NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
12/2024

Levent Ferik

Ein Trauerspiel in Akten: Das Beschäftigtendatengesetz

Kaum ein Thema hält sich so hartnäckig und so erfolglos auf der politischen Agenda wie das Beschäftigtendatenschutzgesetz. Seit Jahrzehnten wird es diskutiert, entworfen, adaptiert, verworfen – und dann wieder hervorgeholt, als sei diesmal endlich der entscheidende Anlauf erreicht. Dabei haben wir inzwischen fast alle Stufen durchlaufen: Wir hatten Expertenanhörungen, öffentliche Diskussionen und sogar ein paar handfeste Entwürfe, die als Hoffnungsträger die Runde machten. Doch jedes Mal schien das Vorhaben wie verhext: Entweder scheiterten die Entwürfe an parteipolitischen Gräben oder in den endlosen Gängen der Bürokratie.

Der letzte Versuch schien durchaus ambitioniert – schließlich wollte die Ampelkoalition frischen Wind und eine klare Linie in den Beschäftigtendatenschutz bringen. Doch wie so oft kam es anders, als man denkt. Mit dem Bruch der sogenannten Ampelkoalition rückt auch das Beschäftigtendatengesetz in weite Ferne. Der Fall ist besonders misslich, weil der Beschäftigtendatenschutz dringender denn je ist: Datenschutzprobleme, Homeoffice-Regelungen und digitale Überwachung schaffen eine Realität, die klare gesetzliche Regelungen erfordert. Doch nun, da die Ampelkoalition nicht nur in Konflikten gefangen, sondern daran zerbrochen ist, tendiert die Wahrscheinlichkeit einer raschen Umsetzung gegen null. Und auch die eine oder andere News dieser Ausgabe der Datenschutz-Newsbox könnte bereits Makulatur geworden sein, wenn Sie sie lesen. ;-)

Wann wird es also tatsächlich ein Beschäftigtendatenschutzgesetz geben? Die Frage mutet inzwischen wie eine rhetorische an, wie ein Running Gag der deutschen Gesetzgebung. Und selbst wenn der nächste Bundestag das Thema aufgreifen sollte – wir wissen ja, wie oft der Berg schon versucht hat zu gebären – und dieses Mal kam nicht mal eine Maus dabei rum.

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Zerbor, Adobe Stock

Kontrollbesuche der BfDI zum Betrieblichen Eingliederungsmanagement

Im Rahmen ihrer Zuständigkeit kann die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Beratungs- und Kontrollbesuche bei den unter ihrer Aufsicht stehenden Verantwortlichen durchführen.

Auch die Verarbeitung personenbezogener Daten von Beschäftigten im Rahmen des Betrieblichen Eingliederungsmanagements (BEM) nach § 167 Abs. 2 SGB IX war bereits Gegenstand von Beratungs- und Kontrollbesuchen der BfDI. Die Ergebnisse der Kontrollen sind auf der Webseite der BfDI abrufbar und können von den Verantwortlichen genutzt werden, um das eigene BEM-Verfahren daraufhin abzugleichen, ob es den aufsichtsbehördlichen Ansprüchen genügt.
Für einen Abgleich kann zum einen der Kontrollbericht zu einem Beratungs- und Kontrollbesuch beim Eisenbahn-Bundesamt (EBA) in Bonn vom 19. bis 21. Februar 2024 herangezogen werden. Zum anderen enthält auch der Bericht zum Beratungs- und Kontrollbesuch bei der Bundesanstalt für Landwirtschaft und Ernährung (BLE) vom 8. bis 10. August 2023 wertvolle Hinweise zum Thema BEM.
Exemplarisch sollen an dieser Stelle einige Aspekte herausgegriffen werden, die von der BfDI im Rahmen des Kontrollbesuchs angesprochen wurden.

1. Gegenstand des Kontrollbesuchs

Gegenstand des Beratungs- und Kontrollbesuchs gemäß Art. 55 Abs. 1, 57 Abs. 1 lit. a) und 58 Abs. 1 lit. b) Datenschutz-Grundverordnung (DS-GVO) i. V. m. § 16 Abs. 1 Bundesdatenschutzgesetz (BDSG) war die Verarbeitung personenbezogener Daten von Beschäftigten im Rahmen des Betrieblichen Eingliederungsmanagements (BEM) nach § 167 Abs. 2 SGB IX.
Diesbezüglich wurde geprüft, ob

a) den Vorgaben von § 167 Abs. 2 SGB IX entsprochen worden ist,
b) die Datenverarbeitung auf der Grundlage einer wirksamen, ordnungsgemäß dokumentierten Einwilligung der betroffenen Person erfolgte und
c) die einschlägigen Aufbewahrungsfristen nach den aktuellen Personalaktenrichtlinien des Bundesministeriums des Innern und für Heimat (BMI) und § 113 Abs. 2 Bundesbeamtengesetz (BBG) eingehalten wurden.

Weiter auf DataAgenda lesen

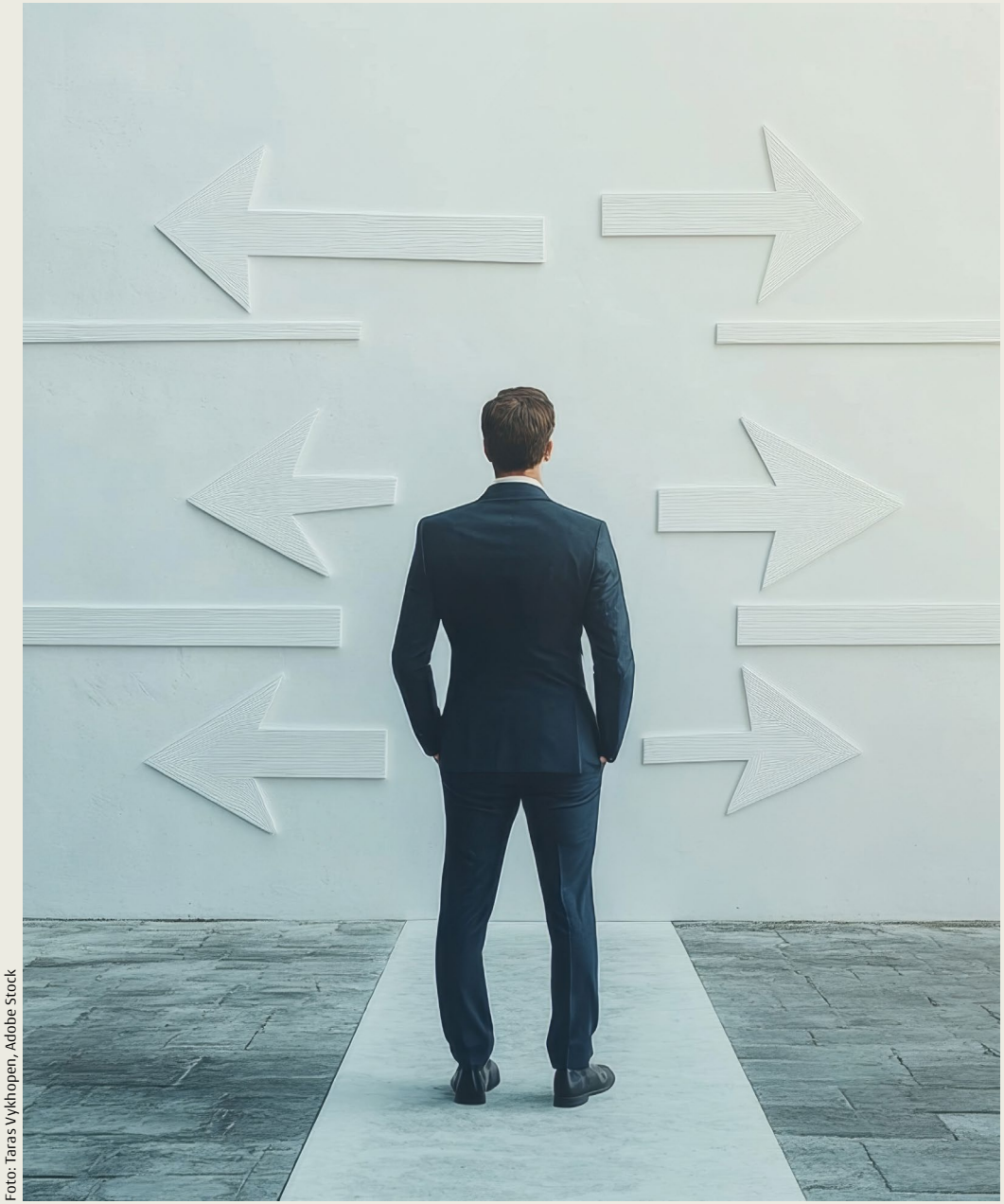

Foto: Taras Vykhopen, Adobe Stock

EDSA veröffentlicht Entwurf zu Art. 6 Abs. 1 lit. f DS-GVO

Am 8. Oktober 2024 veröffentlichte der Europäische Datenschutzausschuss (EDSA) einen Entwurf von Guidelines zur Datenverarbeitung auf Grundlage der allgemeinen Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO.

Dieser enthält wichtige Klarstellungen sowie strenge Auslegungen der datenschutzrechtlichen Anforderungen. Im Folgenden sind die zentralen Punkte zusammengefasst:

Gleichrangigkeit der Erlaubnistatbestände

- Alle Erlaubnistatbestände in Art. 6 Abs. 1 DS-GVO einschließlich lit. f sind gleichwertig.
- Art. 6 Abs. 1 lit. f DS-GVO ist kein „Auffangtatbestand" für fehlende Rechtsgrundlagen.

Berechtigte Interessen

- Bei der Bestimmung des berechtigten Interesses ist ein nicht zu strenger Maßstab anzulegen.
- Hypothetische oder zukünftige Interessen reichen nicht aus.

Weiter auf DataAgenda lesen

Foto: Maxim, Adobe Stock

Stellungnahme der GDD zum NIS-2-Richtlinie

Der Bundestagsinnenausschuss hat am 4. November 2024 den Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes behandelt, das wesentliche Grundzüge für Informationssicherheitsmanagement in der Bundesverwaltung festlegen soll. **Kernpunkte der Gesellschaft für Datenschutz und Datensicherheit (GDD):**

• Begriffsklarheit

Die GDD kritisiert die unklaren Begriffsdefinitionen im Gesetzesentwurf. Sie fordert eine präzisere Sprache, um Missverständnisse und Unsicherheiten für Anwender zu vermeiden.

Weiter auf DataAgenda lesen

Nhan - stock.adobe.com

Foto: thodonal, Adobe Stock

Schadensersatz wegen verspäteter Auskunft

Das Bundesarbeitsgericht (BAG) hat sich mit einem immateriellen Schadensersatzanspruch des Klägers nach Art. 82 Abs. 1 DS-GVO aufgrund einer vermeintlichen Verletzung seines Auskunftsanspruchs gemäß Art. 15 Abs. 1 DS-GVO befasst. Die zentralen Punkte des Urteils lassen sich wie folgt zusammenfassen:

Sachverhalt

- Der Kläger war bei der Beklagten als Koch beschäftigt und forderte Auskunft über zwei Vorgänge (eine Versetzung und eine Abmahnung) nach Art. 15 Abs. 1 DS-GVO.
- Die Beklagte gab teilweise Auskunft, wies jedoch die Unzulässigkeit der Versetzung und die Rechtmäßigkeit der Abmahnung zurück.
- Der Kläger sah seine Auskunftsansprüche nicht vollständig erfüllt und forderte eine Entschädigung in Höhe von 8.000 Euro.

Entscheidungsgründe

Rechtslage: Der Kläger hatte keinen Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DS-GVO, da er keinen immateriellen Schaden dargelegt hatte. Es wurde auf die Voraussetzungen eines solchen Anspruchs hingewiesen:

- Vorliegen eines Schadens,
- Vorliegen eines Verstoßes gegen die DS-GVO,
- Kausalzusammenhang zwischen Schaden und Verstoß.

Darlegungs- und Beweislast: Es wurde betont, dass der Kläger sowohl den Verstoß gegen die DS-GVO als auch den daraus resultierenden Schaden nachweisen muss. Ein bloß hypothetisches Risiko der missbräuchlichen Verwendung seiner Daten reicht nicht aus.

Befürchtungen und negative Gefühle: Negative Gefühle, die der Kläger angibt (z. B. Sorge um die missbräuchliche Verwendung seiner Daten), können nur dann als Schadensersatzanspruch gelten, wenn diese objektiv als begründet angesehen werden können. Der Kläger konnte jedoch nicht ausreichend darlegen, dass ein erhöhtes Risiko für den Missbrauch seiner Daten besteht.

Fehlende Differenzierung: Der Verlust der Kontrolle über personenbezogene Daten durch eine Verletzung des Auskunftsanspruchs führt nicht automatisch zu einem Schadensersatzanspruch, da dieser Verlust bei jeder Verletzung des Art. 15 DS-GVO gegeben ist.

Hilfsweise Ansprüche: Auch die hilfsweise geltend gemachten Ansprüche aus vertraglicher oder deliktischer Haftung waren unbegründet, da ein hinreichend dargelegter Schaden fehlte.

Fazit

Das Urteil stellt klar, dass Betroffene im Fall eines Auskunftsanspruchs nach Art. 15 Abs. 1 DSG-VO nicht nur eine Verletzung der DS-GVO nachweisen müssen, sondern auch den daraus resultierenden immateriellen Schaden substantiiert darlegen müssen. Bloße negative Gefühle oder hypothetische Risiken sind hierfür nicht ausreichend.

Foto: MQ-Illustrations, Adobe Stock

Neuer Entwurf eines Beschäftigtendaten-gesetzes

Die Bundesregierung hat einen Referentenentwurf für ein Beschäftigtendatengesetz (BeschDG) vorgelegt (Bearbeitungsstand: 08.10.2024). Damit soll im letzten Jahr der Legislaturperiode das Koalitionsversprechen eingelöst werden, klare Regelungen für den Beschäftigtendatenschutz zu schaffen.

Hintergrund

Nach dem Urteil des EuGH vom 30. März 2023, das § 26 BDSG für unwirksam erklärte, gab es Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz. Der neue Entwurf greift diese auf und legt umfassende Vorschriften für den Umgang mit Beschäftigtendaten fest.

Kernpunkte des Referentenentwurfs

- **Erforderlichkeitsprüfung**: Datenverarbeitungen im Arbeitsverhältnis unterliegen strengeren Verhältnismäßigkeitsprüfungen.
- **Zweckänderung**: Daten dürfen nur unter strengen Voraussetzungen für neue Zwecke verwendet werden, insbesondere für Leistungsbewertungen.
- **KI-Einsatz**: Beschäftigte haben das Recht auf Information und Einsicht in die Funktionsweise von KI-Systemen.
- **Überwachung**: Videoüberwachung und GPS-Ortung sind streng reguliert, verdeckte Überwachung ist nur bei Verdacht auf Straftaten zulässig.
- **Verwertungsverbot**: Datenschutzwidrig erlangte Daten dürfen nicht in Gerichtsverfahren verwendet werden.
- **Mitbestimmung des Betriebsrats**: Der Betriebsrat erhält erweiterte Rechte beim Einsatz von Technologien und bei der Bestellung von Datenschutzbeauftragten.

Fazit

Das neue Beschäftigtendatengesetz stärkt den Schutz von Beschäftigten, stellt aber auch erhöhte Anforderungen an Arbeitgeber, insbesondere im Umgang mit modernen Technologien wie KI.

Ausblick

Nach dem Bruch der sog. „Ampelkoalition" darf wohl davon ausgegangen werden, dass zumindest in dieser Legislaturperiode die benötigten Mehrheiten für ein Gesetz nicht zusammenkommen werden. Damit dürfte sich auch dieser Versuch, ein Beschäftigtendatenschutzgesetz auf den Weg zu bringen, in die lange Reihe vergangener und erfolgloser Bestrebungen einreihen.

Ausbildung zum/zur Datenschutzauditor/in GDD cert. EU

Datenschutzaudits: Planen und Durchführen

18.–19.02.2025 | Online
Referent: Alexander Forssman

Schwerpunktthemen:

- ✓ Herleitung der Pflicht zur Durchführung eines »Datenschutzaudits«
- ✓ Begriffe, Definitionen, Vorgehensweisen
- ✓ Feststellungen von Konformitäten bzw. Abweichungen
- ✓ Erstellung eines Abschlussberichts
- ✓ Durchführung eines Datenschutzaudits

www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: hodim, Adobe Stock

Einsatz von TikTok durch öffentliche Stellen: Datenschutzrisiken im Fokus

Immer mehr öffentliche Stellen setzen auf Social-Media-Plattformen wie TikTok, um Bürgernähe zu fördern und Informationen zu verbreiten.

Besonders im Hinblick auf die bevorstehenden Kommunalwahlen gewinnt TikTok als Kommunikationskanal an Bedeutung. Allerdings warnt der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) vor erheblichen datenschutzrechtlichen Risiken beim Einsatz solcher Plattformen.

Einschränkungen bei der Datenverarbeitung

Behörden haben nur begrenzten Einfluss auf die Verarbeitung personenbezogener Daten durch große Plattformbetreiber. Die Einhaltung der Datenschutz-Grundverordnung (DS-GVO) – insbesondere der Art. 5, Art. 25 und Art. 6 – wird infrage gestellt, insbesondere bezüglich der Verarbeitung von Daten Minderjähriger und der Transparenz gemäß Art. 13 und 14 DS-GVO.

Checkliste für öffentliche Stellen

Behörden sollten vor der Nutzung von TikTok prüfen:

- Welches Konto wird verwendet (z. B. persönliches oder Business-Konto)?
- Wurde das Konto als „Konto einer Regierung oder politischen Partei“ klassifiziert?
- Welche Datenschutzkonfigurationen und Tools werden eingesetzt?
- Auf welcher Rechtsgrundlage erfolgt die Datenverarbeitung?
- Liegt ein Social-Media-Nutzungskonzept vor, das den Einsatz rechtfertigt?
- Gibt es Alternativen zu TikTok, um eine datenschutzkonforme Kommunikation sicherzustellen?

Der Einsatz von TikTok durch öffentliche Stellen birgt Risiken, insbesondere hinsichtlich des Schutzes personenbezogener Daten. Eine sorgfältige Prüfung der datenschutzrechtlichen Vorgaben ist daher unerlässlich.

Foto: Oleksandr, Adobe Stock

Haftung des Verantwortlichen für seinen Auftragsverarbeiter

Das Oberlandesgericht (OLG) Dresden hat am 10. September 2024 ein Urteil zur Haftung im Rahmen einer Auftragsverarbeitung gefällt (4 U 602/24 / Oberlandesgericht Dresden / 10.09.2024).

Dem Urteil zufolge sind Verantwortliche auch für Datenschutzverletzungen haftbar, die durch Verstöße ihrer Auftragsverarbeiter entstehen.

Kernpunkte des Urteils

- **Haftung des Verantwortlichen**: Verantwortliche haften auch dann, wenn ein Auftragsverarbeiter eine rechtmäßige Weisung missachtet und dadurch Schaden entsteht. Eine Haftungsbefreiung besteht nur, wenn der Verarbeiter eigenständig oder ohne Zustimmung des Verantwortlichen gehandelt hat.
- **Pflicht zur Überwachung**: Art. 28 DS-GVO verpflichtet Verantwortliche zu einer kontinuierlichen Überwachung des Auftragsverarbeiters. Dies schließt ein, sicherzustellen, dass der Verarbeiter Daten nach Auftragsende löscht.
- **Verstöße gegen Informationspflichten**: Das Gericht stellte klar, dass Verstöße gegen Auskunfts- oder Benachrichtigungspflichten allein keinen Schadensersatzanspruch begründen.

Hintergrund des Falls

Ein Hackerangriff auf einen Musik-Streaming-Dienst führte zur Offenlegung personenbezogener Daten. Der Verantwortliche hatte sich eines externen Dienstleisters bedient, versäumte jedoch die regelmäßige Überprüfung und Löschung der Daten nach Beendigung des Auftragsverhältnisses. Der Kläger klagte auf Schadensersatz und verwies auf die unzureichende Kontrolle.

Learning für die Praxis

Datenschutzverantwortliche müssen sicherstellen, dass:

- eine kontinuierliche Überwachung externer Dienstleister stattfindet,
- vertragliche Lösch- und Sicherheitsstandards genau geprüft und eingehalten werden,
- auch nach Beendigung des Vertrags die Löschung der Daten dokumentiert ist.

Diese Entscheidung verdeutlicht, dass die Haftung nicht einfach auf den Auftragsverarbeiter abgewälzt werden kann und betont die Wichtigkeit einer strikten Überwachung von Auftragsverarbeitern.

DATA AGENDA PODCAST

(Quelle: TH Köln/Schmülgen)

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

Folge #**60**

Daten für die Sicherheit

Data Agenda Podcast Episode 60: Daten für die Sicherheit

Datenschutz dient dem Schutz der Privatsphäre. Sie ist von der Verfassung als Recht auf informationelle Selbstbestimmung verbürgt, und die DS-GVO schützt sie seit 2018. Europa legt besonderen Wert auf diesen Schutz, der dem Kontinent wie ein Markenzeichen anhaftet. Die Menschen brauchen und schätzen den Schutz ihrer Privatsphäre vielleicht mehr, als es der Ruf des Datenschutzrechts vermuten lässt. Zu Recht beschweren sich Bürger und staatliche Stellen über überzüchteten Datenschutz, weil er über sein Ziel hinausschießt. Der Streit um das richtige Maß beschäftigt künftig den Vermittlungsausschuss, nachdem das sog. Sicherheitspaket am 18. Oktober im Bundesrat als zu schwach bewertet wurde. Wenn es um maßvolles, rechtskonformes und zugleich wirksames Entscheiden über das Verhältnis von Freiheit, informationelle Selbstbestimmung und Sicherheit geht, ist das Bundesverfassungsgericht gefragt. Im DataAgenda-Podcast werden diese Fragen im Gespräch mit Markus Hartmann, Leitender Oberstaatsanwalt und Leiter der ZAC-NRW, sowie Moritz Köhler von der Kölner Forschungsstelle für Medienrecht beleuchtet.
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