NEWS BOX DATENSCHUTZ

AUSGABE
3/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat sich zuletzt im Jahre 2020 mit der immer wieder gestellten Frage des Umfangs der nötigen Aufwände für die Tätigkeit von Datenschutzbeauftragten auseinandergesetzt (Positionspapier zu Aufwandsabschätzungen des Datenschutzbeauftragten). Die Frage ist sowohl aus der Perspektive des Verantwortlichen, als auch aus der des DSB berechtigt: Kann ich, und wenn ja, mit welchem Zeitaufwand der praktischen Erfüllung der rechtlichen Aufgaben gerecht werden, die sich im Wesentlichen aus Art. 39 DS-GVO ergeben?
Der BvD stellt richtigerweise fest, dass in der Praxis Unternehmen vorstellbar sind, die mit einem geringen Aufwand und weniger Personentage im Jahr ausreichend zu betreuen sind (Handwerksbetriebe, Kleinstgewerbe etc.). In den meisten Fällen aber wirken Faktoren, die den Aufwand jeweils erheblich erhöhen. Dazu gehören bspw.:
Anzahl der Mitarbeiter, die Größe des Unternehmens oder die Anzahl der Standorte, Digitalisierungsgrad des Geschäftsfeldes, Verankerung der Verarbeitung personenbezogener Daten im Kerngeschäft, Verarbeitung besonders schützenswerter Daten (sensible Daten) in größerem Umfang, Umsetzungsgrad der DS-GVO, Komplexitätsgrad der Organisationsstruktur, Anzahl ausgelagerter Datenverarbeitungen, aber auch die Frage, in welche zusätzlichen Bereiche die Unternehmensleitung den DSB einbeziehen will. Wird der DSB bei jeder Anfrage eingebunden oder bei jeder Datenpanne einbezogen, kann das den Kapazitätsbedarf erheblich erhöhen.
Diese Faktoren führen schon deswegen zu erheblichen Mehraufwänden, da es sich bei diesen nach dem Working Paper 48 um Kriterien handelt, die eine Datenschutz-Folgenabschätzung (DSFA) notwendig machen – und bei der Durchführung einer (oftmals zeitaufwendigen) DSFA ist der Datenschutzbeauftragte zumindest beratend (in der Praxis wohl oftmals darüber hinaus!) einzubinden.
Auch der BfDI beschäftigt sich in seiner Broschüre BfDI-Info 4 (Die Datenschutzbeauftragten in Behörden und Betrieben) mit diesem Aspekt. Für öffentliche Stellen des Bundes empfiehlt der BfDI regelmäßig die vollständige Freistellung des Datenschutzbeauftragten ab einer Zahl von 500 Beschäftigten, da dies nach seiner Auffassung bereits die mit dem Beschäftigtendatenschutz zusammenhängenden Aufgaben gebieten. In speziellen Fällen – z. B. bei besonders komplexen oder besonders risikobehafteten Datenverarbeitungen – könne schon bei einer geringeren Beschäftigtenzahl eine vollständige Freistellung von anderen Aufgaben geboten sein. Zudem sei dem Datenschutzbeauftragten in Abhängigkeit der beschäftigten Personen ausreichend Hilfspersonal zur Verfügung zu stellen.
Wenn man sich anschaut, wie sich aktuell sogar auf den ersten Blick „unkritische Datenverarbeitungen", wie die Reichweitenmessung mit Google Analytics, als zeitaufwendige und ressourcenfressende Prüfungen entpuppen, dürften die Zeitaufwände durch immer komplexer werdende (insbesondere im Bereich Drittstaatenübermittlungen bzw. TIA-Prüfungen) eher steigen, als geringer werden, fürchtet

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: MQ-Illustrations, Adobe Stock

Mindestspürbarkeitsschwelle für immateriellen Schadensersatz

Der BITKOM nimmt mehrere Vorabentscheidungsverfahren, die aktuell beim EuGH anhängig sind und die sich mit den Voraussetzungen für einen immateriellen Schadensersatzanspruch nach Artikel 82 DS-GVO befassen, zum Anlass, um sich gegen einen Automatismus zwischen Datenschutzverstoß und immateriellen Schadensersatz nach Art. 82 DS-GVO auszusprechen.

Nach Auffassung der BITKOM könne insbesondere im Bereich des immateriellen Schadens eine fehlerhafte Rechtsentwicklung innerhalb der EU zu enormen, nicht tragbaren Belastungen für die gesamte Wirtschaft führen. Aktuelle Vorabentscheidungsverfahren beim Europäischen Gerichtshof („EuGH") zur Auslegung von Art. 82 Datenschutzgrundverordnung würden die Frage beantworten, unter welchen Bedingungen immaterieller Schadensersatz bei geringfügigen Datenschutzverstößen zu leisten ist.

Es sei essenziell, dass hierbei an bestehenden Grundsätzen und insbesondere einer gewissen Spürbarkeitsschwelle festgehalten werde. Die Schadenskalkulation wäre andernfalls für keinen Bereich der Wirtschaft, die mittlerweile vollumfänglich auch mit personenbezogenen Daten arbeite und daher den Regeln der DS-GVO unterliege, tragbar.

Seine Forderung fasst der BITKOM wie folgt zusammen:

- Immaterielle Schadensersatzansprüche sind zumindest an eine Mindestspürbarkeitsschwelle zu knüpfen und in Fällen, in denen abgesehen von geringfügigen emotionalen Ärgernissen keine weiteren Folgen auftreten, muss ein immaterieller Schadensersatz ausgeschlossen sein.
- Zudem sollte die Anspruchshöhe bei vorsätzlichen Datenschutzverletzungen anders quantifiziert werden als bei fahrlässigen Verstößen oder bei Fällen, in denen Mitverschulden vorliegt. Fallgruppen sind zu entwickeln, in denen tatsächlich ein immaterieller Schadensersatz gerechtfertigt ist.

Quelle: BITKOM

GDD-BASIS-SCHULUNG TEIL 1

Einführung in den Datenschutz für die Privatwirtschaft

02.05.–06.05.2022 I Berlin
RA Andreas Jaspers,
Thomas Müthlein,
Prof. Dr. Rolf Schwartmann

Schwerpunkte:

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

Jetzt anmelden: **www.datakontext.com**

GDD

DATAKONTEXT

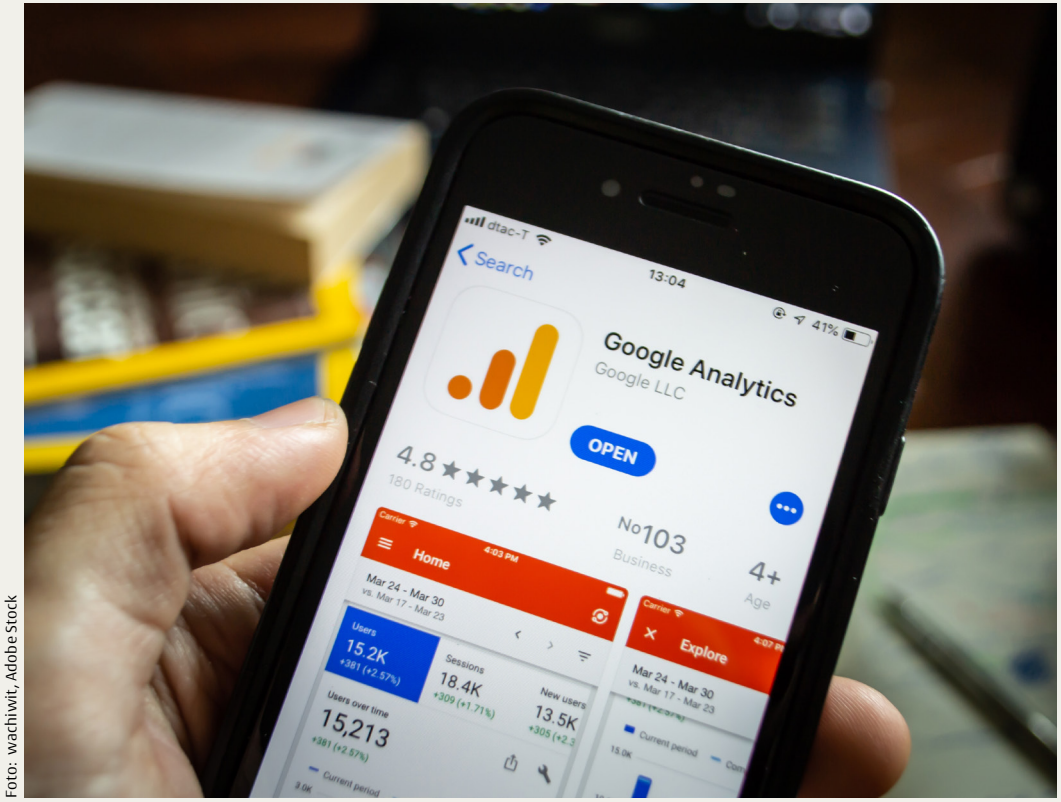

Foto: wachiwit, Adobe Stock

Google Analytics im Visier der Datenschutz-Aufsichtsbehörden

Die Luft wird zunehmend dünner für Google Analytics – oder vielmehr für die Verantwortlichen, die das beliebte Tool zur Reichweitenmessung nutzen.
Bereits Januar 2022 hatte sich die Österreichische Datenschutzbehörde (DSB) im Rahmen eines Beschwerdeverfahrens mit der Vereinbarkeit von Google Analytics und der Datenschutz-Grundverordnung (DS-GVO) befasst.

Weiter auf DataAgenda lesen

Arbeitnehmerüberlassung als Fall des Joint Controllership nach Art. 26 DS-GVO

1. LfDI BW – 35. Tätigkeitsbericht 2019

Der LfDI BW machte in seinem 35. Tätigkeitsbericht aus dem Jahre 2019 (Ziffer 9.1) darauf aufmerksam, dass in der Praxis oftmals eine Auftragsverarbeitung gem. Art. 28 DS-GVO zwischen verantwortlichen Stellen vereinbart wird, um vermeintlichen Anforderungen der DS-GVO nachzukommen, auch wenn im konkreten Fall überhaupt keine Auftragsverarbeitung vorliegt. Würden bspw. Beschäftigtendaten von verschiedenen Unternehmen erhoben oder übermittelt, seien mit Blick auf den Beschäftigtendatenschutz die Datenverarbeitungen besonders sensibel und genauer zu betrachten.

Weiter auf DataAgenda lesen

Foto: Jörg Lantelme, Adobe Stock

Foto: kerkezz, Adobe Stock

Daten von Mietinteressent:innen unzulässig verarbeitet: 1.9 Millionen EUR Bußgeld

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen, basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung (LDI NRW).

Nicht erlaubt sind Fragen bzw. das Einholen von Daten oder Informationen, die für das Mietverhältnis nicht relevant sind. Hierunter fallen Informationen zu Familienstand, Heiratsabsichten, Schwangerschaften, Kinderwünschen, Partei-, Mieterverein- oder Gewerkschaftszugehörigkeit, Staatsangehörigkeit, Religionszugehörigkeit, ethnischer Herkunft, persönlichen Vorlieben, Hobbys oder Krankheiten (vgl. Meine Privatsphäre als Mieter/in Ratgeber zum Datenschutz).
Belege, wie z. B. Einkommensnachweise oder Bonitätsauskünfte, dürfen erst unmittelbar vor Abschluss des Mietvertrags verlangt werden, damit der Vermieter die Informationen, die zuvor im Bewerbungsverfahren angegeben wurden, überprüfen kann (Datenschutz für Vermieter).

Welche Daten im Einzelnen abgefragt werden dürfen, können Sie der Orientierungshilfe Einholung von Selbstauskünften bei Mietinteressentinnen entnehmen.

Einen schwerwiegenden Fall der unzulässigen Datenverarbeitung von Mietinteressent:innen hat die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen (LfDI Bremen) bei der BREBAU GmbH aufgedeckt und Anfang März 2022 als datenschutzrechtliche Aufsichtsbehörde die BREBAU GmbH mit einer Geldbuße in Höhe von 1.9 Millionen EURO nach Artikel 83 DS-GVO belegt.
Die BREBAU GmbH hat nach Informationen der LfDI Bremen mehr als 9.500 Daten über Mietinteressent:innen verarbeitet, ohne dass es hierfür eine Rechtsgrundlage gab. Beispielsweise Informationen über Frisuren, den Körpergeruch und das persönliche Auftreten sind für den Abschluss von Mietverhältnissen nicht erforderlich. Bei mehr als der Hälfte der Fälle handelte es sich darüber hinaus um Daten, die nach der DS-GVO besonders geschützt sind. Rechtswidrig verarbeitet wurden auch Informationen über die Hautfarbe, die ethnische Herkunft, die Religionszugehörigkeit, die sexuelle Orientierung und den Gesundheitszustand.

Foto: Renan, Adobe Stock

1.000 € für Fehlversand einer Nachricht über Xing

LG Darmstadt, Urt. v. 26.05.2020 – 13 O 244/19

Das LG Darmstadt hat in dem Urteil vom 26.05.2020 (Az. 13 O 244/19) entschieden, dass ein potenziell zukünftiger Arbeitgeber schadensersatzpflichtig sein kann, wenn dieser während des Bewerbungsverfahrens unzulässiger Weise die Daten der Bewerber weitergibt.

Weiter auf DataAgenda lesen

Verpflichtung auf die Vertraulichkeit

Das alte Bundesdatenschutzgesetz sah in § 5 BDSG a.F. eine sog. „Verpflichtung auf das Datengeheimnis“ vor.
Eine vergleichbar klare und eindeutige Regelung ist in der DS-GVO nicht mehr enthalten. Insoweit stellte sich datenverarbeitenden Unternehmen, nach Wirksamwerden der DS-GVO, die Frage, ob die klassische Verpflichtung auf das Datengeheimnis weiterhin eine Zukunft hat und als „Verpflichtung auf die Vertraulichkeit“ fortlebt.
Die GDD hatte sich bereits in ihrer Praxishilfe DS-GVO XI – Verpflichtung auf die Vertraulichkeit dahingehend positioniert, dass eine Verpflichtung auf die Vertraulichkeit auch unter dem Regime der DS-GVO ein probates Mittel sein wird, um unmissverständlich auf die Bedeutung und den Umfang datenschutzrechtlicher Regeln hinzuweisen und Mitarbeitern etwaige Risiken von Gesetzesverstößen vor Augen zu führen.

Weiter auf DataAgenda lesen

Foto: Olivier Le Moal, Adobe Stock

Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden

Ihr ständiger Begleiter im Datenschutz-Management

Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Ihre DS-GVO Umsetzung smart auditiert und visualisiert ab 249 €.

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

Direktwerbung nach der DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) regelt die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung neu.

Foto: Jürgen Fälchle, Adobe Stock

Mit der DS-GVO sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen (siehe bisher insbesondere § 28 Abs. 3 und 4 sowie § 29 BDSG-alt). Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist in der DS-GVO, abgesehen von einer Einwilligung der betroffenen Person, eine Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen.
Die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist einerseits ein wichtiger Faktor für Wirtschaftsunternehmen oder spendenfinanzierte Organisationen als Verantwortliche. Die DS-GVO erkennt dies mit dem Erwägungsgrund Nr. 47 Satz 7 auch an, wo es heißt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Andererseits führe gerade die werbliche Verwendung der Kontaktdaten von Verbraucherinnen und Verbrauchern zu vielen Anfragen und Beschwerden bei den Datenschutzaufsichtsbehörden, wobei häufig die fehlende Kenntnis der datenschutz- und verbraucherschutzrechtlichen Regelungen bei den Verantwortlichen oder bei den Verbraucherinnen und Verbrauchern der Anlass sei.
Die Datenschutzkonferenz erläutert in ihrer aktualisierten Orientierungshilfe (Stand Februar 2022), wie die DS-GVO für die direkte Werbeansprache zu verstehen ist.

Quelle: DSK

Foto: Gorodenkoff, Adobe Stock

EDSA prüft Nutzung von Cloud-Diensten im öffentlichen Sektor

Gemäß Artikel 61 Absatz 1 DS-GVO müssen die Aufsichtsbehörden Vorkehrungen für eine wirksame Zusammenarbeit untereinander treffen. Nach Artikel 57 Absatz 1 lit. g) DS-GVO sollen die Aufsichtsbehörden mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung der DS-GVO zu gewährleisten.

Der Rahmen für eine koordinierte Durchsetzung der Verordnung (EU) 2016/679 (Coordinated Enforcement Framework, CEF) bietet eine Struktur für die Koordinierung jährlich wiederkehrender Tätigkeiten der EDSA-Aufsichtsbehörden. Die jährliche koordinierte Maßnahme konzentriert sich auf ein vorher festgelegtes Thema und ermöglicht es den Aufsichtsbehörden, dieses Thema mit der vereinbarten Methodik zu bearbeiten. Der CEF selbst bietet den verfahrenstechnischen Rahmen, innerhalb dessen die koordinierte Maßnahme durchgeführt werden kann. Mitte Februar 2022 ist der Startschuss für die erste „koordinierte Durchsetzungsmaßnahme" des Europäischen Datenschutzausschusses (EDSA), dem Verbund der Datenschutz-Aufsichtsbehörden in der EU zur Durchsetzung der DS-GVO, gefallen.

Das gemeinsame Thema der Überprüfung:

Die Nutzung von Cloud-Diensten durch den öffentlichen Bereich.
Ziel der europaweiten Aktion ist es, den Schutz der personenbezogenen Daten in der EU zu gewährleisten, die Beratung durch die Aufsichtsbehörden zu stärken und Best Practice Beispiele zur datenschutzkonformen Nutzung von Cloud-Diensten herauszuarbeiten. Die Wahl des Untersuchungsgegenstands dürfte damit zusammenhängen, dass sich nach Angaben von EuroStat die Cloud-Nutzung durch Unternehmen in den letzten sechs Jahren europaweit verdoppelt hat. Dabei hat die COVID-19-Pandemie eine beschleunigende Wirkung auf die digitale Transformation der Institutionen ausgelöst. Viele Stellen auch des öffentlichen Bereichs sahen sich gezwungen, ihre Berührungsängste schnell zu überwinden und sich mit der (in der Privatwirtschaft längst etablierten) Cloud-Technologie auseinanderzusetzen.

Dabei können gerade öffentliche Institutionen jedoch auf Schwierigkeiten stoßen, Produkte und Dienstleistungen zu finden, die den EU-Datenschutzvorschriften vollständig entsprechen. Die Nutzung von nicht datenschutzkonformen Produkten und Dienstleistungen im öffentlichen Bereich birgt das besondere Risiko, dass dem Staat anvertraute personenbezogene Daten zweckentfremdet oder gestohlen werden.

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Urteilsübersicht zum Auskunftsrecht nach Art. 15 DS-GVO

Foto: Sikov, Adobe Stock

Mit dem Auskunftsrecht schafft Art. 15 DS-GVO eine Grundlage dafür, dass andere Betroffenenrechte (wie das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, aber auch das Widerspruchsrecht) überhaupt gezielt geltend gemacht werden können.

Nach Art. 12 Abs. 5 DS-GVO darf nur bei offenkundig unbegründeten oder exzessiven Anfragen entweder ein Entgelt verlangt oder die Erteilung einer Auskunft verweigert werden. Exzessiv können Anträge insbesondere im Falle häufiger Wiederholung sein. An das Merkmal „häufige Wiederholung" sind dabei strenge Maßstäbe anzulegen.
In der betrieblichen Praxis stellt sich regelmäßig die Frage zum Umgang mit dem Auskunftsrecht. Die Probleme stellen sich sowohl bei der Frage nach Umfang, den Grenzen und auch der missbräuchlichen Geltendmachung des Auskunftsrechts durch betroffene Personen.

Die Auslegung und Anwendung des Auskunftsanspruchs nach Art. 15 DS-GVO hat in der Praxis für den Verantwortlichen eine enorme Relevanz. Der Bitkom AK Datenschutz hat die aktuelle Rechtsprechung zum Auskunftsanspruch aufbereitet und bringt sich auch nach eigenen Angaben im aktuellen Konsultationsverfahren des Europäischen Datenschutzausschusses ein. Die Übersicht zu den wichtigsten Entscheidungen rund um den Art. 15 DS-GVO bietet der AK Datenschutz zum Download an.

Quelle: Bitkom e. V.

Foto: Chris, Adobe Stock

GDD-Praxishilfe zur Accountability nach DS-GVO

Gemäß Art. 5 Abs. 2 DS-GVO muss der für die Verarbeitung Verantwortliche die Einhaltung der im Abs. 1 des Artikels festgelegten Grundsätze der Verarbeitung personenbezogener Daten nachweisen können. Hieraus folgt eine umfassende Rechenschaftspflicht (engl.: „Accountability“) mit zahlreichen Dokumentations- und Nachweispflichten.

Präzisiert werden die Anforderungen an die Nachweispflicht in Art. 24 Abs. 1 DS-GVO. Hier wird festgelegt, dass der Verantwortliche den Nachweis zu erbringen hat, dass er Maßnahmen getroffen hat, die sicherstellen, dass die Verarbeitung gemäß der DS-GVO erfolgt.

Klare Vorgaben, wie die Nachweispflicht umzusetzen ist, macht die DS-GVO nicht. Die Formulierung in Art. 24 DS-GVO legt jedoch nahe, dass ein Datenschutz-Managementsystem (DSMS) zu implementieren ist, da festgelegt wird, dass die Maßnahmen überprüft und aktualisiert werden müssen. Es genügt also nicht, Maßnahmen einmalig festzulegen und zu implementieren, sondern die Wirksamkeit der ergriffenen Maßnahmen ist regelmäßig zu überprüfen und gegebenenfalls sind Anpassungen vorzunehmen.
Die Nachweispflicht besteht gegenüber den Aufsichtsbehörden. Ein Verstoß gegen die Pflichten kann mit Bußgeldern von bis zu 20 Mio. EUR bzw. bis zu 4 Prozent des weltweit erzielten Jahresumsatzes geahndet werden.
Die neue Praxishilfe soll einen Überblick vermitteln, welche Themen bei der Erfüllung der Rechenschaftspflicht eine Rolle spielen können. Es wird dabei von der Art und den Zwecken der Verarbeitung personenbezogener Daten, der Qualität und Quantität der Daten sowie spezifischen Faktoren des Verantwortlichen, wie Größe, Geschäftsstrategie oder Risikosituation abhängen, welche der aufgezeigten Themenbereiche im jeweiligen Einzelfall zu bearbeiten sind.

Es empfiehlt sich, zu den einzelnen speziellen Themenbereichen die von der GDD veröffentlichten weiteren Praxishilfen als vertiefende Lektüre hinzuzuziehen.

Hier geht es zur GDD-Praxishilfe DS-GVO – Accountability

DGB legt Entwurf eines Beschäftigtendaten-schutzgesetzes vor

Foto: MQ-Illustrations, Adobe Stock

Aus Sicht des Deutschen Gewerkschaftsbunds (DGB) ist es notwendig, den rasch voranschreitenden Entwicklungen insbesondere der elektronischen Datenverarbeitung im Arbeits-, Dienstleistungs- und Produktionsprozess mit immer neuen Digitalisierungsschüben ein interessengerechtes Regelungswerk entgegenzusetzen. Beschäftigte müssten die rechtliche Möglichkeit haben, sich gegen unzulässige Datenverarbeitung oder Überwachung zu wehren. Der DGB und seine Mitgliedsgewerkschaften legten dazu einen Entwurf für ein eigenständiges Beschäftigtendatenschutzgesetz vor.

Mit dem Entwurf eines eigenständigen Beschäftigtendatenschutzgesetzes legen der DGB und seine Mitgliedsgewerkschaften ein individualrechtlich ausgerichtetes Normenpaket vor. Dies sei erforderlich, um die Beschäftigten im digitalen Zeitalter effektiv vor Datenmissbrauch zu schützen und ihre Persönlichkeitsrechte zu wahren.

Der Gesetzentwurf wurde von dem Datenschutzexperten Prof. Dr. Peter Wedde gemeinsam mit dem DGB und seinen Mitgliedsgewerkschaften erarbeitet.

Quelle: Deutscher Gewerkschaftsbund

Folge 13: Der Witz in der Krise

Kunst und Satire können in schlimmen Zeiten trösten. Zugleich können sie sich im Ton vergreifen. Wo liegen die rechtlichen und moralischen Grenzen? Aus einem Gespräch über Datenschutzwitze, das mit dem preisgekrönten Zeichner Heiko Sakurai verabredet war, ist ein Gespräch über den Witz in der Krise geworden. Ein besonderer DataAgenda-Datenschutzpodcast bei dem es nicht nur um den Datenschutz geht.
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