NEWS BOX DATENSCHUTZ

AUSGABE
11/2021

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Das BSI hatte die Angriffswelle auf Microsoft-Exchange-Server im Frühjahr 2021 als extrem kritisch eingestuft. 98 Prozent der in Deutschland geprüften Systeme waren nach Angaben des BSI zeitweise verwundbar. Durch Warnungen sei der Anteil innerhalb von zwei Wochen unter die Zehn-Prozent-Marke gedrückt worden, berichtete das BSI einige Zeit später. Danach habe sich jedoch keine deutliche Verbesserung mehr gezeigt: Nach zwei Monaten waren immer noch knapp neun Prozent der Server ohne Sicherheitsupdate. Irritierend ist jedoch, dass über ein halbes Jahr danach die „olle Lücke" immer noch ausgenutzt wird, wie Experten aus der Szene immer wieder warnen.

Wenn als Datenschutzbeauftragter seine „Bubble" verlässt und sich auch für den Bereich der IT-Sicherheit interessiert, merkt schnell, dass es auch in diesem Bereich im Gebälk knirscht. Datenschutzverletzungen in Folge von Cyberattacken sind an der Tagesordnung, auch im Bereich der KRITIS. Zu bedenken gilt hier, dass naturgemäß eine Datenschutzverletzung nach Art. 33 DS-GVO nicht weit ist, wenn die IT-Fachleute über Cyber-Angriffe reden, die täglich zu verzeichnen sind.

Der Sächsische Datenschutzbeauftragte gibt an, dass eine Cyberattacke im Schnitt 21.818 EUR je Vorfall (Quelle: Statista) koste. Den Zahlen des Sächsischen Datenschutzbeauftragten ist zu entnehmen, dass die Zahl der Angriffe und das Ausmaß der Schäden stark zugenommen haben. Danach hätten im Jahr 2018 Verantwortliche dem Sächsischen Datenschutzbeauftragten 227 Fälle gemeldet. 2019 seien es 450 Meldungen. 2020 habe die Behörde einen Anstieg um 40 Prozent auf 635 Meldungen verzeichnet.

Diese kontinuierliche Steigerung setze sich 2021 fort: In den vergangenen zehn Monaten seien bereits 750 Meldungen registriert worden. Davon seien ein Drittel auf Cyberkriminalität zurückzuführen.

Insgesamt beliefen sich die Kosten für digitale Angriffe auf die deutsche Wirtschaft allein 2020 auf ca. 24,3 Milliarden Euro. Das waren viermal mehr als noch 2019 (Quelle: Bitkom-Studie).

Ein Grund mehr auch für Datenschützer beim Thema IT-Sicherheit mehr zu sehen, als das stupide Ankreuzen von technischen und organisatorischen Maßnahmen in Mustervorlagen, wenn es um Einhaltung von Art. 32 DS-GVO geht. Oftmals sind insbesondere bei Datenschutzbeauftragten mit einem „lediglich" juristischen Background Defizite zu beobachten. Wer als Datenschutzbeauftragter ganzheitlicher beraten und überwachen möchte, benötigt auch bei der IT-Sicherheit solide Kenntnisse. Der Sächsische Datenschutzbeauftragte fasst die Problematik gut zusammen, wenn er sagt: *„Mangelhafte Datensicherheit offenbart meist auch Schwächen beim Datenschutz. Das ist nicht nur für die betroffenen Unternehmen existenzbedrohend, sondern auch für Menschen, deren Daten in den Besitz von Kriminellen gelangen. Identitätsdiebstahl gehört dabei zu den schlimmsten Folgen. Betroffenen droht ein finanzieller und sozialer Totalschaden".*

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: maramade, Adobe Stock

Sicherheit bei Messenger-Diensten: BSI nennt technische Grundlagen

Das Bundeskartellamt hat Anfang November 2021 einen Zwischenbericht „Branchenüberblick und Stimmungsbild Interoperabilität“ zu seiner Sektoruntersuchung Messenger- und Video-Dienste veröffentlicht. Das Bundeskartellamt hat sich im Rahmen der Untersuchung mit Fragen beschäftigt wie:

- Wie sicher sind die persönlichen Daten bei Messenger- und Video-Diensten?
- Sollten Gesetzgeber und Behörden dafür sorgen, dass eine Kommunikation über die verschiedenen Anbieter hinweg möglich ist?

Mit dem Zwischenbericht bietet das Bundeskartellamt zunächst einen Überblick über die Rahmenbedingungen der Branche sowie die verschiedenen Anbietergruppen, Funktionalitäten und Geschäftsmodelle. Außerdem werden die Ergebnisse einer Befragung von über 40 verschiedenen Diensteanbietern zum Thema Interoperabilität dargestellt und eine erste rechtliche, technische und wissenschaftliche Einordnung dazu vorgenommen. Ziel ist es, im kommenden Jahr einen Abschlussbericht mit konkreten Handlungsempfehlungen zu präsentieren.

Das Bundeskartellamt hat sich dabei im Rahmen der bestehenden Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu technischen und sicherheitsrelevanten Fragen bei Messenger- und Video-Diensten ausgetauscht. Seitens des BSI erschien zeitgleich eine ergänzende Publikation zur Funktionsweise sowie zu den Sicherheitsanforderungen und -eigenschaften moderner Messenger.
Die Zusammenarbeit bei diesem Zwischenbericht der Sektoruntersuchung zu Messenger- und Video-Diensten ist die erste in dieser Form.

Das technische Paper des BSI begleitet die Sektoruntersuchung des Bundeskartellamts und beschreibt die grundlegende Funktionsweise von Messengern und die verschiedenen Verschlüsselungsarten. Im Fokus stehen dabei die verwendeten Kommunikationsprotokolle, deren Sicherheitseigenschaften sowie anfallenden Metadaten. Von besonderem Interesse ist eine mögliche zukünftige Interoperabilität verschiedener Messenger, ohne dabei das Sicherheitsniveau einzuschränken.

Foto: Denys Prykhodov, Adobe Stock

Rechtskonformer Einsatz von Chat-Diensten im Unternehmensbereich

Sogenannte Messenger-Dienste haben parallel zur Verbreitung von Smartphones in den letzten Jahren zentrale Bedeutung für den Austausch von Nachrichten erlangt, andere Kommunikationsdienste wie E-Mail oder SMS vielfach ersetzt und zählen im privaten Alltag zu den beliebtesten Kommunikationsformen. Gründe hierfür sind neben der jederzeitigen Nutzbarkeit über Smartphone und der leichten Bedienbarkeit der Funktionsumfang, der es erlaubt, neben Textnachrichten auch Bilder, Videos oder Sprachnachrichten auszutauschen, Sprach- und Videoanrufe durchzuführen und wahlweise mit einzelnen Teilnehmern oder in der Gruppe zu kommunizieren. Hinzu kommt, dass es sich vielfach um unentgeltlich nutzbare Angebote handelt (vgl. Whitepaper des DSK „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“).

Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutz-Vorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen.
Die Rechtslage insbesondere beim Schutz von personenbezogenen Daten und Geschäftsgeheimnissen ist jedoch komplex, und die bei Verstößen drohenden Sanktionen können schnell zum Hemmnis werden.

Weiter auf DataAgenda lesen

Foto: Bihlmayerfotografie, Adobe Stock

3G-Einführung am Arbeitsplatz: BfDI sieht „Luft nach oben“

Nach Art. 38 Abs. 1 und 2 DS-GVO, § 6 Abs. 1 und 2 BDSG haben die öffentlichen und nicht-öffentlichen Stellen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.
Zur Unterstützungspflicht der verantwortlichen Stelle gehört auch, dem Datenschutzbeauftragten durch eine rechtzeitige und frühzeitige Einbindung und Beteiligung bei allen Planungen und Verfahren, die personenbezogene Daten betreffen, die Wahrnehmung seiner Aufgabe zu erleichtern oder gar erst zu ermöglichen. Das Gesetz fordert speziell in Art. 38 Abs. 1 DS-GVO, § 6 Abs. 1 BDSG die ordnungsgemäße und frühzeitige Unterrichtung des Datenschutzbeauftragten über alle mit dem Schutz von personenbezogenen Daten zusammenhängenden Fragen.
Oft klafft eine Lücke zwischen dem vom Normgeber geforderten Zustand und der betrieblichen und auch behördlichen Wirklichkeit. Davor scheint auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nicht gefeit zu sein. Insbesondere beim Thema der 3G-Einführung am Arbeitsplatz scheint die Einbindung des BfDI suboptimal verlaufen zu sein. Der BfDI kritisiert einige Bestandteile der neuen gesetzlichen Regeln zur Kontrolle des Impf-, Genesenen- oder Teststatus (3G) durch Arbeitgeberinnen und Arbeitgeber nicht nur in seiner offiziellen Pressemitteilung, sondern auch über seinen als privat gekennzeichneten und als Prof. Ulrich Kelber betriebenen Twitter-Account.
„Die Vorarbeiten der Bundesregierung für den Deutschen Bundestag sind an einigen Stellen fehlerhaft und verzichten auf datenschutzfreundliche Regelungen. Meine Behörde hätte gerne frühzeitig und begleitend beraten. Darauf hat das federführende Ministerium aber verzichtet. Folge ist ein unnötiges Risiko datenschutzrechtlicher Fehler, die bei Klagen vor Gerichten zu Verzögerungen führen könnten. Der Pandemiebekämpfung würde das massiv schaden“, so der BfDI in seiner Pressemitteilung zur 3G-Einführung.
Zuletzt machte sich Prof. Kelber auch durch einen Tweet seinem Ärger Luft: “ Es wurden 3 Monate vergeudet, gute, grundrechtsschonende und gerichtsfeste Regelungen zu entwickeln, weil man intransparent für sich alleine gearbeitet hat. Wie so oft … Mein Dank geht an die Abgeordneten, die im engen Verfahren noch einige Verbesserungen durchsetzen konnten.“
Die neuen Regelungen fasst der BfDI auf Twitter wie folgt zusammen: „Ergebnis ist ein Gesetzentwurf, der zwar legitim (und zurecht) 3G am Arbeitsplatz vorsieht, aber völlig unnötige Datensammlungen anlegt, Schutzvorkehrungen vermissen lässt und daher vor Gerichten schlechtere Chancen auf Bestand hat als ein ausgewogenerer Entwurf …“

Foto: denisismagilov, Adobe Stock

Mindeststandard für Videokonferenzdienste

Aufgrund der Maßnahmen zur Bekämpfung der Corona-Pandemie haben viele Unternehmen kurzfristig Telearbeitsplätze eingerichtet, sodass ihre Beschäftigten ihren arbeitsvertraglichen Pflichten auch von Zuhause nachkommen können. Um trotzdem die betriebsinterne Kommunikation sicherzustellen, setzen Unternehmen häufig sog. Software as a Service Dienstleister (kurz: SaaS) für Video- und Onlinekonferenzen, -Meetings oder Webinare ein. Hierbei die Vorgaben der DS-GVO einzuhalten, erhöht nicht nur das Datensicherheitsniveau in Organisationen, sondern hilft den ungeregelten Abfluss von solchen Unternehmensinformationen zu verhindern, die im internationalen Wettbewerb die eigene Wertschöpfung sichern sollen.

In den letzten Monaten haben sich nicht nur Anwender und Unternehmen intensiv mit möglichen Videokonferenz-Systemen beschäftigt, sondern auch immer wieder die Datenschutz-Aufsichtsbehörden.

Die Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) hat bereits vor einiger Zeit eine „Orientierungshilfe Videokonferenzsysteme“ veröffentlicht, in der sie die datenschutzrechtlichen Anforderungen an die Durchführung von Videokonferenzen durch Unternehmen, Behörden und anderen Organisationen erläutert. Diese Handreichung soll den Verantwortlichen eine Hilfestellung bieten, wie diese Anforderungen erfüllt werden können.

Auf die gestiegene Nachfrage hatte auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) reagiert und im April 2020 das „Kompendium Videokonferenzsysteme“ vorgestellt. Es solle Anwendern wie zum Beispiel Planern, Beschaffern, Betreibern, Administratoren, Revisoren und Nutzern helfen, den gesamten Lebenszyklus organisationsinterner Videokonferenzsysteme sicher zu gestalten. Betrachtet werden sämtliche Phasen – von der Planung über Beschaffung und Betrieb bis hin zur Notfallvorsorge und Aussonderung. Darüber hinaus hatte das BSI im März 2021 einen Community Draft für einen Mindeststandard für Videokonferenzdienste veröffentlicht. Auf Grundlage der bisher eingegangenen Rückmeldungen hat das BSI nun die finale Version 1.0 erstellt, die zum Download bereitsteht.

Mit einem neuen Mindeststandard stellt das BSI Sicherheitsanforderungen auf, die bei der Planung, der Beschaffung, dem Betrieb und bei der Nutzung von Videokonferenzdiensten durch Stellen des Bundes beachtet werden. Er beschreibt Anforderungen, die eine sichere Planung sowie den sicheren Einsatz geeigneter Produkte ermöglichen. Dabei berücksichtigt er verschiedene Betriebsmodelle, wie selbst- und fremdgehostete Dienste, denn die Umsetzung in der Praxis ist vielfältig. Entscheidend für alle Varianten ist, bewusste und begründete Entscheidungen zu treffen, die die Rahmenbedingungen der jeweiligen Einrichtung berücksichtigen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Praxisthemen:

- ✓ Vorlageverfahren EuGH
- ✓ Aktuelle Entwicklungen in der nationalen und europäischen Bußgeldpraxis
- ✓ Arbeitsaufwand im Datenschutz quantifizieren – am Beispiel Gesundheitswesen
- ✓ „Garantien" im Datenschutz – aktueller Stand zu Verhaltensregeln nach Art. 40 DS-GVO
- ✓ Datenschutz bei Microsoft
- ✓ TTDSG – Anforderungen und Herausforderungen für die Praxis
- ✓ Tracking auf Webseiten
- ✓ Nutzung von Videokonferenzlösungen außereuropäischer Anbieter

24.–25.01.2022
online

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Janet Worg, Adobe Stock

DSK-Beschluss zur Verarbeitung des Impfstatus von Beschäftigten

Eine der häufigsten Fragen im Bereich des Beschäftigtendatenschutzes dürfte in den letzten Monaten gewesen sein, ob Arbeitgeber den Immunisierungsstatus der Beschäftigten (geimpft/genesen) erfragen dürfen. Praxisrelevant wird diese Frage oftmals, wenn es um die Fragestellung geht, ob Arbeitgeber berechtigt sind, von ihren Beschäftigten im Rahmen etwaiger Lohnfortzahlungsansprüche Auskunft über den Impfstatus zu verlangen.
Zu den in diesem Zusammenhang relevant werdenden Fragen, hatte bereits der LfDI BW Stellung bezogen:

- Darf der Arbeitgeber, um die Lohnerstattung von der Behörde zu erhalten, den Beschäftigten nach seinem Impfstatus fragen?
- Ist der Beschäftigte umgekehrt verpflichtet, seinen Impfstatus gegenüber seinem Arbeitgeber zu offenbaren, und/oder muss er dem Arbeitgeber hierzu sogar Belege (Impfpass etc.) überlassen?

Weiter auf DataAgenda lesen

BNetzA zur Einwilligungsdokumentation nach § 7a UWG

Mit dem § 7a UWG wurde am 01.10.2021 für werbende Unternehmen im UWG eine Dokumentations- und Aufbewahrungspflicht eingeführt. Danach muss die vorherige ausdrückliche Einwilligung des Verbrauchers in die Telefonwerbung zum Zeitpunkt der Erteilung in angemessener Form dokumentiert und aufbewahrt werden. Die werbenden Unternehmen müssen diesen Nachweis ab Erteilung der Einwilligung sowie nach jeder Verwendung der Einwilligung fünf Jahre aufbewahren. Die werbenden Unternehmen haben der Bundesnetzagentur den Nachweis auf Verlangen unverzüglich vorzulegen.

Weiter auf DataAgenda lesen

Foto: VadimGuzhva, Adobe Stock

Foto: Ralf, Adobe Stock

Aufbewahrungsfrist für Arbeitsunfähigkeitsbescheinigung

Gesundheitsdaten gehören zu den Daten besonderer Kategorie gem. Art. 9 DS-GVO. Ihre Verarbeitung ist nur unter bestimmten Bedingungen erlaubt. Im Zusammenhang mit einem Beschäftigungsverhältnis sind dies vor allem Fälle, in denen die Verarbeitung von Gesundheitsdaten zur Ausübung von Rechten und Pflichten, die aus einer Erkrankung bzw. auch aus einer Schwerbehinderung entstehen, erforderlich ist. Dies können Rechte und Pflichten sowohl der Beschäftigten als auch des Arbeitgebers sein. Die Erfassung einer Dienst- oder Arbeitsunfähigkeit wegen Krankheit hat verschiedene Aspekte. Erforderlich und damit datenschutzrechtlich zulässig ist sie zur Erfüllung gesetzlicher Vorschriften, z.B. zur Errechnung der Dauer der Lohnfortzahlung oder zur Unterbreitung eines Angebots für eine Maßnahme des betrieblichen Eingliederungsmanagements (BEM). Diese Aufgaben obliegen dem Arbeitgeber, sodass ausschließlich die Personalverwaltung die Datenverarbeitung zu diesem Zweck vornehmen darf und muss.

Weiter auf DataAgenda lesen

IT-Sicherheitslage weiter kritisch

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes. Ihre Aufgabe ist es, Deutschland digital sicherzumachen.

Wie jedes Jahr legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürger:innen und seiner Wirtschaft im Cyber-Raum vor.

Nach Bewertung des BSI war das vergangene Jahr geprägt von einer deutlichen Ausweitung cyber-krimineller Erpressungsmethoden. Die Anzahl der Schadprogramm-Varianten stieg zeitweise rasant an: Mit bis zu 553.000 neuen Varianten pro Tag wurde der höchste jemals gemessene Wert ermittelt. Neben der reinen Quantität der gemessenen Angriffe nahm nach Beobachtungen des BSI aber auch die Qualität der Angriffe weiterhin beträchtlich zu.

Weiter auf DataAgenda lesen

Foto: hkama, Adobe Stock

Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden

Ihr ständiger Begleiter im Datenschutz-Management

Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Ihre DS-GVO Umsetzung smart auditiert und visualisiert ab 249 €.

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

Foto: chinnarach, Adobe Stock

BSI bietet Qualifikation als Digitaler Ersthelfer

Um die Unfallgefahr am Arbeitsplatz möglichst gering zu halten, sind die Deutsche Gesetzliche Unfallversicherung (DGUV) und ihre Träger zu Maßnahmen verpflichtet, die der Unfallprävention dienen. Im Rahmen der Arbeitsplatzsicherheit sind sie unter anderem durch § 23 Absatz 2 des Siebten Sozialgesetzbuchs (SGB VII) für die Aus- und Fortbildung betrieblicher Ersthelfer zuständig. Ersthelfer im Betrieb sind Pflicht. Ersthelfer ersetzen nicht den Arzt, sie können aber bei Unfällen oft die entscheidende Erste Hilfe leisten.

Angelehnt an dieses Prinzip prägt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Begriff des „Digitalen Ersthelfers" und bietet einen Onlinekurs dafür an. Die Qualifikation zum Digitalen Ersthelfer erfolgt anhand eines Basiskurses, der vom BSI kostenlos als Onlinekurs angeboten wird. Als Begleitmaterial zum Basiskurs wird der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer" angeboten. Die inhaltlichen Bestandteile des Basiskurses richten sich nach der technischen Ausstattung und dem Wissensstand von KMU und Bürgern, die vom Digitalen Ersthelfer im Rahmen seiner Tätigkeit im Cyber-Sicherheitsnetzwerk beraten werden sollen.

Der Digitale Ersthelfer hat die Aufgabe, bei IT-Sicherheitsvorfällen eine qualifizierte Einschätzung des Vorfalls zu treffen und dem Betroffenen Ersthilfe bei kleineren IT-Störungen und IT-Vorfällen zu leisten sowie erste Handlungsempfehlungen auszusprechen.

Ein Digitaler Ersthelfer kann jede volljährige Person oder jedes in Deutschland ansässige Unternehmen sein, welches sein Wissen und seine Expertise freiwillig zur Hilfe anderer zur Verfügung stellen möchte. Dies können also Privatpersonen wie Studenten oder IT-affine Bürger oder auch Unternehmen wie IT-Dienstleister oder Computerfirmen sein. Sie helfen Betroffenen einer IT-Störung oder eines IT-Sicherheitsvorfalls mit einer qualifizierten Einschätzung des Problems und leisten bei kleineren IT-Störungen durch gezielte Handlungsempfehlungen Erste-Hilfe. Weitere Informationen erhalten Sie hier.

Folge 10: „Kampf gegen den Cookieterror – kann das TTDSG helfen?“

Rolf Schwartmann im Gespräch mit mit Jan Oetjen United Internet, verantwortlich für web.de und gmx.
Datenschutz und Datenschutz-Grundverordnung (DS-GVO) kennen die meisten. Im Dezember tritt ein neues Gesetz zum Datenschutz in Kraft: das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG). Was hat es damit auf sich und warum ist es wichtig? Wie kann es das „Cookie-Problem“ lösen und wie können Personal Information Management Systeme (PIMS) helfen?
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

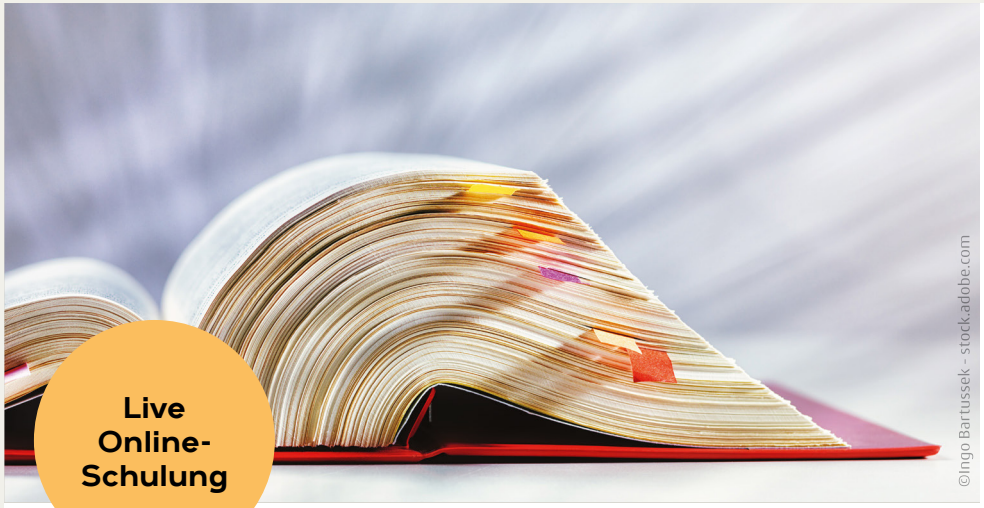
Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

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



Live Online-Schulung

Das neue Betriebsrätemodernisierungs- und Bundespersonalvertretungsgesetz

18. Januar 2022 | online
Referent/in: Yvette Reif, Andreas Jaspers

Schwerpunkte:

- ✓ Anlass für die Neuregelungen im BetrVG und BPersVG
- ✓ Arbeitgeber als Verantwortlicher für die Datenverarbeitung beim Betriebsrat
- ✓ Kontrolle des Betriebsrats durch den Datenschutzbeauftragten (DSB)
- ✓ Neue Verschwiegenheitspflicht des DSB
- ✓ Neue Beteiligungsrechte der Mitarbeitervertretung

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.
DATAKONTEXT