NEWS BOX DATENSCHUTZ

AUSGABE
10/2021

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Würde eine Auszeichnung „Innovativste Deutsche Datenschutz-Aufsichtsbehörde“ existieren, stünde der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) ganz weit oben auf der Anwärter-Liste für diesen noch nicht-existierenden Preis.

Eine App gehört mittlerweile zum guten Ton. Hat der LfDI BW zwar noch nicht so lange, aber dafür muss sich der Nutzer nicht als Early Adopter und Beta-Tester missbrauchen lassen. Die App hat den versprochenen Mehrwert und tut, was sie soll. Einziger Wermutstropfen bislang: Die App funktioniert derzeit auf Apple-Geräten ab Betriebssystem 13.5. Es ist geplant, die App regelmäßig zu aktualisieren. Eine Android-Version der App ist derzeit in Entwicklung und soll bis Ende des Jahres ebenfalls veröffentlicht werden.
Schmankerl: Bürger*innen können auch via App Beschwerden beim LfDI einreichen.

Die neueste Innovation aber ist das sog. LfDI-Tool DS-GVO.clever.
Korrekte Datenschutzerklärungen zu formulieren fällt insbesondere kleineren Unternehmen und Vereinen schwer, da sie nicht über die Ressourcen verfügen, externe Datenschutzbeauftragte einzuschalten oder mit der eigenen Rechtsabteilung tätig zu werden. Externe DSB und sonstige Datenschutzberater werden also nicht sofort arbeitslos durch diesen Legal-Tech-Service, aber vielen Verantwortlichen dürfte diese Service-Offensive des LfDI BW gerade Recht kommen, wenn sie sich über drei Jahre nach Wirksamwerden der DS-GVO so langsam mit dem Thema Datenschutzerklärungen beschäftigen möchten.
Man darf gespannt sein, was die Aufsichtsbehörde aus Baden-Württemberg für die nächsten Jahre noch so im Köcher hat.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Tanja Esser, Adobe Stock

Von Goslar über Bundesverfassungsgericht bis zum Europäischen Gerichtshof

Urteil: AG Goslar, Urteil v. 27.09.2019, Az.: 28 C 7/19

Ein Rechtsanwalt forderte auf Grundlage des Art. 82 DS-GVO einen immateriellen Schadensersatz von 500,- €, da er ohne seine Einwilligung eine Werbe-E-Mail erhalten hat. Das AG Goslar lehnte den Anspruch auf Schadenersatz ab, da dem Gericht die Erheblichkeit des Rechtsverstoßes fehlte (AG Goslar, Urteil v. 27.09.2019, Az.: 28 C 7/19) . Das Gericht begründete seine Entscheidung damit, dass es sich lediglich um eine E-Mail gehandelt hat und diese als Werbung erkennbar war und der Kläger sich deshalb nicht länger damit befassen hätte müssen. Somit sei weder ein materieller noch ein immaterieller Schaden entstanden. Der Kläger legte daraufhin eine Verfassungsbeschwerde beim Bundesverfassungsgericht (BVerfG) vor, weil Rechtsmittel gegen die Entscheidung des Amtsgerichts nicht zugelassen waren.

Weiter auf DataAgenda lesen

Nutzung von Fax-Diensten bei sensiblen Daten unzulässig

Seit der offiziellen Einführung des Faxdienstes in Deutschland durch die damalige Deutsche Bundespost sind mehr als 40 Jahre vergangen. Der Faxdienst wird in Deutschland damit fast genauso lange genutzt, wie es Videotext (Teletext) gibt. Beide Dienste erfreuen sich in Deutschland eines Nutzerkreises in Millionenhöhe.
Geht es nach dem Willen der deutschen Datenschutz-Aufsichtsbehörden geht es einem der Dienste bald an den Kragen. Ein Hinweis darauf, dass das Ende des Faxdienstes besiegelt sein dürfte, sind die regelmäßigen kritischen Äußerungen diverser Aufsichtsbehörden. Auch wenn es so kommen sollte, wird das Fax Dienste wie De-Mail um Jahre überlebt haben.

Weiter auf DataAgenda lesen

Foto: suksawad, Adobe Stock

45. DAFTA

40. RDV-FORUM

Datenschutz im Umbruch: Online-Datenschutz - Internationaler Datentransfer - Schadensersatz für Datenschutzverletzungen

Jetzt anmelden:
datakontext.com/dafta-2021

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: New Africa, Adobe Stock

Datenschutz auf Fetisch-Portalen

Datenschutz ist als Querschnittsmaterie bekannt. Dies wird typischerweise so verstanden, dass er in allen Fachbereichen erforderlich ist, d.h. unabhängig von der konkreten Anwendung überall dort, wo personenbezogene Daten auftreten.
Es ist also egal, ob die Verarbeitung von personenbezogenen Daten in einem ERP-System innerhalb eines Konzernverbundes, bei einer Bäckerei, im Kleintierzuchtverein – oder auf einem Fetisch-Portal für getragene Unterwäsche erfolgt.
Genau mit so einem Portal beschäftigt sich der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg (HmbBfDI) in seinem 29. Tätigkeitsbericht (Abschnitt V. 8.) und beschreibt das Geschäftsmodell in aller Nüchternheit wie folgt:

„Der HmbBfDI hat einen Bußgeldbescheid gegen ein Unternehmen erlassen, das einen Online-Marktplatz insbesondere für getragene Unterwäsche betreibt. Der Shop richtet sich an Kunden, die ein Interesse daran haben, unterschiedlich lange getragene Unterwäsche mit entsprechend intensivem Eigengeruch zu erwerben. Das Unternehmen wirbt damit, hundertprozentige Anonymität zu gewährleisten."

Dass das Geschäftsmodell dem HmbBfDI zu Recht egal ist und es der Behörde ausschließlich um die Einhaltung datenschutzrechtlicher Anforderungen ankommt, lässt sich an der mustergültigen juristischen Prüfung und Subsumtion ablesen. Was war passiert?

Der HmbBfDI erhielt Hinweise, dass zahlreiche, auf dem Portal hochgeladene Fotos, GPS-Koordinaten von Nutzerinnen der Plattform enthielten. Eine Überprüfung bestätigte diesen Hinweis. Die Behörde konnte verifizieren, dass die Restinformationen bzw. Metadaten bei den hochgeladenen Fotos nicht bereinigt worden waren. Folglich konnten die Daten bei beliebigen Kartendiensten eingegeben und der genaue Standort ermittelt werden, an dem das Foto erstellt wurde. Teilweise waren zusätzlich Höheninformationen in den Bildern vermerkt, die eine grobe Aussage über das im Aufnahmemoment bewohnte Stockwerk ermöglichten. Die Zahl der betroffenen Personen belief sich im Kontrollzeitraum auf ca. 760 Frauen zwischen 18 und 50 Jahren. Auf den Amateuraufnahmen wurden die Betroffenen in Unterwäsche abgebildet. Bei einigen Fotos war auch das Gesicht erkennbar.

Welche Verstöße der HmbBfDI daraus ableitete und von welchen rechtlichen Erwägungen er sich leiten ließ, lesen Sie weiter auf DataAgenda

Foto: Thomas Reimer, Adobe Stock

HmbBfDI: Über 900.000 Bußgeld EUR gegen Vattenfall

Derzeit können Kunden bei der Wahl des Strom- und Gasanbieters durch einen regelmäßigen Preisvergleich und den Wechsel des Anbieters von günstigeren Preisen oder besonderen Angeboten für Neukunden profitieren.
Häufig wechselnde Kunden sind für die Unternehmen jedoch weniger interessant als langfristige Kunden. Aus diesem Grund haben die Anbieter ein Interesse daran, möglichst schon vor Vertragsabschluss in Erfahrung zu bringen, wie häufig potenzielle Kunden ihren Energieanbieter wechseln. Bereits letztes Jahr hatte der „Arbeitskreis Auskunfteien" des DSK die Arbeit zu dieser Thematik aufgenommen, die vor allem Verbraucher interessieren dürfte, welche häufig ihren Energieversorger wechseln, um jederzeit den optimalen Tarif für sich zu beanspruchen.

„Aus Sicht des Arbeitskreises bestehen erhebliche Zweifel an der Verarbeitung von Positivdaten wie Angaben zur Vertragsdauer durch Wirtschaftsauskunfteien im Bereich der Energieversorgungsbranche auf der Grundlage des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO. Positivdaten sind Informationen, die keine negativen Zahlungserfahrungen oder anderes nicht vertragsgemäßes Verhalten zum Inhalt haben. Dieses Ergebnis des Arbeitskreises soll der Datenschutzkonferenz als Entscheidungsvorlage zugeleitet werden", so Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz bereits im Jahre 2020.
Dieser Problematik („Bonushopper") dürfte die aktuelle Pressemitteilung des Energieversorgers Vattenfall zuzuordnen sein. Der Meldung ist zu entnehmen, dass die Hamburgische Datenschutzbeauftragte ein Bußgeld in Höhe von gut 900.000 Euro verhängt hat.
Der hauseigenen Mitteilung des Energieversorgers kann weiter entnommen werden, dass das Bußgeld auf fehlende Transparenzinformation nach den Art. 12, 13 DS-GVO gestützt wird. Der HmbBfDI habe die notwendige Aufklärung der betroffenen Kunden über den konkreten Abgleich ihrer Daten bemängelt.
Dass sich ein Verantwortlicher auch bei Zahlung eines sechsstelligen Bußgelds als „Gewinner" eines aufsichtsbehördlichen Verfahrens betrachten kann, zeigt der Fall von Vattenfall. Fokussiert man das Verfahren auf die Frage, ob die Behörde den Fall als schwerwiegenden Datenschutzverstoß bewertet hat, kann diese Ansicht von Vattenfall auch durchaus verständlich sein. Vattenfall weist in der Pressemitteilung darauf hin, dass „die Datenschutzbehörde betont habe, dass es sich um keinen schwerwiegenden und darüber hinaus erstmaligen Verstoß handele. Die Kundendaten der Vattenfall Europe Sales GmbH seien zu keinem Zeitpunkt gefährdet oder Missbrauch ausgesetzt gewesen, lediglich die Transparenz sei aus Sicht der Behörde zu verbessern gewesen".

Foto: Janet Worg, Adobe Stock

Abfrage des Impfstatus auch nicht durch Einwilligung legitimierbar

Eine aktuelle Bewertung zu der immer noch heiklen und äußerst praxisrelevanten Frage, ob und in welchen Fällen der Arbeitgeber den Impfstatus eines Arbeitnehmers abfragen darf, kommt von dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA).
Vor Kurzem wurde hier noch darauf eingegangen, dass in Datenschutzkreisen diskutiert wird, ob durch eine Gesamtschau der Normenkette §§ 22, 26 III BDSG, 241 II, 242, 618 BGB, §§ 3, 5, 16 ArbSchG (Arbeitsschutzgesetz) in Verbindung mit Art. 9 II lit. b), Erwägungsgrund 46 DS-GVO eine Verarbeitung der Daten zum Impfstatus allen Verantwortlichen erlaubt sein könnte. Dieser Vermutung erteilt das BayLDA eine klare Absage und stellt fest, dass die Verarbeitung von Impfdaten durch Arbeitgeber nur für besondere Gründe der Pandemiebekämpfung gesetzlich festgelegt und nur in den in § 23a IfSG und in § 36 Abs. 3 IfSG genannten eng begrenzten Fällen vorgesehen sei. § 36 Abs.3 IfSG setze dabei die Feststellung einer epidemische Lage von nationaler Tragweite durch den Deutschen Bundestag nach § 5 Abs. 1 S. 1 IfSG (derzeit bis zum 24.11.2021) voraus und erlaube eine Abfrage nur insoweit, als dies zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 (COVID-19) erforderlich sei.
Angesichts der ausdrücklichen gesetzgeberischen Entscheidung lasse sich ein allgemeines Fragerecht auch nicht aus Gesichtspunkten des Arbeitsschutzes und der Fürsorgepflicht für die Belegschaft ableiten (insbesondere § 3 Abs. 1 Arbeitsschutzgesetz, §§ 2-4 Corona-ArbSchV i.V.m. § 26 Abs. 3 BDSG). Die SARS-Cov-2 Arbeitsschutzverordnung unterscheide nicht zwischen geimpften und nicht geimpften Beschäftigten und enthalte auch keine Verpflichtung der Beschäftigten, dem Arbeitgeber Auskunft über ihren Impf- oder Genesungsstatus zu erteilen.
Ein Fragerecht des Arbeitgebers nach dem Impfstatus von Beschäftigten bestehe damit, außer in den gesetzlich ausdrücklich genannten Fällen gemäß §§ 23a und künftig § 36 Abs.3 IfSG, nicht.
Auch Verantwortliche, die an eine Einwilligungslösung gedacht haben, um Abfragen zum Impfstatus verarbeiten zu können, werden enttäuscht: Auch auf der Basis einer Einwilligung kommt nach Auffassung des BayLDA eine Abfrage des Impfstatus grundsätzlich nicht in Betracht. Einwilligungen müssten den Anforderungen des Art. 7 und der Erwägungsgründe 32, 42 und 43 DS-GVO genügen (insbesondere Freiwilligkeit). Dies sei infolge der Abhängigkeiten im Beschäftigungsverhältnis in der Regel nicht gegeben.
Einziger Lichtblick für eine pragmatische Lösung in Einzelfällen dürfte sein, dass nach der Bewertung des BayLDA ein Arbeitgeber aber befugt sein könne, den Impfstatus zumindest zu erheben bzw. zur Kenntnis zu nehmen, wenn er vom Beschäftigten freiwillig angegeben werde, um sich gemäß geltender landesrechtlicher Vorschriften zur Pandemie-Eindämmung von einer gesetzlich geregelten Pflicht zur Testung zu befreien.

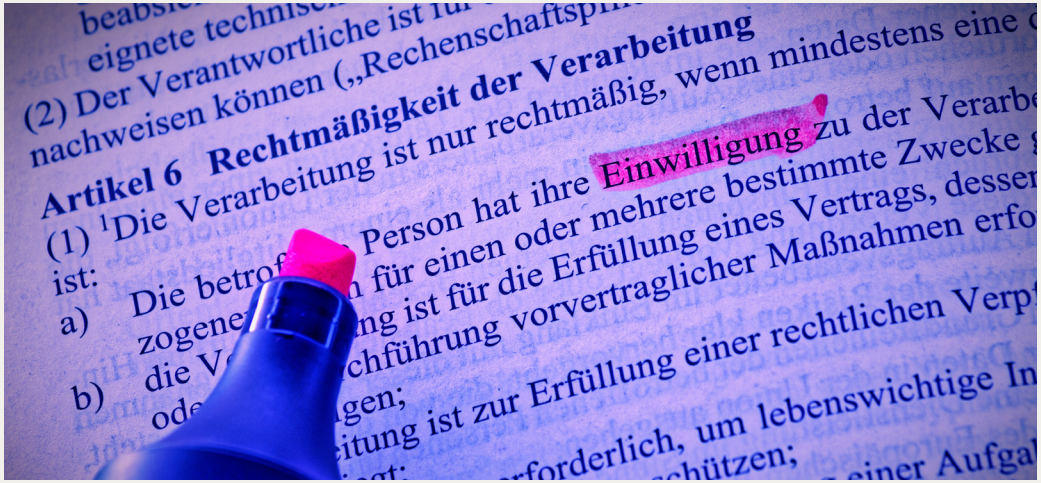

Foto: DatenschutzStockfoto, Adobe Stock

Einwilligung nach der DS-GVO (im öffentlichen Bereich)

Art. 4 Nr. 11 DS-GVO definiert die Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist." Die Einwilligung ist daher einerseits Betroffenenrecht, da sie der betroffenen Person die Möglichkeit gibt, aktiv über die Verarbeitung, ihre Zwecke und näheren Umstände zu bestimmen. Andererseits ist sie aus Sicht des Verantwortlichen ein vollgültiger Erlaubnistatbestand im Sinne von Art. 6 Abs. 1 lit. a DS-GVO.

Weiter auf DataAgenda lesen

Verwarnung wegen Mitarbeiterexzess

Regel: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten
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. Dabei sei nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen. Diese Haftung für Mitarbeiterverschulden ergebe sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besage, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist.

Foto: Robert Kneschke, Adobe Stock

Weiter auf DataAgenda lesen

Folge 9: Hidden Champions aktueller Datenschutzfragen – TTDSG und Löschen und Sperren als Schaden nach DS-GVO

Rolf Schwartmann im Gespräch mit Kristin Benedikt zu den Auswirkungen der Rechtsprechung des Bundesgerichtshofs zum Löschen und Sperren von Inhalten auf Sozialen Netzwerken auf Schadensersatzansprüche gegen die Anbieter nach Art. 82 DS-GVO. Zudem geht es um die Auswirkungen des im Dezember 2021 in Kraft tretenden Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) auf den Onlinedatenschutz.
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