele Quellen finden, die die Risiken einer Personalunion beschreiben und auf eine wie selbstverständlich angenommene Interessenkollision verweisen. Es gibt jedoch sehr wenige Beiträge, die auf die Vorteile einer solchen Personalunion hinweisen. Risiken lassen sich in der Regel mitigieren. Der interessierte Leser fragt sich: Warum nicht auch hier?
Zu den Vorteilen einer Personalunion:

1. **Ganzheitlicher Ansatz:** Eine Person, die sowohl Datenschutz- als auch Informationssicherheitsbelange im Blick hat, kann möglicherweise einen ganzheitlicheren Ansatz bei der Umsetzung von Datenschutz- und Informationssicherheitsmaßnahmen verfolgen. Dies kann dazu beitragen, dass die Gesamtsicherheit des Unternehmens oder der Organisation verbessert wird.
2. **Effizienz:** Wenn eine Organisation nicht über ausreichende personelle Ressourcen verfügt, kann es effizienter sein, wenn eine Person beide Positionen übernimmt. So kann ein einzelner Mitarbeiter möglicherweise besser in der Lage sein, beide Funktionen effektiv zu erfüllen, als zwei separate Personen.
3. **Synergieeffekte:** Datenschutz und Informationssicherheit sind eng miteinander verknüpft. Einzelne Maßnahmen in einem Bereich können Auswirkungen auf den anderen Bereich haben. Wenn eine Person beide Funktionen innehat, kann sie möglicherweise Synergieeffekte nutzen, um effektiver Maßnahmen zu ergreifen, die die Sicherheit von Informationen verbessern und gleichzeitig die Einhaltung von Datenschutzbestimmungen sicherstellen.

Das Risiko einer Personalunion dürfte nur dann tatsächlich zu Tage treten, wenn diese Person bei einem Vorhaben im Bereich der Informationssicherheit jegliches Gespür für Datenschutz aufgeben würde und umgekehrt sich gänzlich nicht um pragmatische Lösungsmöglichkeiten kümmern würde, sondern bloßer „Datenschutz-Subsumtions-Roboter“ agieren würde, wenn der „Schwerpunkt des Vorhabens“ datenschutzrechtliche Themen adressiert. Aber so „funktionieren“ weder Datenschutzbeauftragte noch IT-Sicherheitsbeauftragte in der Regel. Ein (guter) DSB sucht in der Regel immer nach Lösungen und beschränkt seine Beratung nicht darauf, auf ein Problem zu verweisen. Ein (guter) IT-SiBe hat immer auch die datenschutzrechtliche Zulässigkeit im Blick, wenn es um eine Datenverarbeitung geht. Warum sollte eine einzelne Person diese beiden Abwägungen nicht auch in Personalunion durchführen können, fragt sich

Ihr Levent Ferik.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

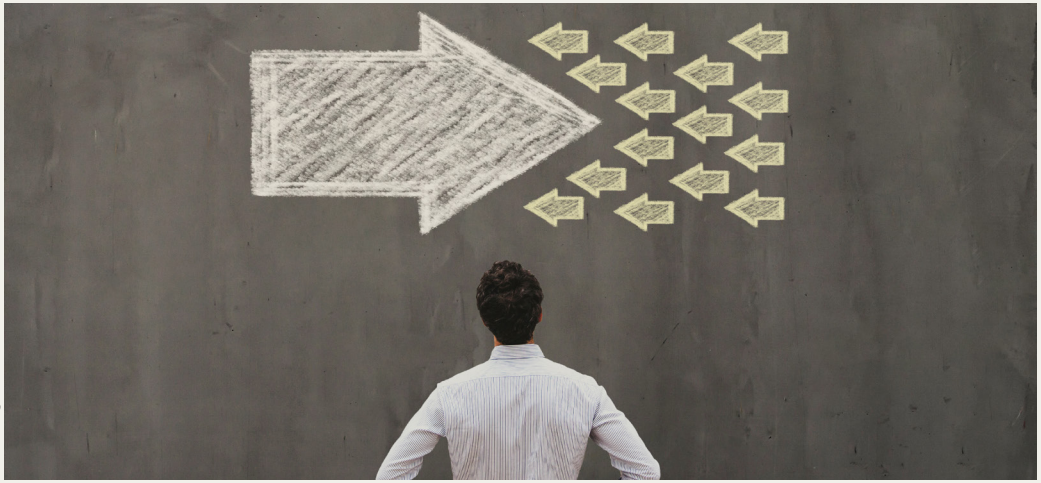

Foto: Song_about_summer, Adobe Stock

Personalunion: Beauftragter für Informationssicherheit und Datenschutzbeauftragter

Die Meinungen zu der Frage, ob und welche zusätzlichen Funktionen einen Datenschutzbeauftragten in eine Interessenkollision bringen, sind uneinheitlich. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI):
Der TLfDI geht in seinem 2. Tätigkeitsbericht zum Datenschutz nach der DS-GVO (Berichtsjahr 2019, veröffentlicht am 22.10.2020) auf die Fragen von möglichen Interessenkollisionen für die Tätigkeit des Datenschutzbeauftragten ein.
In diesem Zusammenhang sei zu beachten, dass auch nach Wirksamkeit der DS-GVO die Tätigkeit eines IT-Sicherheitsbeauftragten und Datenschutzbeauftragten in Personalunion nicht miteinander vereinbar sein, da diese zu Interessenkonflikten führen.
Eine mögliche Interessenkollision sieht der TLfDI u. a. in dem Umstand, dass der IT-Sicherheitsbeauftragte im Rahmen der Gefahrenabwehr von Angriffen Dritter auf IT-Systeme des Unternehmens oftmals an einer umfangreichen Sammlung personenbezogener Daten interessiert sei, um Missbrauch zu entdecken, während der DSB unter Berücksichtigung der Schutzziele der DS-GVO eine Begrenzung der Sammlung personenbezogener Daten anstrebe. Auch in puncto Speicherdauer personenbezogener Daten sei zu erwarten, dass IT-Sicherheitsbeauftragte und Datenschutzbeauftragte häufig unterschiedliche Positionen vertreten müssten.

Die Sächsische Datenschutzbeauftragte:
Die Sächsische Datenschutzbeauftragte bewertet diese Frage in ihrem Tätigkeitsbericht 2021 (Seite 140) etwas differenzierter.

Die Landesbeauftragte für den Datenschutz Niedersachsen:
Eine enge Zusammenarbeit zwischen Datenschutzbeauftragten (DSB) und Informationssicherheitsbeauftragten (ISB) wird von der LfD Niedersachsen als förderlich und erforderlich angesehen. Dem Verantwortlichen wird empfohlen, im Hinblick auf mögliche Interessenkollisionen die Benennung von DSB und ISB in Personalunion zu vermeiden. Eine gleichzeitige Ausübung beider Aufgaben in Personalunion wird allerdings nicht pauschal für unzulässig erklärt.

Bundesamt für Sicherheit in der Informationstechnik (BSI):
Das BSI adressiert dieses Thema ebenfalls unter dem Blickwinkel des Informationssicherheitsmanagements. Nach Auffassung des BSI ist „eine Personalunion mit dem Datenschutzbeauftragten nicht unkritisch." Das BSI verneint eine Personalunion jedoch ebenfalls nicht per se, sondern bewertet wie folgt: „Sollte dies der Fall sein, müssen die Schnittstellen dieser beiden Aufgaben klar definiert werden, um Rollenkonflikte zu vermeiden."

Foto: MQ-Illustrations, Adobe Stock

Social-Media-Nutzung für Mediziner: Wo liegen die Fallstricke?

In der dritten und damit aktualisierten Auflage ihrer Handreichung „Ärztinnen und Ärzte in sozialen Medien“ gibt die Bundesärztekammer Ärztinnen aber auch allen Medizinstudierenden wertvolle Hinweise, die sie bei der Nutzung sozialer Medien beachten sollten.

Die 1. Auflage der Handreichung war aus dem Beschluss des 115. Deutschen Ärztetags 2012 zur Erarbeitung von Empfehlungen für Ärzte in sozialen Medien hervorgegangen.

Obwohl die Nutzung sozialer Medien für die meisten Menschen selbstverständlich geworden ist, bestehen doch trotzdem rechtliche Unsicherheiten – gerade auch für Ärztinnen und Ärzte, Medizinstudierende sowie Patientinnen und Patienten.

Alle diese genannten Personengruppen nutzen regelmäßig Wikis, Chaträume und Blogs, da diese ihnen die Möglichkeiten für Zusammenkünfte zum Teilen und Verbreiten persönlicher Informationen unter Freunden, Verwandten, Kollegen usw. einschließlich gesundheitsbezogener Informationen bieten. Licht und Schatten, Nachteile wie Vorteile liegen hier wie so oft nah beieinander, sodass die Bundesärztekammer zurecht für die Probleme sensibilisiert, denn dieser Austausch über soziale Medien kann das Arzt-Patient-Verhältnis auch ungünstig beeinflussen.

Der Austausch kann auch mit datenschutzrechtlichen Problemen und weiteren juristischen Fragestellungen einhergehen, sodass Ärztinnen alle Maßnahmen ergreifen müssen, um die Vertraulichkeit der individuellen Arzt-Patient-Beziehung und den Datenschutz zu gewährleisten.

Dem Thema Datenschutz und Datensicherheit sowie Vertraulichkeit im virtuellen Raum wird ein eigener Abschnitt gewidmet.

Abgerundet wird die Handreichung durch zahlreiche Fallbeispiele, in denen geschildert wird, wo mögliche Probleme für Ärzte und Medizinstudierende liegen und wie man ihnen begegnen kann. Die Handreichung richtet sich ebenso an Neulinge wie auch an erfahrene Nutzer sozialer Medien.

Foto: michalchm89, Adobe Stock

Beschäftigter lehnt Verpflichtung auf das Datengeheimnis ab: Was tun?

Gemäß Art. 5 Abs. 2 DS-GVO muss der für die Verarbeitung Verantwortliche die Einhaltung der in Absatz 1 des Artikels festgelegten Grundsätze der Verarbeitung personenbezogener Daten nachweisen können. Hieraus folgt eine umfassende Rechenschaftspflicht (engl.: „Accountability“) mit zahlreichen Dokumentations- und Nachweispflichten.
Präzisiert werden die Anforderungen an die Nachweispflicht in Art. 24 Abs. 1 DS-GVO. Hier wird festgelegt, dass der Verantwortliche den Nachweis zu erbringen hat, dass er Maßnahmen getroffen hat, die sicherstellen, dass die Verarbeitung gemäß der DS-GVO erfolgt.

Weiter auf DataAgenda lesen

Eakrin - stock.adobe.com

Foto: Supatman, Adobe Stock

Datenpannen bei Auftragsverarbeitern – Pflichten des Auftragsverarbeiters und des Auftraggebers?

Mit Einführung der DS-GVO ist der Auftragsverarbeiter neben dem Verantwortlichen als Normadressat getreten. Dies gilt sowohl für die Kernnorm der Auftragsverarbeitung gem. Art. 28 DS-GVO als auch viele weitere Normen, in denen die Verantwortlichkeit des Auftragsverarbeiters ausdrücklich genannt wird. Verschärft wird diese Situation durch die Haftungs- und Bußgeldregelungen (Artt. 82 und 83 DS-GVO) sowie ein direktes Klagerecht der betroffenen Personen gegen den Auftragsverarbeiter (vgl. GDD-Praxishilfe DS-GVO – Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO).

Weiter auf DataAgenda lesen

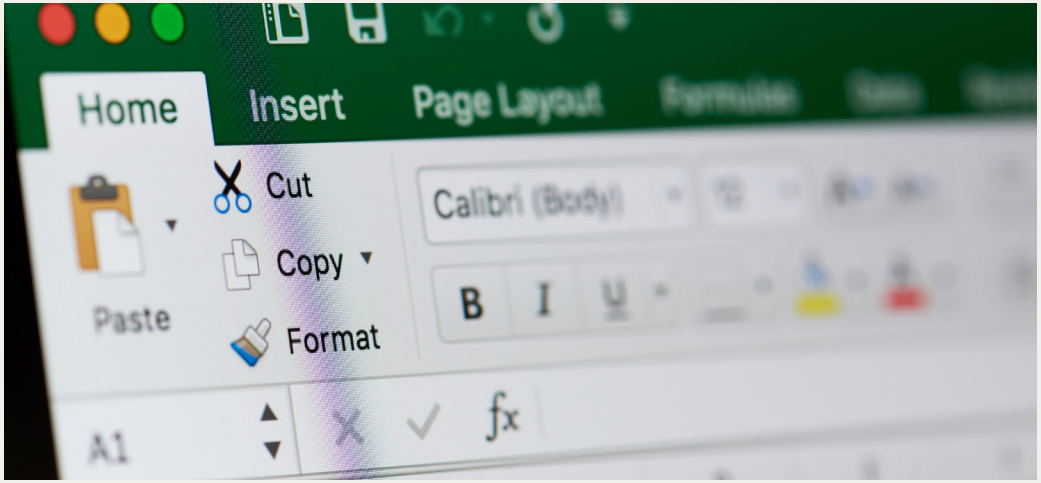

Foto: PixieMe, Adobe Stock

Datenschutz-Tücken im Umgang mit Excel-Dateien

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) berichtete in seinem Tätigkeitsbericht 2019 von einer Beanstandung im Zusammenhang mit der Nutzung von Excel-Dateien. Eine öffentliche Stelle hatte versehentlich eine Excel-Datei mit personenbezogenen Daten einer Gruppe von 45 Lehrerinnen und Lehrern per E-Mail unverschlüsselt an alle Gruppenmitglieder versendet.
Beabsichtigt war, ein Arbeitsblatt mit Kontaktdaten zugänglich zu machen, um die Kommunikation unter den in vergleichbarer Funktion tätigen Lehrerinnen und Lehrern zu erleichtern. Die Excel-Datei enthielt jedoch weitere Arbeitsblätter, aus denen unter anderem eine umfassende Übersicht über die dienstlichen Beurteilungen der Jahre 2010 und 2014 (Beurteilungsprädikate) sowie Aufzeichnungen über das dienstliche Verhalten und die Amtsführung (wertende Aussagen über die Qualität von Arbeitsergebnissen, Tagungsteilnahmen und vereinzelt auch wertende Stellungnahmen anderer öffentlichen Stellen) ersichtlich waren. Diese Arbeitsblätter umfassten zudem Angaben von früheren Gruppenmitgliedern.
Der BayLfD beschreibt in seinem Tätigkeitsbericht einen datenschutzrelevanten Vorfall, der im hektischen Tagesgeschäft schnell passieren kann und im schlimmsten Fall als meldepflichtige Datenschutzpanne bewertet werden muss. Dieses Risiko wohnt jedem Versand einer von einem Tabellenkalkulationsprogramm erstellten Datei inne, die oft auch als Arbeitsmappe bezeichnet wird. Eine solche Datei kann mehrere unterschiedliche Tabellenbereiche besitzen, die auch Arbeitsblätter genannt werden. Typischerweise wird nach dem Öffnen der Datei nur ein Tabellenbereich angezeigt, während eventuell daneben existierende Tabellenbereiche nur über eine zusätzliche Benutzeraktion aktiviert und damit sichtbar gemacht werden können.
Diese besondere Funktionsweise führt zu folgendem Risiko: Die Versenderin oder der Versender einer solchen Datei betrachtet vor dem Versand oft nur den gerade aktivierten Tabellenbereich und übersieht dabei, dass sich in anderen Tabellenbereichen der Datei sensible Daten befinden, die nicht mit versendet werden sollen.
In den seiner Rubrik „Aktuelle Kurz-Information 46: Datenpannen mit Microsoft Excel verursachen und vermeiden“ stellt der BayLfD noch weitere Risiken dar, die bei der Nutzung von Excel eintreten können und beschreibt, wie diese Klippen mit einfachen Maßnahmen umschifft werden können (Personenbezogene Daten können in einer Excel-Datei auch in der Rolle von Metadaten übersehen werden.)

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Foto: agenturfotografin, Adobe Stock

Datenschutz und ärztliche Videosprechstunde

Seit der Aufhebung des Fernbehandlungsverbots im Jahr 2018 durch den deutschen Ärztetag konnten Ärzte das Angebot ihrer telemedizinischen Leistungen sukzessive nach und nach erweitern. Die (Muster-)Berufsordnung-Ärzte (MBO-Ä) wurde entsprechend angepasst. So haben seit dem Jahr 2018 Patient:innen die Möglichkeit, Ärzt:innen auch virtuell zu konsultieren, selbst wenn sie zuvor nicht dort in Behandlung waren.

Der Verbraucherzentrale Bundesverband e.V. (vzbv) hat für interessierte Patient:innen oder Ärzt:innen einen Leitfaden „Datenschutz bei Videosprechstunden“ veröffentlicht, der eine Analyse der Datenschutzerklärungen von Telemedizin-Plattformen und Arzttermin-Portalen bietet. Welche Anforderungen hinsichtlich des Datenschutzes und der Datensicherheit an den Videodienstanbieter gestellt werden, sind in Anlage 31b des Bundesmantelvertrags-Ärzte (BMV-Ä) aufgeführt.
Die Videosprechstunde wird vom vzbv als ergänzendes Instrument im Versorgungsspektrum generell positiv betrachtet. Gezielt eingesetzt, kann sie den Behandlungsprozess ergänzen und optimieren, den Zugang zu ärztlicher Versorgung für Patient:innen verbessern und Ansteckungsrisiken in den Praxen mindern. Sie ist zudem zeit- und ressourcensparend.

Die Untersuchung analysiert anhand von Prüfkategorien neun ausgewählte Telemedizin-Plattformen und Arzttermin-Portale, die Videosprechstunden anbieten. Die Prüfkategorien orientieren sich an den Vorschriften der Datenschutz-Grundverordnung (DS-GVO) und nehmen den Datenschutz der Anbieter, unter Berücksichtigung des besonderen Schutzbedürfnisses von Gesundheitsdaten, in den Blick.

Die Ergebnisse der insgesamt 37 Prüfkategorien zeigen aus Verbrauchersicht jedoch verschiedene kritische Punkte, zum Beispiel hinsichtlich der ausdrücklichen Einwilligung in die Verarbeitung von Gesundheitsdaten, dem Einsatz von Tracking-Anbietern, der namentlichen Nennung von Datenempfängern sowie der Information über die Speicherdauer der personenbezogenen Daten.

Foto: Goffkein, Adobe Stock

Rechtliche Fallstricke: Remote Arbeiten aus dem Ausland

Während das Thema Corona und Arbeiten unter Pandemiebedingungen bei vielen Organisationen dazu geführt hat, dass sie sich das erste Mal mit Themen wie Remote Work oder Homeoffice beschäftigt haben, sind einige Organisationen bereits weiter und beschäftigen sich mit der Möglichkeit des „Remote Work aus dem Ausland".

Die Motivation, sich mit dem Thema auseinanderzusetzen, kann vielfältig sein. Entweder spielen betriebliche Erfordernisse eine Rolle oder die Organisation möchte das Thema als Teil von möglichen Incentive-Maßnahmen für die Beschäftigten vorantreiben, um die eigene Attraktivität für Arbeitnehmer zu steigern.

Der neue Bitkom-Leitfaden „Remote Work aus dem Ausland" beleuchtet die spezifischen Herausforderungen des mobilen Arbeitens im Ausland sowie ihre Lösungsmöglichkeiten und enthält einen kurzen Abschnitt zu den Themen „Datenschutz und IT-Sicherheit".

Foto: PhotoPlus+, Adobe Stock

Aufsichtsbehörde geht weiter gegen Facebook-Fanpages vor

Wer den regen Schlagabtausch der Datenschutz-Aufsichtsbehörden zum Thema Facebook-Fanpages verfolgt hat, dem dürfte die neueste Ankündigung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zum Thema als nur konsequent vorkommen.
Der BfDI hatte sich bereits in den Jahren 2019 und auch 2021 mit einem Rundschreiben an alle Ministerien, Behörden und öffentlichen Stellen gerichtet.

Seine Message an die Adressaten:

1. eine nachdrückliche Empfehlung, diese Seiten bis Ende 2021 abzuschalten, verknüpft mit dem eindrücklichen Hinweis, dass 2. ab Januar 2022 beabsichtigt sei – im Interesse der betroffenen Bürgerinnen und Bürger – schrittweise von den dem BfDI nach Art. 58 DS-GVO zur Verfügung stehenden Abhilfemaßnahmen Gebrauch zu machen.
Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder teilte später mit, dass sie das Urteil des Europäischen Gerichtshofs (EuGH) zur gemeinsamen Verantwortlichkeit der Betreiber im Hinblick auf die betriebenen Facebook-Fanpages zum Anlass genommen haben, um sich im Rahmen einer dazu eingerichteten Taskforce mit den Fragen rund um die Rechtskonformität des Betriebs einer Fanpage zu beschäftigen.
Eben diese Taskforce hatte ein Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages unter Berücksichtigung des seit dem 1. Dezember 2021 geltenden Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG), des Urteils des OVG Schleswig vom 25. November 2021 (Az. 4 LB 20/13) und der aktuellen technischen Umsetzungen erstellt und veröffentlicht. Zuletzt versendete der BfDI ein Anhörungsschreiben an das Bundespresseamt (BPA) zur Nutzung einer Facebook-Fanpage. Gespräche mit dem BPA und Facebook führten jedoch zu keiner Lösung der datenschutzrechtlichen Probleme, so der BfDI.

Am 22.03.2023 ging die Angelegenheit die nächste Runde:

Der BfDI hat das Bundespresseamt (BPA) angewiesen, den Betrieb der Facebook-Fanpage der Bundesregierung einzustellen, da dieser nicht datenschutzkonform sei. Das BPA hat vier Wochen Zeit, um diesen Bescheid umzusetzen. Der BfDI betont, dass der Staat über soziale Medien erreichbar sein soll und Informationen teilen können muss, dies aber nur dann, wenn die Grundrechte der Bürgerinnen und Bürger gewahrt bleiben. Das BPA müsse als Verantwortlicher nachweisen können, dass die Grundsätze des Datenschutzrechts eingehalten werden, was im vorliegenden Fall nicht zutreffend sei.

DataAgenda Podcast Folge 35: ChatGPT- Die Informationsgesellschaft entdeckt das Feuer

Die Nutzung von ChatGPT gerät in Europa sowie darüber hinaus zunehmend in die Kritik. Nicht nur Datenschutzbehörden, sondern auch Stimmen aus Wirtschaft, Verwaltung und Wissenschaft erkennen, dass der unbedarfte Einsatz solcher Software zum Problem wird. Die hochaktuelle Technik kollidiert mit Rechtsgütern und legitimen Interessen der europäischen Werteordnung. Wichtige Fragen lauten: Wie steht es um die Transparenz der Algorithmen? Wie verlässlich sind die Ergebnisse der Software? Wie schützt man Kinder und Jugendliche vor nicht altersgerechten Ergebnissen? Wie schützen die Anbieter Persönlichkeitsrechte, geistiges Eigentum und welche Vorkehrungen treffen sie gegen Fake News?

Prof. Rolf Schwartmann im Gespräch mit Prof. Dr. iur. Tobias Keber, Inhaber der Professur für Medienrecht und Medienpolitik in der digitalen Gesellschaft, Hochschule der Medien (HdM) Stuttgart.

Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter