NEWS BOX DATENSCHUTZ

AUSGABE
10/2023

INHALTSVERZEICHNIS

RDV
DATAKONTEXT

Levent Ferik

EDITORIAL

Wer sich täglich und hauptberuflich mit Datenschutz beschäftigt, merkt eine Sache sehr schnell: Datenschutz ist vieles – aber sicher nicht langweilig. Auch in der betrieblichen Praxis einer Organisation durchdringt das Querschnittsthema Datenschutz so gut wie alle Prozesse oder hat eine Schnittmenge zu diesen.

Da verwundert es nicht, dass auch und gerade die Tätigkeitsberichte der Aufsichtsbehörden ein nie versiegendes Füllhorn an datenschutzrechtlichen Alltäglichkeiten, aber auch ein Kuriositätenkabinett sind. Auf den Internetseiten des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RlP) hat der interessierte Leser die Möglichkeit, sich einen Eindruck von der Bandbreite der dort eingegangenen Eingaben zu verschaffen. „Best of Datenschutz – Spannende Datenschutzfälle aus 2022 und 2023“:

- Einem Spionagefilm könnte die Fragestellung nach einem durch eine Katze verursachten Datenschutzverstoß entsprungen sein. Begeht eine Katze, die eine Kamera am Halsband trägt, einen Datenschutzverstoß?
- Was haben 10.000 nicht zugestellte Briefe mit dem Gaspreis und einer Datenpanne zu tun und was haben Bewerbungsunterlagen im Gebüsch zu suchen?
- Die Lektüre zeigt aber auch, dass Datenschützer keine Verhinderer der Digitalisierung sind, sondern eher Wegbereiter einer Digitalisierung, bei der Persönlichkeitsrechte nicht (zwangsläufig) auf der Strecke bleiben (Stichwort: Telepräsenzroboter für kranke Schüler während der Corona-Pandemie).

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Nattawit, Adobe Stock

Kamera-Attrappen: Beweislast liegt (auch hier) beim Verantwortlichen

Ein sehr praktisches Problem thematisiert der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in seinem 5. Tätigkeitsbericht (Ziffer 3.6) zum Datenschutz nach der DS-GVO und beschäftigt sich mit der Frage, wie Verantwortliche ihrer Darlegungslast im Hinblick auf Kameraattrappen nachkommen können.

Das Problem ergibt sich bei Betrachtung zweier Aspekte, die für sich genommen, eher unproblematisch sind.

1. Rechenschaftspflicht

Diese sogenannte Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO bewirkt eine Darlegungs- und Beweislastumkehr zulasten des Verantwortlichen, sodass nicht der Betroffene oder die Aufsichtsbehörde eine Verletzung der Vorschriften der DS-GVO nachweisen muss, sondern der Verantwortliche die Einhaltung der Vorschriften (vgl. Heberlein in Ehmann/Selmayr DSGVO, 2. Auflage, Art. 5, Rn. 32).

2. Keine Zuständigkeit bei Kameraattrappen

Sofern es sich bei einer Videokamera tatsächlich um eine Attrappe handelt, findet keine Datenverarbeitung nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nrn. 1 und 2 DS-GVO statt. In diesem Fall ist der TLfDI mangels Anwendbarkeit der DS-GVO nicht zuständig und kann keine aufsichtsbehördlichen Maßnahmen ergreifen.

3. Beweislastumkehr

Wendet nun der vermeintlich Verantwortliche ein, er verwende lediglich eine Kameraattrappe, so muss er diese Behauptung gegenüber der Aufsichtsbehörde nachweisen können.
Die oben erwähnte Rechenschaftspflicht führt dazu, dass der Verantwortliche die Funktionslosigkeit der Kamera hinreichend glaubhaft machen muss.

- Wie kann nun in der Praxis glaubhaft gemacht werden, dass eine Kamera keine Daten verarbeitet?
- Soll der Verantwortliche der Behörde ein leeres Speichermedium zusenden (viele Kameras speichern in der Cloud)?
- Soll die Aufsichtsbehörde einen Mitarbeitenden zur Vor-Ort-Untersuchung an den vermeintlichen „Tatort“ schicken?
- Welche Nachweise des Verantwortlichen hält die Behörde für geeignet, um zu belegen, dass es sich tatsächlich um eine Attrappe handelt?

Weiter auf DataAgenda lesen

Foto: DedMityay, Adobe Stock

Lagebild: Cybersicherheit in der Automobilbranche

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist sich sicher: Cyberangriffe werden qualitativ immer ausgereifter und zielgerichteter. Das zeigen die Lageberichte der Behörde, auch im Vergleich der Lageberichte untereinander. Von dieser Bedrohungslage ist natürlich auch die Automobilbranche betroffen.

Automobilhersteller und ihre Zulieferer (Supply-Chain-Angriffe), aber auch kleinere Betriebe mit Alleinstellungsmerkmalen, wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau, wurden in jüngster Vergangenheit Opfer gezielter Cyberangriffe:

- In 2017 kam es bei einem französischen Automobilhersteller zu einem Stillstand der kompletten Produktion, ausgelöst durch die Schadsoftware „Wannacry". Auch dessen Zulieferer waren durch die Auswirkungen betroffen und konnten keine Teile liefern.
- 2020 wurden die Systeme eines deutschen Zulieferers und Dienstleisters verschlüsselt. Mehrere Gigabyte an Daten mit Konstruktionszeichnungen und Arbeitsplänen sind abgeflossen.
- Ebenfalls in 2020 kam es bei einem amerikanischen Zulieferer in Folge eines Ransomware-Angriffs zu massiven Produktionseinschränkungen und zu Lieferproblemen.
- 2021 wurden mehrere deutsche Zulieferer und Entwickler Opfer von Ransomware-Angriffen. In der Folge kam es zu massiven Unterbrechungen ihrer Leistungserbringung.

Das BSI zeigt in seiner Veröffentlichung „Branchenlagebild Automotive – Cyber-Sicherheit in der Automobilbranche 2021/2022" eindrucksvoll, wie im Kontext der weiterhin stark zunehmenden Vernetzung und Globalisierung von Informationssystemen ein vergleichbares Informationssicherheitsniveau aller Beteiligten – über die gesamte Wertschöpfungskette hinweg – von entscheidender Bedeutung ist, um den Risiken zu begegnen, die auch die Automobilbranche gefährden.
Das BSI geht hier auf das Branchenmodell TISAX als IT-Branchenstandard, die regulativen Vorgaben zur Cybersicherheit in Kraftfahrzeugen gemäß UNECE-Regelung UN-R155 (15) sowie den Standard ISO/SAE 21434 „Road Vehicles – Cybersecurity Engineering" ein.

Arbeitspapier zu „Smart Cities“

Unter dem Vorsitz von Prof. Ulrich Kelber hat die Internationale Arbeitsgruppe für Datenschutz in der Technologie (IWGDPT), allgemein bekannt als „Berlin Group“, ein Arbeitspapier zu „Smart Cities“ verabschiedet, das Städten, Dienstleistern und Regulierungsbehörden praktische Empfehlungen bietet, um datenschutzfreundlichere Lösungen für „Smart Cities“ zu identifizieren und zu fördern.

Foto: Montri, Adobe Stock

Städte in der ganzen Welt wenden neue und innovative Verfahren an, um ihre Ziele zu erreichen. Dies kann die Einführung neuer Technologien oder die Anwendung neuer Datenverarbeitungsmethoden mit vorhandenen Daten sein. Die Berlin Group ist davon überzeugt, dass der Weg zu „intelligenten“ oder „vernetzten“ Städten von Anfang an eine sinnvolle Datenverwaltung erfordert, um das Vertrauen der Bürger und der Besucher der Stadt zu erhalten.

Beim Aufbau intelligenter Städte können zahlreiche Akteure beteiligt sein und verschiedenste Verarbeitungsprozesse eine Rolle spielen. Das Arbeitspapier versucht nicht, intelligente Städte zu definieren, sondern untersucht das Thema der Digitalisierung von Städten als Prozess in den drei Phasen Datenerhebung, Datenanalyse und Entscheidung.

Die theoretischen Ausführungen werden am Beispiel der Stadt „Enschede“ weiter veranschaulicht.
Im September 2017 beschloss die Stadtverwaltung von Enschede, eine 24/7-WLAN-Überwachung im Stadtzentrum einzuführen. Ziel war es, die Effektivität kommunaler Investitionen im Hinblick auf eine verantwortungsvolle Mittelverwendung zu messen. Die Stadtverwaltung beauftragte einen Dienstleister, der wiederum eine andere Partei mit der Installation und Wartung der Sensoren und die von den Sensoren erfassten Daten zu sammeln und zu validieren.

Das Arbeitspapier schließt mit einer Sammlung von Empfehlungen zum Thema Smart Cities ab.

Mitarbeiterinformation Datenschutz im Krankenhaus

- ideal für alle Beschäftigten im Krankenhaus
- leicht verständlich und anschaulich illustriert
- Umschlag firmenindividuell gestaltbar

NEU

Jetzt bestellen: **www.datakontext.com/mitarbeiterinformation-KH**

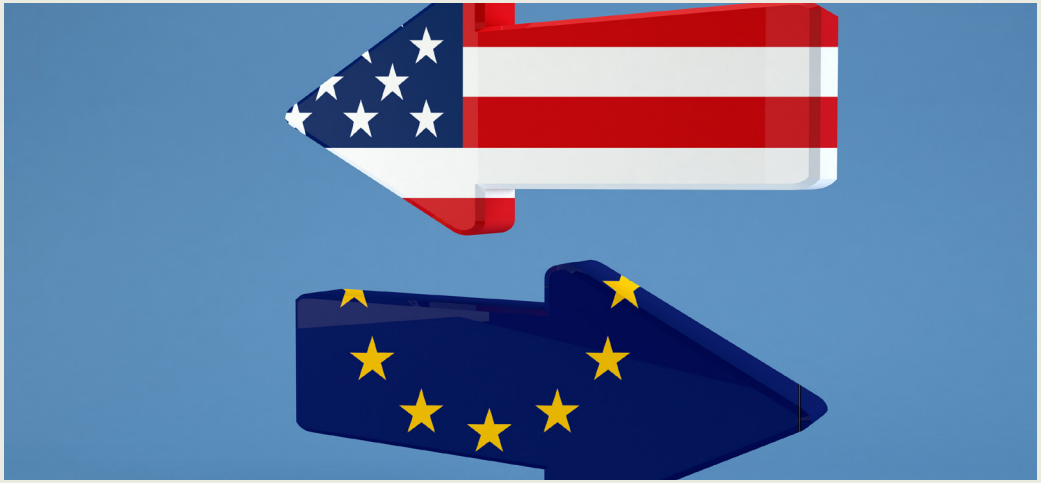

Foto: Weissblick, Adobe Stock

Anwendungshinweise zum EU-US Data Privacy Framework

Am 10. Juli 2023 hat der Europäische Datenschutzausschuss den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework angenommen.

Dieser Beschluss markiert die Fortsetzung des Privacy-Shield-Abkommens, welches bereits im Juli 2020 vom Europäischen Gerichtshof in der Rechtssache „Schrems II“ wegen Unwirksamkeit für nichtig erklärt wurde.
Der Angemessenheitsbeschluss ermöglicht seitdem die Übermittlung von personenbezogenen Daten in die USA. Datenexporteure aus der EU müssen jedoch vorab sicherstellen, dass der Empfänger, an den die Daten übermittelt werden, nach dem EU-U.S. Data Privacy Framework zertifiziert ist.

Fragen und Antworten: Datenschutzrahmen EU-USA

Naturgemäß haben Verantwortliche nach wie vor zahlreiche Fragen rund um den neuen Angemessenheitsbeschluss. Möglicherweise lassen sich einige dieser Fragen mithilfe der FAQ klären, die die Europäische Kommission zwischenzeitlich zur Verfügung gestellt hat.

Anwendungshinweise zum Angemessenheitsbeschluss der DSK

Auch die Datenschutzkonferenz (DSK) hat zu diesem Thema ein Dokument mit umfangreichen Anwendungshinweisen erarbeitet und zum Download bereitgestellt. Diese Hinweise adressieren sowohl Verantwortliche als auch Auftragsverarbeiter in Deutschland, die personenbezogene Daten in die USA übermitteln. Sie beleuchten insbesondere die Reichweite und den Anwendungsbereich der neuen Regelungen, die Nutzung alternativer Mechanismen bei Datenübermittlungen in die USA sowie den Umfang und die Durchsetzung der Rechte von betroffenen Personen gegenüber US-amerikanischen Stellen.

Änderung des Bundesdatenschutzgesetzes: GDD nimmt Stellung

Foto: netpics, Adobe Stock

Das Bundesministerium des Innern und für Heimat (BMI) hat am 9. August 2023 einen Referentenentwurf für ein Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes vorgelegt.

Der Gesetzentwurf zielt darauf ab, Vereinbarungen des Koalitionsvertrags 2021 bis 2025 aufzugreifen. Zudem sollen mit dem Entwurf die Ergebnisse der Evaluierung des Bundesdatenschutzgesetzes (BDSG) umgesetzt werden.

Die GDD wurde gebeten, zu den geplanten Änderungen Stellung zu nehmen. Die Stellungnahme der GDD vom 6. September 2023 kann hier abgerufen werden.

Die geplante Änderung des Bundesdatenschutzgesetzes ist Bestandteil der vom Bundeskabinett Ende August beschlossenen Nationalen Datenstrategie.
Neben den beschriebenen Änderungen des BDSG plant die Bundesregierung zudem neue spezielle Regelungen zum Beschäftigtendatenschutz. Auch dieses Vorhaben ist Teil der angesprochenen Nationalen Datenstrategie. Die Neuregelung des Beschäftigtendatenschutzes soll jedoch in einem eigenständigen Gesetzgebungsverfahren erfolgen.

Die Stellungnahme der GDD zu den geplanten Regelungen im Bereich des Beschäftigtendatenschutzes ist hier abrufbar.

Foto: scharfsinn86, Adobe Stock

Autohersteller patzen beim Datenschutz?

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wies bereits im Jahr 2014 im Rahmen einer Entschließung auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen.

Das Gremium stellte bereits damals fest, dass die Datenverarbeitung in modernen Fahrzeugen Begehrlichkeiten schafft, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen.

Die Aufsichtsbehörden sahen bereits damals die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten würden Auskunft über das Fahrverhalten und die Aufenthaltsorte geben und könnten zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Fast ein Jahrzehnt später beschäftigt sich die Mozilla Foundation im Rahmen einer Studie mit dem Thema „Datenschutz in Fahrzeugen“. Die kompakte Aussage der Studie lautet: „Autos sind in puncto Datenschutz die übelste Produktkategorie, die wir je getestet haben“. Allen 25 Automarken habe man den „Datenschutz nicht inbegriffen“-Warnhinweis verliehen. Folgende Gründe gibt die Mozilla Foundation für dieses Ergebnis an:

1. Sie (die Autos) sammeln zu viele persönliche Daten (gilt für ALLE Marken).
2. Die meisten (84 %) geben Ihre Daten weiter oder verkaufen sie.
3. Die meisten (92 %) geben Fahrer*innen wenig bis keine Kontrolle über ihre persönlichen Daten.
4. Wir konnten nicht bestätigen, dass überhaupt irgendeine Marke unsere Mindestsicherheitsstandards erfüllt.

Nicht ganz überraschend werden die Ergebnisse von den Autoherstellern nicht geteilt. BMW hat bereits mit einem Statement zu den Ergebnissen der Mozilla Foundation reagiert.

Foto: Andrey Popov, Adobe Stock

Reaktion auf einen Cyberangriff: LDI NRW mit Schritt-für-Schritt-Anleitung

Ein IT-Sicherheitsvorfall bezieht sich auf eine Situation, in der die Integrität, Vertraulichkeit oder Verfügbarkeit von IT-Systemen oder Daten in einem Unternehmen gefährdet ist oder verletzt wurde.

Dies kann verschiedene Formen annehmen, z. B. den unbefugten Zugriff auf sensible Informationen, Datenlecks, Malware-Infektionen, Denial-of-Service-Angriffe, Phishing oder Social Engineering.

Weiter auf DataAgenda lesen

Foto: Matthew Cerff/peopleimages.com, Adobe Stock

Mitarbeiterexzess löst Auskunftsanspruch aus

Nach Auffassung der Datenschutzkonferenz (DSK) als Gremium der deutschen Datenschutzaufsichtsbehörden sollen Unternehmen im Rahmen von Art. 83 DS-GVO für Datenschutzverstöße eines jeden Beschäftigten haften, wenn der Mitarbeiter nicht im Exzess (für eigene Zwecke) gehandelt hat.

In bestimmen Fällen kann aber auch der Arbeitnehmer unmittelbar Adressat einer aufsichtsbehördlichen (Sanktions-)Maßnahme sein. Dafür muss der Beschäftigte als „Verantwortlicher" im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren sein. Die DSK hat in seiner Entschließung vom 3. April 2019 („Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!") betont, dass sogenannte „Exzesse" der Beschäftigten, die bei verständiger Würdigung nicht der unternehmerischen Tätigkeit zugeordnet werden können, nicht von der Haftung des Unternehmens erfasst sind.

Dass ein sog. Mitarbeiterexzess trotzdem unmittelbare Konsequenzen für die verantwortliche Stelle haben kann, zeigt ein Fall des Landgerichts Baden-Baden (Urteil vom 24.08.2023).

Das Landgericht Baden-Baden hat einem Unternehmen auferlegt, einer Kundin die Namen der Mitarbeiter offenzulegen, die personenbezogene Kundendaten des Unternehmens in privater Funktion verarbeitet haben. Ferner wurde dem Unternehmen untersagt, seinen Mitarbeitern die weitere Nutzung dieser Kundendaten auf privaten Kommunikationsgeräten zu gestatten.

Die Rechtfertigung des Gerichts beruht auf der Datenschutz-Grundverordnung (DS-GVO), die in Art. 15 Abs. 1 lit. c) das Recht auf Auskunft für die Kundin vorsieht. Dieses Recht erstreckt sich in diesem Fall darauf, dass der klagenden Kundin die Mitarbeiter des Unternehmens genannt werden, die gemäß Art. 4 Nr. 9 der DS-GVO als Empfänger der von ihr bereitgestellten personenbezogenen Daten gelten.

Beschäftigte gelten in der Regel nicht als Empfänger im Sinne von Art. 156 DS-GVO, sofern sie unter der Aufsicht des Verantwortlichen agieren und gemäß seinen Weisungen handeln. Hier jedoch stellte das Gericht fest, dass eine Mitarbeiterin eigenmächtig über ihren privaten Account Kontakt zu einer Kundin aufgenommen hatte, um Fragen im Zusammenhang mit einem Kauf zu klären.

Da die Kundin die Mitarbeiteridentität benötigte, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen und gegebenenfalls Ansprüche nach der DS-GVO gegen die Mitarbeiter geltend zu machen, wurde festgestellt, dass ein Auskunftsanspruch auf Nennung der Mitarbeiter besteht.

Foto: Lila DK, Adobe Stock

BSI bietet weitere Einstiegsmöglichkeit in die „Basis-Absicherung“

Die IT-Grundschutz-Methodik bietet neben der grundlegenden Absicherung zwei weitere Ansätze, die je nach den spezifischen Sicherheitsanforderungen einer Organisation angewendet werden können. Verantwortliche für die Informationssicherheit haben somit die Möglichkeit, zwischen Basis-, Standard- und Kern-Absicherung zu wählen. Die Basis-Absicherung ermöglicht einen initialen Einstieg in das Sicherheitsmanagement, um schnell die größten Risiken zu mindern. Im Gegensatz dazu dient die Kern-Absicherung dem Schutz essenzieller Geschäftsprozesse und Ressourcen.
Nach erfolgreicher Implementierung der Basis-Absicherung in einer Organisation empfiehlt das BSI, mit der Standard- oder Kern-Absicherung fortzufahren, um eine robuste Informationssicherheit zu gewährleisten. Ideal ist die schrittweise Umsetzung einer umfassenden Standard-Absicherung gemäß BSI-Standard 200-2 im Laufe der Zeit, um ein dem Schutzbedarf angemessenes Sicherheitsniveau zu erreichen.
Das BSI bietet den Verantwortlichen nun einen „sanften Einstieg“ bzw. einen weiteren Weg hin zu einer Basis-Absicherung.
Um den Einstieg in den IT-Grundschutz zu erleichtern, hat das BSI das Projekt „Weg in die Basis-Absicherung (WiBa)“ ins Leben gerufen. Dies ist vor allem vor dem Hintergrund geschehen, dass die Einführung der Basis-Absicherung nach wie vor als zu zeitaufwendig empfunden wird und in kleineren Kommunen die Ressourcen für die Umsetzung fehlen.
Hauptziel ist es, den Zugang zum IT-Grundschutz praxisorientierter zu gestalten, um die Implementierungsaufwände weiter zu reduzieren. Dabei liegt der Fokus auf kommunalen Institutionen.
Durch die Verwendung von prüfungsrelevanten Fragen, die in spezifischen Checklisten zusammengefasst sind, soll die Möglichkeit geschaffen werden, Informationen zur Informationssicherheit zu sammeln und die erforderlichen Maßnahmen zu identifizieren, selbst ohne detaillierte Kenntnisse der Methodik.
Die prüfungsrelevanten Fragen auf Basis des IT-Grundschutz-Profils für die Basis-Absicherung von Kommunalverwaltungen decken die wichtigsten Aspekte ab, die bei der Priorisierung und tatsächlichen Umsetzung der Absicherung berücksichtigt werden müssen. Nach Abschluss dieser Phase kann nach Einschätzung des BSI nahtlos mit der vollständigen Umsetzung des oben genannten Profils fortgefahren werden.
Auch wenn hier in erster Linie Verwaltungen angesprochen werden, können die frei zugänglichen Checklisten auch von der Privatwirtschaft mit einem Mehrwert als „entmystifizierende“ Einstiegshilfe in das komplexe Themenfeld genutzt werden. WiBA führt noch nicht zur Etablierung eines Informationssicherheits-Managementsystems (ISMS). Vielmehr bietet WiBA einen Einstieg in das Thema und gibt konkrete Handlungsempfehlungen.
Die Dokumente liegen als sog. „Community Draft“ vor, so dass sich in den finalen Dokumenten noch Änderungen ergeben können.

(Quelle: TH Köln/Schmülgen)

Data Agenda Podcast Folge 44: Regulierung generativer KI zwischen Digitalwirtschaft und Datenschutzaufsicht

„Zeichne mir einen Menschen in der Küche". Diese Aufforderung muss eine bildgenerierende künstliche Intelligenz (KI) geschlechtsneutral erledigen, wenn kein geschlechterdiskriminierendes Menschenbild erzeugt werden soll. Die Daten, auf die Anwendungen zugreifen, die Sprache oder Bilder erzeugen, müssen unser Verständnis von Gut und Böse kennen, um die Welt so abbilden zu können, wie wir sie wahrnehmen. Zugleich soll die Datenbasis neutral und unschuldig sein. Aber warum soll eine generative KI-Anwendung eigentlich nicht werten dürfen? Und wer entscheidet, ob eine Datenbasis Gutes oder Böses hervorbringt – die Programmierer, die Nutzer oder doch die Gesellschaft? Wie sieht das die Digitalwirtschaft und wie die Datenschutzaufsicht?
Ein DataAgenda-Podcast mit den Gründern von Aleph Alpha **Jonas Andrulis** und **Samuel Weinbach** im Gespräch mit DSK und ULD-Schleswig Holstein Chefin **Dr. hc. Marit Hansen** und dem LfDI aus Baden-Württemberg **Prof. Dr. Tobias Keber**.
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