NEWS BOX DATENSCHUTZ

AUSGABE
4/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, hat am Dienstag, den 05.04.2022, der Präsidentin des Deutschen Bundestages seinen 30. Tätigkeitsbericht für das Jahr 2021 übergeben.

Schon beim Lesen des Vorworts mag sich der eine oder andere Datenschutzbeauftragte denken, dass den Bundesbeauftragten für den Datenschutz ähnliche Sorgen plagen, wie den „ganz normalen Datenschutzbeauftragten von nebenan". So bemerkt der BfDI:

„[...] Wie schon 2020 legte die Bundesregierung dabei Gesetzentwürfe und Verordnungen zur Pandemie-Bekämpfung im Akkord vor, und wie im Vorjahr gab es selten Zeit, diese Entwürfe sachgerecht zu prüfen und die Bundesregierung zu beraten. Bei allem Verständnis für die zum Teil gebotene Eile hätten ein wenig mehr Sorgfalt und eine Einbindung von Beginn an – wie eigentlich vorgeschrieben – der Sache sicher gutgetan."

Wie bitte?! Auch der BfDI wird oftmals (manchmal?) nicht frühzeitig eingebunden? Es ist also nicht nur Schicksal der „ganz gewöhnlichen Datenschutzbeauftragten" dieser Republik, dass Art. 38 Abs.1 DS-GVO immer mal wieder geflissentlich ignoriert wird?

So kann der interessierte Leser weiter erfahren, dass es dem BfDI auch schon mal passiert, dass er zwar eingebunden wird, dann aber *„mit einer extrem kurzen Prüf- und Stellungnahmefrist"*. Jeder DSB kann bestätigen, dass sich die Kürze der Stellungnahmefristen bei bestimmten Projekten (von der Fachabteilung gewollt oder ungewollt) umgekehrt proportional zu der Komplexität der aufgeworfenen Fragen verhält.

Weiter schreibt der BfDI: *„Stattdessen werden Lösungsvorschläge – auch solche, die bei richtiger Ausgestaltung datenschutzrechtlich möglich wären – oft gar nicht erst vorgelegt oder besprochen. Vielmehr wird öffentlich lamentiert, „der Datenschutz" würde im Weg stehen."* Unvorstellbar, dass es auch einen DSB gibt, der/die diesen Vorwurf noch nie in seinem Berufsleben gehört hat.

Die Einstellung des BfDI zu diesen „Phänomen" ist jedoch vorbildlich: *„[...] Entgegen dieser immer wieder vorgebrachten Kritik hat der Datenschutz und damit auch meine Behörde aber keine einzige geeignete Pandemiebekämpfungsmaßnahme der Bundesregierung beschränkt oder gar gestoppt. So müßig es mittlerweile geworden ist, werde ich auch in Zukunft nicht müde werden, dies richtigzustellen und mich Schwarzer-Peter-Spielen entgegenstellen, die nur den Blick auf die notwendigen Maßnahmen behindern."*

Mit dieser Hartnäckigkeit, die der BfDI auch immer wieder in den Sozialen Medien gegen „verleumderische Behauptungen", dass der Datenschutz [beliebiges Projekt einsetzen] behindere, an den Tag legt, hat er sogar ein „Meme" hierzu geschaffen: „Kelbers Law".

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Miha Creative, Adobe Stock

Ungeklärte Fragen des Auskunftsrechts nach DS-GVO

Der Europäische Datenschutzausschuss (EDSA) hat am 18. Januar dieses Jahres die Guidelines 01/2022 zum Auskunftsrecht nach Art. 15 DS-GVO veröffentlicht.

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. Wenig überraschend hat der EDSA den Auskunftsanspruch in seinen 60-seitigen Guidelines tendenziell weit ausgelegt. Die interessierte Öffentlichkeit hatte bis zum 11.03.2022 Gelegenheit, Stellungnahmen zu den Guidelines einzureichen. Auch die GDD hat sich über ihren europäischen Dachverband CEDPO an dem Konsultationsverfahren beteiligt. Das Papier des EDSA zur Auskunft kann hier abgerufen werden.

>> Die Stellungnahme von CEDPO finden Sie hier.

Foto: berkay08, Adobe Stock

Schadensersatz soll abschreckende Wirkung haben

ArbG Dresden, Urt. v. 26.08.2020 – 13 Ca 1046/20

Gesundheitsdaten unterliegen laut der DS-GVO einem besonderen Schutzbedarf. Die Weitergabe solcher Daten ist nur in den ausdrücklich in Art. 9 Abs. 2 DS-GVO genannten Fällen erlaubt. Daher sollte ein Arbeitgeber besonders sensibilisiert sein, wenn er diese an Dritte weitergibt.

Weiter auf DataAgenda lesen

DATAAGENDA UND LATHAM & WATKINS LLP

DS-GVO-Schadensersatztabelle

RA Tim Wybitul / Dr. Tobias Jacquemain, LL.M.

Stand Januar 2022

LATHAM & WATKINS LLP

DATAKONTEXT

Foto: LuckyStep, Adobe Stock

Pseudonymisierung im Gesundheitswesen

Die DS-GVO sieht die Pseudonymisierung als eine mögliche Maßnahme an, deren Einsatz die Gewährleistung eines angemessenen Schutzniveaus unterstützen kann. Die DS-GVO verweist an verschiedenen Stellen, wie z. B. bei den Anforderungen bzgl. Privacy by Design/Default (Art. 25) oder bei der Verarbeitung von Forschungsarbeiten, auf diese Maßnahme.

In Bezug auf die Pseudonymisierung schreibt der europäische Gesetzgeber in ErwGr. 28 DS-GVO: „Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann [...] die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen".

Dabei wird sowohl die Anonymisierung als auch die Pseudonymisierung als eine Verarbeitung im Sinne der DS-GVO betrachtet, mit der Konsequenz, dass hierfür eine Rechtsgrundlage („Erlaubnistatbestand") für die Durchführung einer Anonymisierung oder auch einer Pseudonymisierung benötigt wird.

Die **Agentur der Europäischen Union für Cybersicherheit (ENISA**: ***E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency*) hat zu der praxisrelevanten Frage der Einsatzmöglichkeit der Pseudonymisierung eine Orientierungshilfe veröffentlicht. Nach Auffassung der ENISA entwickelt sich die Pseudonymisierung zunehmend zu einer wichtigen Sicherheitsmaßnahme, die die Verarbeitung personenbezogener Daten erleichtern kann und gleichzeitig starke Garantien für den Schutz personenbezogener Daten und damit für die Wahrung der Rechte und Freiheiten des Einzelnen bietet. Ergänzend zu früheren Arbeiten der ENISA zeigt dieser Bericht auf, wie die Pseudonymisierung in der Praxis eingesetzt werden kann, um den Schutz von Gesundheitsdaten während der Verarbeitung weiter zu fördern.

Interessierten zum Thema der Pseudonymisierung im Gesundheitswesen kann ebenfalls die „Arbeitshilfe zur Pseudonymisierung/Anonymisierung" der GMDS Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen" empfohlen werden (Stand der Ausarbeitung: 29. Juni 2018).

Quelle: ENISA

Nachfolge für das „Privacy-Shield“ in Sicht

Foto: Kittiphat, Adobe Stock

Die Europäische Kommission und die Vereinigten Staaten haben bekannt gegeben, dass sie sich grundsätzlich auf einen neuen transatlantischen Datenschutzrahmen geeinigt haben, der den transatlantischen Datenverkehr fördern und die vom EuGH in der Schrems-II-Entscheidung vom Juli 2020 geäußerten Bedenken ausräumen soll. Das gaben die Präsidentin der Europäischen Kommission, Ursula von der Leyen und US-Präsident Joe Biden, im Rahmen von Bidens Besuch in Brüssel bekannt.

Das Nachfolgeabkommen des Privacy Shield soll „Trans-Atlantic Data Privacy Framework“ lauten.
Der Nachfolger des Privacy Shield sei das Ergebnis von mehr als einem Jahr detaillierter Verhandlungen zwischen den USA und der EU unter der Leitung von Handelsministerin Gina Raimondo und Justizkommissar Didier Reynders. Er werde eine dauerhafte Grundlage für den transatlantischen Datenverkehr schaffen, der für den Schutz der Bürgerrechte und die Ermöglichung des transatlantischen Handels in allen Wirtschaftssektoren, auch für kleine und mittlere Unternehmen, von entscheidender Bedeutung sein werde.
Die wichtigsten Grundsätze des neuen Abkommen werden in einem Fact-Sheet zusammengefasst.

Löschen leicht gemacht!

DATA AGENDA Löschmanager

- ✓ erfassen
- ✓ dokumentieren
- ✓ umsetzen

Die Softwarelösung zur Erstellung eines DS-GVO- und DIN 66398-kompatiblen Löschkonzeptes.

Jetzt informieren: **www.DataAgenda.de/Loeschmanager**

DATAKONTEXT

Datenschutzkonforme Vernichtung von 3G-Nachweis und Kontaktdaten

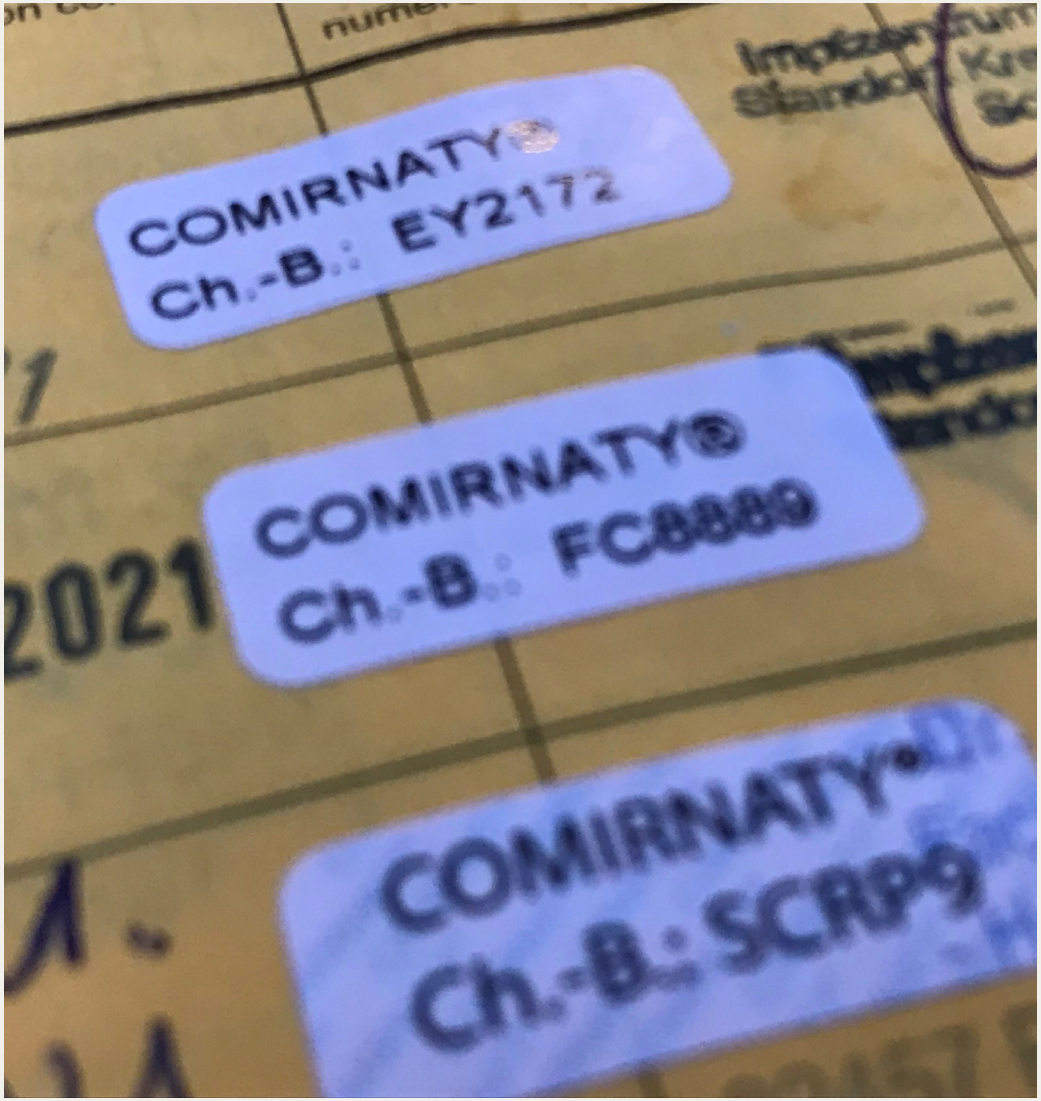


Foto: bierwirm, Adobe Stock

Bettina Gayk, Landesbeauftrage für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, weist auf einen Umstand hin, der ggf. in Vergessenheit geraten könnte. Es bringt nichts, Löschkonzepte zu erstellen und Löschfristen festzulegen oder wie in diesem Fall diese vorgegebenen Fristen zu notieren – wenn diese nicht am Ende auch technisch umgesetzt werden.

Die LDI NRW mahnt an, dass infolge der aktuellen Lockerungen im Rahmen des Infektionsschutzgesetzes des Bundes, die von den Arbeitgeber*innen erhobenen Daten spätestens sechs Monate nach Erhebung vernichtet oder gelöscht werden müssen. „Da die Rechtsgrundlage entfallen ist, gehen wir davon aus, dass die Speicherung regelmäßig nicht mehr erforderlich ist und die Daten schon jetzt gelöscht werden sollten“, so Bettina Gayk.

Insbesondere Gesundheitsdaten von Beschäftigten und – sofern noch vorhanden – Daten zur Kontaktnachverfolgung müssten gelöscht, also vollständig und unwiderruflich vernichtet werden. Bei Daten, die in Papierform erhoben wurden, sollte ein geeigneter Aktenvernichter verwendet werden.
Die LDI NRW betont, dass für das Löschen personenbezogener Daten durch Aktenvernichter-Geräte der Sicherheitsstufe 4 oder höher gemäß dieser DIN geeignet sind.

Quelle: LDI NRW

Foto: Sai, Adobe Stock

Zweifel an Datenschutz-Konformität von Facebook-Fanpages

Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder teilt mit, dass sie das Urteil des EuGH zur gemeinsamen Verantwortlichkeit der Betreiber im Hinblick auf die betriebenen Facebook-Fanpages zum Anlass genommen haben, um sich, im Rahmen einer dazu eingerichteten Taskforce, mit den Fragen rund um die Rechtskonformität des Betriebs einer Fanpage zu beschäftigen.

Eben diese Taskforce hat ein Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages unter Berücksichtigung des seit dem 1. Dezember 2021 geltenden Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG), des Urteils des OVG Schleswig vom 25. November 2021 (Az. 4 LB 20/13) und der aktuellen technischen Umsetzungen erstellt und nunmehr veröffentlicht.

In einem weiteren Beschluss informiert die DSK darüber, dass sie das von der Taskforce Facebook-Fanpages erstellte Kurzgutachten zur Frage der datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 18.03.2022 zur Kenntnis nimmt und der Bewertung zustimmt.

Damit rücken wieder die öffentlichen und nicht öffentlichen Stellen, die Facebook-Fanpages betreiben, in das Blickfeld der aufsichtsbehördlichen Tätigkeit, wobei die DSK klar kommuniziert, dass aufgrund ihrer Vorbildfunktion öffentliche Stellen zuvörderst im Fokus stehen. Ähnliche Prüfungen hatte der BfDI bereits letztes Jahr auch für Anfang 2022 in Aussicht gestellt.

Diese müssten bald damit rechnen, dass

- die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zeitnah informieren werden,
- überprüft wird, ob Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben,
- darauf aufsichtsbehördlich darauf hingewirkt wird, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

Dem Beschluss können Verantwortliche ebenfalls entnehmen, welche Nachweise für die datenschutzrechtliche Konformität von den Aufsichtsbehörden verlangt werden dürften.

Foto: Sashkin, Adobe Stock

BayLfD: Hinweise zur datenschutzkonformen Einbindung von Webfonts

Vor kurzem hatten wir bereits an dieser Stelle berichtet, dass auch das Thema „Nutzung bzw. Einbindung von Schriftarten auf Webseiten" durchaus ein Datenschutz-Problem sein kann (Vgl. Urteil des Landgerichts München, Urteil vom 20.01.2022, Az. 3 O 17493/20). Das Gericht sprach hier einen Unterlassungsanspruch und Schadensersatz (hier 100 €) wg. Weitergabe von IP-Adresse an Google durch Nutzung von Google Fonts gegen den Beklagten aus.

Weiter auf DataAgenda lesen

CNIL veröffentlicht Praxisleitfaden zum Datenschutzbeauftragten

Warum, wann und wie sollte man Datenschutzbeauftragte benennen? Welche Mittel und Ressourcen sollten ihnen zur Verfügung gestellt werden, um ihre Aufgaben zu erfüllen?

Die CNIL (Commission nationale de l'informatique et des libertés), die nationale Datenschutzbehörde Frankreichs veröffentlicht einen Leitfaden für Datenschutzbeauftragte, der auf über 50 Seiten nützliches Wissen und bewährte Verfahren zusammenfasst, um Organisationen bei der Benennung und Unterstützung von Datenschutzbeauftragten zu helfen.

Weiter auf DataAgenda lesen

Foto: magele-picture, Adobe Stock

Foto: sarayut_sy, Adobe Stock

BSI warnt vor Kaspersky-Virenschutzprodukten

Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Doch mit der Zunahme digitaler Prozesse vergrößert sich gleichzeitig die Angriffsfläche für Kriminelle. Schadprogramme, Datenmissbrauch, Passwort- und Identitätsdiebstahl sind nur einige Gefahren.

Weiter auf DataAgenda lesen

Foto: MQ-Illustrations, Adobe Stock

GDD-Stellungnahme zur „Orientierungshilfe Telemedien 2021" der DSK

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 20.12.2021 eine neue Fassung ihrer Orientierungshilfe für Anbieter von Telemedien veröffentlicht („Orientierungshilfe Telemedien 2021").

Mittels des überarbeiteten Papiers soll Betreibenden von Webseiten, Apps oder Smarthome-Anwendungen konkrete Hilfestellung bei der Umsetzung der am 01.12.2021 in Kraft getretenen Vorschriften des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) gegeben werden. Zudem soll das Papier betroffenen Bürgerinnen und Bürgern ein besseres Bild der rechtlichen Rahmenbedingungen bei der Verarbeitung ihrer Daten im Onlinebereich vermitteln.
Mit dem TTDSG hat der Bundesgesetzgeber nach über einem Jahrzehnt Verzögerung die Vorgaben der europäischen ePrivacy-Richtlinie in nationales Recht umgesetzt. § 25 TTDSG, welcher die Integrität des Endgeräts schützen soll, wurde dabei eng am Wortlaut der europäischen Vorgaben formuliert und fordert grundsätzlich eine Einwilligung der betroffenen Nutzer/-innen, wenn Informationen auf deren Endeinrichtungen gespeichert werden oder auf in den Endeinrichtungen bereits vorhandene Informationen zugegriffen wird.

Vor diesem Hintergrund ist es nach Ansicht der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) begrüßenswert, dass die DSK nicht nur ausführlich ihre Sichtweise auf die Neuregelung in § 25 TTDSG darstellt, sondern hierzu am 14.01. dieses Jahres auch ein Konsultationsverfahren gestartet hat. Stellungnahmen durch Vertreter/-innen aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung konnten bis zum 15.03.2022 eingereicht werden.
Auch die GDD hat im Rahmen des Konsultationsverfahrens eine Stellungnahme abgegeben. Sie verbindet die Teilnahme an dem Verfahren mit der Hoffnung, dass die DSK sich mit den im Rahmen des Verfahrens vorgebrachten Argumenten substanziell auseinandersetzt und die Inhalte der OH Telemedien 2021 diesbezüglich überprüft.

Quelle: Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)

DATA AGENDA
PODCAST

Der **Experten-Talk** mit
Prof. Schwartmann

Folge #**14**

Krieg mit
Informationen

Folge #**15**

Privacy Sells
Das TTDSG als Motor für datenschutz-
freundliche Geschäftsmodelle in der EU

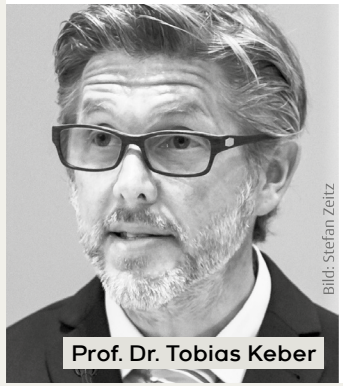
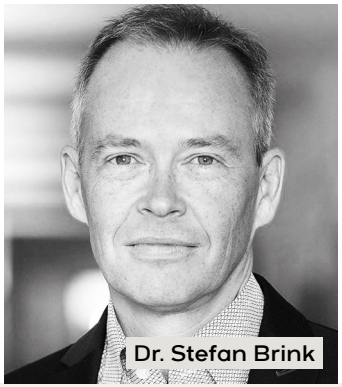


Bild: Stefan Zeitz

Prof. Dr. Tobias Keber



Dr. Stefan Brink

Christian Völkel

Folge 14: Krieg mit Informationen

Russlands Krieg gegen die Ukraine ist auch ein Krieg mit Informationen und damit auch mit Daten im Netz. Viele wollen der Ukraine aus guten Gründen beistehen und begeben sich als private Hacker im Netz eigenmächtig auf den Kriegspfad. Experten befürchten, dass dies die Situation noch eskalieren kann. Rechtsdurchsetzung ist aber auch im Krieg ebenso eine Staatsangelegenheit, wie die Kriegsführung und deren Vermeidung selbst. Klar ist: Wenn man auf dem Pulverfass sitzt, muss man besonnen sein. Welche Möglichkeiten haben Staaten, Medienunternehmen und Private? Ein Gespräch mit Professor Dr. Tobias Keber von der Hochschule der Medien in Stuttgart über Daten als Waffen.
Zum Podcast bitte hier klicken.

Folge 15: Privacy Sells – Das TTDSG als Motor für datenschutzfreundliche Geschäftsmodelle in der EU

Rolf Schwartmann im Gespräch mit Dr. Stefan Brink, LfDI BW, und Christian Völkel, DSB Porsche AG.
Vernetzt und künftig autonom fahrende Autos sind ein entscheidender Faktor der Digitalisierung. Sie bringen Menschen von A nach B. Zugleich sind Autos vernetzte Endgeräte, die eine Vielzahl von Daten über das Fahrzeug, dessen Fahrer und Beifahrer und die Umgebung verarbeiten. Die Datenschutzabteilung der Porsche AG hat sich beim LfDI BW zu Fragen der Anwendung des TTDSG beim vernetzten Fahren beraten lassen. Das Ergebnis ist für die Onlinewirtschaft insgesamt interessant.
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