NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 3/2023

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Einen der Tagesordnungspunkte der 1030. Sitzung am 10.02.2023 des Bundesrats hatten sowohl Compliance-Beauftragte als auch Datenschutzbeauftragte fest im Blick, nämlich das Gesetz für einen besseren Schutz hinweisgebender Personen.
Das Gesetz, das der Bundestag im Dezember 2022 verabschiedet hatte, regelt den Umgang mit Meldungen zu Betrügereien, Korruption und anderen Missständen in Behörden und Unternehmen.
Behörden und Unternehmen sollen gesonderte interne Anlaufstellen schaffen und auch anonyme Hinweise entgegennehmen. Zusätzlich will der Bund eine externe Meldestelle beim Bundesamt für Justiz errichten. Die Länder können eigene externe Meldestellen einrichten. Der Bundestagsbeschluss regelt Verfahren und Vertraulichkeit der Meldungen und Maßnahmen zum Schutz der Hinweisgeber vor Repressalien – aber auch Haftung, Schadensersatz und Bußgelder im Fall bewusst falscher Angaben. Hintergrund sind Vorgaben einer EU-Richtlinie, die in deutsches Recht umzusetzen sind. Das Gesetz sollte drei Monate nach Verkündung im Bundesgesetzblatt in Kraft treten.
Am 10.02.2023 passierte aber etwas, womit wohl die meisten Beobachter nicht gerechnet hatten: Der Bundestagsbeschluss zum Schutz von sogenannten Whistleblowern erhielt am 10. Februar 2023 nicht die erforderliche Zustimmung im Bundesrat. Es kann daher erst einmal nicht in Kraft treten.
Ratlos blieben diejenigen zurück, die schon gedanklich den Starttermin für das neue oder angepasste Hinweisgebersystem notiert hatten und stellten sich vor allem die Frage, was denn nun zu der fehlenden Zustimmung geführt hat.
Der allgemeine Tenor: „Einigen Ländern gingen die Regelungen zu weit." Es wurde weiter befürchtet, dass nicht alle Hinweisgebenden „Gutes im Schilde" führen würden. Genauso wage und nicht viel plausibler wurde argumentiert, dass die oftmals erforderlichen IT-Systeme für die Umsetzung des Hinweisgeberschutzgesetzes (HinSchG) zu einem Mehraufwand für die deutschen Unternehmen führen würden, der wohl nicht zu stemmen sei.
Datenschutzbeauftragte dürften diese Entwicklung ggf. genauso unverständlich finden wie ihre Kollegen aus dem Bereich Compliance. Die datenschutzrechtliche Schnittmenge mit dem Thema Hinweisgeberschutz jedoch dürfte in den relevanten Organisationen erst bei der Durchführung einer Datenschutz-Folgenabschätzung zum Tragen kommen. Vor dem Go-live der Hinweisgebersysteme wird der Datenschutzbeauftragte bei der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO eingebunden werden müssen. Die unerwartete Verzögerung im Bundesrat führt also bei einer positiven Sichtweise dazu, dass sich hier noch einmal ein Zeitfenster aufgetan hat, um das Thema intensiver zu durchdenken, findet Ihr

Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: TeamDaf, Adobe Stock

bitkom und GDD: Praxisleitfaden/ Muster zur Auftragsverarbeitung aktualisiert

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat ihre „Praxishilfe DS-GVO – Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO“ aktualisiert (Stand: Januar 2023).

Diese Praxishilfe der GDD möchte Hilfestellungen für Auftragsverarbeiter geben, wie die gesetzlichen Vorgaben insbesondere an der Schnittstelle zu seinen Auftraggebern umgesetzt werden können. Weitergehende grundsätzliche Hinweise zur Auftragsverarbeitung sowie einen Mustervertrag finden Sie in der „GDD-Praxishilfe DS-GVO – Mustervertrag zur Auftragsverarbeitung“.

Auch der bitkom hat seinen bewährten Praxisleitfaden zur Auftragsverarbeitung aktualisiert. Dieser besteht aus verschiedenen Dokumenten: Mustervertragsanlage sowie

- Anlage 1 zur Mustervertragsanlage
- Anlage 2 zur Mustervertragsanlage: Auftraggeber
- Anlage 3 zur Mustervertragsanlage: Auftragsverarbeiter

BSI aktualisiert IT-Grundschutz-Kompendium (2023)

Foto: hkama, Adobe Stock

Mit dem IT-Grundschutz-Kompendium richtet sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) gezielt an alle Unternehmen und Behörden, die sich grundlegend mit IT-Sicherheit befassen möchten oder müssen. Zusammen mit den BSI-Standards bildet es die Basis für eine umfassende Betrachtung der Informationssicherheit.

Das Kompendium ist noch einmal gewachsen. Das in aktueller Auflage (2023) komplett überarbeitete Kompendium beinhaltet 111 Bausteine, die sich nicht nur mit technischen, sondern auch mit infrastrukturellen, organisatorischen sowie personellen Aspekten der IT-Sicherheit befassen. Vorhandene Bausteine, wie zum Outsourcing, wurden grundlegend überarbeitet. Hinzu kommen zahlreiche weitere Ergänzungen und Aktualisierungen, die auf der Grundlage des Anwenderbedarfs erarbeitet wurden.
Für Anwender der öffentlichen Verwaltung ist insbesondere der neue Baustein CON.11.1 Geheimschutz Verschlusssachen – nur für den Dienstgebrauch (VS-NfD) von Interesse.
Das Kompendium beschäftigt sich im zweiten Abschnitt von „Konzepte und Vorgehensweisen“ (CON) explizit mit dem Thema Datenschutz. Erklärtes Ziel des Bausteins ist es, die Verbindung der Anforderungen des Datenschutzes, die durch das Standard-Datenschutzmodell operationalisiert werden, zum IT-Grundschutz darzustellen.

Interessierte können ein changelog abrufen:
Änderungsdokumente (Edition 2023)

Foto: askaja, Adobe Stock

BRAK äußert sich zur Nutzbarkeit von Microsoft 365 durch Rechtsanwälte

Wie zuvor schon berichtet, besteht momentan (bzw. immer noch) Unsicherheit darüber, ob Microsoft 365 (nicht lokal installierte Version) in datenschutzrechtlicher Hinsicht (unproblematisch) zulässigerweise nutzbar ist.
Diese Frage stellt sich für sog. Berufsgeheimnisträger wie bspw. Rechtsanwälte (vgl. § 203 StGB) umso mehr. Um diesen Unsicherheiten zu begegnen, hat sich die Bundesrechtsanwaltskammer (BRAK) in einem öffentlichen Schreiben an die Anwaltschaft gerichtet.

Naturgemäß kann auch die BRAK der umstrittenen Anwendung nicht die Art von Absolution, insbesondere im Hinblick auf die einzuhaltende Vertraulichkeit beim Einsatz von Microsoft Office erteilen, die den Rechtsanwälten tatsächlich eine Hilfe sein könnte. Die BRAK betont jedoch, dass vor dem Hintergrund des Berufsrechts die Vertraulichkeit von Mandatsinformationen selbstverständlich zu gewährleisten ist (§ 43a Abs. 2 und 43e BRAO, § 2 BORA, 203 Abs. 1 Nr. 3 StGB) und weist auf die bestehenden zusätzlichen Anforderungen hin, die hinsichtlich etwaiger Übermittlungen von Mandatsinformationen ins Ausland (§ 43e Abs. 4 BRAO) existieren.

Es könne von der BRAK insbesondere nicht beurteilt werden, ob bei Nutzung der von Microsoft mittlerweile angebotenen Möglichkeit der Datenhaltung in Deutschland noch Mandatsinformationen in die USA übertragen werden. Microsoft selbst erachte die Möglichkeit einer Nutzung durch Berufsgeheimnisträger für gegeben und bietet den Abschluss einer entsprechenden Verschwiegenheitsvereinbarung an, so die BRAK.

Ob der Hinweis bzw. die Mutmaßung der BRAK, dass ihrer Einschätzung nach zunächst gegen öffentlich-rechtliche und institutionelle Verantwortliche vorgegangen werden dürfte und ihr gegenwärtig keine konkreten aufsichtsbehördlichen Beanstandungen des Einsatzes von Microsoft 365 in Rechtsanwaltskanzleien bekannt sind, für die betroffenen Rechtsanwälte eine hilfreiche Information darstellt, wird jeder wohl am Ende für sich selbst entscheiden müssen.

GDD-BASIS-SCHULUNG TEIL 1

Einführung in den Datenschutz für die Privatwirtschaft

08.–12.05.2023 I Berlin
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: HNFOTO, Adobe Stock

BEM: Die Wirksamkeit hängt (auch) von der Einhaltung des Datenschutzes ab

Die Öffnungsklauseln der DS-GVO lassen nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext öffentlicher Stellen zu (siehe Art. 6 Abs. 2 und Abs. 3 lit. b) DS-GVO sowie Art. 88 DS-GVO). Der Bundesgesetzgeber hat unter anderem mit den spezialgesetzlichen Regelungen in den Sozialgesetzbüchern hiervon Gebrauch gemacht.

Weiter auf DataAgenda lesen

Foto: hkama, Adobe Stock

Datenschutz-Schulung: Der Arbeitgeber hat die Kosten für Büropersonal der SBV zu tragen

Mit Beschluss vom 03.11.2022 (Az. 26 TaBV 751/22) äußerte sich das Landesarbeitsgericht (LArbG) Berlin-Brandenburg zu der Frage, ob und wann ein Arbeitgeber die Kosten zu tragen hat, die der Bürokraft einer Schwerbehindertenvertretung (SBV) für die Teilnahme an einem Seminar zum Thema Datenschutz entstanden sind.

Weiter auf DataAgenda lesen

Foto: DatenschutzStockfoto, Adobe Stock

Taskforce Cookie-Banner legt Abschlussbericht vor

NOYB (None of Your Business), eine Nichtregierungsorganisation mit Sitz in Wien, die sich für die Durchsetzung des Datenschutzes innerhalb der Europäischen einsetzt, hatte im August 2022 bei 18 Behörden 226 Datenschutzbeschwerden gegen Websites eingereicht, die die beliebte Cookie-Banner-Software („OneTrust“) verwenden. Nach Auffassung von NOYB wurden bei der Nutzung der Cookie-Banner irreführende Einstellungen verwendet. Nach einer ersten Reihe von Beschwerden im Mai 2021 haben viele Websites, die OneTrust verwenden, ihre Einstellungen angepasst und „Ablehnen“-Buttons hinzugefügt. OneTrust änderte auch die Standardeinstellungen, um eine größere Konformität mit der DS-GVO zu erreichen.

Der Europäische Datenschutzausschuss (EDPB) hatte anlässlich der Vielzahl der eingereichten Beschwerden eine spezielle Taskforce eingerichtet, um die Reaktionen der Datenschutzbehörden zu koordinieren.
Wie der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) informiert, ist nach Bewertung der jeweiligen Beschwerdegenstände die Arbeit der Task Force mit dem am 18. Januar 2023 veröffentlichten Abschlussbericht nunmehr beendet.
Als ein wichtiges Ergebnis hebt der HmbBfDI hervor, dass unter den europäischen Aufsichtsbehörden mit großer Mehrheit die Auffassung vertreten wird, dass

- Nutzende auf derselben Ebene des Cookie-Banners, auf der sie ihre Einwilligung erteilen können, gleichzeitig die Möglichkeit haben müssen, keine Einwilligung zu erteilen;
- die Nichterteilung der Einwilligung nicht aufwendiger sein darf als ihre Erteilung.

Darüber hinaus wurden Maßstäbe zur Beurteilung irreführender Banner-Gestaltung wie etwa im Fließtext des Banners als Link versteckte und daher kaum erkennbare „Ablehnfunktionen“ erarbeitet. Außerdem wird es als unzulässig erachtet, vorausgewählte Kästchen auf der zweiten Ebene des Cookie-Banners anzubieten.

Foto: Rawf8, Adobe Stock

Praxishilfe: ePrivacy und Datenschutz beim Onlineauftritt

Der ***Europäische Datenschutztag*** ist ein auf Initiative des Europarats ins Leben gerufener Aktionstag für den Datenschutz. Er wird seit 2007 jährlich um den 28. Januar gerum begangen. Dieses Datum wurde gewählt, weil die Europäische Datenschutzkonvention am 28. Januar 1981 unterzeichnet worden war.

Anlässlich des 17. Europäischen Datenschutztags am 28.01.2023 hat die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. eine neue Praxishilfe zum aktuellen Thema „ePrivacy und Datenschutz beim Onlineauftritt“ veröffentlicht.

Betreiber von Websites, Apps und Co. haben die Vorgaben des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), insbes. § 25 TTDSG, sowie die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) zu beachten. § 25 TTDSG setzt europäische Vorgaben, konkret: Art. 5 Abs. 3 ePrivacy-RL (RL 2002/58/EG), nahezu wortgleich in nationales Recht um. Die Interpretation der europäischen Norm kann insofern auch für die Auslegung und Anwendung der TTDSG-Bestimmung herangezogen werden. Ursprünglich war vorgesehen, dass zeitgleich mit der DS-GVO am 25.05.2018 auch eine diese ergänzende und die ePrivacy-RL ersetzende ePrivacy-VO als in allen EU-Mitgliedstaaten unmittelbar geltendes Recht in Kraft treten sollte. Dies ist nicht geschehen. Ob beziehungsweise wann es noch zum Inkrafttreten der ePrivacy-VO kommen wird, ist unklar. Bis zur Geltung der ePrivacy-VO gilt das bestehende europäische ePrivacy Recht fort, also die ePrivacy-RL in Fassung der sog. „Cookie-Richtlinie“ (Richtlinie 2009/136/EG).

Es wird erläutert, auf welche Verhaltensweisen des Websitebetreibers § 25 TTDSG beziehungsweise die DS-GVO konkret Anwendung finden, also ihr sachlicher Anwendungsbereich. Zudem wird der Rechtsrahmen dargestellt, der sich aus § 25 TTDSG respektive der DS-GVO ergibt, also was konkret mit den personenbezogenen Daten der Websitenutzer/-innen gemacht werden bzw. unter welchen Voraussetzungen beim Einsatz von Cookies und Co. auf deren Endgeräte zugegriffen werden darf.

>> Die neue Praxishilfe können Sie hier kostenfrei downloaden (Direktdownload)
oder unter PRAX – Neustrukturierung — GDD e.V. (Rubrik „1. Rechtliche Grundlagen“)

10. Hamburger Datenschutztage

Datenschutz – weil so viel auf dem Spiel steht

Konferenz: 15.–16.06.2023
Pre-Seminar: 14.06.2023

Jetzt anmelden: **www.datenschutz.com/DS-Tage**

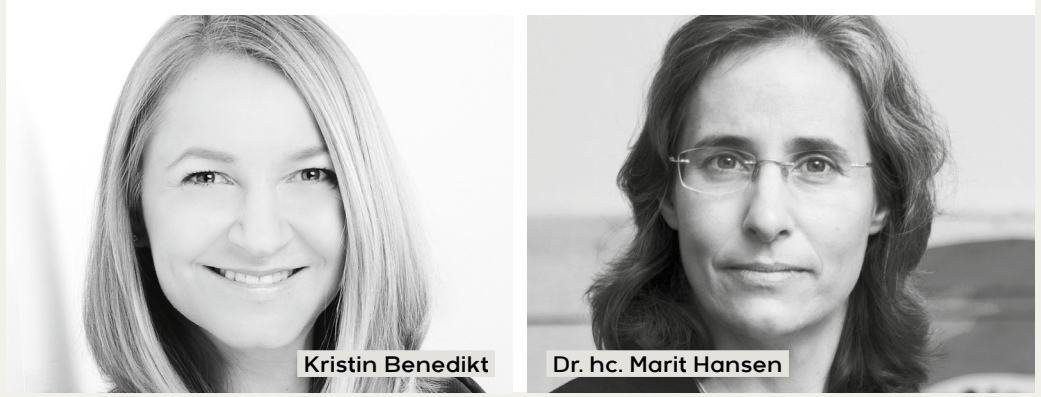
IBS data protection

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Folge #32

ChatGPT – Herausforderungen für den Datenschutz



DataAgenda Podcast Folge 32: ChatGPT – Herausforderungen für den Datenschutz

Seit November 2022 ist die Software ChatGPT für jedermann frei verfügbar. Der Textroboter hat das Potential, die Menschheit an neue Grenzen zu bringen. Die Welt ist offen für die neue Technik, auch wenn deren Risiken offenkundig sind. Da man die Anwendung nicht verbieten kann, soll man lernen sie zu nutzen und zu verstehen. Das gilt auch für das Datenschutzrecht.

Eine frühe Einordnung von Dr. hc. Marit Hansen, Landesdatenschutzbeauftragten Schleswig-Holstein und Vorsitzenden der DSK, Kristin Benedikt vom VG Regensburg und Professor Dr. Rolf Schwartmann.

Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Foto: metamorworks, Adobe Stock

„Social Media Leitfaden für Beschäftigte im Öffentlichen Dienst“

Mehr als 150 Länder – darunter auch Deutschland – nahmen am 7. Februar 2023 am Safer Internet Day teil. Die jährlich stattfindende Kampagne verfolgt das Ziel, das Bewusstsein für (neue) Onlineprobleme und aktuelle Sorgen zu schärfen.
Das TUM Center for Digital Public Services (CDPS) hat sich als allgemeines Ziel gesetzt, die Digitalisierung rechtssicher und praxistauglich zu gestalten. Vor dem Hintergrund, dass die Digitalisierung der alltäglichen zwischenmenschlichen Kommunikation größtenteils über Social Media erfolgt, hat das CDPS im Rahmen seiner Aktion die Bediensteten im öffentlichen Dienst adressiert und stellt eine Publikation mit dem Titel „Social Media Leitfaden für Beschäftigte im Öffentlichen Dienst“ zum Download bereit.

Angestellte im öffentlichen Dienst kommen nicht nur im beruflichen Kontext mit Social Media in Berührung, sondern verfügen zumeist über ein eigenes Konto oder Profil auf einer Social-Media-Plattform, so die Autoren. Der Leitfaden geht auf die besondere Situation der Beschäftigten des öffentlichen Dienstes ein, denn diese sehen sich bei der Nutzung von sozialen Medien mit einer „Doppelrolle“ konfrontiert:
Einerseits sind sie als Privatperson auf Social Media unterwegs, anderseits müssen sie gleichzeitig aufgrund ihrer Berufswahl Besonderheiten beachten, da sie als Angestellter oder Angestellte im öffentlichen Dienst gleichzeitig staatliche Aufgaben erfüllen und den Staat repräsentieren. Die Ansprüche an das gesamte Verhalten – d.h. sowohl im dienstlichen als auch außerdienstlichen Bereich – der Beamtinnen sind daher in der Regel höher als bei Angestellten der Privatwirtschaft.
Der „Social Media Leitfaden für Beschäftigte im Öffentlichen Dienst“ geht auf Fragen ein, wie man sich auf Social-Media-Plattformen rechtskonform verhält bzw. was im Umgang mit Social Media erlaubt oder nicht erlaubt ist. Die Ausführungen sollen Unklarheiten beseitigen und einen ersten Einblick darin geben, was bei der privaten Nutzung von sozialen Medien aus rechtlicher Sicht zu beachten ist.

Konkrete Fragen sind beispielsweise:

- Welche (Re-)Posts sind erlaubt?
- Mit wem darf man sich vernetzen?
- Darf man während der Arbeitszeit Social Media nutzen?
- Darf ich andere Nutzerinnen und Nutzer blockieren?
- Darf ich über meine Arbeit bei der Behörde schreiben?
- Wo ist die Grenze zwischen der Kundgabe erlaubter Privatmeinung und unzulässiger Meinungsäußerung?

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