NEWS BOX DATENSCHUTZ

AUSGABE
1/2023

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Die letzten Tage hat der „KI-Chatbot“ des Forschungsunternehmens Open AI für viel Furore und großes Erstaunen gesorgt. Da war es fast klar, dass ChatGPT auch das Verfassen des Editorials der aktuellen Ausgabe der Newsbox übernimmt:
„Schreibe ein Editorial für einen monatlich erscheinenden Datenschutz-Newsletter namens ‚Datenschutz Newsbox‘. Im Editorial soll es um die neue KI-Richtlinie gehen und das Editorial soll Bezüge zu ChatGPT haben. Schließe mit Neujahrsgrüßen für das Jahr 2023 ab.“

„Liebe Leserinnen und Leser der Datenschutz Newsbox,

wir begrüßen Sie zu einer neuen Ausgabe unseres Newsletters und möchten Sie in dieser Ausgabe über eine wichtige neue Entwicklung im Bereich der Künstlichen Intelligenz informieren: Die EU hat kürzlich eine neue KI-Richtlinie verabschiedet, die für Unternehmen und Entwickler von KI-Systemen wichtige neue Regeln mit sich bringt. Diese neue Richtlinie ist insbesondere für Anbieter von KI-Systemen wie ChatGPT von großer Bedeutung, da sie die Verantwortung für den Einsatz von KI-Technologien stärker regelt und damit auch die Verantwortung der Unternehmen für die Privatsphäre der Nutzer erhöht. Dies bedeutet, dass Unternehmen wie ChatGPT künftig noch genauer darauf achten müssen, wie ihre KI-Systeme eingesetzt werden und welche Daten sie verarbeiten. Für die Nutzer von ChatGPT und anderen KI-Systemen bedeutet dies, dass sie sich in Zukunft noch sicherer fühlen können, was den Schutz ihrer Privatsphäre angeht. Die neue KI-Richtlinie stärkt die Rechte der Nutzer und sorgt dafür, dass Unternehmen wie ChatGPT ihre KI-Systeme verantwortungsbewusst einsetzen. Wir von ChatGPT begrüßen die neue KI-Richtlinie und sehen sie als wichtigen Schritt zu einem verantwortungsvollen Einsatz von KI-Technologien. Wir werden die neuen Regeln natürlich beachten und uns weiter dafür einsetzen, unsere KI-Systeme so zu entwickeln, dass sie die Privatsphäre der Nutzer schützen.

Wir hoffen, dass die neue KI-Richtlinie auch für Sie von Interesse ist und wünschen Ihnen und Ihren Lieben ein frohes und erfolgreiches neues Jahr 2023.“

Den Neujahrswünschen von ChatGPT schließe ich mich natürlich an und verspreche, dass das nächste Editorial wieder ohne KI-Unterstützung entstehen wird.

Machen Sie es gut,
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: hkama, Adobe Stock

Anforderungen aus dem EuGH-Urteil „Schrems II" (C-311/18) vom 16.07.2020

Der Gerichtshof der Europäischen Union (EuGH) hat mit seinem Urteil „Schrems II" entschieden, dass europäische Unternehmen ihre Datenübermittlung in die USA nicht mehr auf das zwischen der EU-Kommission und US-Regierung ausgehandelte Privacy Shield-Abkommen stützen können. Bis dahin wurden die meisten Datenübermittlungen in die USA auf den Durchführungsbeschluss (EU) 2016/1250, das sog. EU-US-Privacy Shield, gestützt. Mit seinem Urteil aus dem Juli 2020 hat der EuGH entschieden, dass das Privacy-Shield-Abkommen unwirksam ist.

Datenübermittlungen in die USA für immer unmöglich?

Der EuGH erklärte das Privacy Shield für ungültig, jedoch könne eine Datenübermittlung an ein Drittland aufgrund von Standardvertragsklauseln weiterhin zulässig sein.
Die Übermittlung personenbezogener Daten ist seit der DS-GVO nur zulässig, wenn ein angemessenes Datenschutzniveau im Drittland gewährleistet werden kann. Aufgrund der weitreichenden Zugriffsmöglichkeiten der amerikanischen Sicherheitsbehörden auf elektronisch gespeicherte Daten sind die europäischen Anforderungen an den Datenschutz für in die USA übertragene Nutzerdaten nicht gewährleistet. Auch sei der Rechtsschutz für Betroffene unzureichend, stellte der EuGH fest. Datenübermittlungen in die USA, die ausschließlich auf das Privacy Shield gestützt werden, sind seit Sommer 2020 nicht mehr rechtmäßig. Sie müssen eingestellt werden oder aufgrund eines alternativen Übermittlungstatbestands erfolgen.

Privacy Shield muss raus aus jeder Datenschutzerklärung

Beinhaltet eine Datenschutzerklärung Bezug auf das Privacy Shield als Übermittlungstatbestand für die Übermittlung personenbezogener Daten in die USA (z.B. aufgrund von Cookies, Social-Media-Plugins, Einbindung von Google Maps usw.), muss diese unbedingt und unverzüglich geändert werden. Da das Privacy Shield seit dem besagten EuGH-Urteil ungültig ist, kann dieses auch nicht mehr als Übermittlungstatbestand genutzt werden und mithin darf darauf in der Datenschutzerklärung auch nicht mehr verwiesen werden. Bei Fortführung der Datenübermittlung bedarf es eines alternativen Tatbestands nach Art. 44 ff. DS-GVO, der dann anstelle des Privacy Shield in der Datenschutzerklärung transparent benannt werden muss.

DS-GVO verlangt wirksamen Datenschutz international

Bei der Übermittlung personenbezogener Daten muss neben einer gültigen Rechtsgrundlage auch eine der Bedingungen gemäß Art. 44 ff. DS-GVO erfüllt sein. Danach ist die Datenübermittlung in solche Drittstaaten problemlos möglich, für welche die EU-Kommission einen Angemessenheitsbeschluss gefasst hat. Gibt es wie im Falle der USA jedoch keinen entsprechenden Beschluss, so bleiben in der Praxis nur noch Binding Corporate Rules (BCR) und Standarddatenschutzklauseln als Alternativen übrig. Die „SCC" (Standard Contractual Clauses), häufiger bekannt als Standardvertragsklauseln, stellen eine Garantiefiktion für eine sichere Datenübermittlung in Staaten außerhalb des EWR dar.

Standardvertragsklauseln 2021: Mehr Möglichkeiten, neue Pflichten

Um zumindest einen Teil der sich aus Schrems II-Urteil ergebenden Anforderungen zu berücksichtigen, hat die Europäische Kommission im Juni 2021 den Durchführungsbeschluss für die neuen Standardvertragsklauseln veröffentlicht. Damit wurden fünf Jahre nach Beschluss der DS-GVO die bisherigen Standards aus 2001 bzw. 2010 ersetzt. Die neuen Klauseln sind modular aufgebaut, was die vertragliche Ausgestaltung aller möglichen Transferkonstellationen erlaubt. Beide Vertragsparteien müssen sich ab sofort noch stärker mit der Rechtslage im Drittland und der Vereinbarkeit mit den Vertragsklauseln auseinandersetzen. Das Datenschutzniveau im Drittstaat muss vor Beginn der Datenübermittlung auf seine Angemessenheit nach EU-Standards überprüft werden. Die eingesetzten Vertragsklauseln unterliegen der ständigen Kontrolle durch die Aufsichtsbehörden.

Einwilligung als alternative Lösung?

Zu den Übermittlungstatbeständen für Datenübermittlungen in Drittstaaten gehört nach der DS-GVO auch die Einwilligung. Kann eine Einwilligung die Lösung des Problems darstellen? Art. 49 DS-GVO sieht als weitere Möglichkeit vor, dass die betroffene Person ausdrücklich in Datenübermittlung einwilligt. Doch dies ist aus rechtlicher Sicht nicht so einfach wie es zunächst klingt: Die betroffene Person muss vorher umfassend über die für sie bestehenden möglichen Risiken einer solchen Datenübermittlung unterrichtet werden. Der Normüberschrift des Art. 49 DS-GVO nach darf eine Einwilligung nur in Ausnahmefällen herangezogen werden. So sieht es auch der Europäische Datenschutzausschuss (EDSA): „In Bezug auf Übermittlungen, die für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich sind, ist zu berücksichtigen, dass personenbezogene Daten nur dann übermittelt werden dürfen, wenn die Übermittlung nur gelegentlich erfolgt."

Wie sieht die Datenübermittlungen in die USA zukünftig aus?

Erfahren Sie mehr zum neuen transatlantischen Datenschutzrahmen auf dem 11. GDD-Winter-Workshop

Foto: MQ-Illustrations, Adobe Stock

Orientierungshilfe für Anbieter:innen von Telemedien

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

Mittels des überarbeiteten Papiers sollte 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 sollte das Papier betroffenen Bürgerinnen und Bürgern ein besseres Bild der rechtlichen Rahmenbedingungen bei der Verarbeitung ihrer Daten im Onlinebereich vermitteln.

Eine Aktualisierung dieser Orientierungshilfe ist im Dezember 2022 erschienen.

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.

Die Aufsichtsbehörden weisen darauf hin, dass auch die aktuelle Orientierungshilfe unter dem ausdrücklichen Vorbehalt eines zukünftigen – möglicherweise abweichenden – Verständnisses der maßgeblichen Vorschriften steht, welche durch den Europäischen Datenschutzausschuss (EDSA), durch maßgebliche europäische Rechtsprechung sowie Änderungen des europäischen Rechtsrahmens entstehen können.

Eine ausführliche Bewertung der Stellungnahmen findet sich im Auswertungsbericht des Arbeitskreises Medien „Konsultation zur Orientierungshilfe für Anbieter von Telemedien“.

Foto: WrightStudio, Adobe Stock

Version 3.0 des Standard-Datenschutzmodells veröffentlicht

Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass sie durch die Nutzung ihrer personenbezogenen Daten durch Dritte in der Ausübung von Grundrechten beeinträchtigt werden.

Von zentraler Bedeutung ist dabei der Artikel 5 DS-GVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise als Schutzziele ausgewiesen sind. Das Standard-Datenschutzmodell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutz- bzw. Gewährleistungszielen systematisch überwachen zu können.

Weiter auf DataAgenda lesen

Foto: redaktion93, Adobe Stock

Kopien von Prüfungsarbeiten: Datenschutzrecht als Anspruchsgrundlage

Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person u.a. das Recht auf Auskunft über ihre personenbezogenen Daten. Gemäß Art. 15 Abs. 3 Satz 1 DS-GVO kann sie von dem Verantwortlichen die Überlassung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, verlangen.

Aus Art. 12 Abs. 5 Satz 1 i.V.m. Art. 15 Abs. 3 Satz 2 DS-GVO ergibt sich, dass die erste derartige Kopie unentgeltlich zur Verfügung gestellt werden muss. Durch die Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) ist seit dem Jahr 2017 geklärt, dass die schriftlichen Prüfungsleistungen in einer berufsbezogenen Prüfung und die Anmerkungen der Prüfer dazu wegen der in ihnen jeweils enthaltenen Informationen über den Prüfling insgesamt – das heißt letztlich Wort für Wort – personenbezogene Daten des Prüflings darstellen.

Absolventen der zweiten juristischen Staatsprüfung haben gemäß Art. 15 Abs. 1 und Abs. 3 Satz 1 i.V.m. Art. 12 Abs. 5 Satz 1 der Datenschutz-Grundverordnung (DS-GVO) einen Anspruch darauf, dass ihnen das Landesjustizprüfungsamt unentgeltlich eine Kopie der von ihnen angefertigten Aufsichtsarbeiten mitsamt den zugehörigen Prüfergutachten zur Verfügung stellt.

Dem von dem Kläger geltend gemachten Anspruch stünden keine Ausschlussgründe nach der Datenschutz-Grundverordnung entgegen. Insbesondere handele es sich nicht um einen exzessiven Antrag im Sinne des Art. 12 Abs. 5 Satz 2 DS-GVO. Der Umfang, den seine Bearbeitung nach den tatsächlichen Feststellungen des Oberverwaltungsgerichts bei dem Landesjustizprüfungsamt verursache, sei als vergleichsweise gering zu beurteilen. Der Anspruch beziehe sich vorliegend auf acht Klausuren mit insgesamt 348 Seiten. Durchgreifende Anhaltspunkte für eine rechtsmissbräuchliche Anspruchsverfolgung hat das Oberverwaltungsgericht verneint. Es hat ferner festgestellt, dass der fristgebundene Einsichtsanspruch nach dem nordrhein-westfälischen Juristenausbildungsgesetz den datenschutzrechtlichen Anspruch unberührt lässt. Dies hat das Bundesverwaltungsgericht in Leipzig entschieden (BVerwG 6 C 10.21 – Urteil vom 30. November 2022).

Foto: Wit, Adobe Stock

Datenschutz-Folgenabschätzung für Facebook-Fanpages

Genauso wie die lang anhaltenden Unsicherheiten bzgl. der Verwendung von Office 365 bzw. Microsoft 365, gibt es auch hinsichtlich der datenschutzkonformen Nutzbarkeit der sog. Facebook-Fanpages eine lange Vorgeschichte. Die letzten beiden Episoden in dieser Serie, deren Hauptakteure Facebook selbst, die Datenschutz-Aufsichtsbehörden (DSK) sowie die Verantwortlichen, insbesondere die sog. „öffentlichen Stellen" bzw. Bundesbehörden sind, drehen sich um die Ergebnisse des Kurzgutachtens zu der datenschutzrechtlichen Zulässigkeit der Fanpages, welches von einer Taskforce erstellt wurde, die der DSK ins Leben gerufen hatte.

Weiter auf DataAgenda lesen

eAU und Datenschutz: Orientierungshilfe der LfD Niedersachsen

Arbeitnehmer sind grundsätzlich ab dem vierten Tag ihrer Arbeitsunfähigkeit verpflichtet, dem Arbeitgeber eine Arbeitsunfähigkeitsbescheinigung vorzulegen (§ 5 EZFG). Der Arbeitgeber darf sogar am ersten Tag ein Attest fordern.
Gesetzlich krankenversicherte Arbeitnehmer informieren ihren Arbeitgeber daher unverzüglich über ihre Arbeitsunfähigkeit und suchen – sofern erforderlich – einen Arzt auf.
Ab dem 1. Januar 2023 ist der Abruf von AU-Daten bei den Krankenkassen für Arbeitgeber verpflichtend. Arbeitnehmer müssen ihrem Arbeitgeber von da an auch keine AU-Bescheinigung mehr vorlegen. Der Arbeitnehmer hat weiterhin die Pflicht, dem Arbeitgeber seine Arbeitsunfähigkeit zu melden und diese ärztlich feststellen zu lassen.

Weiter auf DataAgenda lesen

Foto: tippapatt, Adobe Stock

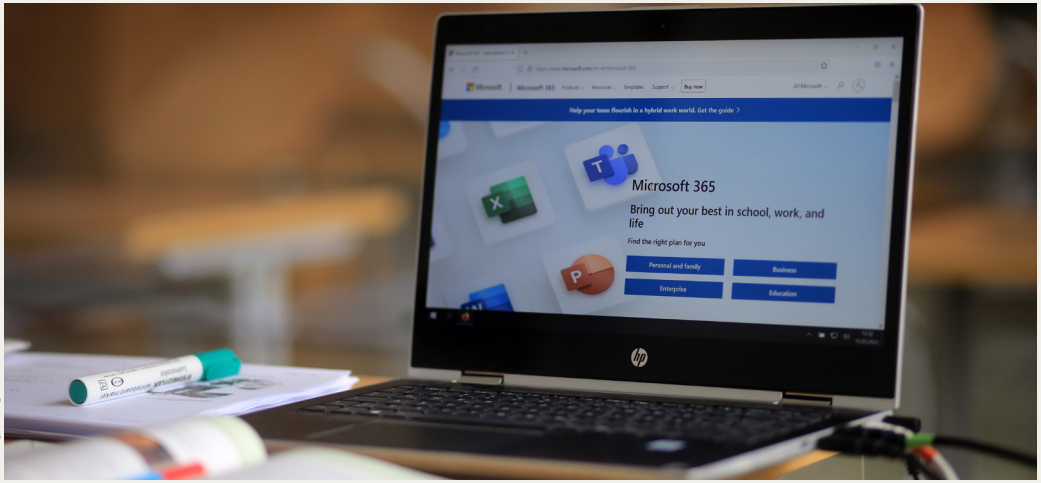

Foto: griangraf, Adobe Stock

Microsoft 365: Datenschutzkonform nutzbar oder nicht?

Die Frage wird, möglicherweise nicht so verwunderlich, momentan sehr unterschiedlich beantwortet. Dabei geht es leider nicht nur um Nuancen.
Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder sagt in ihrer neuesten Veröffentlichung relativ deutlich und klar:

„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“

Dem gegenüber stellt Microsoft als „Reaktion“ auf diesen Bericht die Datenschutzkonformität fest und unterstreicht die Positionen, die Microsoft bereits im August 2022 vertreten hatte.
„Wir stellen sicher, dass unsere M365-Produkte die strengen EU-Datenschutzgesetze nicht nur erfüllen, sondern oft sogar übertreffen. Unsere Kunden in Deutschland und in der gesamten EU können M365-Produkte weiterhin bedenkenlos und rechtssicher nutzen.“

Nach Auffassung von Microsoft berücksichtigen die von der DSK geäußerten Bedenken berücksichtigen die von Microsoft bereits vorgenommenen Änderungen nicht angemessener Weise und beruhen auf mehreren Missverständnissen hinsichtlich der Funktionsweise der Microsoft-Dienste und der von Microsoft bereits ergriffenen Maßnahmen.

Ebenfalls unterstütze Microsoft auch das EU-US Data Privacy Framework, das Microsoft-Kunden wichtige Rechtssicherheit und mehr Klarheit über den Datenschutz bei der transatlantischen Übermittlung von Daten bieten werde und sehen einem positiven Angemessenheitsbeschluss der Europäischen Kommission im Rahmen der DS-GVO im Jahr 2023 entgegen.

Verantwortlichen, die MS 365 bereits einsetzen oder den Einsatz planen, dürften mit diesen beiden widerstreitenden Positionen von Microsoft und der DSK nicht wirklich geholfen sein.

Teil 1: Einführung in den Datenschutz für die Privatwirtschaft

Einführung in das Datenschutzrecht
Schwerpunkt Arbeitnehmerdatenschutz - mit Fallübungen

27.02.-03.03.2023 | Köln
Referenten: RA Andreas Jaspers, Thomas Müthlein, Prof. Dr. Rolf Schwartmann

Praxisthemen:

- ✓ Einführung in das Datenschutzrecht
- ✓ Arbeitnehmerdatenschutz
- ✓ Kundendatenschutz und Fallübungen
- ✓ Umsetzung des Datenschutzes in der Praxis

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: IB Photography, Adobe Stock

Aufsichtsbehörden bezweifeln weiterhin datenschutzkonformen Einsatz von Microsoft 365

Viele Verantwortliche möchten gerne Office 365 (jetzt: Microsoft 365) nutzen – jedoch sind Unternehmen wie Behörden seit Jahren mit erheb-lichen rechtlichen Unsicherheiten konfrontiert, was die Bewertung der datenschutzrechtlichen Zulässigkeit angeht.
Zuletzt hatte der „Arbeitskreis Verwaltung" der DSK September 2020 festgestellt, dass „auf Basis dieser Unterlagen kein datenschutz-gerechter Einsatz von Microsoft Office 365 möglich sei". Mit „dieser Unterlagen" waren die dem Microsoft 365 zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) gemeint.

Weiter auf DataAgenda lesen

Interne Untersuchungen? – Bitte nur mit Datenschutz!

Viele Unternehmen bekennen sich zur weltweiten Bekämpfung von Korruption, unterstützen nationale und internationale Anstrengungen und lehnen jegliches korruptes Verhalten ab. Die Geschäftsleitung kann den Aufbau und den Betrieb eines Compliance-Management-Systems delegieren. In der Regel übernimmt diese Aufgabe ein Compliance-Officer oder je nach Ausgestaltung und Größe des Unternehmens, ein Chief Compliance Officer, welche dann als Hauptakteure eines Compliance-Management-Systems (CMS) für die Einhaltung von gesetzlichen Vorschriften eintreten, in dem sie zusammen mit allen anderen Beschäftigten des Unternehmens dafür Sorge tragen, dass sowohl unternehmensinterne Richtlinien/Anweisungen als auch gesetzliche Regelungen sichergestellt und überwacht werden.

Weiter auf DataAgenda lesen

Foto: Song_about_summer, Adobe Stock

46. DAFTA: Wissenschaftspreis für Datenschutz und Datensicherheit

Foto: bilderstoeckchen, Adobe Stock

Anlässlich der 46. Datenschutzfachtagung (DAFTA) wurden die Wissenschaftspreise der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) verliehen.

Jedes Jahr vergibt der wissenschaftliche Beirat der GDD unter Vorsitz von Prof. Dr. Tobias Keber den GDD-Wissenschaftspreis als Würdigung für herausragende wissenschaftliche Arbeiten. Der Preis ist auf 5.000 € dotiert und geht an Nachwuchswissenschaftler aller Disziplinen, die sich mit Fragestellungen des Datenschutzes und der Datensicherheit befassen. Die Auszeichnung soll dazu beitragen, Lücken zwischen gesellschaftlichen, rechtlichen und technischen Rahmenbedingungen des Datenschutzes und der Datensicherheit zu füllen.
Wegen ihrer hohen wissenschaftlichen Exzellenz wurden in diesem Jahr aus einer Vielzahl von Einsendungen drei Arbeiten ausgewählt und mit dem diesjährigen GDD-Wissenschaftspreis honoriert.

Die aktuellen Preisträger sind **Dr. Stefan Michel** für seine Dissertation „Bewertungsportale – Schnittstellen, Pfadabhängigkeiten und Konkurrenzprobleme des äußerungsrechtlichen und datenschutzrechtlichen Persönlichkeitsschutzes“ sowie **Dr. Marc Ohm** mit der Dissertation „Software Supply Chain Angriffe – Analyse und Erkennung“. **Olaf Hoffmann** erhält den Förderpreis für seine Masterarbeit „Lokale Webkonferenz-Artefakte, Bewertung der forensischen Aussagekraft und der Datensicherheit“.

Foto: xxxxx, Adobe Stock

LfDI BW erhält GDD-Datenschutzpreis 2022

Der **GDD-Datenschutzpreis** in Form einer bronzenen Plakette des Kölner Bildhauers Heribert Calleen wird seit 2013 durch den Vorstand des Vereins an Persönlichkeiten verliehen, die sich um die Entwicklung und Akzeptanz von Datenschutz und Datensicherheit in Deutschland und Europa verdient gemacht haben.

Anlässlich der 46. Datenschutzfachtagung (DAFTA) hat die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. Herrn Dr. Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, den GDD-Datenschutzpreis 2022 verliehen.

Seit Anfang 2017 ist Dr. Stefan Brink Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Dr. Brink wird nicht mehr für das Amt des LfDI BW kandidieren und zum Ende 2022 seine Tätigkeit als LfDI BW beenden.
Während seiner Amtszeit hat er die Behörde hinsichtlich der Anzahl der Mitarbeiter zur größten Datenschutzaufsichtsbehörde auf Landesebene aufgebaut und durch sein öffentlich wirksames Auftreten dem Datenschutz in Persona ein Gesicht gegeben.
Dr. Brink ist ausgewiesener Experte auf der ganzen Breite des Datenschutzes und kann komplexe Sachverhalte für die Praxis verständlich und nachvollziehbar erläutern. Dies macht ihn zu einem viel gefragten Referenten auf Fachtagungen und Kongressen zum Datenschutz, ebenso wie bei regionalen Veranstaltungen von kleineren und mittleren Unternehmen und Vereinen in Baden-Württemberg zur Anwendung der DS-GVO. Durch die Veröffentlichung praktisch verwertbarer Arbeitshilfen und Muster hat er als LfDI einen wertvollen Beitrag zur Unterstützung der Datenschutzcommunity geleistet.
Sein politisches Verständnis des Datenschutzes: „Datenschutz und Informationsfreiheit sind moderne Bürgerrechte. Sie garantieren unsere Selbstbestimmung im digitalen Zeitalter: Die Freiheit, unsere Daten zu nützen – aber auch die Freiheit, unsere Daten zu schützen!“ Sein politisches Statement für eine praktische Konkordanz von Persönlichkeitsrecht und unternehmerischer Freiheit entspricht damit im Grundsatz dem Leitbild der GDD von einem sinnvollen, vertretbaren und technisch realisierbaren Datenschutz. In verschiedenen Datenschutzfragen weicht seine Auffassung von derjenigen der GDD ab, jedoch stets substantiiert und qualifiziert.
Großes Lob für seine Tätigkeit erhielt Dr. Brink von allen im Landtag BW vertretenen Parteien anlässlich der Einweihung der neuen Räumlichkeiten des LfDI 2021. Die GDD schließt sich mit dem Datenschutzpreis diesem Lob an.
Die Laudatio auf Dr. Brink hielt der im Vorjahr mit dem GDD-Datenschutzpreis ausgezeichnete Werner Koch, deutscher Programmierer und Hauptentwickler von Gnu Privacy Guard (GnuPG).

DataAgenda Podcast Folge 25

Einwilligungsverwaltungsdienste nach § 26 TTDSG im Praxischeck – das sagen Techniker

Im Sommer 2022 wurde der Entwurf des Digitalministeriums zu einer Verordnung zur Umsetzung des § 26 TTDSG geleakt. Es geht um anerkannte Dienste zur Einwilligungsverwaltung. Sie sollen die Datensouveränität der Menschen erhöhen und in der Perspektive „Cookiebanner" entbehrlich machen. Im November 2022 arbeitet das Ministerium an einem angekündigten neuen Entwurf. Diese Phase kann genutzt werden, um den Hintergrund der Verordnung auszuleuchten. Das soll in der 25. Folge des DataAgenda-Podcasts mit Blick auf die technischen Hintergründe erfolgen. Gäste sind Dr. Jochen Eisinger, „Director of Engineering" bei Google, und Achim Schlosser, Technik-Vorstand der Europaen netID-Foundation.
Zum Podcast bitte hier klicken.

DataAgenda Podcast Folge 26

Microsoft 365 – Die Anforderungen der DSK auf dem rechtlichen Prüfstand

Die Datenschutzkonferenz (DSK) kann zwar formal nichts entscheiden, hat aber eine enorme faktische Macht, weil sie Leitlinien für das Handeln der einzelnen Behörden vorgibt. Diese Leitlinien sind jedoch nicht immer verständlich. Kürzlich etwa hat die DSK die Nutzung von Microsoft 365 faktisch „verboten", indem es die datenschutzkonforme Nutzung der Software, sprich Word und Teams in Abrede stellt. Damit sind Unternehmen und Behörden in Deutschland digital nicht mehr handlungsfähig. Sie sollen nun prüfen, wie Office-Lösungen aus der Cloud datenschutzkonform eingesetzt werden können. Wie das gehen soll, sagen die Behörden nicht. Was Behörden beschließen, ist rechtlich nicht in Stein gemeißelt. Im Gegenteil, kann und soll es Anlass für Diskussion und – falls erforderlich – konstruktive Kritik sein. Wie der DSK-Beschluss zu Microsoft 365 zu bewerten ist wird mit Kristin Benedikt, Thomas Kranig und Achim Pabst diskutiert. Zum Podcast bitte hier klicken.
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