NEWS BOX DATENSCHUTZ

AUSGABE
9/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Seit dem 25. Mai 2018 gilt die DS-GVO in der gesamten EU. Schon vor diesem Termin hatten viele Unternehmen befürchtet, dass nun auch Abmahnungen von Wettbewerbern auf sie zukommen könnten, mit denen diese das neue Datenschutzgesetz durchsetzen wollten. Bislang ist diese Abmahnwelle ausgeblieben, die Unsicherheit ist aber trotzdem bei vielen geblieben.

Bereits Anfang 2022 gab es Verwirrung um die Nutzung bzw. Einbindung von Schriftarten auf Webseiten. Grund war ein Urteil des Landgerichts München (Urteil vom 20.01.2022, Az. 3 O 17493/20). Das Gericht sprach einen Unterlassungsanspruch und Schadensersatz (hier 100,00 EUR) wegen der Weitergabe von IP-Adressen an Google durch Nutzung von Google Fonts gegen den Beklagten aus. Day BayLfD versuchte bereits früh, die entstandene Unsicherheit mit Fakten rund um die Thematik auszuräumen. Die immer noch bestehende Unsicherheit wird aktuell jedoch wieder verstärkt und die Begriffe „Datenschutz“ und „Abmahnwelle“ werden wieder in einem Atemzug genannt. Grund dafür ist, dass Unternehmen von Privatpersonen angeschrieben und auf vermeintliche Verstöße gegen das Datenschutzrecht im Zusammenhang mit der Nutzung der Google Fonts hingewiesen werden. Den Websitebetreibern wird angeboten, die Angelegenheit durch Zahlung eines Pauschalbetrages in Höhe von 100,00 EUR gütlich beizulegen. Suggeriert wird, dass sich so eine Klage oder eine Eingabe bei der zuständigen Datenschutzaufsichtsbehörde vermeiden ließe.

Die Netzgemeinde und auch Teile des „#Teamdatenschutz/twitter“ reagierten auf diese „Abmahnmasche“ und haben betroffene Unternehmen rasch sowohl mit Informationen (1, 2, 3, 4, 5, 6) rund um das Thema versorgt, als auch mit „Muster-Antworten“ und „Antwort-Generatoren“ oder einem „Google-Fonts-Checker“ Erste Hilfe geleistet. An dieser Stelle allen ein herzliches Dankeschön.

Ihr Levent Ferik

P.S.: Die 46. DAFTA und das 41. RDV-Forum finden in diesem Jahr hybrid vom 16.11. bis zum 19.11.2022 statt. Das Programm finden Sie hier.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Datenschutzkonformität von Microsoft 365 und Microsoft Teams

Foto: Diego, Adobe Stock

Können Microsoft 365 und Microsoft Teams in Unternehmen und im öffentlichen Sektor – insbesondere im Bildungsbereich – datenschutzkonform eingesetzt werden?

Dazu haben einzelne Aufsichtsbehörden, insbesondere auch vor dem Hintergrund der Nutzung in Schulen, IT-Sicherheitsexperten, aber natürlich auch Microsoft unterschiedliche Auffassungen. Die aktuellste Stellungnahme zum Thema aus dem Hause Microsoft dürfte aus August 2022 sein. In dem Papier „Stellungnahme von Microsoft Deutschland zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams“ fasst Herr Wolfgang Döring, Head of Legal Microsoft, seine Sicht der Dinge zusammen:

Die wichtigsten Punkte im Überblick:

- **„Alle Microsoft Produkte und Dienste können in der Privatwirtschaft und im öffentlichen Sektor (z.B. an Schulen) datenschutzkonform eingesetzt werden und sind auch selbst datenschutzkonform**. Microsoft hält die Anforderungen des geltenden Datenschutzrechts ein.
- **Microsoft bietet Kunden vertragliche Zusagen und technische Mittel, um Microsoft Produkte und Dienste datenschutzkonform nutzen zu können**, insbesondere vertragliche Zusagen: z.B. verwendet Microsoft Kundendaten nicht für sachfremde Zwecke wie Werbung und ergreift rechtliche Schutzmaßnahmen gegen unrechtmäßige Herausgabeverlangen von Behörden oder Dritten.
- **Microsoft speichert Daten weitgehend regional in Rechenzentren in der EU**. Zusätzlich wird die **Microsoft EU Data Boundary** es künftig in der EU ansässigen Kunden aus dem öffentlichen Sektor und Unternehmenskunden ermöglichen, ihre Daten innerhalb der EU zu verarbeiten und zu speichern.“

Foto: N. Theiss, Adobe Stock

Drittlandtransfer: Gleichsetzung von Zugriffsrisiko und Übermittlung?

Der Beschluss der Vergabekammer Baden-Württemberg (Az. 1 VK 23/22) vom 13. Juli 2022 adressiert u.a. auch die Frage, ob US-Anbieter digitaler Server- und Cloud-Leistungen ihre Dienstleistungen über europäische Tochtergesellschaften erbringen können. Die Vergabekammer scheint davon auszugehen, dass eine Zusammenarbeit mit US-Anbietern nach Wegfall des Privacy-Shields-Abkommens mit der EU (vgl. EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18; „Schrems-II"), trotz der Verwendung sog. Standarddatenschutzklauseln, per se unzulässig ist.

Weiter auf DataAgenda lesen

Interessenkonflikte bei Datenschutzbeauftragten

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche, verpflichtende Regelung zur Benennung betrieblicher und behördlicher Datenschutzbeauftragter. Während die EG-Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Benennung von Datenschutzbeauftragten lediglich als Alternative vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, ergibt sich mit der Geltung der DS-GVO erstmals eine Benennungspflicht unmittelbar aus dem Europarecht. Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt.

Weiter auf DataAgenda lesen

Foto: Song_about_summer, Adobe Stock

46. DAFTA

41. RDV-FORUM

DATENSCHUTZ - GESTALTUNGSAUFTRAG
IM ZEITALTER DER DIGITALISIERUNG

Jetzt anmelden:
datakontext.com/dafta-2022

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Kittiphat, Adobe Stock

BITKOM-Leitfaden zur Drittlandübermittlung

Der europäische Gesetzgeber hat vor dem Hintergrund der Ausweitung des internationalen Handels die Übermittlung personenbezogener Daten an Datenempfänger in Drittländern unter besondere datenschutzrechtliche Anforderungen gestellt, um Rechte und Freiheiten von Betroffenen zu schützen. Ziel ist es, das durch die Datenschutz-Grundverordnung (DS-GVO) unionsweit gewährleistete Schutzniveau für natürliche Personen nicht zu untergraben, wenn personenbezogene Daten in ein Drittland transferiert werden. Der Art. 44 ff. aus Kapitel V der DS-GVO gibt die Bedingungen vor, nach denen Verantwortliche oder Auftragsverarbeiter, die der DS-GVO unterliegen, personenbezogene Daten in Drittländer übermitteln dürfen.

Der AK Datenschutz des Digitalverbands BITKOM e.V. hat seinen Leitfaden „Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer“ aktualisiert. Der neue Leitfaden mit dem Titel „Verarbeitung personenbezogener Daten in Drittländern“ weist mit dem Untertitel „Auf Basis der EU-Datenschutz-Grundverordnung post Schrems II“ auf den Umstand hin, der eine Aktualisierung notwendig machte.

Die Version 1.3 berücksichtigt die Auswirkungen des am 16.07.2020 ergangenen EuGH-Urteils „Schrems II“ (C-311/18), in dem der Angemessenheitsbeschluss (EU)2016/1250 der Europäischen Kommission vom 12. Juli 2016 zum US-EU Privacy Shield Framework – die Übermittlung personenbezogener Daten in die USA betreffend – für ungültig erklärt wurde. Das Urteil bringt unterdessen nicht nur für Datentransfers in die USA, sondern im Allgemeinen für die Verarbeitung personenbezogener Daten in Drittländern erhebliche Auswirkungen mit sich.

Quelle: Bitkom e.V.

Prüfcheckliste für Absicherung von E-Mail-Accounts

Foto: tippapatt, Adobe Stock

Nach dem einige Datenschutz-Aufsichtsbehörden jüngst eine äußerst hilfreiche Checkliste für die Prüfung von Auftragsverarbeitungsvereinbarungen aus dem Bereich des Webhostings zur Verfügung gestellt haben, bietet das BayLDA ein „Informationsblatt zur Absicherung von E-Mail-Accounts zum Schutz vor Phishing und Cyberattacken“ sowie eine „Handreichung bzw. einen Prüfbogen mit Details zur Absicherung von E-Mail-Accounts – Schwerpunkt Phishing“ an.

Nach Ansicht des BayLDA sind E-Mail-Accounts immer noch die verwundbarste Stelle vieler Unternehmen, die Cyberkriminelle gerne nutzen. Ihre Absicherung gelingt nur, wenn zeitgemäße technische Schutzmaßnahmen vorliegen und zugleich ein hohes Maß an Aufklärung und Sensibilisierung der Nutzerinnen und Nutzer sichergestellt werden, so das BayLDA. Die mit Abstand wichtigste Maßnahme zum aktiven Schutz vor solchen Cyberattacken stelle die Sensibilisierung des eigenen Personals dar. Die Stabsstelle Prüfverfahren des BayLDA habe sich daher aufgrund der akuten Bedrohungslage im Cyberraum entschieden, nach dem Bereich Ransomware nun auch die Absicherung von E-Mail-Accounts großflächig im Bayern zu kontrollieren.

Diese oben genannte Checkliste stellt wesentliche Elemente zu den untersuchten Prüfungsschwerpunkten dar und kann von interessierten Verantwortlichen auch außerhalb von Bayern sehr gut für eine Selbstprüfung genutzt werden.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Foto: metamorworks, Adobe Stock

Mitarbeiterexzess und Beschäftigtendaten-schutz

Nach Auffassung der Datenschutzkonferenz (DSK) als Gremium der deutschen Datenschutzaufsichtsbehörden sollen Unternehmen im Rahmen von Art. 83 DS-GVO für Datenschutzverstöße eines jeden Beschäftigten haften, wenn der Mitarbeiter nicht im Exzess (für eigene Zwecke) gehandelt hat. In bestimmten Fällen kann aber auch der Arbeitnehmer unmittelbar Adressat einer aufsichtsbehördlichen (Sanktions-)Maßnahme sein. Dafür muss der Beschäftigte als „Verantwortlicher" im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren sein. Die DSK hat in seiner Entschließung vom 3.4.2019 betont, dass sogenannte „Exzesse" der Beschäftigten, die bei verständiger Würdigung nicht der unternehmerischen Tätigkeit zugeordnet werden können, nicht von der Haftung des Unternehmens erfasst sind.

Weiter auf DataAgenda lesen

Foto: Jirapong, Adobe Stock

Joint Controllership oder Auftragsverarbeitung: Immobilienwirtschaft

Art. 26 DS-GVO enthält eine Regelung zur gemeinsamen Verantwortlichkeit für die Datenverarbeitung (Joint Controllership). Der Umstand, dass bei Zusammenarbeit mehrerer Stellen diese gemeinsam für eine Datenverarbeitung verantwortlich sein können, ist nicht neu. Allerdings erfuhr die Rechtsfigur vor Geltung der DS-GVO wenig praktische Relevanz. Stattdessen wurde in diesen Fällen häufig eine Auftragsverarbeitung angenommen und der (Mit-)Verantwortliche zum vermeintlichen Auftragsverarbeiter erklärt. Die Rechtsfigur der gemeinsamen Verantwortlichkeit hat zu einer nicht unerheblichen Verunsicherung geführt und wirft zahlreiche praxisrelevante Fragen auf. So bedarf es der Abgrenzung zur Auftragsverarbeitung (Art. 28 DS-GVO) einerseits und zur alleinigen Verantwortlichkeit andererseits.

In seinem 29. Tätigkeitsbericht thematisiert auch der Landesdatenschutzbeauftragte Rheinland-Pfalz diese Verunsicherung aus dem Blickwinkel der Behörde. Dem LfDI seien im Berichtszeitraum sowohl seitens der Wohnungseigentümergemeinschaften (WEG) als auch von den Hausverwaltungen immer wieder Fragen im Hinblick auf die datenschutzrechtliche Verantwortlichkeit dieser Stellen gerichtet worden. Ein Grund dafür könne sein, dass auch das Amtsgericht Mannheim (Urt. v. 11.09.2019 – 5 C 1733/19 WEG) Stellung zu dieser Frage genommen habe. Die im Rahmen von Tätigkeiten der WEG und Hausverwaltungen entstehenden Datenverarbeitungsvorgänge bewertet der LfDI wie folgt:

„1. Der Verwalter ist überwiegend alleinverantwortlich, soweit er seine originären Verwalteraufgaben (vgl. §§ 27, 28 Wohnungseigentumsgesetz) ausführt.

2. Führt der Verwalter einen Beschluss der Eigentümergemeinschaft aus (z.B. Entscheidung über eine Videoüberwachung im Haus), so ist es wahrscheinlich, dass die WEG datenschutzrechtlich verantwortlich ist und der Verwalter die Aufgaben nur auf Weisung der WEG ausführt und somit keine eigenen Entscheidungen über Zwecke und Mittel der Verarbeitung trifft. Wenn diese der Fall ist, liegt ggf. eine Auftragsverarbeitung i.S.v. Art 28 DS-GVO vor. Für die Frage, ob es sich gegebenenfalls um eine Auftragsverarbeitung handelt, sollte jedoch immer der konkrete Beschluss bzw. die Datenverarbeitung im Einzelfall geprüft werden.

Weiter auf der nächsten Seite.

3. Es ist nicht ausgeschlossen, dass es auch Fälle geben kann, in denen die WEG und der Verwalter als gemeinsame Verantwortliche i.S.v. Art. 26 DS-GVO agieren. Auch dies ist anhand des konkreten Einzelfalles zu beurteilen."

Der LfDI ist mit der Datenschutzkonferenz nicht der Auffassung, dass die Verwaltung für WEG grundsätzlich eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO darstellt. Die Hausverwaltung verarbeitet personenbezogene Daten in eigener Verantwortung. Sie ist mithin Verantwortlicher im Sinne der DS-GVO.
In einem internen Arbeitskreis der Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sei das Urteil des AG Mannheims vom 11. September 2019 bereits im Herbst 2019 thematisiert und einhellig besprochen worden, dass dieses nichts an der bisherigen Rechtsauffassung der DSK ändert.

Quelle: Der Landesdatenschutzbeauftragte Rheinland-Pfalz

Joint Controllership oder Auftragsverarbeitung: Werbende & Adresshändler

Wie zuvor erläutert (bspw. in der Immobilienwirtschaft), hat die Rechtsfigur der gemeinsamen Verantwortlichkeit nach Wirksamwerden der DS-GVO zu einer nicht unerheblichen Verunsicherung geführt und wirft zahlreiche praxisrelevante Fragen auf. So bedarf es der Abgrenzung zur Auftragsverarbeitung (Art. 28 DS-GVO) einerseits und zur alleinigen Verantwortlichkeit andererseits.
Verunsicherungen diesbezüglich scheinen auch im Bereich des Adresshandels immer wieder aufzutreten. Der LfDI Rheinland-Pfalz hat sich im Berichtszeitraum des 29. Tätigkeitsberichts auch mit der Frage der Verantwortlichkeit von Unternehmen beschäftigt, die Adressen mieten oder Werbung im Lettershop-Verfahren versenden lassen.

Weiter auf DataAgenda lesen

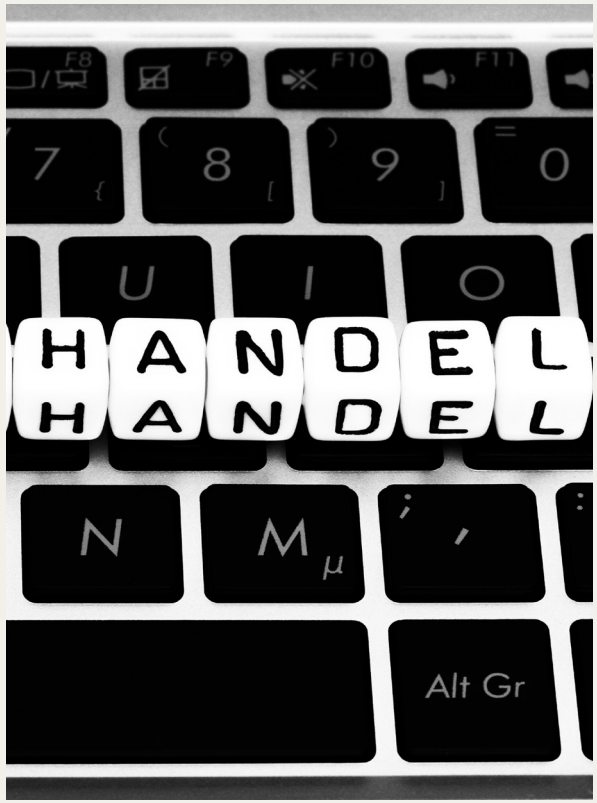

Foto: blende11.photo, Adobe Stock

Reifegradmodell für TOMs im Rahmen der Auftragsverarbeitung

Foto: ra2 studio, Adobe Stock

Der AK Datenschutz des BITKOM e.V. möchte mit seiner neuen Publikation zum Thema „Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung“, insbesondere Auftragsverarbeitern eine Hilfestellung bieten. Motivation des Arbeitskreises ist es, diesen eine Richtschnur mit Best Practices zur Identifikation und Umsetzung relevanter technischer und organisatorischer Maßnahmen hinsichtlich Privacy by Design und Sicherheit der Verarbeitung zu geben. Darüber hinaus soll es auch eine Diskussionsgrundlage innerhalb des Bitkom und mit anderen Verbänden sowie Behörden und Ministerien darstellen.

Sie sollen bei der schnellen und pragmatischen Erreichung von ausreichenden Niveaus für Datenschutz unterstützt werden. Formuliertes Ziel des Reifegradmodells ist damit, insbesondere Auftragsverarbeitern im Sinne der DS-GVO, eine praktische Unterstützung bei der systematischen Bewertung ihrer Fähigkeiten und des Reifegrads der Organisation in den Bereichen Datenschutz und Informationssicherheit (Baseline) zugeben. Sie sollen bei der zielgerichteten Weiterentwicklung der Fähigkeiten und des Reifegrads der Organisation unterstützt werden.

Das Datenschutz-Reifegradmodell ist in eine Reihe von Themengebieten strukturiert, die jeweils bestimmte Zwecke hinsichtlich Datenschutz und den damit verbundenen Schutzzielen wie Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität verfolgen und unterstützen.

Quelle: Bitkom e. V.

DATA AGENDA PODCAST

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

Folge #21

Grenzen des Informationshandelns der Datenschutzaufsicht

Folge #22

DS-GVO im Spiegel von Data Act, Data Governance Act und KI-Verordnung


Kristin Benedikt


Prof. Dr. Boris Paal


Prof. Herwig Hofmann

Data Agenda Podcast Folge 21: Grenzen des Informationshandelns der Datenschutzaufsicht

In der Praxis nutzen Datenschutzaufsichtsbehörden ein Bündel von Maßnahmen, um ihre Aufgaben zu erfüllen. Dazu gehört neben Orientierungshilfen und Tätigkeitsberichten insbesondere auch die Öffentlichkeitsarbeit. Eine Besonderheit der Öffentlichkeitsarbeit besteht bei Datenschutzaufsichtsbehörden darin, dass jede öffentlich gemachte Maßnahme der Behörde Verantwortliche in der öffentlichen Wahrnehmung in die Nähe einer „Datensünders" stellt, obwohl einer Warnung oft keine abgeschlossene Prüfung vorausgegangen ist. Jede öffentliche Warnung oder Information stellt also ein Damoklesschwert und möglicherweise schon eine (faktische) Sanktion dar. Auf der anderen Seite sind die Anforderungen des Verwaltungsverfahrensrechts an amtliche Ermittlung von Sachverhalten und die Bestimmtheit von Maßnahmen hoch. Professor Dr. Rolf Schwartmann im Gespräch mit Kristin Benedikt und Professor Dr. Boris Paal über Voraussetzungen und die rechtlichen Grenzen der Öffentlichkeitsarbeit von Aufsichtsbehörden.

Zum Podcast bitte hier klicken.

DataAgenda Podcast Folge 22: DS-GVO im Spiegel von Data Act, Data Governance Act und KI-Verordnung

Europas Digitalwirtschaft soll im internationalen Wettbewerb zu einem Ökosystem der fairen digitalen Wertschöpfung werden. Der Datenschutz soll kein Bremsklotz der wirtschaftlichen Entwicklung sein, sondern integraler Bestandteil der Datenstrategie. Aktuell beherrschen die Tech-Giganten aus USA und China den europäischen Markt. Wie kann sich die EU rüsten, wenn es darum geht, „Big Data" und Anwendungen Künstlicher Intelligenz für den Binnenmarkt fit zu machen.
Ein Gespräch mit Herwig Hofmann, Professor für europäisches und transnationales öffentliches Recht an der Universität Luxemburg. Als Prozessvertreter ist er spezialisiert auf Verfahren vor dem EuGH. Er hat Max Schrems in den Verfahren Safe Harbour (2015) und Privacy Shield (2020) vertreten.
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