Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2017

Liebe Leserin, lieber Leser,

der „Standort Hannover“ ist seit dem 15.08.2017 nun tatsächlich einer: aus dem beschaulichen Burgwedel sind wir direkt in Hannovers Innenstadt an den Thielenplatz 3 gezogen. Schauen Sie gern einmal vorbei wenn Sie in der Nähe sind.

Während wir uns in den kommenden Wochen nun weiter einrichten, wünschen wir Ihnen in der Zwischenzeit interessante Einblicke und Anregungen mit der vorliegenden Ausgabe unseres Kundenmagazins. Gleich auf der ersten Seite beleuchten wir beispielsweise eine neue Generation von „Haushaltsgeräten“ wie Google Home bzw. Amazon Echo.

Wir wünschen wieder eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

© K. Borchhardt
www.miniansichten.de

Wenn der Lautsprecher zuhört

Ein modernes Webradio in der Teeküche sorgt nicht nur für schöne Musik und aktuelle Wetterdaten, es kann auch zu einem echten Datenrisiko werden. Denn in immer mehr Geräten stecken Assistenten wie Alexa, die dauerhaft lauschen.

Gute Musik hebt die Stimmung, aktuelle Wetterinformationen helfen bei der Planung von Dienstreisen und Events. Da macht ein Webradio im Büro oder in der Teeküche schon Sinn. Dank Online-Verbindung bieten die Internetradios zahlreiche Radiosender, ob national oder international.

Doch die neuen Webradios können mehr: Über die Geräte lassen sich

In dieser Ausgabe:

Wenn der Lautsprecher zuhört	**1**
Optimierung des Fahrverhaltens – oder Kündigung!	**3**
Datenschutzbeauftragte jetzt überall in der EU	**5**
Künstliche Intelligenz: Was die schlaue IT über uns wissen könnte	**6**
Tipps zur Prüfung einer Datenschutzerklärung	**8**
Arbeitshilfen und Muster zur Datenschutzgrundverordnung	**10**
Aktuelles	**11**

digitale Assistenten wie Alexa nutzen. Fragen Sie also das Küchenradio nach dem aktuellen Wetter – und Sie bekommen eine Sprachantwort. Sogar moderne Lautsprecher, mit denen sich Musik vom Smartphone hören lässt, haben inzwischen Alexa oder einen anderen digitalen Assistenten wie Siri an Bord. Deshalb wissen auch Lautsprecher, wie das Wetter wird.

Schlaue Radios mit Nebenwirkung

Die Frage ist allerdings, was sie noch alles wissen oder hören: Solche Webradios und Lautsprecher verfügen für die Spracheingabe über Mikrofone. Und die sind in aller Regel immer aktiv.

Damit der digitale Assistent im Webradio oder im Lautsprecher auf Zuruf den Radiosender oder das abgespielte Lied ändern oder die aktuellen Wetterdaten vorlesen kann, muss er den Nutzer hören können. Das gilt für Smartphones und Tablets genauso, die im Fall von Android auf „Ok Google“ reagieren. Das ist nur möglich, wenn sie bereits vor den Worten „Ok Google“ oder „Hi Alexa“ zuhören.

Immer auf Empfang, auch das Mikrofon

Bei bestehender Internetverbindung hören die Webradios und Lautsprecher nicht nur zu, sie speichern auch die gesprochenen Worte, in der Regel in der Cloud des jeweiligen digitalen Assistenten.

Im Fall eines Webradios oder Lautsprechers mit Alexa an Bord werden die Worte, die das Mikrofon empfängt, in einer Amazon-Cloud gespeichert. Beendet man die Internetverbindung, wird die Aufzeichnung gestoppt – aber dafür geht das Webradio dann auch nicht mehr.

Vertrauliche Gespräche im Büro oder in der Teeküche: Lieber nicht!

So schön die reiche Auswahl an Radiosendern bei Webradios auch ist, so toll es sein kann, die Smartphone-Musik auf den Lautsprecher in der Teeküche zu übertragen und so praktisch der Wetterbericht auf Zuruf sein kann: Wer vertraulich im Büro oder an einem anderen Ort sprechen will, sollte auf Geräte verzichten, die immer zuhören könnten. Das können heute sogar Lautsprecher sein, die früher nicht zuhörten, sondern nur Töne von sich gaben.

Es ist damit zu rechnen, dass digitale Assistenten wie Alexa in immer mehr Geräte Einzug halten werden, und damit auch Mikrofone, die aktiv geschaltet sind, das gesprochene Wort aufnehmen und in eine Cloud übertragen. Nicht nur bei Lebensmitteln sollte man also fragen, was alles drin ist, sondern auch bei Geräten. &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, Thomas Althammer

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

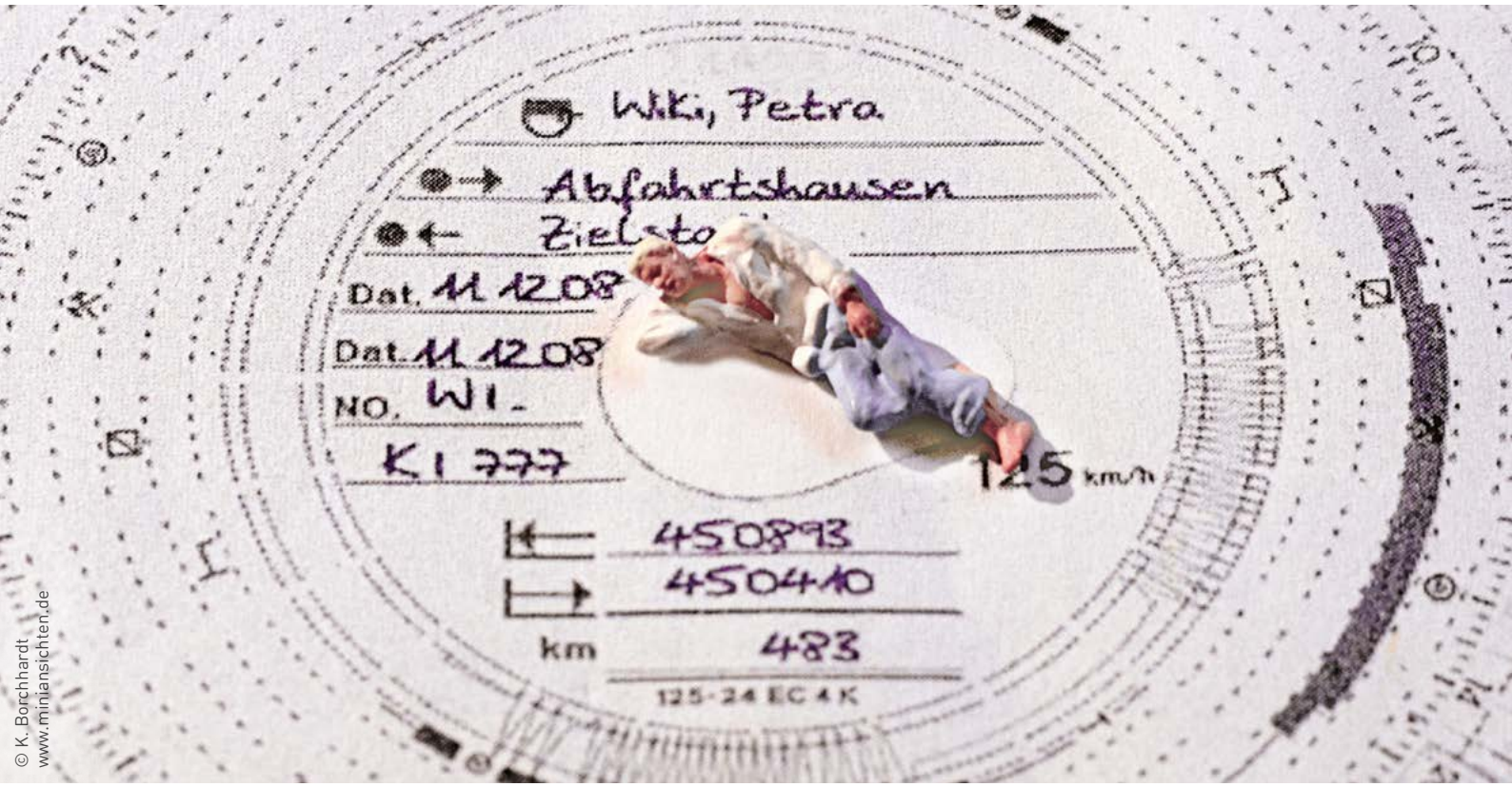
Anschrift:
Althammer & Kill GmbH & Co. KG
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Schutzgebühr Print-Ausgabe: 10,– €

3

Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2017

ALTHAMMER & KILL



Optimierung des Fahrverhaltens – oder Kündigung!

Ein Arbeitgeber möchte das Fahrverhalten seiner Berufskraftfahrer optimieren. Deshalb installiert er in den Fahrzeugen ein System namens RIBAS. Ein altgedienter Fahrer hält das alles für Unfug und aktiviert das System nicht. Sage und schreibe drei Mal mahnt ihn der Arbeitgeber ab. Auch das hilft nicht. Da kündigt ihm der Arbeitgeber. Wird die Kündigung vor den Gerichten Bestand haben?

Ein Nahverkehrsunternehmen will den Fahrkomfort für die Fahrgäste verbessern und außerdem Sprit sparen. Deshalb lässt es in seinen Bussen ein System mit Namen RIBAS installieren. Es ist inzwischen in ganz Deutschland weit verbreitet.

Es geht um Geld und um Fahrkomfort

Wenn ein Busfahrer zu hochtourig fährt, zu scharf bremst, überhöht beschleunigt oder die zulässige Geschwindigkeit überschreitet, leuchtet eine Warnlampe auf. Außerdem zeichnet das System die entsprechenden Daten solcher Vorfälle auf. Eine dauernde Aufzeichnung von Fahrdaten erfolgt dagegen nicht. Falls ein Busfahrer wiederholt auffällt, muss er an einer Schulung teilnehmen.

Betriebsvereinbarung für ein Überwachungssystem

Im Unternehmen besteht eine Betriebsvereinbarung. Gemäß dieser Betriebsvereinbarung muss jeder Fahrer an dem System teilnehmen. Das kann auf zwei verschiedene Weisen geschehen. Sofern der Fahrer damit einverstanden ist, ordnet das System die Daten immer sofort seiner Person zu. Kommt es zu keinen oder nur zu geringen Auffälligkeiten, hat er die Chance, deshalb eine Prämie zu bekommen.

Anonymisierter Systemschlüssel

Möchte der Fahrer dies nicht, bekommt er dagegen einen sogenannten anonymisierten Systemschlüssel. In diesem Fall werden die Daten erst dann seiner Person zugeordnet, wenn ein Vergleich zwischen allen Busfahrern ergibt, dass einzelne Busfahrer besonders auffallen. Sie werden dann „heraussortiert“. Diese

Zuordnung erfolgt in Abstimmung mit dem Betriebsrat.

Drei erfolglose Abmahnungen

Ein seit langen Jahren bei dem Unternehmen tätiger Fahrer sah nicht ein, warum er sich an einem solchen System beteiligen solle. Er verweigerte jede Mitwirkung. Deshalb mahnte ihn der Arbeitgeber dreimal ab. Als auch das keine Wirkung zeigte, kündigte ihm der Arbeitgeber.

Außerordentliche Kündigung

Diese Kündigung erfolgte in Form einer außerordentlichen Kündigung. Der Grund: Wegen seiner langen Betriebszugehörigkeit konnte dem Busfahrer nur noch „aus wichtigem Grund" gekündigt werden. Das ergab sich aus dem Tarifvertrag. Der Busfahrer ging davon aus, dass ihm wegen dieses besonderen Schutzes nichts passieren könne. Beim Bundesarbeitsgericht erlebte er allerdings eine herbe Enttäuschung.

Zulässige Betriebsvereinbarung

Nach Auffassung des Bundesarbeitsgerichts kann eine Betriebsvereinbarung festlegen, dass Arbeitnehmer bei einem solchen System mitwirken. Das Persönlichkeitsrecht wird dadurch nicht unzulässig beeinträchtigt.

Wichtig: keine Dauerüberwachung

Dabei spielt es eine besondere Rolle, dass keine Dauerüberwachung erfolgt. Es werden lediglich einzelne negative Ereignisse aufgezeichnet. Der Arbeitgeber verfolgt mit dem System legitime Ziele, nämlich die Einsparung von Sprit und einen besseren Komfort für die Fahrgäste. Das System ist dazu geeignet, diese Ziele zu erreichen.

Erhebliche Pflichtverletzung

Der Busfahrer hat hartnäckig und beharrlich gegen seine Pflicht verstoßen, an dem System mitzuwirken. Das rechtfertigt in seinem Fall sogar eine außerordentliche Kündigung. Eine ordentliche Kündigung ist wegen seiner langen Betriebszugehörigkeit laut Tarifvertrag nicht mehr möglich. Aus diesem Grund kann man es dem Arbeitgeber nicht verweigern, eine außerordentliche Kündigung auszusprechen. Ansonsten hätte das Fehlverhalten des Busfahrers nämlich trotz mehrfacher Abmahnung keinerlei Folgen.

Auslauffrist als Zugeständnis

Der besondere Kündigungsschutz hat lediglich die Wirkung, dass dem Busfahrer eine sogenannte „Auslauffrist" zusteht. Sie ist entsprechend der Kündigungsfrist bei einer ordentlichen Kündigung zu bemessen. Darüber hinausgehende Wirkungen hat der besondere Kündigungsschutz jedoch nicht.

Ein deutliches Warnsignal für viele

Die Entscheidung des Bundesarbeitsgerichts trägt das Aktenzeichen 2 AZR 730/15 und ist mit diesem Aktenzeichen problemlos im Internet zu finden. Sie ist ein deutliches Warnsignal. Anders als manche glauben ist keineswegs jede Überwachung von Arbeitnehmern unzulässig. Wenn der Arbeitgeber damit vernünftige Ziele verfolgt, darf er vielmehr Arbeitnehmer durchaus überwachen. Dabei ist vor allem eine punktuelle Überwachung relativ problemlos. &

Datenschutzbeauftragte jetzt überall in der EU

In Deutschland ist man Datenschutzbeauftragte in Unternehmen seit Jahrzehnten ganz selbstverständlich gewohnt. Für andere Länder in der Europäischen Union (EU) sind sie dagegen etwas Neues. Die Datenschutz-Grundverordnung führt sie auch dort ein. Ergänzende nationale Vorschriften sind dabei weiterhin zulässig. Deutschland hat sie Mitte Mai 2017 eingeführt. Diese Kombination stellt sicher, dass im Ergebnis alles so bleibt, wie es sich bewährt hat.

Bisher ist es so: Besondere EU-Regelungen für Datenschutzbeauftragte gibt es nicht. Jeder Mitgliedstaat kann selbst entscheiden, ob er Datenschutzbeauftragte im Unternehmen vorschreibt. Deutschland hat dies schon vor Jahrzehnten getan. Im Ergebnis müssen lediglich kleine Unternehmen mit weniger als zehn Beschäftigten keinen Datenschutzbeauftragten haben.

Neuerungen durch die Datenschutz-Grundverordnung

Ab dem 25. Mai 2018 ändert sich die Situation auf EU-Ebene deutlich. Ab diesem Tag gilt die Datenschutz-Grundverordnung der EU. Erstmals sind dann in allen Mitgliedstaaten Datenschutzbeauftragte für Unternehmen vorgeschrieben. Dabei kommt es nicht auf die Zahl der Beschäftigten an.

Das Beispiel Gesundheitsdaten

Entscheidend ist vielmehr, worin die Kerntätigkeit eines Unternehmens besteht. Wenn es beispielsweise in großem Umfang Gesundheitsdaten verarbeitet, muss ein Datenschutzbeauftragter schon nach den Vorgaben der Grundverordnung vorhanden sein. Beispiele für solche Unternehmen sind natürlich Krankenhäuser, aber etwa auch Apotheken.

Das Beispiel SCHUFA & Co.

Ein weiteres Beispiel bilden Unternehmen wie die SCHUFA. Diese Auskunfteien verarbeiten in umfangreicher Weise Daten über Personen und beobachten das wirtschaftliche Verhalten von Personen auf Dauer. Auch das führt dazu, dass die Grundverordnung einen Datenschutzbeauftragten fordert. Die Grundverordnung formuliert dies etwas kompliziert so: Die Kerntätigkeit eines solchen Unternehmens besteht darin, dass eine umfangreiche regelmäßige und systematische Überwachung von Personen erfolgt.

Ergänzende nationale Regelungen

Alles in allem bleiben relativ viele Unternehmen übrig, die nach den Vorgaben der Grundverordnung keinen Datenschutzbeauftragten bestellen müssten. Hier kommt dann das nationale Recht in Spiel. Die Grundverordnung erlaubt es den Mitgliedstaaten der EU, ergänzende Regelungen für Datenschutzbeauftragte beizubehalten oder neu einzuführen.

In Deutschland bleibt alles wie bisher

Deutschland macht von dieser Möglichkeit Gebrauch. Mitte Mai 2017 wurde ein Nachfolgegesetz zum derzeit geltenden Bundesdatenschutz-

gesetz beschlossen. Es sieht im Ergebnis vor, dass die jetzt geltenden Regelungen auch künftig fortbestehen. Mit anderen Worten: Unternehmen, die jetzt schon einen Datenschutzbeauftragten haben, müssen ihn auch künftig haben.

Kontrolle der Aufsichtsbehörden

Immer wieder hört man die Vermutung, dass manche Unternehmen keinen Datenschutzbeauftragten bestellt haben, obwohl sie es müssten. Künftig dürfte es schwierig werden, die gesetzlichen Vorgaben zu umgehen. Die Grundverordnung schreibt nämlich im Gegensatz zum bisherigen Bundesdatenschutzgesetz vor, dass die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitzuteilen sind.

Logische Konsequenz: Fehlt eine solche Mitteilung im Einzelfall, wird die Aufsichtsbehörde nachfragen. Dabei kommt dann sehr schnell zutage, ob lediglich die Mitteilung versäumt wurde oder ob gar kein Datenschutzbeauftragter vorhanden ist.

Aufgabe des Datenschutzbeauftragten

Die Aufgaben eines Datenschutzbeauftragten sieht die Grundverordnung übrigens ganz genauso wie das deutsche Recht. Im Fokus steht die Beratung des Unternehmens in Datenschutzfragen. Daneben ist die Funktion als Anlaufstelle für Betroffene besonders wichtig. Dass der Datenschutzbeauftragte zu Geheimhaltung und zur Vertraulichkeit verpflichtet ist, hebt die Grundverordnung ausdrücklich hervor.

Schulung und Information der Mitarbeiter

Datenschutz im Unternehmen kann nur gelingen, wenn die Mitarbeiterinnen und Mitarbeiter mitziehen. Die Sensibilisierung und Schulung der Mitarbeiter hebt die Grundverordnung deshalb als besonders wichtige Aufgabe des Datenschutzbeauftragten hervor. Für sie ist völlig klar: Datenschutz geht im Unternehmen alle an!

Freiwillig bestellte Datenschutzbeauftragte

Bemerkenswert ist, wie viele freiwillig bestellte Datenschutzbeauftragte es bereits jetzt in anderen EU-Staaten gibt. In Frankreich, dem wichtigsten Handelspartner Deutschlands in der EU, sind es deutlich über 3000. Dies ist vor allem ein Signal dafür, dass die Unternehmen den Datenschutz ernst nehmen – ganz unabhängig davon, was im Gesetz im Einzelnen vorgeschrieben ist. &

Künstliche Intelligenz: Was die schlaue IT über uns wissen könnte

Was früher als Science Fiction galt, wird langsam in der IT Realität: Maschinen, die selbst lernen und immer intelligenter werden. Das bleibt natürlich nicht ohne Folgen für den Menschen.

In Kinofilmen gibt es sie schon lange: Maschinen, die ohne Kommando eines Menschen aktiv werden, scheinbar selbst entscheiden, was sie tun, und letztlich zur Gefahr für den Menschen werden. Hollywood zeigt uns in den Filmen Roboter, die sich gegen ihre Erbauer richten und die Weltherrschaft anstreben.

Solche Filme mögen ein Grund dafür sein, dass viele Menschen ein Unwohlsein verspüren, wenn sie an schlaue Maschinen, an sogenannte Künstliche Intelligenz (KI) oder Artificial Intelligence (AI) denken. Denn Intelligente Maschinen scheinen sich nicht von uns Menschen beherrschen zu lassen.

Andere Sorgen gelten zum Beispiel den Arbeitsplätzen: Schlaue IT-Systeme werden Arbeitsplätze kosten. Auch wenn sie an anderer Stelle Arbeitsplätze schaffen, werden bestimmte Arbeiten den Menschen ab- und damit weggenommen. Doch was hat das mit dem Datenschutz zu tun? Eine ganze Menge!

Maschinen lernen von uns Menschen

Basis der Künstlichen Intelligenz und damit schlauer IT-Systeme wie der digitalen Assistenten Alexa, Siri & Co. ist das maschinelle Lernen. Die IT lernt genau wie wir Menschen, indem sie Erfahrungen macht und ihre Regeln auf dieser Basis anpasst. Dabei spielen wir Menschen die entscheidende Rolle: Programmierer machen die Regeln, nach denen die Maschinen dann lernen. Außerdem soll die schlaue IT vielfach uns Menschen nachahmen. Dazu sammeln solche Systeme dann Informationen über die Nutzer und über andere Personen, die mit ihren Aufgaben zu tun haben.

Wenn also eine Künstliche Intelligenz dem Menschen etwas vorschlägt und dieser es als falsch ablehnt, lernt die Maschine. Sie lernt aber auch etwas über den Menschen: was er für richtig oder falsch hält, wie er das IT-System nutzt, wann er es nutzt, wozu er es nutzt, wo er es nutzt, abhängig davon, welche Sensoren der Maschine zur Verfügung stehen, um diese Daten zu messen. Maschinen werden so intelligenter und passen sich uns Menschen besser an, auch indem sie Profile der Nutzer erstellen. Damit ist der Datenschutz betroffen.

Künstliche Intelligenz braucht Schranken

Bei IT-Systemen mit Künstlicher Intelligenz besteht die Gefahr, dass sie immer mehr Daten sammeln und auswerten (Big Data) und dass auf der Basis der Datenanalyse dann Entscheidungen vorbereitet oder sogar getroffen werden, die uns als Menschen betreffen. Der einzelne Mensch ist umso mehr betroffen, je persönlicher die Datenanalysen sind. Der Schlüssel liegt also im Datenschutz.

Künstliche Intelligenz, die bald in immer mehr Geräte Einzug hält, gleich ob Auto, Radio oder Kühlschrank, darf nicht unbegrenzt personenbezogene Daten auswerten, um den einzelnen Nutzer möglichst passgenau unterstützen zu können.

Datenschutz hat somit in der Zukunft eine weiterhin große Bedeutung und sorgt mit dafür, dass intelligente Maschinen den Menschen helfen, ohne ihn dafür komplett zu durchleuchten. Auch wenn die Intelligenz und der Komfort der Maschinen dadurch scheinbar sinken sollten: Die Beschränkung des Zugriffs auf personenbezogene Daten darf bei Maschinen nicht aufgegeben werden, nur um sie so intelligent wie möglich zu machen! &

Wie schätzen Sie die Gefahren durch Künstliche Intelligenz (KI) ein? Machen Sie den Test!

Frage: Maschinen sind dumm, sie können nur das, was man ihnen als Programm mitgibt. Stimmt das?

a. Ja, woher sollten Maschinen auch mehr wissen und können?
b. Nein, die Entwicklung hin zur Künstlichen Intelligenz (KI) bedeutet, dass Maschinen selbstlernend werden.

Lösung: Die Antwort b. ist richtig. Für den Datenschutz bedeutet das, dass die IT-Systeme von den Menschen lernen und dazu möglichst viele Daten sammeln und auswerten sollen. Hier muss Privacy by Design oberstes Gebot sein.

Frage: Digitale Assistenten wie Alexa sind Beispiele für die Entwicklung hin zu KI-Systemen. Was sie lernen, bleibt wie beim menschlichen Gehirn innerhalb des Systems. Stimmt das?

a. Nein, solche Systeme sind mit dem Internet verbunden und speichern vieles in einer Cloud.
b. Ja, die Daten sind immer innerhalb des Systems geschützt.

Lösung: Die Antwort a ist richtig. Intelligente Geräte haben ihre KI-Fähigkeiten meist nicht lokal, sondern nutzen Rechenleistungen aus dem Internet und speichern Daten in der Cloud. Tatsächlich tauschen solche Systeme auch Daten untereinander aus, um so weitere Rückschlüsse zu ziehen. Personenbezogene Daten bleiben deshalb in der Regel nicht in dem jeweiligen System, sondern werden übermittelt. Deshalb sind Datenschutz-Prüfungen vor dem Einsatz intelligenter Systeme so wichtig. Die Prüfungen sind allerdings nicht leicht, denn die IT-Systeme werden immer komplexer. Aus diesem Grund muss der Zugriff auf die Daten von Beginn an begrenzt werden, nicht erst bei einer späterer Auswertung, die kaum noch nachvollzogen werden kann.

Tipps zur Prüfung einer Datenschutzerklärung

Was macht der Betreiber der Webseite eigentlich mit meinen Daten? Die Antwort sollten Sie in der Datenschutzerklärung finden. Doch wie verschafft man sich da eine Übersicht angesichts oft langer Texte?

Es erscheint paradox: Datenschützer pochen darauf, dass es bei Internetauftritten, Online-Shops und anderen Online-Diensten eine Datenschutzerklärung gibt. Rechtlich gefordert wird dies im sogenannten Telemediengesetz (TMG). Wie Umfragen unter Internetnutzern zeigen, werden diese Datenschutzerklärungen aber kaum gelesen.

Wichtige Informationen

Dabei sind in den Datenschutzerklärungen wichtige Informationen enthalten: Sie können dort erfahren, welche personenbezogenen Daten der Anbieter erhebt, zu welchem Zweck er sie erhebt, ob er Cookies einsetzt, an wen der Anbieter die Daten wozu weitergibt, welche Analyseprogramme (wie Google Analytics) im Einsatz sind, was getan wird, um Ihre Daten zu schützen, und an wen Sie sich bei Fragen zum Datenschutz bei diesem Unternehmen wenden können.

Viele Webseiten bieten eine Zusammenfassung

Da viele Datenschutzerklärungen sehr lang erscheinen und die meisten Internetnutzer keine rechte Freude an juristisch anmutenden Texten haben, bleiben die Informationen zum Datenschutz meistens ungelesen. Doch es gibt Möglichkeiten, sich einen ersten Überblick zu verschaffen, ohne die langen Ausführungen lesen zu müssen.

Immer mehr Webseiten bieten neben der Datenschutzerklärung eine kurze Übersicht, die zwar rechtlich gesehen die Datenschutzerklärung nicht ersetzt, aber dem Nutzer eine große Hilfe sein kann. Bereits 2015 hat die vom Bundesministerium der Justiz und für Verbraucherschutz geleitete Plattform „Verbrau-

cherschutz in der digitalen Welt“ ein Muster für Datenschutzhinweise auf einer Seite vorgestellt, den sogenannten One-Pager. Auf vielen Webseiten wurde dies bereits umgesetzt. Sie finden das Muster unter http://ogy.de/muster-onepager.

Mit der Datenschutz-Grundverordnung (DSGVO/GDPR) kommt zudem die Verpflichtung, die Informationen zum Datenschutz verständlicher zu formulieren. So sagt die DSGVO: „Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen (...), die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.“

Auch Apps brauchen eine Datenschutzerklärung

Während die meisten Webseiten bereits über eine Datenschutzerklärung verfügen, haben mobile Applikationen, die Apps für Smartphones und Tablets, häufig noch keine entsprechende Privacy Policy, wie dies international genannt wird. Das ist nicht richtig so, auch wenn es auf den relativ kleinen Displays der mobilen Geräte meist noch weniger Vergnügen bereitet, Texte wie eine Datenschutzerklärung zu lesen.

Im Bereich der Smartphones und Tablets jedoch gibt es Werkzeuge, die bei der Prüfung des Datenschutzes helfen können. Meist werden diese Werkzeuge Datenschutz-Scanner oder Privacy-Scanner genannt. Sie finden diese Scanner entweder als eigene App im jeweiligen App-Store Ihres mobilen Betriebssystems (wie Google Play Store bei Android-Geräten) oder als Funktion einer App für mobile Sicherheit (Mobile Security App).

Die Privacy-Scanner-Apps oder -Funktionen untersuchen andere Apps auf die Nutzung und Weitergabe von Daten. Entsprechend helfen die Privacy-Scanner auch bei der Prüfung einer Datenschutzerklärung – sogar dann, wenn es noch gar keine Datenschutzerklärung für eine App gibt. Denn diese Scanner untersuchen die Datennutzung direkt und nicht nur die Erklärung zur App.

Bald könnte es Datenschutzerklärer geben

In Zukunft wird es weitere Helfer geben, wenn es um die Prüfung der Datenschutzerklärung geht. Fast könnte man sagen, dass es bald Datenschutzerklärer geben wird. Es wird an sogenannten Privacy Bots gearbeitet. Bots sind virtuelle Assistenten. Die Privacy Bots sollen die Datenschutzerklärungen von Internetdiensten scannen und mit den Voreinstellungen des Nutzers abgleichen. Bestehende Wahlmöglichkeiten bei den Datenschutzeinstellungen sollen so leichter im Sinne des Anwenders genutzt werden. Die Privacy Bots sollen sich dabei nicht nur an einzelne Anbieter wie Facebook, Amazon oder Reiseportale richten, sondern für sämtliche Dienste nutzbar sein.

Das Ziel ist es, dass der Nutzer mithilfe des Bots nur einmal seine gewünschten Datenschutzstandards eingibt und der digitale Assistent daraufhin sämtliche Internetdienste prüft, die jeweiligen Datenschutzeinstellungen darin anpasst oder Dienste nicht akzeptiert. Dem Nutzer bleibt es damit erspart, sich bei jedem Dienst mit den Datenschutzeinstellungen und Datenschutzerklärungen auseinandersetzen zu müssen.

Noch ist dies Zukunftsmusik, doch es wird nicht mehr lange dauern, bis es digitale Helfer gibt, die die Prüfung der Datenschutzerklärungen einfacher machen. &

Wir überprüfen Impressum und Datenschutzerklärung

Die eigene Homepage ist nicht mehr nur eine elektronische Visitenkarte im Netz. Websites haben sich zu multimedialen Informationsplattformen entwickelt, bei denen Marketing, Vertrieb, Kundenkommunikation und die Darstellung inhaltlicher Themen immer weiter miteinander verschmelzen. Wichtiger denn je ist, Impressum und Datenschutzerklärung stets auf einem aktuellen Stand zu halten und an rechtliche Entwicklungen laufend anzupassen. Haben Sie in jüngster Zeit das Kleingedruckte auf Ihrer Website überprüft und aktualisiert?

Gern unterstützen wir Sie bei der Formulierung der Inhalte, überprüfen Impressum und Datenschutzerklärung oder führen eine Analyse auf IT-Sicherheit und Datenschutzkonformität Ihres Webservers durch. Auf Anfrage beraten wir Sie gern:

info@althammer-kill.de

Arbeitshilfen und Muster zur Datenschutzgrundverordnung

Aufsichtsbehörden verständigen sich auf einheitliche Vorlagen

Eine Arbeitsgruppe der Aufsichtsbehörden hat sich auf Muster für die Verzeichnisse nach Artikel 30 DSGVO („Verzeichnis von Verarbeitungstätigkeiten") geeinigt. Das berichtet der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. auf seiner Website und veröffentlicht die erarbeiteten Dokumente.

Dokumentationspflichten ausgeweitet

Zum einen haben die Aufsichtsbehörden damit eine hilfreiche Kommentierung vorgelegt und ihre Erwartungshaltung zur Interpretation des Art. 30 abgestimmt. Die Dokumente sind in deutscher Sprache und schriftlich, jedoch nicht zwingend in Papierform zu führen. Darüber hinaus muss eine Änderungshistorie von 12 Monaten gewährleistet sein.

Zum anderen finden sich konkrete Vorlagen zur Strukturierung und Gestaltung der Verzeichnisse von Verarbeitungstätigkeiten Verantwortlicher (Art. 30 Abs. 1 DSGVO), der Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO) und der Aufstellung von technischen und organisatorischen Maßnahmen (TOMs) (Art. 32 Abs. 1 DSGVO). Durch den Art. 32 Abs. 1 DSGVO werden die bisherigen TOMs nach Anlage 1 zu § 9 BDSG abgelöst.

Die Dokumente können direkt von der Homepage des BvD e.V. heruntergeladen werden:

https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

Orientierungshilfen in Kurzform

Auf den Websites der Aufsichtsbehörden werden teilweise im Monatstakt Arbeitshilfen und anderes Material zur Datenschutzgrundverordnung veröffentlicht. Einen guten Überblick zu den gesetzlichen Neuerungen gibt beispielweise das Bayerische Landesamt für Datenschutzaufsicht mit seinem Verzeichnis von Kurzpapieren:

https://www.lda.bayern.de/de/datenschutz_eu.htm

Benötigen Sie weitere Informationen?

Haben Sie Fragen oder benötigen Sie Unterstützung im Bereich Datenschutz oder Informationssicherheit? Wir freuen uns über Ihre Kontaktaufnahme:
info@althammer-kill.de

11 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2017

ALTHAMMER & KILL

News

Aus unserem aktuellen Newsletter:

Der König ist tot, es lebe der König – das neue Bundesdatenschutzgesetz
https://www.althammer-kill.de/news-detail/der-koenig-ist-tot-es-lebe-der-koenig-das-neue-bundesdatenschutzgesetz-300/

WhatsApp-Nutzer müssen Einwilligung ihrer Kontakte einholen
https://www.althammer-kill.de/news-detail/whatsapp-nutzer-muessen-einwilligung-ihrer-kontakte-einholen/

Aufzeichnung Webinar EU Datenschutz-Grundverordnung
https://www.althammer-kill.de/news-detail/aufzeichnung-webinar-eu-datenschutz-grundverordnung/

Datensicherheit wird verschärft
https://www.althammer-kill.de/news-detail/datensicherheit-wird-verschaerft/

Hacken ist menschlich: WannaCry-Cyberattacke per Zufall gestoppt
https://www.althammer-kill.de/news-detail/hacken-ist-menschlich-wannacry-cyberattacke-per-zufall-gestoppt/

Anmeldemöglichkeiten zum Newsletter finden Sie unter:
www.althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

08.09.2017, Berlin
Symposium Stiftung Zukunft Berlin
Auf dem Symposium informiert Niels Kill in einem Workshop am Runden Tisch zum Thema „Rechtlich sicher durch den digitalen Raum".

12.09.2017, Paderborn
Privacy by Design: Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht
Spätestens mit der EU Datenschutz-Grundverordnung (DS-GVO) sollten Unternehmen bereits bei der Auswahl von IT-Lösungen berücksichtigen, inwieweit diese datenschutzrechtlichen Anforderungen genügen.

12.09.2017, Online (stifter-helfen.de)
Kostenloses Webinar „EU Datenschutz-Grundverordnung" für Non-Profit-Organisationen
Durch die Verabschiedung der neuen DS-GVO ändert sich die datenschutzrechtliche Situation in Deutschland. In unserem Webinar lernen Sie den Status quo von Änderungen, Auswirkungen und Umsetzung kennen.

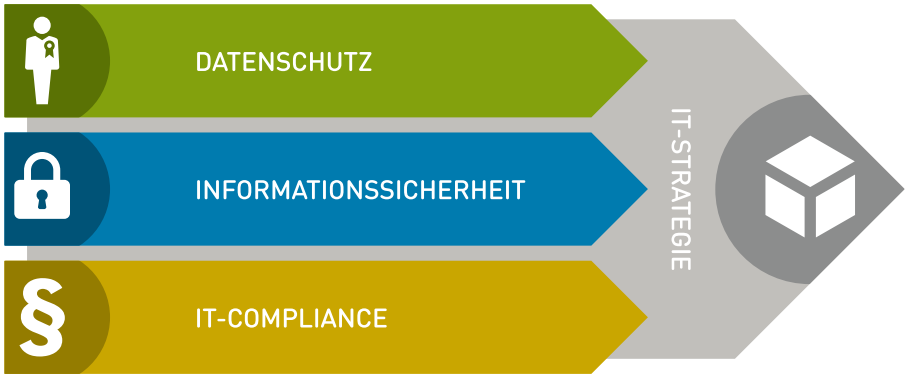
19.09.2017, Düsseldorf
IT-Sicherheit für mittelständische Unternehmen
Neueste Entwicklungen in der IT-Sicherheit, typische Angriffspunkte auf mittelständische Unternehmen, effizienter und praktikabler Schutz. Unser Seminar zeigt Ihnen, wie mittelständische Unternehmen ökonomisch und effizient ein angemessenes IT-Sicherheits-Niveau erreichen können.

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

ALTHAMMER & KILL

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ). &

Niels Kill
Geschäftsführer
Tel. +49 211 936748-20
nk@althammer-kill.de

Thomas Althammer
Geschäftsführer
Tel. +49 511 330603-10
ta@althammer-kill.de

Katja Borchhardt
Marketing und Organisation
Tel. +49 211 936748-0
kb@althammer-kill.de

Mariusz Bucki
Berater für IT-Sicherheit u. Datenschutz
Tel. +49 511 330603-30
mb@althammer-kill.de

Sören Hartmann
Assistent der Geschäftsführung
Tel. +49 511 330603-36
sh@althammer-kill.de

Andreas Hellmann
Berater für Datenschutz u. IT-Sicherheit
Tel. +49 211 936748-34
ah@althammer-kill.de

Daniela Hörnicke
Beraterin für Datenschutz
Tel. +49 511 330603-38
dh@althammer-kill.de

Dr. Jan Holling
Berater für Datenschutz
Tel. +49 511 330603-32
jh@althammer-kill.de

Klaus Hopp
Berater für Datenschutz
Tel. +49 211 936748-42
kh@althammer-kill.de

Frank Keusemann
Fachkraft für Arbeitssicherheit
Tel. +49 211 936748-60
fk@althammer-kill.de

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 511 330603-0
ak@althammer-kill.de

Althammer & Kill GmbH & Co. KG

www.althammer-kill.de

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0

Standort Hannover:
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0