NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 6/2022

DATAKONTEXT

Levent Ferik

EDITORIAL

Es gibt Ideen und politische Vorschläge, die sich offensichtlich nicht ausrotten lassen, obwohl diese immer wieder als nicht zielführend, nicht zulässig oder gar als verfassungswidrig eingestuft werden.

Wie oft mussten sich Richter, bis hin zum EuGH, bspw. mit dem Thema Vorratsdatenspeicherung befassen?

Die EU-Kommission hat nun aktuell ein flächendeckendes, aus Brüssel gesteuertes Überwachungssystem vorgeschlagen. Auch auf diesen Vorstoß gibt es scharfe Kritik aus Zivilgesellschaft und Politik. Die sog. Chatkontrolle will Chat- und Messenger-Providern vorschreiben, private Chats, Nachrichten und E-Mails massenhaft, anlass- und unterschiedslos auf verdächtige Inhalte zu durchsuchen. Nicht wenige befürchten, dass damit eine nie dagewesene Massenüberwachung durch vollautomatisierte Echtzeit-Chatkontrolle und damit die Abschaffung des digitalen Briefgeheimnisses einherginge.

Ein anderes Datenschutz-Thema, das nicht „totzukriegen ist“: die Benennungspflicht für Datenschutzbeauftragte. Alle paar Jahre glimmt eine Diskussion um die Schwellwerte für die Benennung von Datenschutzbeauftragten auf, bis dieses vollständig gelöscht geglaubte Glutnest ein wiederholtes Mal durch die Vernunft der Vielen erstickt werden muss. Die Erfahrungen der Datenschutz-Verbände, aber auch wissenschaftliche Untersuchungen zeigen, dass im Falle der Nichtbenennung eines Datenschutzbeauftragten oft niemand die Überwachung und Beratung hinsichtlich der Datenschutzpflichten wahrnimmt. Dies ist nicht nur aus Sicht der Personen kritisch, deren personenbezogene Daten verarbeitet werden. Angesichts der immensen Bußgeldrahmen der DS-GVO ist dies auch für die Unternehmen selbst riskant, denn Datenschutzbeauftragte helfen auch bei der Reduzierung von Unternehmensrisiken.
Warum also gibt es Vorstöße zu Themen, deren Ausgang für die Initiatoren klar sein müsste? Mir fällt da spontan nur die Redewendung ein: „Der Tropfen höhlt den Stein nicht durch Kraft, sondern durch stetes Fallen.“

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Masson, Adobe Stock

Anhörung zu Facebook-Fanpages

Der Fall „Facebook-Fanpages“ geht in die nächste Runde.

1. Runde:
Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-201/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und -Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Facebook-Fanpage – ergeben. Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DS-GVO) unter anderem eine Vereinbarung zwischen den Beteiligten. Diese soll klarstellen, wie die Pflichten aus der DS-GVO erfüllt werden.

2. Runde:
Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nach Ansicht der DSK nicht die Anforderungen an eine Vereinbarung nach Art. 26 DS-GVO. Insbesondere stehe es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten“ einräumen lassen wolle. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar, so die Aufsichtsbehörden. Sie seien nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpages zu ermöglichen.

3. Runde:
Die Verantwortlichen sind angesichts der Geschehnisse verunsichert. Die Gesellschaft für Datenschutz und Datensicherheit berichtet bspw., dass an sie mehrfach die Frage herangetragen worden sei, ob unternehmenseigene Facebook-Fanpages noch weiterbetrieben werden können oder diese sofort abzuschalten sind.

Lesen Sie die komplette Chronologie der Geschehnisse weiter auf DataAgenda.

15. GDD

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Sommer-Workshop

FÜR DATENSCHUTZBEAUFTRAGTE UND -BERATER SOWIE DATENSCHUTZDIENSTLEISTER

8. bis 10. August 2022

in **Timmendorfer Strand**

Praxisthemen

- Aktuelle Entwicklungen im Datenschutz
- Datenschutzaufsicht in Deutschland und Europa – Zusammenarbeit und Wechselwirkungen
- Das praxisrelevanteste und umstrittenste Betroffenenrecht – Recht auf Auskunft und Kopie nach Art. 15 DS-GVO
- Digitales Vertragsrecht: Dürfen Verbraucher mit Daten bezahlen?
- Google Analytics – Tracking und Marketing
- Beschäftigtendatenschutz im Zeitalter der Digitalisierung
- Data Governance Act, Data Act & Co. – Praxischeck
- Elektronische Arbeitsunfähigkeitsbescheinigung (eAU) und Datenschutzaspekte
- Standardvertragsklauseln in der praktischen Umsetzung
- Die aktuelle IT-Sicherheitsgesetzgebung
- Cybersicherheit im Jahre 2022 – was Datenschutzbeauftragte wissen sollten

Jetzt anmelden: www.datakontext.com/sommerworkshop

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Risikoanalyse und Datenschutz-Folgenabschätzung

Auch öffentliche Stellen sind grundsätzlich zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) verpflichtet, insbesondere wenn sie Verarbeitungen personenbezogener Daten durchführen, die in einer der Blacklists der Aufsichtsbehörde genannt sind.

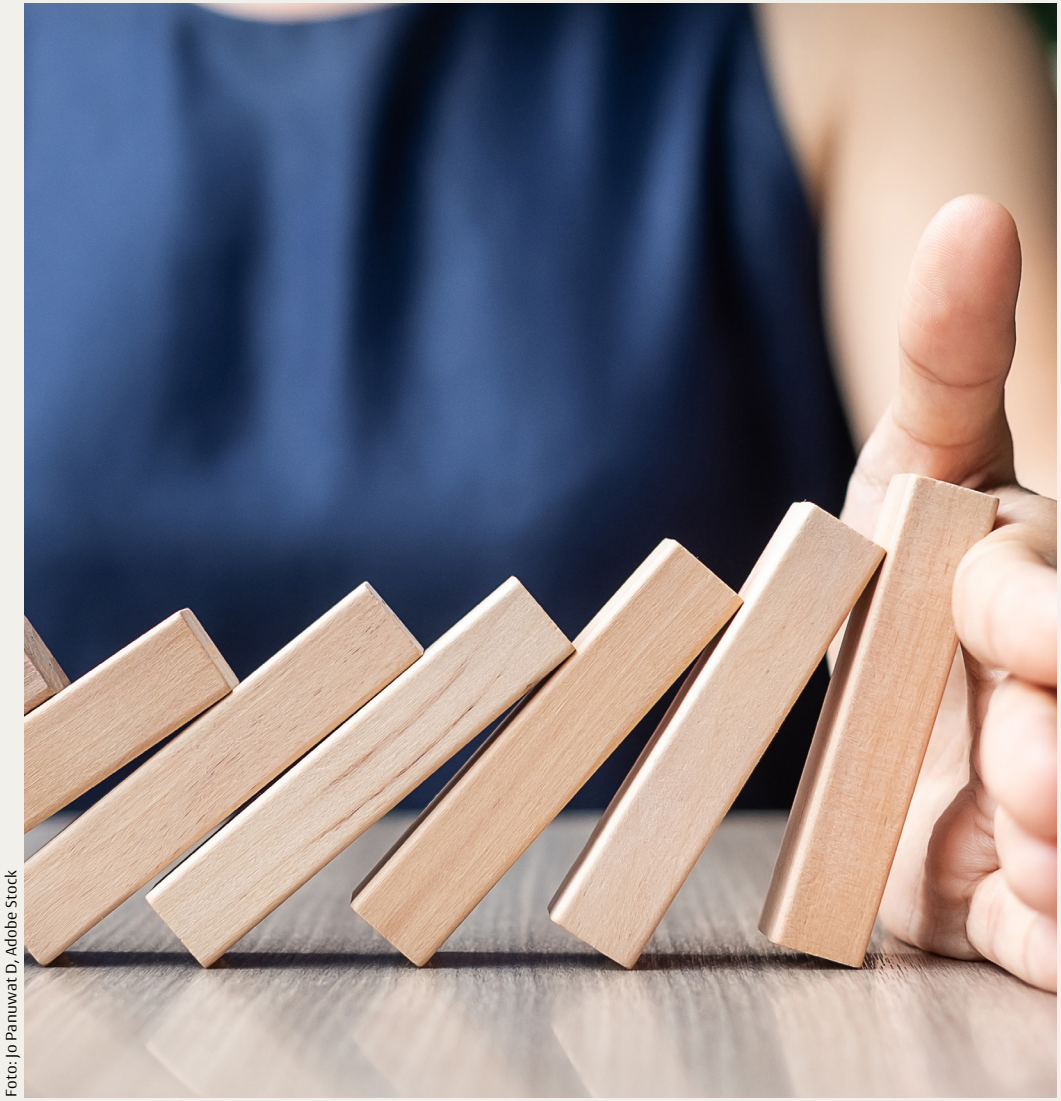

Foto: Jo Panuwat D, Adobe Stock

Als Hilfestellung für bayerische öffentliche Stellen bietet der BayLfD auf seinem Internetauftritt umfangreiche Informationen und Tools an, die im Rahmen der Prüfung (soweit die relevante Verarbeitung also nicht ohnehin in der jeweiligen Blacklist enthalten ist) einer Datenschutz-Folgenabschätzung genutzt werden können. Allgemeine Informationen in Hinblick auf das Instrument der Datenschutz-Folgenabschätzung bietet die angebotene Orientierungshilfe.

Das bisher vom BayLfD angebotene Arbeitspapier mit dem Titel „Datenschutz-Folgenabschätzung – Methodik und Fallstudie“, in welchem dem Leser die methodische Einführung an einem konkreten Beispiel an einer Verarbeitungstätigkeit vorgestellt wurde und erforderliche Arbeitsschritte und Hilfsmittel anschaulich vermittelte, wird nun ersetzt durch die Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele“).
Weitere praktische Orientierung erhält der Interessierte anhand der angebotenen Leerformulare und Ausfüllbeispiele:
Modul 1: Beschreibung einer Verarbeitungstätigkeit
Modul 2: DSFA-Erforderlichkeitsprüfung
Modul 3: DSFA-Bericht für eine Verarbeitungstätigkeit
Modul 4: Betriebsmittel „IT-Personalverwaltungssystem“
Modul 5: Betriebsmittel „Videokonferenzsystem“
Modul 6: Betriebsmittel „Bildschirmarbeitsplatz“
Die Informationen zum Thema Datenschutz-Folgeabschätzung werden mit einer Download-Möglichkeit des PIA-Tools (deutsche Übersetzung) der CNIL abgerundet.

Foto: N. Theiss, Adobe Stock

Unzulässige Listen für „Probezeit-Kündigungen“

Die Probezeit ist eine vertraglich vereinbarte Testphase zu Beginn eines Arbeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber. Die Vereinbarung einer solchen Probezeit ist gesetzlich nicht vorgeschrieben. Nichtsdestotrotz sind Vereinbarungen für eine Probezeit im Arbeitsvertrag heutzutage aber üblich. Zur maximalen Länge der Probezeit enthält das BGB jedoch eine Regelung: Nach § 622 Abs. 3 BGB darf die vereinbarte Probezeit eine Dauer von sechs Monaten nicht überschreiten.

Dass Arbeitgeber hier aber auch durchaus in datenschutzrechtliche Fallstricke geraten können, zeigt ein Fall, den die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BInBDI) in ihrem aktuellen Tätigkeitsbericht 2021 schildert (Ziffer 8.1. Beschäftigtendatenschutz).

Weiter auf DataAgenda lesen

Zulässige Erhebung privater Kontaktdaten von Beschäftigten

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI), Prof. Dr. Dieter Kugelmann, hat Anfang Mai 2022 den 29. Tätigkeitsbericht zum Datenschutz veröffentlicht.
Unter Ziffer 6 des Tätigkeitsberichts bespricht der LfDI RLP einige Fragen aus dem Bereich des Beschäftigtendatenschutzes, die sich der Behörde vor dem Hintergrund der Bekämpfung der Corona-Pandemie gestellt haben.
Konkret geht es darum, ob und wenn ja in welchem Umfang der Arbeitgeber/Dienstherr private Kontaktdaten von Beschäftigten erheben darf. Obwohl sich der LfDI RLP bei der Beantwortung nach § 20 Abs. 1 Landesdatenschutzgesetz (LDSG) orientiert, können die dort getroffenen Abwägungen und insbesondere die Vornahme dieser Abwägungen an der Erforderlichkeit der Datenverarbeitung, naturgemäß auch bei einer Prüfung anhand des § 26 BDSG, vorgenommen werden.

Weiter auf DataAgenda lesen

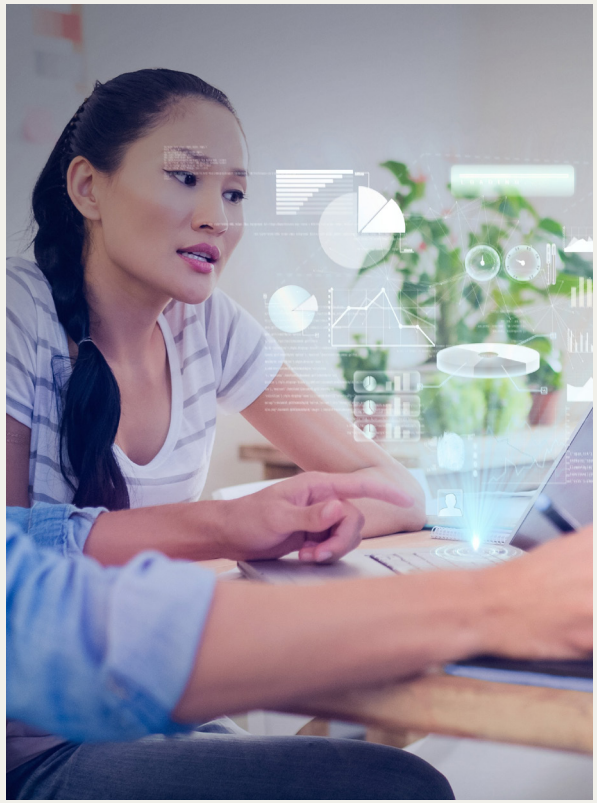

Foto: vectorfusionart, Adobe Stock

Foto: Sikov, Adobe Stock

Gesonderte Entgeltpflicht für Kontrollen/Audit bei der Auftragsverarbeitung?

Im Rahmen seiner sog. „Aktuellen Kurzinformationen 6 “ (AKI) wies der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) bereits 2018 auf einen Umstand hin, der die Parteien einer Auftragsverarbeitung beschäftigen kann.

Es kommt nicht selten vor, dass Vereinbarungen zur Auftragsverarbeitung vorsehen, dass es dem Auftraggeber nur gegen Zahlung eines besonderen Entgelts möglich sein soll, eine Vor-Ort-Kontrolle bei dem Auftragsverarbeiter durchzuführen.

Weiter auf DataAgenda lesen

Foto: William W. Potter, Adobe Stock

DSK sieht Gast-Zugang als Voraussetzung für datenschutzkonformen Online-Handel

Der aktuelle Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder dürfte einige Online-Händler aufgeschreckt haben, da die Umsetzung dieses „Beschlusses" (Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang) mit zusätzlichem Aufwand und somit auch mit zusätzlichen Kosten verbunden sein dürfte.

Im Kern fordert der Beschluss Folgendes:
*„Verantwortliche, die Waren oder Dienstleistungen im Online-Handel anbieten, müssen ihren Kund*innen unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kund*innenkonto) zur Verfügung stellen, grundsätzlich einen Gast-Zugang (Online-Geschäft ohne Anlegen eines fortlaufenden Kund*innenkontos) für die Bestellung bereitstellen."*

Die Nutzer von solchen Gast-Konten und damit die Betroffenen dürften ein nachvollziehbares Interesse daran haben, dass der Beschluss in der Praxis Akzeptanz findet. Kundenkontos erleichtern die Bestellungen im Online-Handel, bedeuten aber für den Kunden, der „eben mal nur etwas bestellen möchte", dass er den gewünschten Kauf nicht tätigen kann, ohne eine Reihe von personenbezogenen Daten zu hinterlassen und diese dann auch für längere Zeit gespeichert bleiben. Sieht der Onlineshop die Eröffnung eines Kundenkontos vor, lässt sich die Zusammenführung der gesammelten Kundendaten als Datenverarbeitung im Sinne von Art. 4 DS-GVO betrachten.

Sucht man nach einem Erlaubnistatbestand für diese Datenverarbeitung, gelangt man zu dem Fazit, dass diese Verarbeitung über eine Einwilligung des Kunden zu legitimieren ist. Die erforderliche Einwilligung in die Datenverarbeitung ist nach der DS-GVO nur wirksam, wenn diese vom Kunden auch freiwillig erteilt worden ist (vgl. Art. 7 Abs. 4 DS-GVO). Das ist zumindest die Herleitung der DSK für die von ihr aufgestellten weiteren Kernforderungen:

- Ohne einen Gast-Zugang bzw. ohne eine gleichwertige Bestellmöglichkeit kann die Freiwilligkeit einer Einwilligung nicht gewährleistet werden.
- Die mit einem fortlaufenden Online-Konto verbundenen Möglichkeiten der Auswertung der Vertragshistorie für Werbezwecke sowie die Speicherung von Informationen über Zahlungsmittel bedürfen einer informierten Einwilligung.
- Die von den Verantwortlichen verarbeiteten Daten müssen in einer für die Kund*innen transparenten Weise verarbeitet werden.

Foto: peterschreiber.media, Adobe Stock

Bußgelder für Datenschutzverstöße sollen europaweit harmonisiert werden

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits im Oktober 2019 ihr angekündigtes Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DS-GVO durch Unternehmen vorgelegt. Das Konzept für Bußgeldzumessung gestaltete im Wesentlichen die Vorgaben des Art. 83 DS-GVO aus und war auf Fortentwicklung angelegt. Ziel des Konzepts war es, den Datenschutzaufsichtsbehörden eine einheitliche Methode für eine systematische, transparente und nachvollziehbare Bemessung von Geldbußen zur Verfügung zu stellen.

Mit der Veröffentlichung des Konzeptes zur Bemessung von Geldbußen sollte nach Auffassung der deutschen Datenschutz-Aufsichtsbehörden ein Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts geleistet werden, so die DSK in ihrem damaligen Konzeptpapier. Es sollte Verantwortliche und Auftragsverarbeiter in die Lage versetzen, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen. Die Aufsichtsbehörden wiesen bereits in dem damaligen Papier darauf hin, dass die vorgestellten Leitlinien nicht als erschöpfend zu verstehen sind, und die Konkretisierung der Festsetzungsmethodik späteren Leitlinien des EDSA (Europäischer Datenschutzausschuss) vorbehalten bleibe.

Eine solche Leitlinie zur Bußgeldbemessung hat der EDSA („Guidelines on the calculation of fines“) nun vorgestellt.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, sieht eine weitere Harmonisierung der europäischen Bußgeldpraxis als wesentliches Ziel der Leitlinien.
Neben Regelungen zur maximalen Bußgeldhöhe sei Kernelement der Leitlinien – ähnlich wie im Bußgeldkonzept der DSK – die Festlegung eines Grundbetrags („starting point“) für die Zumessung. Dieser bestimme sich aus drei Größen:

- der Einordnung der Tat anhand der verletzten Norm,
- der Schwere der konkreten Tat sowie
- des Unternehmensumsatzes.

So sei beispielsweise der Grundbetrag, welcher bei mittelschweren Verstößen bis zu 20 Prozent der gesetzlichen Bußgeldgrenze betragen kann, bei Kleinstunternehmen mit einem Umsatz von höchstens 2 Millionen Euro auf 0,2 Prozent dieses Betrags zu reduzieren. Der EDSA mache damit deutlich, dass der Unternehmensumsatz auch für die konkrete Bußgeldberechnung eine maßgebliche Größe ist, Bußgelder umgekehrt die Unternehmen auch nicht überfordern dürfen.

Foto: Daniel Jędzura, Adobe Stock

BfDI genehmigt Code of Conduct für Notare

Die Datenschutz-Grundverordnung (DS-GVO) bietet mit den sog. Verhaltensregeln (oft auch „Code of Conduct" CoC genannt) nach Art. 40 DS-GVO ein Instrument der Selbstregulierung. Branchenverbände und andere Vereinigungen, die von dieser Möglichkeit Gebrauch machen, können damit die z.T. abstrakten Vorgaben der DS-GVO für ihren Geschäftsbereich konkretisieren.

Nach Erwägungsgrund 98 der DS-GVO sollen Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist.

Zwar kann ein Branchenverband grundsätzlich ohne Beachtung bestimmter Vorgaben Selbstverpflichtungen für seine Mitglieder entwerfen und intern für verbindlich erklären. Die im Datenschutzrecht für Verhaltensregeln vorgesehenen Rechtswirkungen treten aber nur ein, wenn das in Art. 40 DSGVO vorgesehene Verfahren zum Erlass solcher Codes of Conduct eingehalten wird.
Schon das BayLDA stellte in seinem Papier Verhaltensregeln – Art. 40 DS-GVO fest, dass Branchenverbände dieses Instrument sehr zögerlich in Anspruch nehmen. Die DS-GVO versuche weitere Anreize zu schaffen. Es werde sich zeigen, ob diese ausreichen, damit künftig mehr Branchen sich solchen Regelungen unterwerfen. Vor allem zum Nachweis der in der DS-GVO in unterschiedlichem Kontext oft genannten Garantien könnten Verhaltensregeln hilfreich sein, Rechtssicherheit zu schaffen, so die damalige Prognose des BayLDA.

Nun hat Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Anfang Mai 2022 erstmalig eine Genehmigung auf Bundesebene nach Art. 40 DS-GVO erteilt. Konkret geht es um datenschutzrechtliche Verhaltensregeln zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf elektronische Aufzeichnungen und Hilfsmitteln.
Die Bundesnotarkammer hatte auf ihrer 125. Generalversammlung einen Entwurf der Verhaltensregeln beschlossen und dem BfDI als zuständiger Aufsichtsbehörde zur Genehmigung vorgelegt.
Ziel dieser Verhaltensregeln ist es, zum einen den Notarinnen und Notaren für die Umsetzung der technischen und organisatorischen Maßnahmen ein Regelwerk an die Hand zu geben und so mehr Klarheit für die Praxis zu schaffen und zum anderen den Bürgerinnen und Bürgern die Sicherheit zu geben, dass ihre personenbezogenen Daten bundesweit durch Notarinnen und Notare auf einem einheitlichen und verbindlichen Schutzniveau verarbeitet werden.

Folge #18

A fair AI regulation for fair competition – global economy meets EU politics

DataAgenda Podcast

DataAgenda Podcast „Der Experten-Talk" mit Prof. Schwartmann – Meinungen, kontroverse Diskussionen und die Einordnung von aktuellen Datenschutz-Themen – das bietet in kurzweiligen Talks der neue DataAgenda Datenschutz Podcast. Mit immer wechselnden Gesprächspartnern aus der deutschen Datenschutzszene bringt Herr Prof. Schwartmann die aktuell spannenden Themen auf den Punkt, verständlich und informativ.

Folge 18: A fair AI regulation for fair competition – global economy meets EU politics

The European Union's AI Regulation is an important building block of the EU data strategy. According to current plans, it is to be adopted by the end of 2022. The EU wants to establish a special right for high-risk applications in the field of AI, which could be monitored by a new body to be created. The AI Regulation must follow the one risk-based approach of the GDPR. On this basis, it must not overstretch the legal requirements for risks of AI applications. The AI Regulation must also set a framework that makes applications from Europe fair and economically feasible. In DataAgenda Podcast Monish Darda, one of the two founders and CTO of ICERTIS, a global leader in contract software, based on AI discusses with Axel Voß. He is a member of the European Parliament and the European Parliament's rapporteur for the AI Regulation.
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Foto: Suphachai, Adobe Stock

Vor-Ort-Kontrolle der Aufsichtsbehörde: Wie vorbereiten?

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel, hat am 2. Juni 2022 im Innenausschuss des Niedersächsischen Landtags ihren Tätigkeitsbericht für 2021 vorgestellt. Darin berichtet sie über die Nachkontrollen, die im Jahr 2021 abgeschlossen werden konnten, nachdem diese bereits anlässlich der Querschnittsprüfung von Wirtschaftsunternehmen aus dem Jahre 2018 initiiert worden waren (Abschnitt 6.1.).

Hilfreich sind die Hinweise der LfD Niedersachsen, wie sich Verantwortliche auf Vor-Ort-Kontrollen vorbereiten sollten:

Es ist insbesondere ratsam,

- die vorhandene Datenschutzdokumentation zu sichten, Lücken zu identifizieren und zu füllen;
- zu prüfen, ob die Dokumente aktuell sind oder ob sich seit der Erstellung der Dokumente Veränderungen ergeben haben, die noch nicht berücksichtigt wurden;
- die Dokumentation so zu ordnen, dass während der Vor-Ort-Kontrolle Unterlagen auf Anfrage unmittelbar vorgelegt werden können;
- die eigene Dokumentation auf Widersprüche zu prüfen;
- Abweichungen von den einschlägigen Veröffentlichungen meiner Behörde, der Datenschutzkonferenz und des Europäischen Datenschutzausschusses zu prüfen;
- den Datenschutzbeauftragten des Unternehmens bei der Vorbereitung eng einzubinden;
- ggf. einen externen Datenschutzberater einen unbefangenen Blick auf die Umsetzung des Datenschutzrechts im Unternehmen werfen zu lassen;
- die Verfügbarkeit der Verantwortlichen aus den jeweiligen Fachbereichen für den Kontrolltermin sicherzustellen, die tiefergehende Nachfragen zu einzelnen Verarbeitungstätigkeiten beantworten können;
- einen Umsetzungsplan zu erstellen, welcher der Aufsichtsbehörde vorgelegt werden kann, falls bis zur Vor-Ort-Kontrolle nicht alle Dokumente erstellt oder technisch-organisatorischen Maßnahmen implementiert werden konnten.

Wie anschließend das weitere Verfahren verlaufe und ob es zu einem Bußgeld und/oder aufsichtsbehördlichen Maßnahmen komme, sei immer eine Frage des Einzelfalls und hänge von den in der Vor-Ort-Kontrolle gemachten Feststellungen ab.

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