NEWS BOX DATENSCHUTZ

AUSGABE
7/2021

INHALTSVERZEICHNIS

2 Editorial:
3 Aufsichtsbehörden bemängeln Cookie-Einwilligungen und Nudging
5 Übermittlung personenbezogener Daten an das Vereinigte Königreich „wieder sicher"
6 Neue EU-Standardvertragsklauseln machen ergänzende Maßnahmen nicht obsolet
7 Betriebsarzt und DSB als eigene Verantwortliche?
8 Meldungen von Datenpannen erreichen Höchststand
9 Biometrische Arbeitszeiterfassung mittels Fingerabdruck nur mit Einwilligung
9 GDD veröffentlicht Praxishilfe zum TTDSG
11 Praxishinweise zum Fragebogen der Aufsichtsbehörden
12 DataAgendaDatenschutz Podcast
13 Impressum

DATAKONTEXT

Levent Ferik

EDITORIAL:

Man kann dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) nicht vorwerfen, dass er untätig ist. Wenn man sich allein das Inhaltsverzeichnis des 29. Tätigkeitsberichts durchliest sowie seine Mitwirkung in Gremien und die behandelten Fachthemen betrachtet, kann man die vielfältigen Bereiche nur erahnen, die er seit einigen Jahren vorantreibt.
Auch in den sozialen Medien und insbesondere auf Twitter findet der BfDI Zeit, eine Lanze für den Datenschutz zu brechen und diesen vor zumeist unsachlichen Angriffen à la „Der Datenschutz ist schuld an der schleppenden Pandemiebekämpfung, an der behäbigen Digitalisierung [passendes Defizit eintragen]“ zu verteidigen.
Eben auf diesem Medium wies der BfDI am 25. Juni 2021 auf sein aktuelles Rundschreiben hin, welches zuallererst die Bundesministerien und die obersten Bundesbehörden adressiert, aber auch die sog. öffentlichen Stellen des Bundes. Inhalt des Schreibens ist die Feststellung des BfDI, dass der datenschutzkonforme Betrieb einer Facebook-Fanpage gegenwärtig nicht möglich sei. Dieser Feststellung vorangegangen war eine Karenzzeit, die der BfDI den obersten Bundesbehörden und einzelnen Ressorts gewährt hatte, um zu einer „Lösung“ für den datenschutzkonformen Betrieb dieser Fanpages zu kommen.
Diese Bemühungen sieht der BfDI nunmehr als gescheitert an und informiert darüber, dass ihm ein weiteres Abwarten angesichts der fortdauernden Verletzung des Schutzes personenbezogener Daten der Nutzerinnen und Nutzer nicht mehr möglich sei.
Seine Message an die Adressaten:
1. Eine nachdrückliche Empfehlung, diese Seiten bis Ende dieses Jahres 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.
Wie gesagt, kann man dem BfDI keine Untätigkeit vorwerfen. Es ist aber abzusehen, dass ihm nicht wenige ggf. Inkonsequenz vorwerfen könnten, angesichts der Tatsache, dass sein Hinweis auf Twitter erfolgte, einem Dienst, der mit einem vergleichbaren Makel behaftet ist, wie die angeprangerte Problematik der Facebook-Fanpages. („Es wäre erforderlich, dass öffentliche Stellen, die eine Fanpage betreiben, eine Vereinbarung mit Facebook zur gemeinsamen Verantwortlichkeit schließen, die den Anforderungen von Art. 26 Datenschutz-Grundverordnung (DS-GVO) entspricht.“)
Ob sich nun die für die Privatwirtschaft zuständigen Aufsichtsbehörden mit einer ähnlichen Offensive an die Verantwortlichen wenden werden, bleibt abzuwarten, erscheint aber unwahrscheinlich, bis nicht auch die letzten Bundesbehörden und öffentlichen Stellen ihre Fanpages stillgelegt haben.
Ebenfalls abzuwarten bleibt, ob der BfDI es ggf. dem LfDI BW gleich tut und sich von Twitter auf mastodon zurückzieht. Zu wünschen wäre das nicht, da der Twitter-Auftritt des BfDI oder besser gesagt, von Herrn Prof. Ulrich Kelber (als Privatperson) als Bereicherung angesehen wird,

findet
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Artur, Adobe Stock

Aufsichtsbehörden bemängeln Cookie-Einwilligungen und Nudging

Wie zahlreiche Datenschutz-Aufsichtsbehörden einstimmig vermelden, wurden im Rahmen einer konzertierten Aktion die Webseiten von Medienunternehmen in Bezug auf den Einsatz von Cookies und die Einbindung von Drittdiensten untersucht. Dabei wurden, auf Basis eines gemeinsamen Prüfkatalogs, 49 Webangebote in 11 Bundesländern geprüft. Schwerpunkt dabei war das Nutzertracking zu Werbezwecken. Nach den Feststellungen der Aufsichtsbehörden entsprechen die geprüften Webseiten nicht den rechtlichen Anforderungen für den Einsatz von Cookies und anderen Trackingtechniken. Die Medienunternehmen verstoßen damit gegen das Recht ihrer Nutzerinnen und Nutzer auf Schutz ihrer personenbezogenen Daten, so die Bewertung der verschiedenen Datenschutzbehörden. Die Webseiten fragen zwar in der Regel differenzierte Einwilligungen der Nutzerinnen und Nutzer für die Verwendung von Cookies und Drittdiensten ab. In der Mehrheit der Fälle sind diese Einwilligungen allerdings nach Auffassung der Aufsichtsbehörden nicht wirksam. Im Rahmen der Prüfung wurden vor allem die folgenden Mängel festgestellt:

- Falsche Reihenfolge: Häufig werden einwilligungsbedürftige Drittdienste bereits beim Öffnen der Webseiten eingebunden und Cookies gesetzt – also noch vor der Einwilligungsabfrage.
- Fehlende Informationen: Auf der ersten Ebene der Einwilligungsbanner werden zudem nur unzureichende oder falsche Informationen über das Nutzertracking gegeben.
- Unzureichender Einwilligungsumfang: Selbst, wenn der Nutzer die Möglichkeit wahrnimmt, bereits auf der ersten Ebene des Einwilligungsbanners alles abzulehnen, bleiben zahlreiche Cookies und Drittdienste aktiv, die eine Einwilligung erfordern.
- Keine einfache Ablehnung: Während bei allen Einwilligungsbannern auf der ersten Ebene eine Schaltfläche vorhanden ist, mit der eine Zustimmung zu sämtlichen Cookies und Drittdiensten erteilt werden kann, fehlt auf dieser Ebene häufig eine ebenso einfache Möglichkeit, das einwilligungsbedürftige Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können.
- Manipulation der Nutzerinnen und Nutzer: Die Ausgestaltung der Einwilligungsbanner weist zahlreiche Formen des Nudging auf. Das bedeutet, Nutzerinnen und Nutzer werden unterschwellig zur Abgabe einer Einwilligung gedrängt, indem die Schaltfläche für die Zustimmung beispielsweise durch eine farbliche Hervorhebung deutlich auffälliger gestaltet ist, als die Schaltfläche zum Ablehnen oder indem die Verweigerung der Einwilligung unnötig verkompliziert wird.

Quelle: LDI NRW

14. GDD

Gesellschaft für Datenschutz
und Datenschutzsicherheit e.V.

Sommer-Workshop

FÜR DATENSCHUTZBEAUFTRAGTE UND -BERATER SOWIE DATENSCHUTZDIENSTLEISTER

9. bis 11. August 2021

in Timmendorfer Strand

Praxisthemen

- Aktuelle Entwicklungen im Datenschutz
- Anforderungen an einen Beschäftigtendatenschutz
- Richtiger Umgang mit Richtlinien zur Vermeidung von Bußgeldern
- Der Auskunftsanspruch nach Art. 15 DS-GVO
- Die neuen Standarddatenschutzklauseln im Praxischeck
- Binding Corporate Rules – Interne Datenschutzvorschriften für Unternehmen
- Gute Gründe warum man amerikanische Bürosoftware nutzen darf
- Personal Information Management Systeme (PIMS) – Wege zum systematischen Einwilligungs- und Widerspruchsmanagement
- Privacy by Design & Default im Automotive-Umfeld
- Daten in der Corona-Pandemie
- Hacken
- Pandemiebekämpfung mit Apps & Co - Datenschutz als Showstopper?
- Schadensersatz nach DS-GVO: Kleine Preise, aber große Gefahr für Unternehmen?!

Übermittlung personenbezogener Daten an das Vereinigte Königreich „wieder sicher“

Foto: Pixelbliss, Adobe Stock

Die DS-GVO ordnet alle Länder außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) als sog. „Drittländer“ ein. Das bedeutet, dass im Falle eines geplanten Drittlandtransfers nicht davon ausgegangen werden kann, dass in dem jeweiligen Land ein „angemessenes Datenschutzniveau“ herrscht.
Sichere Drittländer sind solche, denen die Europäische Kommission per Angemessenheitsbeschlusses ein angemessenes Datenschutzniveau bestätigt hat. Dort gewährleisten die nationalen Gesetze einen Schutz von personenbezogenen Daten, welcher mit dem des EU-Rechts vergleichbar ist (sein soll), so die gewünschte Fiktion eines Angemessenheitsbeschlusses.
Da seit dem Vollzug des sog. Brexit (1. Januar 2021) Großbritannien bekanntermaßen kein Teil der EU mehr ist und Ende Juni 2021 zudem auch die Übergangsphase beendet sein wird, bedeutet dies in Konsequenz, dass personenbezogene Daten nicht ohne Weiteres in das Vereinigte Königreich transferiert werden dürfen (Art. 44 DS-GVO).
Wie oben schon erwähnt, kann ein „Angemessenheitsbeschluss“ eine Lösung für eine solche „Drittlandproblematik“ sein.
Gerade noch rechtzeitig (am 28. Juni 2021) hat die Europäische Kommission die in die Wege geleiteten Angemessenheitsbeschlüsse für die Übermittlung personenbezogener Daten an das Vereinigte Königreich, gemäß der DS-GVO und der Strafverfolgungsrichtlinie (LED), angenommen.
Mit der Anerkennung des angemessenen Datenschutzniveaus bedürfen Datenübermittlungen aus dem EWR an das Vereinigte Königreich, im Rahmen des Anwendungsbereichs der Beschlüsse, keiner besonderen Genehmigung. Die Prüfung, ob die allgemeinen datenschutzrechtlichen Voraussetzungen für eine Datenübermittlung erfüllt sind, ist davon unabhängig erforderlich und vorzunehmen.

Neue EU-Standardvertragsklauseln machen ergänzende Maßnahmen nicht obsolet

Foto: Bernulius, Adobe Stock

In einem aktuellen Papier „Ergänzende Prüfungen und Maßnahmen trotz neuer EU-Standardvertragsklauseln für Datenexporte nötig“ gibt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Hinweise dazu, wie es sich auswirkt, dass mit Durchführungsbeschluss vom 4. Juni 2021 die Europäische Kommission neue Standardvertragsklauseln erlassen hat, die eine rechtskonforme Übermittlung personenbezogener Daten in Drittländer ermöglichen sollen.

Die DSK macht insbesondere darauf aufmerksam, dass alleine die Nutzung der neuen Standardvertragsklauseln nicht dazu führt, dass im Fall von Datenübermittlungen in die USA, ergänzende Maßnahmen, die einen Zugriff der US-Behörden auf die verarbeiteten Daten verhindern sollen, obsolet werden.

Nach wie vor gelte, dass Unternehmen und andere Akteure, die personenbezogene Daten in Drittländer übermitteln, gegenüber der Aufsichtsbehörde nachweisen müssen, dass sie die aufsichtsbehördlich geforderte Prüfung zum Schutzniveau im Drittland im Einzelfall durchgeführt haben und zu einem positiven Ergebnis gekommen sind.

Auch bei Verwendung der neuen EU-Standardvertragsklauseln bleibt also nach Bewertung der DSK eine Prüfung der Rechtslage im Drittland und zusätzlicher ergänzender Maßnahmen erforderlich.

Weitere hilfreiche Informationen zur Thematik finden Sie auf dem Blog der KREMER RECHTSANWÄLTE.

Quelle: DSK

Foto: s_l, Adobe Stock

Betriebsarzt und DSB als eigene Verant-wortliche?

Ob es sich beim Betriebsrat um einen eigenen Verantwortlichen handelt oder ob er Teil der verantwortlichen Stelle ist, wurde in der Datenschutzwelt in den letzten Jahren zuhauf diskutiert. Das Thema fand auch innerhalb der Tätigkeitsberichte der Aufsichtsbehörden immer mal wieder seinen Platz.
In dem Tätigkeitsbericht zum Jahr 2020 des Sächsischen Datenschutzbeauftragten wird jedoch erläutert, ob eine etwaige eigene Verantwortlichkeit auch im Falle des Betriebsarztes (Ziffer 2.1.1) und des (externen) Datenschutzbeauftragten (Ziffer 2.1.2) infrage kommen kann.
Weiter auf DataAgenda lesen

Quelle: Sächsischer Datenschutzbeauftragter

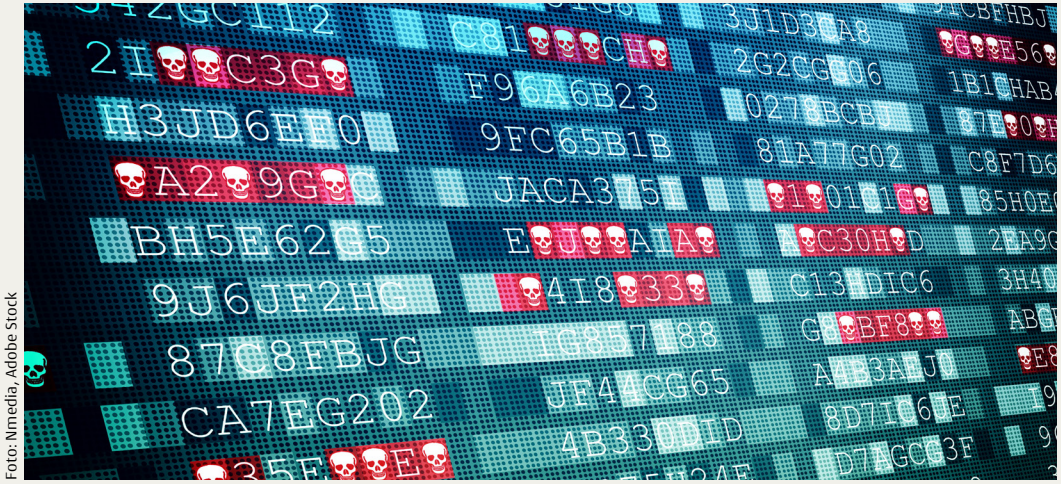

Foto: Nmedia, Adobe Stock

Meldungen von Datenpannen erreichen Höchststand

Im April 2021 hatte die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., im Rahmen der Konsultation des Europäischen Datenschutzausschusses zu Beispielfällen einer Datenschutzverletzung, eine Umfrage für die Öffentlichkeit initiiert, deren Ergebnisse die Bedeutung dieser Thematik für die Datenschutzpraxis einordnen sollte und Datenschutzpraktikern einen tieferen Einblick anhand von fünf Beispielfällen aus der Praxis im Umgang mit „Datenpannen" geben sollte.

Die unbeabsichtigte Übermittlung personenbezogener Daten an falsche Empfänger ist die mit Abstand am häufigsten gemeldete Kategorie (47 %). Cyberangriffe gaben ebenfalls einen Anlass für Datenschutzverletzungen (14 %), wobei sich diese nochmals in Unterkategorien einteilen lassen, so bspw. Phishing-, Ransomware- oder andere Attacken zur Umgehung von Zugangsbeschränkungen bzw. Rechteeskalation.

Der Sächsische Datenschutzbeauftragte hat am 17. Juni 2021 seinen Tätigkeitsbericht für das zurückliegende Jahr vorgestellt. Auch hier spielt das Thema „Meldung von Datenschutzpannen" eine gewichtige Rolle und es fällt ins Auge, dass sich hier ein ähnliches Bild abzeichnet, wie im GDD-Praxisreport.
Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

- Cyberkriminalität: Typische Handlungsfelder waren die Verschlüsselung und das Abgreifen von personenbezogenen Daten aus E-Mail-Postfächern, von Servern oder anderweitigen Datenträgern.
- Fehlversand: Auf diese Fallgruppe entfielen im Berichtszeitraum die meisten Meldungen. Typische Fälle: Unterlagen mit falscher Zuordnung, fehlerhafter Kuvertierung oder Verwechslung der Empfängerperson. Vielfach waren Gesundheitsdaten betroffen, die aufgrund ihrer hohen Sensibilität und Vertraulichkeit ein besonders hohes Maß an Sorgfalt von der verantwortlichen Stelle fordern.
- Offene E-Mail-Verteiler stellen nach wie vor den Klassiker der Datenschutzverletzung dar. Obgleich hierbei in der Regel das Risiko für die Betroffenen als durchaus gering eingeschätzt werden kann, ist eine solche Datenschutzverletzung gemäß Datenschutz-Grundverordnung in den meisten Fällen meldepflichtig.
- Der Verlust von Unterlagen auf dem Postweg trat im Berichtsjahr häufig auf. Bei Bekanntwerden einer solchen Problematik ist eine kritische Bewertung des Versanddienstleisters geboten.
- Einbrüche und Diebstähle sind besonders problematisch. Sie zählen zu den kriminellen Handlungen, und damit ist das verbundene Risiko für die betroffenen Personen besonders hoch. Daher sind technisch-organisatorische Maßnahmen geboten, wie zum Beispiel die ordnungsgemäße Verwahrung und Verschlüsselung von Datenträgern.

Foto: katz23, Adobe Stock

Biometrische Arbeitszeiterfassung mittels Fingerabdruck nur mit Einwilligung

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit beschäftigt sich in seinem 49. Tätigkeitsbericht zum Datenschutz und dem 3. Tätigkeitsbericht zur Informationsfreiheit ausführlich mit der Frage, ob Verantwortliche, die ihre Beschäftigten verpflichten, an Systemen teilzunehmen, welche die Zeit mittels Fingerabdrucks erfassen, um hierdurch Missbrauch und Manipulation zu verhindern, gegen die Bestimmungen der DS-GVO verstoßen und welche aufsichtsbehördlichen Konsequenzen daraus erwachsen können (Ziffer 7.1).
Weiter auf DataAgenda lesen

Quelle: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

GDD veröffentlicht Praxishilfe zum TTDSG

Ab dem 1. Dezember 2021 gilt das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Ziel des TTDSG ist die erforderliche Anpassung der Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die Datenschutz-Grundverordnung (DS-GVO) sowie die – bereits lange ausstehende – Umsetzung der ePrivacy-Richtlinie (RiLi 2002/58/EG in der durch die RiLi 2009/136/EG geänderten Fassung). Zugleich soll mit der Gesetzesänderung die Rechtsunsicherheit beseitigt werden, die durch das bisherige Nebeneinander von DS-GVO, TMG und TKG entstand.
Die Datenschutzbestimmungen von TKG und TMG werden hierzu in einem Gesetz zusammengefasst. Parallel zur Schaffung des TTDSG hat der Bundesgesetzgeber auch das TKG modernisiert. Mit der Novellierung des TKG und der Schaffung des TTDSG werden bestehende Schutzlücken geschlossen und der europäische Kodex für die elektronische Kommunikation umgesetzt (RL (EU) 2018/1972). Mit ihrer neuen Praxishilfe gibt die GDD einen Überblick über die Neuregelungen und den sich hieraus für die Datenschutzpraxis ergebenden Handlungsbedarf. Die Praxishilfe kann auf den Seiten der GDD abgerufen werden.

Foto: nmann77, Adobe Stock

Praxishinweise zum Fragebogen der Aufsichtsbehörden

Foto: metamorworks, Adobe Stock

Die GDD gibt Unternehmen Hinweise zur Beantwortung des Fragebogens der Aufsichtsbehörden zum konzerninternen Datenverkehr nach Schrems II.

Anlässlich einer koordinierten Kontrolle von grenzüberschreitenden Datenübermittlungen in Drittländer seitens der deutschen Aufsichtsbehörden sollen ausgewählte Unternehmen auf Basis eines Fragenkataloges angeschrieben werden. Insgesamt fünf Themenbereiche werden von unterschiedlichen Fragebögen abgedeckt. Diese sind:

- Bewerberportale
- Konzerninterner Datenverkehr
- Mailhoster
- Tracking
- Webhoster

Hintergrund ist das Urteil des EuGH zu Schrems II. Dort wurde zum einen festgestellt, dass Übermittlungen in die USA nicht länger auf Basis des EU-U.S.-Privacy Shields erfolgen können. Die Verwendung von EU-Standardvertragsklauseln steht unter dem Vorbehalt, dass der Datenimporteur im Drittland keinen Gesetzen unterliegt, die ihm die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

Die GDD möchte betroffene Unternehmen und deren Datenschutzbeauftragte unterstützen und allgemeine Hinweise zur Beantwortung des Fragebogens zum konzerninternen Datenverkehr geben. Teile dieser Fragen werden auch in den übrigen Fragebögen verwendet, sodass diese Hinweise dort ebenfalls Gültigkeit haben.

Die GDD-Praxishinweise sind hier abrufbar.

Quelle: Gesellschaft für Datenschutz und Datensicherheit

DATA AGENDA PODCAST

Der 10-Minuten-Talk mit Prof. Schwartmann

Folge #3

Update Beschäftigtendatenschutz in der Pandemie

Prof. Dr. Jürgen Kühling

Folge #4

Drei Jahre DS-GVO – Licht und Schatten

Prof. Dr. Gregor Thüsing

Folge 3: Update Beschäftigtendatenschutz in der Pandemie

In der hoffentlich ausklingenden Pandemie stellen sich Fragen nach der Zukunft des Homeoffice. Wie ist die Rechtslage nach dem 30. Juni 2021, wenn die „Homeoffice-Pflicht" endet? Was bringt das neue Betriebsräte-modernisierungsgesetz für den Datenschutz beim Betriebsrat und empfiehlt der Beirat zum Beschäftigtendatenschutz des Bundesministeriums für Arbeit und Soziales die Verabschiedung eines Beschäftigtendatenschutzgesetzes? Darum geht es im DataAgenda Datenschutzpodcast „Update Beschäftigtendatenschutz in der Pandemie" mit Professor Dr. Gregor Thüsing. Er ist er Mitglied des Beirats zum Beschäftigtendatenschutz und im Hauptberuf Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit an der Universität Bonn und im Ehrenamt Mitglied im Vorstand der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.).
Zum Podcast bitte hier klicken.

Folge 4: Drei Jahre DS-GVO – Licht und Schatten

Ist die Datenschutzgrund-Verordnung ein bürokratisches Monster oder ist sie in der Digitalisierung unverzichtbar? Wie steht es um die Datenschutzaufsicht in Deutschland und Europa, nach drei Jahren DS-GVO? Gibt das aktuelle Datenschutzrecht die richtigen Antworten die die Geschäftsmodelle von Google, Apple, Facebook und Amazon und sind Einwilligungsmanagementsysteme nach dem TTDSG eine Modell für die ePrivacy-Debatte? Darüber sprechen Rolf Schwartmann und Jürgen Kühling, Professor an der Universität Regensburg und Vorsitzender der Monopolkommission unter der Überschrift „Drei Jahre DS-GVO – Licht und Schatten" im DataAgenda-Podcast.
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

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

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Hans-Günter Böse, 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