NEWS BOX DATENSCHUTZ

AUSGABE
2/2023

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Auskunftsbegehren von betroffenen Personen und die Geltendmachung des Rechts auf Datenkopie sind von großer Relevanz für die Praxis, wesentliche Detailfragen zu Reichweite und Umfang sind aber noch ungeklärt. Umstritten ist etwa, ob Auskunftsbegehren der Einwand des Rechtsmissbrauchs entgegengehalten werden kann, wenn es dem Antragsteller bei Geltendmachung des Auskunftsanspruchs nicht um die Kontrolle der Verarbeitung seiner personenbezogenen Daten geht, sondern Interessen außerhalb des Datenschutzes verfolgt werden, z.B. die Vorbereitung der Geltendmachung eines Anspruchs auf Überstundenvergütung mittels eines Auskunftsbegehrens bezüglich gespeicherter Arbeitszeitdaten. Die nationalen Gerichte sind vielfach der Ansicht, auch einem Begehren nach Art. 15 DS-GVO könne der Einwand des Rechtsmissbrauchs entgegengehalten werden. Unklar ist auch die Reichweite des Rechts auf Datenkopie aus Art. 15 Abs. 3 DS-GVO sowie das Verhältnis dieser Regelung zum Grundtatbestand der Auskunft in Art. 15 Abs. 1 DS-GVO.
Dabei handelt es sich beim Auskunftsrecht um eine Thematik, deren Ausgestaltung als Datenschutzprozess den Verantwortlichen durchaus Probleme, aber zumindest größere Aufwände bereitet. Dies hängt nicht nur damit zusammen, dass die Beauskunftung von Betroffenenanfragen generell viele Ressourcen binden kann. Jede Konkretisierung durch den Europäischen Datenschutzausschuss (EDSA) und jede Entscheidung des Europäischen Gerichtshofs (EuGH), die zu mehr Handlungs- und Rechtssicherheit beiträgt, dürfte diesen für die Verantwortlichen schwer zu bändigenden Prozess etwas praktikabler machen.
Daher bedeutet auch die aktuelle Entscheidung des EuGH, die davon ausgeht, dass im Rahmen einer Beauskunftung nicht nur Kategorien von Empfängern, sondern die Identität der Empfänger zu benennen ist, möglicherweise mehr Aufwand für den Verantwortlichen. Wenn dieser Aufwand jedoch am Ende mehr Klarheit bringt, ist dies im Sinne einer größeren Rechtssicherheit ein akzeptabler Preis, meint Ihr

Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: momius, Adobe Stock

Löschen oder Archivieren: Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) bietet ein Arbeitspapier

Ein effektives Datenschutzmanagement erfordert vom Verantwortlichen sich nicht nur, sich Gedanken um die Zulässigkeit der Datenerhebung zu machen. Der datenschutzkonforme Umgang muss sich auf den gesamten Lebenszyklus von personenbezogenen Daten erstrecken und damit auch auf den Vorgang des Löschens. Generell sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle „zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist". Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen.

In der Praxis kann sich die Frage stellen, ob der Verantwortliche durch die Archivierung von personenbezogenen Daten den Datenschutz umsetzen kann oder vielleicht sogar muss (Archivierung als Löschungssurrogat).

Den damit zusammenhängenden Fragen widmet sich ein Arbeitspapier (Löschung oder Archivierung?), das der Bayerische Landesbeauftragte für den Datenschutz als Datenschutz-Aufsichtsbehörde für den bayerischen öffentlichen Sektor und die Generaldirektion der Staatlichen Archive Bayerns als zentrale staatliche Fachbehörde für alle Fragen des Archivwesens gemeinsam erarbeitet haben. Das Arbeitspapier skizziert die wesentlichen Aspekte der archivrechtlichen Aufbewahrungs- und der datenschutzrechtlichen Löschungsregelungen; es behandelt Gemeinsamkeiten, Unterschiede und grundlegende Wertungen, die im Schnittbereich beider Rechtsmaterien auftauchen.

Es charakterisiert die Archivierung als Löschungssurrogat und geht – unter Berücksichtigung der je eigenen Perspektive von Datenschutz- und Archivrecht – auf die Frage der Aufbewahrungsdauer ein. Der Aspekt der datenschutzrechtlichen Informationspflichten bei der Archivierung von Unterlagen bleibt ebenfalls nicht unbeachtet. Damit stellt das Arbeitspapier auch einen guten Ratgeber für die Herausforderungen dar, denen sich Verantwortliche nicht nur aus dem öffentlichen Bereich im Rahmen der Digitalisierung konfrontiert sehen. Damit dürfte das Arbeitspapier auch für Verantwortliche aus dem privatrechtlichen Bereich hilfreiche Anregungen bieten, die die Verarbeitung personenbezogener Daten im Spannungsfeld von Datenschutz- und Archivrecht organisieren müssen.

EuGH konkretisiert Auskunftsrecht: Identität der Empfänger sind offenzulegen

Foto: Zerbor, Adobe Stock

Mit dem Auskunftsrecht gem. Art. 15 DS-GVO hat der Verordnungsgeber eine Grundlage dafür geschaffen, dass andere Betroffenenrechte (wie das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, aber auch das Widerspruchsrecht) überhaupt gezielt geltend gemacht werden können.

Die praktische Wirksamkeit dieser „nachgelagerten" Betroffenenrechte hängt oftmals davon ab, wie weit das Recht auf Auskunft verstanden wird. Möchte der Betroffene bspw. wissen, wer nun neben dem Verantwortlichen ebenfalls seine Daten hat, nützt es ihm nicht viel, wenn er von der beauskunftenden Stelle lediglich die „Kategorien der Empfänger" als Auskunft erhält.

Nun hat der Europäische Gerichtshof (EuGH) (Urteil v. 12.01.2023 – Rs. C-154/21) anlässlich einer Vorlagefrage des österreichischen Obersten Gerichtshofs zu Art. 15 Abs. 1 lit. c) DS-GVO entschieden:

Jeder hat das Recht zu erfahren, an wen seine personenbezogenen Daten weitergegeben werden. Grundsätzlich hat der für die Datenverarbeitung Verantwortliche dabei auf Anfrage des Betroffenen die konkrete Identität des Empfängers der offengelegten Daten mitzuteilen. Lediglich dann, wenn der Empfänger (noch) nicht identifiziert werden kann oder der Antrag offenkundig unbegründet oder exzessiv ist, kann sich die Mitteilung auf die Kategorien der Empfänger beschränken. Es genügt grundsätzlich nicht, nur Kategorien von Empfängern mitzuteilen.

Verantwortliche sollten diese Entscheidung dazu nutzen, ob und wie dieser Aspekt in den organisationsinternen Prozessen zum Management der Betroffenenrechte Berücksichtigung findet.

Bild: NDABCREATIVITY - stock.adobe.com

NEU

Ausbildung zum/zur Datenschutzkoordinator/in

Grundlagenwissen mit Zertifizierungsmöglichkeit

28.–29.03.2023 I Köln
22.–23.05.2023 I Mannheim
Referent: Thomas Mühtlein

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

Schwerpunkte:

Grundlagen

- ✓ Rollen und Aufgaben in der Datenschutz-Organisation
- ✓ Stellung und Aufgabe als Datenschutzkoordinator/in

Wichtige Datenschutz-Prozesse

- ✓ Bearbeitung von Betroffenenrechten
- ✓ Reaktionen bei Datenpannen
- ✓ Zusammenarbeit mit Dienstleistern

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: batjaket, Adobe Stock

Mindeststandard zur Protokollierung und Detektion von Cyber-angriffen

Immer häufiger werden Cyberangriffe auf Unternehmen und Regierungen bekannt, die folgenschwere Konsequenzen für die Betroffenen auslösen. Die meisten IT-Systeme in Organisationen verfügen über Möglichkeiten, um ein Audit-Logging zu aktivieren. Bereits mit den Standardeinstellungen werden dabei in der Regel alle wichtigen Ereignisse aufgezeichnet. Damit dabei aber keine gigantischen Datenmengen entstehen, die nur mit hohem Aufwand zu verarbeiten und speichern sind, werden normalerweise nicht alle Ereignisse in maximaler Detailtiefe protokolliert.

Daher ist es nicht ausgeschlossen, dass nach einem Cyberangriff für die Analyse des Angriffs benötigte Protokolldateien nicht oder nicht mehr verfügbar sind.

Auch vor diesem Hintergrund hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Entwurf des Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen Version 1.0a.4 als Community Draft veröffentlicht. Das BSI lädt das interessierte Fachpublikum ein, Kommentierungen und Rückmeldungen zur Mitgestaltung bis zum 10. Februar 2023 per E-Mail an mindeststandards@bsi.bund.de zu richten.

Um Cyberangriffe auf die Bundesverwaltung erkennen und behandeln zu können, reguliert dieser Mindeststandard die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen in der Kommunikationstechnik des Bundes.
Der Mindeststandard „Protokollierung und Detektion von Cyber-Angriffen“ (MST PD) definiert gemäß § 8 Abs. 1 BSIG das Mindestniveau für die Informationssicherheit des Bundes im Bereich der Protokollierung von Ereignissen und in der Detektion von daraus folgenden sicherheitsrelevanten Ereignissen (SRE), um ein zielgerichtetes und einheitliches Vorgehen zur Erkennung und Abwehr von Cyberangriffen auf die Kommunikationstechnik des Bundes (§ 2 Abs. 3 S. 1 BSIG) zu etablieren.

Der Mindeststandard dient insbesondere den IT-Verantwortlichen und Informationssicherheitsbeauftragten als Grundlage für die Einforderung und Umsetzung von organisatorischen und technischen Maßnahmen. Die erforderlichen personellen Ressourcen sind zu ermitteln und bereitzustellen.

Foto: N. Theiss, Adobe Stock

Datenschutzbeauftragter freiwillig benannt? Kein Sonderkündigungsschutz

Mit Urteil vom 6. Oktober 2022, Az. 18 Sa 271/22 (Volltext) hat sich das Landesarbeitsgericht Hamm mit der Frage beschäftigt, ob und in welchen Fällen ein interner Datenschutzbeauftragter sich auf einen Sonderkündigungsschutz berufen kann. In diesem besonderen Fall war der Knackpunkt die Frage, ob hier die verantwortliche Stelle überhaupt zur Benennung verpflichtet war.

Im Rahmen einer arbeitsgerichtlichen Kündigungsschutzklage wandte der Kläger gegen die Beendigung des Arbeitsverhältnisses ein, er sei als betrieblicher Datenschutzbeauftragter bestellt und genieße daher den besonderen Kündigungsschutz nach § 6 Abs. 4 BDSG.

Die Pflicht zur Benennung eines Datenschutzbeauftragten kann sich nicht nur aus der DS-GVO selbst ergeben. Art. 37 Abs. 4 Satz 1 Hs. 2 DS-GVO gestattet dem Unionsgesetzgeber wie auch den nationalen Gesetzgebern, im Verhältnis zur DS-GVO, weitergehende Pflichten zur Benennung eines Datenschutzbeauftragten vorzusehen. Von dieser Befugnis hat der deutsche Gesetzgeber Gebrauch gemacht.

Nach § 38 Abs. 1 Satz 1 BDSG haben Verantwortliche und Auftragsverarbeiter ergänzend zu den Vorgaben der DS-GVO einen Datenschutzbeauftragten zu bestellen, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Zudem schreibt § 38 Abs. 1 Satz 2 BDSG vor, dass schwellenwertunabhängig ein Datenschutzbeauftragter zu benennen ist, sofern der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet.

In seiner Urteilsbegründung geht das Landesarbeitsgericht (LAG) Hamm auf alle Varianten ein, die zu einer Benennungspflicht nach DS-GVO und nach BDSG führen könnten und verneint nach einer Auseinandersetzung mit diesen Aspekten alle infrage kommenden Möglichkeiten.

Im Ergebnis gab das LAG Hamm dem Arbeitgeber Recht: Die Benennung des Datenschutzbeauftragten sei freiwillig erfolgt und keiner der Fälle, in denen das Gesetz die Bestellung verlange, sei anzunehmen. Insofern greife hier auch der Kündigungsschutz nicht.

Quelle: Landesarbeitsgericht Hamm, 18 Sa 271/22

EDSA fordert die Umsetzung der PNR-Richtlinie

Der Europäische Datenschutzausschuss (EDSA) hat die EU-Mitgliedstaaten aufgefordert, das PNR-Urteil des Europäischen Gerichtshofs (EuGH) unverzüglich umzusetzen.

Foto: metamorworks, Adobe Stock

Die Verarbeitung von sog. PNR-Daten (Passenger Name Record, zu deutsch Fluggastdatensatz) zu Sicherheitszwecken kombiniert zwei grundsätzliche Probleme im Bereich des Datenschutzes im Sicherheitsbereich:
PNR-Daten werden so genutzt, dass sämtliche Flugreisende mit abstrakt formulierten Gefährderprofilen („Mustern“) abgeglichen werden, denn PNR-Daten sind nicht erforderlich, um bekannte Gefährder oder Straftäter bei der Grenzkontrolle zu fassen. Sie dienen dem Generieren von Verdächtigen, also dem Aufspüren von Reisenden, die eine Gefahr darstellen könnten und den Sicherheitsbehörden noch nicht bekannt sind. Gleichzeitig schafft die PNR-Richtlinie eine weitere Vorratsspeicherung von Daten, weil die Sicherheitsbehörden PNR-Daten verdachtslos über Jahre speichern.

Am 21. Juni 2022 fällte der EuGH auf Vorlage des belgischen Verfassungsgerichts sein Urteil über die PNR-Richtlinie. Der Gerichtshof stellte zwar fest, dass die Gültigkeit der PNR-Richtlinie nicht beeinträchtigt ist, entschied aber, dass die PNR-Richtlinie so ausgelegt werden muss, dass sie wichtige Beschränkungen für die Verarbeitung personenbezogener Daten enthält, um die Einhaltung der EU-Grundrechtecharta (die Charta) zu gewährleisten. Einige dieser Einschränkungen sind die Anwendung des PNR-Systems nur auf terroristische Straftaten und schwere Kriminalität, die in einem objektiven Zusammenhang mit der Beförderung von Fluggästen stehen, und die nichtdiskriminierende Anwendung der allgemeinen Aufbewahrungsfrist von fünf Jahren auf alle personenbezogenen Daten von Fluggästen.

Weiter auf DataAgenda lesen

Foto: NicoElNino, Adobe Stock

LfDI BW genehmigt Verhaltensregel „Trusted Data Processor“

Gemäß Art. 40 Abs. 2 DS-GVO dürfen „Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten“ Verhaltensregeln ausarbeiten. Verhaltensregeln (auch „Code of Conduct“ genannt) sind verbindliche Vorgaben eines (Branchen-)Verbands oder einer anderen Vereinigung, die datenschutzrechtliche Verhaltensweisen der jeweiligen Mitglieder festlegen.

Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Insbesondere könnten in diesen Verhaltensregeln – unter Berücksichtigung des mit der Verarbeitung wahrscheinlich einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen – die Pflichten der Verantwortlichen und der Auftragsverarbeiter bestimmt werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, hat die nationale Verhaltensregel „Trusted Data Processor“ genehmigt.
Mit der Verhaltensregel „Trusted Data Processor“ erhalten deutsche Unternehmen die Möglichkeit, Rechtssicherheit im Bereich Auftragsverarbeitung zu erhalten. Trusted Data Processor soll durch Standardisierung für eine Vereinfachung sowohl für diejenigen, die sich der Verhaltensregel unterwerfen, als auch für ihren Kundenkreis und die Unternehmenspartner sorgen. Die Beteiligten setzen dabei auf ein Kostensenkungspotenzial als Argument.

An der Entwicklung von Trusted Data Processor wirkten maßgeblich Experten der Fachverbände „Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.“ und „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“ mit.

Durch eine Selbstverpflichtung auf die Verhaltensregel „Trusted Data Processor“ sollen Auftragsverarbeiter nach außen sichtbar machen, dass sie sowohl den in der Verhaltensregel festgelegten Vorgaben folgen als auch sich deren Überwachung durch eine Überwachungsstelle unterwerfen. Die Überwachungsstelle ist Anlaufstelle für Beschwerden und kontrolliert regelmäßig die Einhaltung der Verhaltensregel.

Quelle: DSZ Datenschutz Zertifizierungsgesellschaft mbH

Foto: miss_mafalda, Adobe Stock

Falschparker-Fotos können zulässig sein

In einem Verfahren des Verwaltungsgerichts Ansbach gegen das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ging es um die folgende Frage:
Durfte die Aufsichtsbehörde Bürgern verbieten, Fotos von „Falschparkern" bzw. von falsch geparkten Autos anzufertigen, um die Ordnungswidrigkeit mithilfe der Fotos bei den Behörden zu melden?
Das Verwaltungsgericht Ansbach bejahte diese Frage und hob die Verwarnung des BayLDA gegen den klagenden Bürger auf.

Als „Freibrief" für ein solches Verhalten darf die Aufhebung der Verwarnung gleichwohl nicht verstanden werden. Es lohnt sich, die konkreten Aspekte des Falls zu beachten. Wie auch das BayLDA betont, sollten folgende Feinheiten betrachtet werden:

1. Kein rein „privater Vorgang"

Die Übermittlung solcher Fotoaufnahmen ist nicht als rein privater Vorgang der Anzeigeerstattenden zu bewerten und fällt in den Regelungsbereich der DS-GVO. Zudem bezieht sich die Entscheidung nur auf die Meldung von Vorfällen an Polizei und Ordnungsamt und bspw. nicht in sozialen Netzwerken.

2. Beachtung von Betroffenenansprüchen

Die Anzeigeerstattenden können Einzelfällen eine Befugnis zur Datenverarbeitung haben, bleiben aber bei der Nutzung von Bildaufnahmen in der Pflicht, grundlegenden Betroffenenansprüchen wie dem Recht auf Auskunft oder Löschung nachzukommen.

3. Gebot der Datenminimierung ist zu beachten

Ausdrücklich betont das Gericht im Übrigen auch das Gebot der Datenminimierung. Es unterstreicht damit, dass etwa das Fotografieren unbeteiligter Passanten im Umfeld der verkehrswidrig parkenden Fahrzeuge zu vermeiden ist. Zur Datenminimierung dürfte es auch gehören, stets darauf zu achten, keine Menschen zu fotografieren, möglichst wenig öffentlichen Raum zu erfassen und ggfs. weitere zufällig erfasste Kennzeichen zu schwärzen.

Quelle: (VG Ansbach, Urteile vom 2. November 2022 – AN 14 K 22.00468 und AN 14 K 21.01431)

Foto: MQ-Illustrations, Adobe Stock

Gutachten: Handelsregister und Datenschutz

Seit dem 1. August 2022 sind über das Portal „Handelsregister.de“ sämtliche Einträge in den Handels-, Genossenschafts-, Partnerschafts- und Vereinsregistern ohne weitere Einschränkungen kostenfrei abrufbar. Das hat auf den ersten Blick Vorteile in puncto Transparenz. Bei dem Handelsregister handelt es sich um die zentrale Registerplattform des Bundes für Firmen in Deutschland. Der Umstand, dass die Abrufe aus diesem Portal kostenfrei und ohne das Anlegen eines vorherigen Accounts erfolgen können, ist Ergebnis des seit dem 1. August geltenden Gesetzes zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) der EU vom Juni 2019. Unter anderem wollte die EU damit Registerauskünfte vereinfachen.
Da das Handelsregister (erreichbar unter http://www.handelsregister.de/) eine Publikations-, Beweis-, Kontroll- und Schutzfunktion erfüllen soll, enthält es notwendiger- und typischerweise unter anderem Informationen über Firma, Sitz, Niederlassung und Zweigniederlassungen, den Gegenstand des Unternehmens, vertretungsberechtigte Personen, die Rechtsform des Unternehmens sowie das Grund- oder Stammkapital und den Namen des Geschäftsinhabers.

Es wurde in jüngster Zeit wiederholt kritisiert, dass ein angemessener Schutz dieser oben genannten Informationen im Konzept des Handelsregisters nicht vorhanden zu sein scheint. Technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten, wie bspw. Schwärzungen von nicht benötigten Informationen beim Upload von Scans, scheinen keine obligatorisch eingeforderte Anforderung zu sein. Auch ohne großen Argumentationsaufwand dürfte nachvollziehbar sein, dass der ungeschützte Abruf dieser Informationen Tür und Tor für Missbrauchsszenarien, wie bspw. Identitätsdiebstahl eröffnen kann.

Das Netzwerk Datenschutzexpertise setzt sich in seinem aktuellen Gutachten mit dieser Problematik auseinander. Das Gutachten kommt nach einer ausführlichen Darstellung zu dem Ergebnis, dass die Harmonisierung des Registerrechts mit dem Datenschutzrecht sowohl rechtlich als auch praktisch misslungen ist.

Die unmissverständliche Forderung des Gutachters:
„Der Bundesgesetzgeber sowie der Verordnungsgeber auf Bundesebene sind aufgefordert, die bestehenden Defizite zu beseitigen. Das Justizministerium NRW ist aufgefordert, die unkorrekten Angaben auf der Seite handelregister.de zu berichtigen. Eine zeitliche Begrenzung der voraussetzungslosen Online-Abrufmöglichkeit muss normativ vorgesehen und umgesetzt werden. Ebenso ist der Zugriff auf nachweisende Dokumente einzuschränken. Das Justizministerium NRW ist aufgefordert und rechtlich dazu verpflichtet, bei der Wahrnehmung von Betroffenenrechten mit den Amtsgerichten zusammenzuarbeiten. Die Amtsgerichte sind aufgefordert, sukzessive oder auf Antrag der Betroffenen für die Publizität nicht erforderliche Daten Dritten vorzuenthalten.“

Foto: photon_photo, Adobe Stock

Schmerzensgeld bei Identitätsdiebstahl

Landgericht München I, Urteil v. 09.12.2021 – 31 O 16606/20

Im Oktober 2020 benachrichtigte der bekannte Broker „Scalable Capital" seine Kunden über eine Datenschutzverletzung, bei der bestimmte Kundeninformationen wie insbesondere ID-Daten, Namen und Adressen, Wertpapierauszüge, Steuerdaten u.v.m. von unbekannten Dritten gestohlen wurden. Die Zahl der von diesem Identitätsdiebstahl betroffenen Kunden wird auf mehr als 30.000 geschätzt.

Weiter auf DataAgenda lesen

Data Agenda Podcast Folge 27

Wenn drei Herausgeber von führenden Kommentaren zum Datenschutzrecht und ein Richter am für Datenschutzrecht zuständigen Senat des Bundesgerichtshofs sich den Fragen einer im Datenschutz ausgewiesenen Verwaltungsrichterin zu einer Diskussion über das Datenschutzrecht stellen, dann lässt die Zusammensetzung der Runde aufhorchen. „**Datenschutz im Spannungsfeld zwischen Gemeinwohl und Privatheit – ein Digitalisierungsrecht für das 21. Jahrhundert“ war die Überschrift eines Online-Symposiums** der Kölner Forschungsstelle für Medienrecht der TH Köln in Kooperation mit den Universitäten Regensburg und Leipzig, welches im November 2022 stattfand.
Moderiert von **der Regensburger Verwaltungsrichterin** Kristin Benedikt diskutierten Dr. Peter Allgayer als Richter am VI. Zivilsenat des Bundesgerichtshofs und die Professoren Dr. Jürgen Kühling von der Universität Regensburg und derzeit Vorsitzender der Monopolkommission, Dr. Boris Paal von der Universität Leipzig und Richter am LG Hamburg sowie Dr. Rolf Schwartmann, der Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Teil 1: Aktuelle Entwicklungen im Recht der Digitalisierung

- Zahlen, Daten
- DS-GVO Schadensersatz und Abmahnungen
- Vorratsdatenspeicherung

Zum Podcast bitte hier klicken.

Teil 2: Die Zukunft des EU-Datenrechts

- Daten und Tech-Giganten
- Daten in der Pandemie (Corona-Warn-App)
- Neue EU-Datenakte

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