Datenschutz newsbox

Ausgabe 9 2019

DATAKONTEXT

Editorial:

Bekannt gewordene Datenschutzverstöße und der Umgang der Aufsichtsbehörden mit diesen, insbesondere verhängte Bußgelder und die Höhe der Bußgelder, sind Themen, die die Diskussion um die DS-GVO seit Anbeginn prägen.

Auf der Seite www.enforcementtracker.com kann der interessierte Leser einen Überblick über die (bekannten) Bußgelder und Sanktionen erhalten, die die europäischen Datenschutzbehörden bislang verhängt haben.

Deutsche Aufsichtsbehörden stehen mit dem Instrument der Sanktionierung von Datenschutz-Vergehen nach eigenen Worten „noch ganz am Anfang“, zumindest was die Ausschöpfung der Höhe möglicher Bußgelder angeht.
Der Markt (Datenschutz-Berater und Unternehmen) bereitet sich darauf vor, dass sich die Höhe der Bußgelder bald auf einem europäisch höheren Niveau einpendeln könnte.
Die Einschläge dazu scheinen auch auf deutschem Boden näher zu kommen.

Die aktuelle Diskussion um dieses Thema wird insbesondere durch ein „neues Bußgeldmodell“ genährt, welches die Aufsichtsbehörden aktuell testen sollen.
Auch die DSK selbst informiert in einem aktuellen Papier, dass sie gegenwärtig ein Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DS-GVO erarbeitet, mit dem Ziel, eine systematische, transparente und nachvollziehbare Bußgeldzumessung zu gewährleisten.

Weitere Details nennen die Aufsichtsbehörden derzeit nicht. Auch die Anfrage eines auf Datenschutz spezialisierten Anwalts auf Informationszugang bzgl. des neuen Bußgeldkonzepts wurde vom LfDI Rheinland-Pfalz abgelehnt.

Die DSK will das Bußgeldkonzept auf ihrer nächsten Konferenz im November weiter beraten. Dort wollen die Behörden dann auch über eine Veröffentlichung des Bußgeldkonzepts entscheiden.

Bis es demnächst also ggf. transparenter und einheitlicher wird, können sich Verantwortliche zumindest auf einen Grundsatz verlassen: Nach Art. 83 Abs .1 DS-GVO müssen die von den Behörden verhängten Bußgelder „wirksam, abschreckend und verhältnismäßig“ sein.

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

ePrivacy-Verordnung: Woran es aus deutscher Sicht stockt

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) anwendungspflichtig. Ursprünglich sollte auch ab diesem Tag die ePrivacy-Verordnung (ePrivacy-VO) gelten. Das Gesetzgebungsverfahren zur ePrivacy-VO verzögert sich jedoch nach wie vor.
Mit der zeitlichen Verschiebung des Inkrafttretens der ePrivacy-VO ergeben sich insbesondere Fragen zum Verhältnis zwischen DS-GVO und nationalen Vorschriften. Das bereichsspezifische Datenschutzrecht für elektronische Kommunikation ist bislang durch die ePrivacy-Richtlinie geregelt, die in Deutschland im TKG, TMG und UWG umgesetzt wurde. Sicher ist nur: Trotz Änderung des übergeordneten Datenschutzrechts durch die DS-GVO bleiben vom Gesetzgeber TKG und TMG unberührt.
Nach ursprünglicher Planung der EU sollte die ePrivacy-RL mit der Anwendungspflicht der DS-GVO durch eine ePrivacy-VO ersetzt werden. Die Richtlinie hat sich als Instrument zur europaweiten Angleichung des Datenschutzrechts als ungeeignet erwiesen. Zudem hat der technologische Fortschritt die rechtlichen Rahmenbedingungen überholt. Das jüngste Datenschutzrecht der EU, die DS-GVO, vermag die spezifische Regelungslücke für den Bereich der elektronischen Kommunikation nicht zu schließen.
Gegenwärtig gibt es zur ePrivacy-VO nur Entwürfe der Kommission und des Europäischen Parlaments. Es ist fraglich, inwieweit das Diskontinuitätsprinzip nun dazu führt, dass sich das Europäische Parlament erneut mit der ePrivacy-VO befassen wird oder befassen muss.
In der vergangenen Legislatur des Europäischen Parlaments (2014-2019) hätte eine finale Positionierung des Rats den sog. Trilog ermöglichen und das Gesetzgebungsverfahren abschließen können. In dem aus den Regierungen der 28 EU-Mitgliedstaaten bestehenden Rat drückt vor allem Deutschland auf die Bremse. Interessant waren deshalb die Aussagen des Bundeskanzleramtsministers Helge Braun auf einer Konferenz zum 15. Geburtstag von netzpolitik.org.

Mehr auf DataAgenda

Jährliche Überprüfung des EU-US Privacy Shields

Seit dem 1. August 2016 dient der EU-US-Datenschutzschild dem Schutz personenbezogener Daten, die aus der EU zu kommerziellen Zwecken in die USA übermittelt werden. Der Datenschutzschild schafft rechtliche Klarheit für Unternehmen, die auf die Übermittlung personenbezogener Daten über den Atlantik hinweg angewiesen sind. Inzwischen sind mehr als 5000 Unternehmen auf der Grundlage des Datenschutzschilds zertifiziert und haben sich damit verpflichtet, die Datenschutzanforderungen zu erfüllen.
Wie zu Beginn seiner Einführung vereinbart, wird der EU-US-Datenschutzschild jährlich überprüft, um festzustellen, ob er weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet. Am 12. September 2019 leitete die für Justiz, Verbraucher und Gleichstellung zuständige EU-Kommissarin Vâra Jourová zusammen mit dem amerikanischen Handelsminister Wilbur Ross die dritte jährliche Überprüfung des EU-US-Datenschutzschilds ein. Die Berichte über die erste und zweite Überprüfung finden Sie hier. Der Bericht über die dritte Überprüfung wird zu einem späteren Zeitpunkt folgen.

Quelle: Europäische Kommission

LfDI BW informiert zum Thema Fotografieren und Datenschutz

Der nach wie vor herrschenden Unsicherheit im Hinblick auf die Frage, welche datenschutzrechtlichen Anforderungen beim Thema Fotografieren zu beachten sind, möchte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg mit der Broschüre „Fotografieren und Datenschutz – Kompakt und praxisorientiert“ entgegenwirken.
Insbesondere die Frage, ob nach Wirksamwerden der DS-GVO die Vorschriften des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) keine Gültigkeit mehr hat und auf welcher Rechtsgrundlage Fotos angefertigt und verbreitet werden dürfen, wird in der Broschüre einer näheren Betrachtung unterzogen.
Aus gegebenem Anlass hat der LfDI BW auch eine abschließende Wertung zum Thema „Fotografieverbot an Schulen“. Dazu seine Einschätzung:
„Ein generelles Fotografierverbot ist sicher keine vernünftige Lösung. Die Schule kann z. B. in einem Elternbrief oder im Rahmen der Veranstaltung darauf hinweisen, dass Fotos von einem Schulfest nicht ohne die Erlaubnis der fotografierten Personen ins Netz gestellt werden dürfen. Alternativ könnte die Schule auch darum bitten, während der Veranstaltung nicht zu fotografieren, und gleichzeitig anbieten, am Ende der Veranstaltung an einem bestimmten Ort der Schule Fotos anfertigen zu können. Auf diese Weise können Personen, die nicht fotografiert werden wollen, dies vermeiden, indem sie diesem Ort fernbleiben. Will die Schule selbst Fotos der Veranstaltung veröffentlichen, hat sie freilich in der Regel die Einwilligung der Betroffenen einzuholen, die sich auf das jeweils zur Veröffentlichung verwendete Medium beziehen muss.“

Quelle: Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Telematik: DSK positioniert sich zu Personenkennzeichen und Verantwortlichkeit

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat sich gestern mit der Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen zur direkten Identifizierung von Bürgerinnen und Bürgern befasst. Was die Bundesregierung derzeit verfolgt, lehnt die DSK hingegen ab.
In ihrer diesbezüglichen Entschließung weist die DSK darauf hin, dass die Schaffung einer Infrastruktur mit verwaltungsübergreifenden eindeutigen Personenkennzeichen erhebliche datenschutzrechtlichen Risiken und verfassungsrechtliche Bedenken auslösen würde. Sie erinnert dabei daran, dass das Bundesverfassungsgericht (BVerfG) schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt.
Es mag zwar hilfreich erscheinen, wenn Bürgerinnen und Bürger Dienstleistungen der Verwaltung durch die Nutzung einmal hinterlegter Daten leichter in Anspruch nehmen können. Dieser Vorteil und die erwarteten Effizienzsteigerungen für die öffentliche Verwaltung muss aber zwingend mit einem hohen Maß an Datenschutz einhergehen.

Ein weiteres Thema der Konferenz war die Verteilung der datenschutzrechtlichen Verantwortung in der Telematik Infrastruktur des Gesundheitswesens (TI). Bei den zum Anschluss von Arztpraxen an die TI verwendeten Konnektoren, sieht die DSK eine datenschutzrechtliche Mitverantwortung von Arztpraxen und der Gesellschaft für Telematikanwendungen (gematik). Hier bestand seit längerer Zeit Unklarheit, ob die sogenannten Konnektoren, die als Schnitt- und Verbindungsstelle zwischen den Praxissystemen in z.B. Arztpraxen und der TI fungieren, unter die Verantwortung der Praxisbetreiber oder der gematik fallen.
Es ist die gesetzliche Aufgabe der gematik, den operativen und sicheren Betrieb der TI zu gewährleisten und in diesem Rahmen die Mittel für die Datenverarbeitung in der TI maßgeblich zu bestimmen. Aus dieser gesetzlichen Zuschreibung kam die DSK zu der Auffassung, dass der gematik neben den Betreibern der Arztpraxen eine datenschutzrechtliche Mitverantwortung für die Konnektoren zufällt. Um diese Verantwortungsteilung künftig rechtssicher zu regeln, empfiehlt die DSK dem Gesetzgeber, hier eine normenklare gesetzliche Regelung zu schaffen.

EDSA veröffentlicht Entwurf für Richtlinien bzgl. Videoaufnahmen

Der Europäische Datenschutzausschuss (EDSA) hat kürzlich seine Leitlinien im Hinblick auf die Verarbeitung personenbezogener Daten durch Videoaufnahmen zur Konsultation veröffentlicht. Obwohl die Leitlinien Beispiele für die Datenverarbeitung durch Videoaufnahmen enthalten, erhebt der EDSA keinen Anspruch auf Vollständigkeit der Beispiele. Die Leitlinien sollen vielmehr Orientierung für die Anwendung der DS-GVO in allen Bereichen bieten, in denen Videoaufnahmen relevant werden kann.

Zu den wichtigsten Elementen der Leitlinie gehören:

- Anwendungsbereich
- Rechtmäßigkeit der Verarbeitung
- Zweckbindung
- Verarbeitung spezieller Datenkategorien (z.B. biometrische Daten)
- Transparenz der Verarbeitung
- Aufbewahrungsfristen
- Technisch und organisatorische Maßnahmen / Datensicherheit

Die Leitlinien werden bis zum 9. September 2019 öffentlich zugänglich sein. Es wird erwartet, dass die EDSA bis Ende des Jahres eine überarbeitete und endgültige Version verabschiedet.

Quelle: Europäischer Datenschutzausschuss

Gesamtschuldnerische Haftung bei einer Auftragsverarbeitung

Frage des GDD-Erfa-Kreises Würzburg:
Nach der DS-GVO besteht nun in bestimmten Fällen eine gesamtschuldnerische Haftung von Auftraggeber und Auftragnehmer (Art. 82 DS-GVO). Kann hieraus abgeleitet werden, dass nun auch der Auftragnehmer für den Abschluss des ADV haftet, d.h. er hier in die Haftung genommen werden kann, wenn er sich weigert, einen ADV zu unterzeichnen? Wenn der Abschluss eines derartigen Vertrages höchstens im Interesse des Auftragsverarbeiters wäre, aber aufgrund fehlender Mitwirkung nicht geschlossen wird bzw. nicht die gesetzlichen Mindestinhalte erhält, würde auch nach der DS-GVO ein Bußgeld allein den Auftraggeber treffen.

Antwort BayLDA:
Die Haftungsregelung nach Art. 82 DS-GVO wegen einer Person entstandener materieller oder immaterieller Schäden muss getrennt von den Verantwortlichkeiten bei der Verhängung von Geldbußen nach Art. 83 Abs. 4 und 5 DS-GVO gesehen werden.
Eine Geldbuße nach Art. 83 DS-GVO kann gegen denjenigen Verantwortlichen oder Auftragsverarbeiter verhängt werden, der bestimmte datenschutzrechtliche Pflichten, insbesondere aus der DS-GVO, verletzt.
Die Pflicht, nur Auftragsverarbeiter aufgrund einer ausreichenden Vertragsregelung nach Art. 28 Abs. 3 DS-GVO einzusetzen, trifft den Verantwortlichen als Auftraggeber, Art. 28 Abs. 1, Art. 24 Abs. 1 und Art. 5 Abs. 2 DS-GVO.
Verweigert sich ein potentieller Auftragsverarbeiter einer Vertragsregelung gemäß Art. 28 Abs. 3 DS-GVO, darf der Verantwortliche ihm keine personenbezogenen Daten übergeben bzw. die Möglichkeit einer Kenntnisnahme von Daten zulassen. Denn ein solcher Auftragsverarbeiter bietet keine hinreichenden Garantien im Sinne von Art. 28 Abs. 1 DS-GVO.

Meldung einer Datenpanne

Frage des GDD-Erfa-Kreises Würzburg:
Nach dem Wesen der Auftragsverarbeitung bilden Auftragsverarbeiter und Auftraggeber eine Handlungs-/Haftungseinheit. Wird die Aufsicht vor diesem Hintergrund eine Anrechnung schon beim Auftragsverarbeiter bis zur Eigenmeldung an den Verantwortlichen abgelaufener Meldefristanteile beim Auftraggeber vornehmen/anstreben? Würde also die (verbleibende) Meldefrist für den Auftraggeber auf 60 Stunden verkürzt, wenn der Auftragsverarbeiter selbst zwölf Stunden ins Land gehen lässt, bis er den Auftraggeber über eine Datenpanne bei ihm informiert?
Nach Art. 33 Abs. 1 DS-GVO ist der Verantwortliche zur Meldung einer Datenpanne an die Aufsicht binnen 72 Stunden nach Kenntnis verpflichtet. Der Auftragsverarbeiter selbst ist nach Art. 33 Abs. 2 DS-GVO zur unverzüglichen Meldung an den Verantwortlichen verpflichtet, wenn er Anhaltspunkte für eine Datenpanne hat.
Wenn dies entsprechend dem Gesetzeswortlaut nicht der Fall ist: Ist „unverzüglich" hinsichtlich des Auftragsverarbeiters so zu verstehen, dass er selbst auch 72 Stunden zur Meldung von Datenschutzverletzungen an den Auftraggeber hat oder gilt hier ein abweichender Maßstab bzw. welche Zeitspanne würde hier aufsichtlich toleriert?

Antwort des BayLDA:
Die 72 Stunden beginnen ab Kenntniserlangung durch den Verantwortlichen, d.h. ab dem Zeitpunkt, an dem der Auftragsverarbeiter den Verantwortlichen informiert hat.
Die Zeitspanne, in der der Auftragsverarbeiter den Verantwortlichen informiert, muss so kurz wie möglich – auch weniger als 72 Stunden sein.
Wie weit „unverzüglich" ausgelegt wird, wird sich im Rahmen der Harmonisierung des europäischen Vollzugs zeigen.

Handreichung zum Beschäftigtendatenschutz

Zu Recht weist Frederick Richter, Vorstand der Stiftung Datenschutz, im Vorwort der aktuellen Veröffentlichung der Stiftung Datenschutz darauf hin, dass es verwunderlich ist, dass es noch kein spezielles Recht für den Beschäftigtendatenschutz gibt, obwohl dies schon seit vielen Jahren von DatenschutzexpterInnen, Personalprofis, Betriebsräten und anderen gefordert wird. Da sich dies auch mit der DS-GVO nicht wesentlich geändert hat, beschäftigt sich die neue Publikation der Stiftung Datenschutz mit dem eher stiefmütterlich behandelten Thema des Datenschutzes.
Die „Handreichung Beschäftigtendatenschutz" trägt die wichtigsten Grundsätze und Regeln zusammen, die für den Datenschutz in Beschäftigungsverhältnissen gelten. Abgerundet wird die Handreichung mit Fallbeispielen zum Thema.
Die Handreichung adressiert nach eigenen Angaben vor allem Personalverantwortliche in kleinen und mittelständischen Unternehmen, aber auch Betriebsräte und ganz allgemein an Beschäftigte.
Es sei an dieser Stelle erwähnt, dass der LfDI Baden-Württemberg seinen „Ratgeber Beschäftigtendatenschutz" im August 2019 aktualisiert hat und nun in der 3. Auflage anbietet.

Quelle: Stiftung Datenschutz

HmbBfDI erläutert rechtliche Vorgaben für Sprachassistenzsysteme

Der Hamburgische Beauftragte für Datenschutz und die Informationsfreiheit (HmbBfDI) hatte jüngst darauf hingewiesen, dass die Nutzung von automatischen Sprachassistenten von Anbietern wie Google, Apple und Amazon sich als hoch risikoreich für die Privat- und Intimsphäre von Betroffenen erweist. Dies gelte nicht nur für Personen, die einen Sprachassistenten betreiben, sondern für alle, die damit in Kontakt kommen, etwa wenn sie in einem Haushalt leben, in dem Geräte verwendet werden, auf denen z.B. Google Assistant installiert ist.
Gestützt auf Mitschnitte, die von Whistleblowern zugespielt wurden, wurde in den Medien kürzlich berichtet, dass Google im Rahmen seines Sprachassistenten Google Home akustische Aufnahmen der Nutzer von Menschen auswerten lässt, um die Spracherkennungsfähigkeit des Google Assistant zu optimieren. Bei diesen Auswertungen hören Mitarbeiter von Google bzw. von beauftragten Firmen die Sprachaufzeichnungen ab und transkribieren diese, um zu analysieren, ob die aufgenommenen akustischen Informationen von dem dahinter stehenden KI-System korrekt verarbeitet wurden.
Der HmbBfDI hatte vor diesem Hintergrund ein Verwaltungsverfahren eröffnet, um Google zu untersagen, entsprechende Auswertungen durch Mitarbeiter oder Dritte für den Zeitraum von drei Monaten vorzunehmen. Damit sollen die Persönlichkeitsrechte der Betroffenen zunächst vorläufig geschützt werden.
Der HmbBfDI hat den Vertretern von Google in der letzten Woche die rechtlichen Vorgaben erläutert, die vor einer Wiederaufnahme der beanstandeten Praxis umzusetzen sind:

- Solange die Transkription und Auswertung von Audioaufnahmen von Sprachassistenzsystemen durch Menschen nicht den DSGVO-Standards entsprechen, wird diese Praxis nicht durchgeführt.
- Als Rechtsgrundlage für die Speicherung von Audioaufnahmen ist eine Einwilligung der Nutzer einzuholen (Opt-in). Dies gilt bereits für den regulären Betrieb, auch wenn keine Transkription und Auswertung von Fehlfunktionen durch Menschen erfolgen.
- Sprachassistenzsysteme werden in einem undefinierten Prozentsatz von Fällen fälschlicherweise aktiviert. Sprachaufnahmen ohne Wissen oder Absicht der Benutzer stellen ein hohes Risiko für die Privatsphäre der Benutzer und anderer Personen wie Besucher und Kinder dar. Transparente Informationen über das Risiko von Fehlauslösungen sind daher eine zentrale Voraussetzung für die Verarbeitung von Audiodaten.
- Die Transkription von Sprachaufnahmen durch Menschen verstärkt die Auswirkungen auf die Persönlichkeitsrechte der Nutzer. Die Auswertung von Audioausschnitten durch Auftragnehmer oder Mitarbeiter zur Verbesserung von Sprachassistenzsystemen ohne eine zusätzliche informierte Zustimmung zu dieser Praxis verletzt die Datenschutzrechte und -freiheiten der Nutzer.
- Die Nutzer müssen darüber informiert werden, dass die Datenschutzrechte und -freiheiten anderer Personen bei der Nutzung von Sprachassistenzsystemen beeinträchtigt werden können. Dies ist besonders wichtig bei der Betrachtung der Möglichkeit, dass Sprachaufzeichnungen von Nicht-Nutzern fehlerhaft verarbeitet werden können. Der Einsatz von Technologien wie der Stimmenerkennung kann die Rechte von Nicht-Nutzern schützen, insbesondere durch die Verhinderung der Sammlung von Audioaufnahmen ihrer Stimmen.

Quelle: Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit

Müssen Vereinbarungen zur Auftragsverarbeitung unterzeichnet werden?

Frage des GDD-Erfa-Kreises Coburg:
Bei uns kam die Diskussion auf, ob AV-Verträge nun unterzeichnet werden müssen oder nicht. In der DS-GVO steht gem. Art. 28 Abs. 9 „Der Vertrag ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann".
Ist das i.O. die Verträge zu unterzeichnen, und im gescannten Format abzulegen, und elektronisch aufzubewahren, oder ist es sogar möglich, einen Onlinefragebogen auszufüllen und ohne Unterschrift zu verschicken, wie bei der Textform?

Antwort des BayLDA:
Nach Art. 28 Abs. 9 DS-GVO ist der Vertrag zur Auftragsverarbeitung schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Was mit dem elektronischen Format genau gemeint ist, und auf welchen Wegen solche Verträge geschlossen werden können, wird derzeit unterschiedlich diskutiert.
Jedenfalls ist es dabei aber Sache der Vertragspartner, den elektronischen Vertragsabschluss (per übereinstimmender Willenserklärungen) für eigene Zwecke und für Kontrollzwecke der Datenschutzaufsichtsbehörden sowie anderer Aufsichtsinstanzen (bei den Kreditinstituten: BaFin, Prüfungsverband, Bundesbank etc.) hinreichend und beweiskräftig zu dokumentieren, z. B. durch unterschriebene und eingescannte Texte mit Protokollierung des dazu geführten E-Mail-Verkehrs, durch eine Verfahrensweise nach § 126a BGB mit einer qualifizierten elektronische Signatur usw.
Eine qualifizierte elektronische Signatur ist also nicht zwingend, sondern nur eine der denkbaren elektronischen Möglichkeiten, so zumindest die herrschende Auffassung in Deutschland.
Eine Abstimmung unter den deutschen Aufsichtsbehörden zu Art. 28 Abs. 9 DS-GVO gibt es allerdings derzeit noch nicht.

Risiken bei der Nutzung von Office 365

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (LfDI) nimmt zahlreiche Nachfragen zur cloud-basierten Bürosoftware Office 365 von Microsoft zum Anlass, den Einsatz der Software im Hinblick auf die Sicherheit und Rechtmäßigkeit der Verarbeitung personenbezogener Daten genauer zu betrachten.
Der Senat der Freien Hansestadt Bremen hat bereits angekündigt, Microsoft Office 365, aufgrund der damit verbundenen datenschutzrechtlichen Risiken, nicht einzusetzen, siehe Beschluss aus der 34. Sitzung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit. Aus diesem Grund befragt die LfDI nun auch Unternehmen zur Nutzung von Microsoft Office 365.
Die angeschriebenen Unternehmen wurden aufgefordert, den ihnen zugesandten Fragebogen bis zum 30. September 2019 zu beantworten. Fragebogen und Hinweise zum Ausfüllen des Fragebogens stehen in elektronischer Form zum Download bereit.

Fragebogen (pdf, 266.9 KB)
Hinweise zum Fragebogen (pdf, 75.3 KB)
Quelle: Die Landesbeauftragte für Datenschutz und Informationsfreiheit

BfDI startet Transparenz-Offensive

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat sich entschlossen, Inhalte seiner Arbeit in zunehmendem Maße der Öffentlichkeit bereitzustellen.
In einem ersten Schritt stellt die Behörde Reden und Gastbeiträge des BfDI sowie aufgrund von IFG-Anfragen herausgegebene Informationen auf der eigenen Website ein.

Für Datenschutzbeauftragte und Datenschutzverantwortliche dürften insbesondere die veröffentlichten Kontrollberichte interessant sein, die bereits in einem IFG-Verfahren herausgegeben wurden. Die Kontrollberichte enthalten Details und Hinweise zum Vorgehen aus den datenschutzrechtlichen Beratungs- und Kontrollbesuchen des BfDI.

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit