NEWS BOX DATENSCHUTZ

AUSGABE
1/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Bereits am 16.12.2020 stellte die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) NRW fest, dass dort, wo Daten erhoben werden, auch immer neue Begehrlichkeiten geweckt werden, diese Daten zu anderen Zwecken zu nutzen. Diese Feststellung der LDI NRW betraf zwar in diesem konkreten Fall die zweckwidrige Nutzung der Corona-Kontaktlisten für die Strafverfolgung, jedoch bewahrheiteten sich in der Vergangenheit die meisten diesbezüglichen „Prognosen". Nutzung von Mautdaten zur Strafverfolgung, Zugriff auf Smarthome-Daten zur Strafverfolgung, Tesla gibt Filmaufnahmen und Daten an die Ermittlungsbehörden: Die Liste der oftmals zweckwidrigen Nutzung von einmal generierten personenbezogenen Daten ließe sich ohne Probleme fortführen.
Aus Sicht der Betroffenen kam im Fall der Zugriffe auf Corona-Kontaktlisten erschwerend hinzu, dass die Möglichkeit der zweckändernden Verwendung zur Strafverfolgung vielfach zuvor nicht bekannt war.
Der Unmut bei den Betroffenen ist naturgemäß vorprogrammiert, wenn, wie in diesem konkreten Fall, zuvor durch öffentliche Stellen der Eindruck erweckt wurde, dass diese Daten ausschließlich für die Bekämpfung der Corona-Pandemie genutzt werden dürfen. Weitere Gefahren einer intransparenten und (unzulässigen) Zweckänderung: Risiken für die Akzeptanz der breiten Bevölkerung, einschneidende Maßnahmen, wie die im Zusammenhang mit der Corona-Pandemie, weiter hinzunehmen, sowie die abnehmende Akzeptanz, wahrheitsgemäße Angaben zu machen.
Dass die Lösung nicht nur darin liegen kann, eine enge Verwendungsbeschränkung im Sinne des § 28a Abs. 4 Infektionsschutzgesetz (IfSG) einzuführen, zeigt der neuerliche Fall der Mainzer Polizei ganz deutlich: Diese nutzte Daten aus der Luca-App ohne Rechtsgrundlage. Ein Besucher war Ende November nach dem Verlassen einer Gaststätte offenbar so gestürzt, dass er einige Tage später aufgrund seiner Verletzungen starb. Mittels der Datenabfrage wurden weitere Besucher der Gaststätte in der Mainzer Innenstadt ausfindig gemacht, um diese als mögliche Zeugen des Vorfalls zu gewinnen. Nach der o. g. Norm dürfen diese Daten nur noch für die Zwecke verwendet werden, für die sie erhoben wurden. Eine Nutzung zu Strafverfolgungszwecken ist danach ausgeschlossen.
Einen anderen „Lösungsweg" aus dieser Misere zeigt bereits die Datenschutz-Grundverordnung (DS-GVO) mit Art. 25 selbst auf: Eine staatliche Überwachung mittels der aktuellen deutschen Corona-Warn-App ist bspw. ausgeschlossen – „by design". Durch den Ansatz, den Quellcode offenzulegen, hat die Bundesregierung zudem für eine maximal mögliche Transparenz gesorgt. GPS-Daten werden weder erfasst noch übertragen. Angesichts aller anderen Apps, die auf den Smartphones (vor-)installiert sind und rund um die Uhr umfangreiche Daten sammeln und an die Anbieter übermitteln, sollte die Corona-Warn-App den geringsten Anlass zur Sorge um die Grundrechte geben. Für ganz Wissbegierige hält die Datenschutz-Folgenabschätzung auf über 220 Seiten weitere Details bereit. Ein Grund mehr, auf die Corona-Warn-App zu setzen, findet Ihr

Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: VideoFlow, Adobe Stock

Der 10. GDD-Winter-Workshop macht den Jahresauftakt – Datenschutz bleibt auch in 2022 spannend

Datenschutzbeauftragte, Datenschutzberater und Dienstleister aus ganz Deutschland treffen sich alljährlich zum GDD-Winter-Workshop, der Fachtagung zum Anfang des Jahres für Datenschutz in Deutschland. Das Corona-Virus macht allerdings leider vor keinem Lebensbereich halt und so kann der Winter-Workshop auch dieses Mal nicht wie gewohnt stattfinden. Die aktuellen Entwicklungen und Problemfelder sind aber zu drängend, um sie gänzlich ausfallen zu lassen. Um der pandemischen Lage gerecht zu werden, findet der Workshop auch in diesem Jahr wieder online statt.

Das neue TTDSG regelt Tracking auf Webseiten und Vieles mehr

Seit der Anwendungspflicht des neuen Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) besteht aktuell starke Rechtsunsicherheit beim Einsatz von Tracking-Tools. Erfolgt etwa die Einwilligung nun nach Art. 6 Abs. 1 lit. a DS-GVO oder aufgrund von § 25 TTDSG? Sollte das Gesetz doch eigentlich vor allem die Rechtsunklarheiten klären, stehen Unternehmen und Verbraucher nun erneut vor ungeklärten Fragen. *Christian Dürschmied* vom Bundesverband für Digitale Wirtschaft (BVDW) e.V. wird deshalb seine Erfahrungen aus der Praxis speziell in der Digitalen Wirtschaft im Zusammenhang mit dem länderübergreifenden Prüfverfahren zum Einsatz von Tracking-Tools auf Webseiten erläutern.

Möglichkeiten, Grenzen, Risiken bei der Nutzung von Videokonferenzlösungen von US-Anbietern

Spätestens seit der Corona-Pandemie ermöglichen immer mehr Unternehmen den Beschäftigten aus dem Home-Office zu arbeiten. Gerade bei den „Software as a Service" (SaaS)-Angeboten aus den USA ist Datenschutz ein Thema. Für den rechtmäßigen Einsatz solcher Videokonferenzlösungen ist ein angemessenes Schutzniveau und die Einhaltung der Vorgaben der DS-GVO erforderlich. Der stellvertretende Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz, *Helmut Eiermann*, wird zu diesem Thema referieren und auf mögliche Risiken, rechtliche und technische Anforderungen sowie die Reaktionen der Aufsichtsbehörden eingehen. Außerdem ist er bemüht Lösungswege zu den datenschutzkonformen Möglichkeiten im Umgang aufzeigen.

Datenschutz praktisch umsetzen beim Einsatz von Microsoft

Nicht nur der Einsatz von Videokonferenztechnik steht durch das „Schrems II"-Urteil des EuGH vor großen Herausforderungen, sondern grundsätzlich jeder Datentransfer in die USA oder in andere Drittstaaten. Gerade beim Einsatz von Standard-Software macht sich das für nahezu jedes Unternehmen bemerkbar. Microsoft hat auf das Urteil reagiert und seine integrierten Standarddatenschutzklauseln in den Kundenverträgen um „Additional Safeguards Addendum to Standard Contractual Clauses" ergänzt. Wie die Datenschutzgrundsätze bei Microsoft explizit aussehen, wie es sich mit der EU-Regulatorik verhält und was „Defendig your data" bedeutet, werden *Rebecca Beerman-Wendel* und *Stephanus Schulte* von Microsoft Deutschland GmbH in ihrem Vortrag erläutern.

Top-Experten als Referenten auf dem GDD-Winter-Workshop

Neben weiteren Aufsichtsbehördenvertretern wie Barbara Thiel, Landesdatenschutzbeauftragte Niedersachsen, und Dr. Stefan Brink aus Baden-Württemberg werden zahlreiche weitere Datenschutz-Experten (RA Andreas Jaspers, RA Thomas Müthlein, Prof. Dr. Rolf Schwartmann, Dr. Bernd Schütze und Kristin Benedikt) ausgewählte und aktuelle Themen für Sie präsentieren. Stellen Sie Top-Experten Ihre Fragen und genießen Sie die den fachlichen Austausch.

Eine detaillierte Übersicht inklusive Ablaufplan über den angebotenen Workshop und weitere Informationen finden Sie hier

Foto: Iettas, Adobe Stock

Datenschutzkonformes Auslesen und Prüfen digitaler Impfnachweise

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat die Nr. 40 seiner sog. „Aktuellen Kurz-Information“ (AKI) dem datenschutzkonformen Auslesen und Prüfen digitaler Impfnachweise gewidmet.

Ein digitales Zertifikat enthält neben den Grunddaten (Name und Vornamen, Geburtsdatum und Typ des Nachweises) insbesondere folgende Daten:

- bei einem Impfnachweis: Impfstoff; Impfstoffhersteller; Anzahl der Impfungen; jeweiliges Datum der einzelnen Impfungen; Land, in dem die jeweilige Impfung erfolgte;
- bei einem Testnachweis: Art des Tests; Herstellerdaten; Datum der Testdurchführung; Ergebnis des Tests; Testzentrum; Land, in dem die Testung stattfand;
- bei einem Genesenennachweis: Datum des ersten positiven Tests; Land, in dem der Test durchgeführt wurde.

Der BayLfD fasst die Kernaussagen der AKI 40 wie folgt zusammen:

- Ein gesicherter digitaler Impfnachweis ist nur im QR-Code enthalten und kann zuverlässig mit technischen Hilfsmitteln geprüft werden.
- Zur Prüfung kann die CovPassCheck-App verwendet werden. Die CovPass-App oder die Corona-Warn-App darf dafür nicht verwendet werden.
- Bei der Prüfung muss der Grundsatz der Datenminimierung beachtet werden.

Nach Auffassung des BayLfD ist für eine Prüfung ausschließlich eine Prüf-App zu nutzen (CovPassCheck) und nicht eine App, die zum Speichern der Zertifikate verwendet wird (CovPass- oder Corona-Warn-App), da ansonsten die Zertifikate nicht geprüft, sondern auf dem Mobiltelefon der prüfenden Person dauerhaft gespeichert würden.
Wichtige Hinweise erfolgen auch unter dem Aspekt der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DS-GVO. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Möchte ein Verantwortlicher beispielsweise den 3G-Status einer Person prüfen, so sieht der BayLfD es nicht als notwendig an, den verwendeten Impfstoff zu erheben. Grundsätzlich sei es im Rahmen von 3G-Zutrittsregeln nicht einmal nötig, zwischen Impf-, Genesenen- und Testnachweis zu unterscheiden.

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Foto: elenabsl, Adobe Stock

Fallbasierte Leitlinien für Datenschutzverletzungen

Der Europäische Datenschutzausschuss (EDSA) hat seine aktualisierten Leitlinien zu Datenschutzverletzungen veröffentlicht.

Die DS-GVO schreibt in bestimmten Fällen vor, dass eine Verletzung des Schutzes personenbezogener Daten der zuständigen nationalen Aufsichtsbehörde gemeldet werden muss und dass die Personen, deren personenbezogene Daten von der Verletzung betroffen sind, über die Verletzung zu informieren sind (Art. 33 und 34 DS-GVO). Die Artikel-29-Datenschutzgruppe hatte bereits im Oktober 2017 einen allgemeinen Leitfaden zur Meldung von Datenschutzverletzungen erstellt, in dem die einschlägigen Abschnitte der DS-GVO analysiert wurden („Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679“) (im Folgenden Working Paper 250 bzw. WP 250). Aufgrund ihrer Art und ihres Veröffentlichungszeitpunkts wurden in dieser Leitlinie jedoch nicht alle praktischen Fragen hinreichend ausführlich behandelt. Daher hat der ESDA den Bedarf an einem praxisorientierten, fallbasierten Leitfaden erkannt, der die von den nationalen Aufsichtsbehörden seit der Anwendbarkeit der Datenschutz-Grundverordnung gesammelten Erfahrungen in einer Leitlinie für die Verantwortlichen nutzbar macht.
Die neue fallbasierte Leitlinie ist als Ergänzung zu dem WP 250 gedacht und spiegelt die gemeinsamen Erfahrungen der nationalen Aufsichtsbehörden des Europäischen Wirtschaftsraums (EWR) seit dem Wirksamwerden der DS-GVO wider. Es soll den für die Datenverarbeitung Verantwortlichen bei der Entscheidung helfen, wie mit Datenschutzverletzungen umzugehen ist und welche Faktoren bei der Risikobewertung zu berücksichtigen sind.

Die dargestellten Fälle sind im Wesentlichen nach folgenden Themen unterteilt:

1. Ransomware
2. Data Exfiltration ATTACKS
3. Internal Human Risk Source
4. Lost or stolen devices and paper documents
5. Mispostal
6. Other Cases – Social Engineering

Quelle: EDSA

Foto: Chris, Adobe Stock

Viele Wege führen nach Rom: das Verzeichnis der Verarbeitungstätigkeiten

Was das sog. Verzeichnis der Verarbeitungstätigkeiten (VVT) angeht, dürften tatsächlich nicht ALLE Wege, aber doch zumindest VIELE Wege nach Rom führen. Obwohl ein VVT nicht erst seit Wirksamwerden der DS-GVO von den allermeisten Daten verarbeitenden Stellen (Verantwortlichen) geführt werden muss, gibt es doch immer noch viel Unwissen, Halbwissen und Missverständnisse in Bezug auf dieses Thema. Dabei gehen die Meinungen auch hinsichtlich der tatsächlichen Erstellung eines VVT oft auseinander.

Weiter auf DataAgenda lesen

Beschäftigtendatenschutz und Pandemiebekämpfung

Grundsätzlich findet die Datenschutz-Grundverordnung auch für die Verarbeitung von Beschäftigtendaten Anwendung. Sie ermöglicht es den Mitgliedstaaten, spezifische Vorschriften für den Beschäftigtendatenschutz zu erlassen.

Foto: PhotoSG, Adobe Stock

Die maßgebliche – aber nicht ausschließliche – Norm, die vom deutschen Gesetzgeber erlassen wurde, ist § 26 Bundesdatenschutzgesetz (BDSG). Was die Verarbeitung von Beschäftigtendaten im Rahmen der aktuellen Pandemiebekämpfung angeht, kommen zu dem ohnehin mit Unsicherheiten behafteten Beschäftigtendatenschutz Fragen hinzu, die sich bislang so noch nicht gestellt hatten.

Wie die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in ihrem aktuellen Papier „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie“ (Stand: 20.12.2021) treffend feststellt, enthält die DS-GVO selbst keine konkreten, bereichsspezifischen Regelungen zur Verarbeitung von personenbezogenen Daten (pbD) im Beschäftigtenkontext für den Fall einer Pandemie. Stattdessen beinhalten Art. 6 Abs. 2 und Abs. 3 DS-GVO, Art. 9 Abs. 2 und Abs. 4 DS-GVO sowie Art. 88 Abs. 1 DS-GVO sogenannte Öffnungsklauseln.

Das aktuelle Papier befasst sich daher mit den häufigsten Fragen, die in der jüngeren Vergangenheit der Pandemiebekämpfung die meisten Verantwortlichen beschäftigt haben dürften, und bietet auf 18 Seiten ein wenig mehr Handlungs- und Rechtssicherheit. Es sollte von den Verantwortlichen genutzt werden, noch zu etablierende Verfahren rechtzeitig auf eine rechtlich belastbare Grundlage zu stützen oder bereits etablierte Verfahren auf ihre rechtliche Zulässigkeit zu überprüfen.

Foto: Prostock-studio, Adobe Stock

Foto ohne Einwilligung – Beschäftigte erhält 5.000 Euro Schadensersatz

ArbG Münster, Urt. v. 25.03.2021 – 3 Ca 391/20

Mit einem Urteil vom 25.03.2021 (3 Ca 391/20) hat das Arbeitsgericht (ArbG) Münster entschieden, dass einer Beschäftigten einer Hochschule eine Entschädigung in Höhe von 5.000 Euro zusteht, da die Universität ein Foto von der Mitarbeiterin zu Marketingzwecken verwendet hat, ohne die erforderliche Einwilligung eingeholt zu haben.

Was war geschehen?

Folgender Sachverhalt liegt der Entscheidung zugrunde: Die Mitarbeiterin einer Universität wehrte sich in einem arbeitsrechtlichen Verfahren gegen die Verwendung ihres Fotos. Das Foto der Beschäftigten wurde aufgrund ihrer Ethnie und Hautfarbe als Ausweis für die Internationalisierung der Universität genutzt. Die Klägerin arbeitet jedoch als Postdoc und hat somit originär nichts mit der Internationalisierung der Hochschule zu tun. Bei der Erstellung von Foto-Aufnahmen der Universität hat sie aktiv teilgenommen, jedoch keine Einwilligung erteilt. Die Klägerin ließ lediglich mündlich offen, dass sie möglicherweise zustimmen würde, wenn die Fotos für ihre Tätigkeit verwendet würden. Nach Veröffentlichung der Fotos und Kenntnisnahme der Klägerin teilte diese mit, dass sie mit der Art der Verwendung ihrer Bilder nicht einverstanden ist. Die Universität erklärte daraufhin, dass ihr Foto gelöscht worden sei, aber es nicht möglich sei, die bereits gedruckten Broschüren zurückzuziehen. Die Klägerin forderte dann Schadensersatz gemäß Art. 82 DS-GVO, aber ebenso auf Grundlage des Kunsturheberrechtsgesetzes (KUG) und § 823 Bürgerliches Gesetzbuch (BGB).

Klage gegen Arbeitgeber hat Erfolg

Das ArbG Münster entschied, dass der Klägerin ein immaterieller Schadensersatz in Höhe von 5.000 Euro zusteht. Diese Zahlung wird gerne auch als Schmerzensgeld bezeichnet, stellt aber im Sinne der DS-GVO einen immateriellen Schadensersatz und nach Logik des deutschen Schuldrechts eine billige Entschädigung in Geld dar. Bemerkenswert ist, dass die immaterielle Schadenshöhe hier ihrem monatlichen Bruttolohn entspricht. Bei der richterlichen Schadensbemessung wurde ausdrücklich auch die Bedeutung der ethnischen Herkunft und der Hautfarbe der Mitarbeiterin für die Veröffentlichung des Fotos gewürdigt.
Die Entscheidung des Arbeitsgerichts Münster hat die Folgen einer rechtswidrigen Datenverarbeitung noch einmal klargestellt: Wer Bildnisse ohne Zustimmung der betroffenen Person nutzt, muss mit einer nicht unerheblichen Summe für die Entschädigung nach Art. 82 DS-GVO rechnen.

Datenschutz-Leitfaden für KMU

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt (Albert Cohaus als Vertreter im Amt) hat seinen Leitfaden „Datenschutz ist Chefsache“ für kleine und mittlere Unternehmen (KMU) in zweiter Auflage veröffentlicht.

Foto: DOC RABE Media, Adobe Stock

Als Adressat des Leitfadens sieht die Datenschutzaufsicht ganz explizit Unternehmer, Geschäftsführer und Führungskräfte eines kleinen oder mittleren Unternehmens bzw. alle Personen, die in sonstiger Funktion mit Fragen des Datenschutzes befasst sind.

Tatsächlich handelt sich bei dem Leitfaden um eine kompakte Darstellung, die die wesentlichen datenschutzrechtlichen Themen anreißt und für eine detailliertere Einarbeitung sensibilisiert. Der Leitfaden soll nach den Worten der Behörde als Orientierungshilfe bei der Durchführung notwendiger Maßnahmen zur Umsetzung von Datenschutz und Datensicherheit sowie zur Selbstüberprüfung dienen.
Das Onlinewerk, welches bald auch in einer Printversion erscheinen soll, untergliedert sich in 18 Kapitel und enthält grundlegende Informationen zu Fragestellungen, die in jedem kleinen und mittleren Unternehmen relevant sein können. In den jeweiligen Kapiteln befinden sich Hinweise zu vertiefenden, mitunter sehr ausführlichen Quellen, hilfreichen Formularen, Vorlagen usw., die sich alle auf der Homepage des Landesbeauftragten befinden. Die Hinweise erfolgen in Form von schreibbaren Kurzlinks.

Quelle: Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Foto: MASHKA, Adobe Stock

Log4Shell-Sicherheitslücke kann zur Datenpannen-Meldepflicht führen

Die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer extrem kritischen Bedrohungslage. Das BSI hat daher seine bestehende Cyber-Sicherheitswarnung auf die Warnstufe Rot hochgestuft. Ursächlich für diese Einschätzung sind die sehr weite Verbreitung des betroffenen Produkts und die damit verbundenen Auswirkungen auf unzählige weitere Produkte.

Weiter auf DataAgenda lesen

Fristlose Kündigung wegen Datenschutzverstoß

Liest eine Arbeitnehmerin, die im Rahmen ihrer Buchhaltungsaufgaben Zugriff auf den PC und das E-Mail-Konto ihres Arbeitgebers hat, unbefugt eine an ihren Vorgesetzten gerichtete E-Mail …

Foto: Pixelot, Adobe Stock

… und fertigt von dem Anhang einer offensichtlich privaten E-Mail eine Kopie an, die sie an eine dritte Person weitergibt, so rechtfertigt dies eine fristlose Kündigung. Dies hat das Landesarbeitsgericht (LAG) Köln am 02.11.2021 entschieden und das anderslautende Urteil des ArbG Aachen aufgehoben.

Die gegen die Kündigung erhobene Kündigungsschutzklage war beim Arbeitsgericht Aachen in erster Instanz erfolgreich, da die Richter zwar die Auffassung vertraten, dass ein wichtiger Grund für eine fristlose Kündigung im Sinne von § 626 BGB vorliegen würde. Jedoch gaben sie der Klage statt, weil sie im Rahmen der vorzunehmenden Güterabwägung zugunsten der Klägerin berücksichtigt hatten, dass das Arbeitsverhältnis 23 Jahre lang unproblematisch verlaufen sei und mangels Wiederholungsgefahr eine fristlose Kündigung unverhältnismäßig wäre.

Das sah das LAG Köln anders. Die Richter sahen hier das für die Aufgaben der Klägerin erforderliche notwendige Vertrauensverhältnis als unwiederbringlich zerstört an. Die Klägerin habe, so die Richter, mit der unbefugten Kenntnisnahme und Weitergabe fremder Daten einen schwerwiegenden Verstoß gegen das arbeitsvertragliche Rücksichtnahmegebot begangen. Dies insbesondere auch deshalb, weil mit ihrem Verhalten eine Verletzung von Persönlichkeitsrechten einhergeht.

Quelle: LAG Köln

Folge #11 Das Telegram-Dilemma

NRW-Justizminister Peter Biesenbach und
Oberstaatsanwalt Markus Hartmann von der ZAC-NRW


Peter Biesenbach


Markus Hartmann

Folge 11: „Das Telegram-Dilemma“

Das Telegram-Dilemma: Telegram ist ein Messengerdienst, mit dem man individuell oder in Gruppen von bis zu 200.000 Mitgliedern kommunizieren kann. Weil dort Gewaltaufrufe verbreitet werden, ist Telegram zu einem Problem für den öffentlichen Frieden geworden. Unterfällt der Dienst dem Netzwerkdurchsetzungsgesetz (NetzDG) und was hilft das? Kann man Telegram in Deutschland zur Not blockieren? Welche Auswege gibt es im Rechtsstaat? DataAgenda Podcast mit NRW-Justizminister Peter Biesenbach und Oberstaatsanwalt Markus Hartmann von der Zentral- und Ansprechstelle Cybercrime (ZAC) NRW
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:
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