Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2016

Liebe Leserin, lieber Leser,

während alle von einer Zukunft mit selbstfahrenden Autos sprechen, funken heutige KFZ bereits fleißig Daten an die Hersteller. Jede Fahrt wird überwacht, Profile über Fahr- und Bremsverhalten werden erstellt. Die wichtigsten Erkenntnisse einer ADAC-Untersuchung stellen wir auf Seite 9 vor.

Weitere Schwerpunkte dieser Ausgabe sind das Internet der Dinge und die anstehenden gesetzlichen Veränderungen.

An dieser Stellte möchten wir ganz herzlich zwei neue Kollegen im Team von Althammer & Kill begrüßen:

Mit Dr. Jan Holling konnten wir einen Juristen mit Erfahrung in internationalen Fragestellungen gewinnen. Andreas Hellmann verfügt über langjährige Erfahrung als Berater für IT, Datenschutz und Informationssicherheit.

Eine spannende Lektüre wünschen

Thomas Althammer & Niels Kill

Internet of Things: Nicht die Dinge, sondern Sie selbst sind betroffen

Kennen Sie das Internet der Dinge? Ob ja oder nein: In jedem Fall wird das Internet der Dinge bald Sie kennen – und zwar besser, als Ihnen lieb sein dürfte.

Was haben Spielzeuge, Fitness-Tracker, Autos und Kühlschränke gemeinsam? Scheinbar nicht viel. In Wirklichkeit aber bilden sie eine Gemeinschaft: Sie gehören zum sogenannten Internet of Things, kurz IoT.

Viele Geräte sind inzwischen mit dem Internet verbunden oder werden es bald sein, im Büro, im Haus, in der Garage. Ob man daheim, unterwegs oder in der Arbeit ist: Das Internet kommt überall mit.

In dieser Ausgabe:

Das Internet ist überall

Das Internet hat Beine bekommen. Das wissen Unternehmen und Nutzer durch die beliebten Smartphones und Tablets. Nun haben aber auch andere Geräte einen Internetzugang, die früher nie mit dem Internet in Verbindung gebracht wurden: Uhren am Handgelenk, Kaffee-Automaten, die Heizung, Glühbirnen, Autoradios oder die Rollos am Bürofenster.

IoT ist ein Datenschutz-Problem

So mancher freut sich auf das Internet der Dinge, wenn der Firmen- oder Privatwagen mit dem Parkplatz kommuniziert und so automatisch eine freie Lücke findet oder wenn der Kaffee-Automat die Kaffee-Lieferung oder den Wartungsdienst bestellt.

Aber viele machen sich auch Sorgen: Laut Umfragen bestehen die größten Bedenken, wenn es um den Schutz personenbezogener Daten geht. Vielleicht sind Sie jetzt überrascht, was vernetzte Dinge im Internet mit personenbezogenen Daten zu tun haben. Leider sehr viel. Denn die Dinge sind meist eng mit ihren Nutzern verknüpft. Das kann nicht nur der Fall sein, wenn sich die Smartwatch am Handgelenk befindet. Viele der vernetzten Geräte haben integrierte Sensoren und Funkschnittstellen. Sie können so den Nutzer vermessen oder andere Geräte des Nutzers erreichen.

Geräte-Tracking = Nutzer-Tracking

Zu den Informationen, die die Geräte austauschen und ins Internet übertragen, gehört oftmals auch der Standort des Geräts, der aber mit dem Standort des Nutzers identisch oder sehr ähnlich sein kann.

Gelingt es also, ein Gerät einem Nutzer zuzuordnen, wird aus dem scheinbar harmlosen Orten von Dingen das Orten von Personen. Die Betroffenen sind sich aber häufig gar nicht bewusst, dass ihre Bewegungsprofile an den App-Anbieter oder den Gerätehersteller gesendet werden könnten.

„Dass zum Beispiel Jalousien, Beleuchtung, die Waschmaschine oder auch Hauskameras vernetzt, per Smartphone gesteuert und Abläufe programmiert werden können, ist für die meisten Menschen Neuland. Daher ist es umso wichtiger, dass technisch innovative Angebote wie Smart-Home-Systeme von vornherein so konzipiert werden, dass Verbraucherinnen und Verbraucher sich auf die Sicherheit und den Schutz ihrer Daten verlassen können müssen“, so der Rheinland-Pfälzer Verbraucherschutzminister Robbers.

Da das bisher nicht der Fall ist, müssen wir alle als Nutzer genau auf unsere Daten achten, gerade im Internet der Dinge. &

Impressum

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

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

Schutzgebühr Print-Ausgabe: 10,– €

Datenschutz-Grundverordnung – was kommt auf uns zu?

Selbst Tageszeitungen haben darüber berichtet: In Brüssel hat man sich auf eine EU-Datenschutz-Grundverordnung geeinigt. Lesen Sie, warum die Verordnung zwar erst ab Mitte 2018 gilt, aber schon jetzt eine gewisse Beachtung verdient.

Einheitliche Datenschutzregelungen für die gesamte EU fordern gerade exportorientierte Unternehmen schon lange. Aber auch für Verbraucher, die gern über das Internet jenseits der deutschen Grenzen einkaufen, sind einheitliche Vorgaben von Vorteil. In erstaunlich kurzer Zeit haben sich die EU-Instanzen nun auf solche EU-weiten Regelungen geeinigt.

EU-Verordnungen wirken wie Gesetze

Das zentrale rechtliche Instrument bildet dabei die Datenschutz-Grundverordnung. Es handelt sich um eine europäische „Verordnung". Das bedeutet nach den Vorgaben des EU-Rechts, dass sie innerhalb der EU wie ein Gesetz wirkt. Sie muss also nicht erst von den Mitgliedstaaten in nationales Recht umgesetzt werden. Das war bei der EG-Datenschutzrichtlinie von 1995, die bisher noch die maßgebliche EU-Regelung für den Datenschutz darstellt, anders. Sie hatte für sich allein keine rechtliche Wirkung für Unternehmen und Privatpersonen. Die erforderliche Umsetzung im Recht der Mitgliedsstaaten geschah erst mit jahrelanger Verzögerung.

Übergangsfrist bis Mai 2018

Bei der Datenschutz-Grundverordnung wird es anders ablaufen. Anfang Mai 2016 wurde sie im Amtsblatt der EU veröffentlicht. Nun läuft eine Übergangszeit von zwei Jahren. Und dann gilt die Verordnung ab dem 25. Mai 2018 über Nacht in vollem Umfang für alle Unternehmen und Privatpersonen innerhalb der EU.

Folge dadurch: „Fallbeileffekt"

Dieser „Fallbeileffekt" wird alle Unternehmen dazu zwingen, sich bis Mitte 2018 zunehmend stärker auf die Verordnung vorzubereiten. Wundern Sie sich also nicht, wenn demnächst viele Informationen im Unternehmen gesammelt werden müssen,

Datenaustauschabkommen EU-US-Privacy Shield

Das EU-US-Privacy Shield soll Unternehmen die Übertragung von personenbezogenen Daten in die USA erlauben und EU-Bürger gleichzeitig vor Überwachung schützen. Auch wenn Kritiker meinen, dass es das nicht schafft, hat die EU-Kommission es, mit sofortiger Wirkung, nun in Kraft gesetzt. US-Unternehmen können sich allerdings erst ab dem 1. August für die Teilnahme an EU-US-Privacy Shield anmelden – ihre Übertragungen von Daten von EU-Bürgern in die USA fallen also erst ab dann unter das neue Abkommen.

Zudem bleibt abzuwarten, wie die nationalen Aufsichtsbehörden auf das neue Abkommen reagieren werden. Der EuGH hatte in seinem Urteil explizit darauf hingewiesen, dass es originäre Aufgabe der Aufsichtsbehörden sei, die Einhaltung europäischen Datenschutzrechts zu überwachen und zu kontrollieren. Diese Kompetenz sei keineswegs durch eine Angemessenheitsentscheidung der Europäischen Kommission eingeschränkt. Demnach ist es also allen europäischen Aufsichtsbehörden zukünftig möglich, Datenübermittlungen in die USA auf der Grundlage des neuen EU-US-Privacy Shields zu untersagen.

Darüber hinaus bleibt mit Spannung abzuwarten, wie der EuGH auf eine – wahrscheinliche – erneute Vorlage durch nationale Gerichte, die mit Klagen gegen Datenübermittlungen in die USA auf der Grundlage des EU-US-Privacy Shields befasst sind, reagieren wird. &

obwohl die Verordnung streng rechtlich gesehen noch gar nicht gültig ist. Zu den Vorgaben der Grundverordnung gehört es nämlich, dass Unternehmen in vielerlei Hinsicht zusätzliche Dokumente erstellen müssen. So müssen sie etwa nachweisen, dass sie erforderliche technische Schutzmaßnahmen bei der Datenverarbeitung und bei der Auftragsdatenverarbeitung tatsächlich einhalten.

Extrem hohe Bußgelder möglich

„Schlampereien" können dabei teuer zu stehen kommen. Im Extremfall sind nämlich Bußgelder bis zu 20 Millionen Euro möglich. Das Bundesdatenschutzgesetz legt für Bußgelder bisher noch eine Obergrenze von 300.000 Euro fest.

Der Vergleich der beiden Beträge zeigt deutlich, wie sehr die Zügel angezogen werden. Bitte haben Sie also Verständnis dafür, wenn notwendige Unterlagen auch einmal etwas drängend angefordert werden. Nur so lässt sich möglicher Schaden vom Unternehmen abwenden.

Betriebliche Datenschutzbeauftragte in der gesamten EU

Nichts ändert sich übrigens daran, dass es einen betrieblichen Datenschutzbeauftragten geben muss. Die Einzelheiten dafür, wann dies erforderlich ist, überlässt die Verordnung zwar weiterhin dem Recht der Mitgliedsstaaten. Für Behörden schreibt sie jedoch europaweit behördliche Datenschutzbeauftragte vor.

Für Unternehmen gilt dies dann, wenn es bei ihren Kernaktivitäten um die regelmäßige und systematische Beobachtung von Betroffenen geht oder um besonders sensible Daten.

Einwilligungen von Kunden gelten weiter

Für die Praxis wichtig: Einwilligungen von Kunden, die bereits vorliegen, wenn die Verordnung Mitte 2018 gültig wird, bleiben auch danach wirksam! Bedingung ist nur, dass sie unter Beachtung der Vorgaben des bisherigen Rechts eingeholt wurden.

Beachten Sie also weiterhin peinlich genau das geltende Recht, wenn eine Einwilligung erfolgt! Das macht sich bezahlt, wenn die neue Verordnung ab Mai 2018 gilt.

Betriebsvereinbarungen bleiben in Kraft

Auch Betriebsvereinbarungen zum Datenschutz bleiben unverändert in Kraft. Eine entsprechende Klarstellung konnte bei den Verhandlungen in Brüssel erreicht werden. Es ist also nicht notwendig, wegen der Datenschutz-Grundverordnung bewährte Betriebsvereinbarungen neu zu verhandeln.

Anpacken statt abwarten!

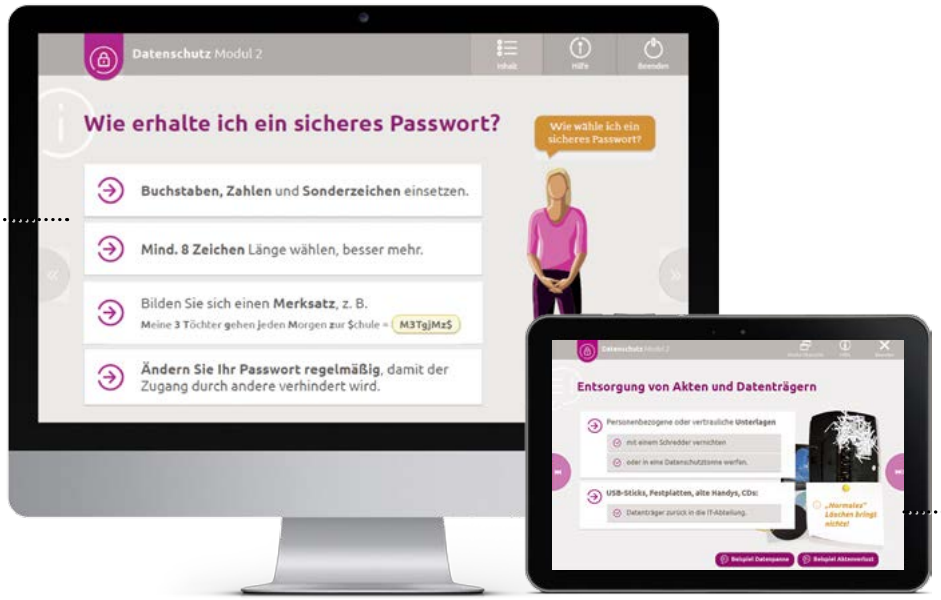
Insgesamt gesehen wird es notwendig sein, die Datenschutz-Grundverordnung bis Mitte 2018 mehr und mehr zu berücksichtigen. Nur so lässt sich vermeiden, dass dann alles Mögliche sozusagen „über Nacht" neu gestaltet werden muss. &

ALTHAMMER & KILL

E-Learning Datenschutz und IT-Sicherheit

Zur Erfüllung der Unterweisungspflichten nach § 4 g BDSG, § 22 DSG-EKD, § 21 KDO, LDSG und ITSVO-EKD

Hochwertige didaktische Aufbereitung



Verständlich und anschaulich

Ziele:
Die Sensibilisierung Ihrer Mitarbeiter ist wichtiger denn je: Datenschutz und IT-Sicherheit sind in den Fokus gerückt. Verstöße oder Datenpannen haben unter Umständen größere Auswirkungen auf Ihre Kundenbeziehungen.

Inhalte:
Zusammen mit dem Vincentz-Verlag haben wir ein E-Learning-Modul entwickelt. Die Inhalte sind verständlich, anschaulich und hochwertig didaktisch aufbereitet. Wir garantieren einfachste Bedienung über einen Webbrowser ohne Installation oder sonstige Betriebskosten.

althammer-kill.de/e-learning

In Zusammenarbeit mit: VINCENTZ

Data Breach Notification: wichtig wegen unserer Kundendaten

Wer häufig mit Kundendaten zu tun hat, sollte diese Frage beantworten können: Was muss ich tun, wenn die Daten möglicherweise in die falschen Hände geraten sind? Typisches Beispiel: Ein Datenträger mit Kundendaten geht verloren.

Data Breach Notification ist sicher kein schöner Begriff und viele verstehen ihn schlicht nicht. Aber ehrlich gesagt – ist „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten" (so die Überschrift von § 42a Bundesdatenschutzgesetz) besser? Beides meint dieselbe Situation: Daten etwa von Kunden sind möglicherweise in die Hände von Unbefugten geraten. Das kann beispielsweise der Fall sein, wenn ein Laptop mit Kundendaten irgendwo liegen bleibt oder ein USB-Stick mit Daten nicht mehr zu finden ist.

Dann stellt sich die Frage, ob eine Datenschutzverletzung (Data Breach) vorliegt, über die eine Mitteilung (Notification) notwendig ist – an wen auch immer.

Mögliche Folge: Benachrichtigungspflichten

Schon seit einigen Jahren sieht das Bundesdatenschutzgesetz vor, dass in solchen Situationen unter bestimmten Voraussetzungen sowohl die Datenschutzaufsichtsbehörde wie auch die Betroffenen selbst benachrichtigt werden müssen. Die Einzelheiten sind kompliziert, aber damit muss sich der „Normalarbeitnehmer" im Unternehmen nicht herumschlagen. Für ihn genügt es zunächst einmal, zu wissen, dass es eine solche Benachrichtigungspflicht je nach Situation geben kann.

Wichtig: rasche Information der Vorgesetzten bei Pannen!

Wichtig deshalb: Wenn ein Datenträger mit Kundendaten einfach nicht mehr zu finden ist, auf keinen Fall den Kopf in den Sand stecken! Das macht im Ernstfall alles nur schlimmer. Informieren Sie vielmehr zügig Ihre Vorgesetzten. Diese werden dann in aller Regel den internen Datenschutzbeauftragten einschalten. Dann lässt sich gemeinsam überlegen, was zu tun ist, um zusätzlichen Schaden zu vermeiden.

Meist maßvolle Reaktion der Datenschutzaufsicht

Die Aufsichtsbehörden für den Datenschutz reagieren bei frühzeitigen Meldungen, die nichts verschleiern, durchweg mit viel Augenmaß. Nur in ganz besonderen Extremfällen kommt es dazu, dass betroffene Kunden beispielsweise über Zeitungsanzeigen informiert werden müssen. Das hat es in Einzelfällen bei Kliniken gegeben, wenn sehr sensible Daten betroffen waren und nicht einmal ungefähr festzustellen war, um die Daten welcher Patienten es dabei ging. Im Normalfall akzeptieren es die Aufsichtsbehörden, wenn das Unternehmen selbst die konkret betroffenen Kunden individuell informiert.

Kunden oft verständnisvoller als gedacht

Kunden reagieren auf eine solche individuelle Benachrichtigung meistens sehr sachlich, manchmal sogar dankbar. Zu verärgerten Reaktionen kommt es normalerweise nur, wenn betroffene Kunden erst aus den Medien erfahren, dass etwas mit ihren Daten passiert sein könnte. Deshalb ist es wichtig, dass das Unternehmen die Situation möglichst von Anfang an selbst in der Hand hat.

Dazu sind rasche interne Informationen notwendig, die man dann in geeigneter Form bei der Kommunikation mit betroffenen Kunden verwenden kann.

Künftig verschärfte Rechtslage

Nach der augenblicklichen Rechtslage müssen die Kunden und die zuständige Aufsichtsbehörde nur informiert werden, wenn es um besonders sensible Daten geht. Beispiele hierfür sind etwa Daten, die der ärztlichen Schweigepflicht unterliegen, oder Daten zu Bank- und Kreditkartenkonten. Diese Einschränkung hat für die Praxis im Unternehmen allerdings eine eher geringe Bedeutung.

Zum einen lässt sich nicht immer leicht entscheiden, ob zumindest einzelne besonders sensible Daten betroffen sein könnten. Diese Einschätzung müssen Fachleute treffen. Zum anderen wird die Datenschutz-Grundverordnung der EU ab Mai 2018 hier eine neue Rechtslage bringen. Ab dann kommt es nicht mehr darauf an, ob es um besonders sensible Daten geht. Vielmehr sind dann Datenschutzverletzungen hinsichtlich aller Arten von Daten zu melden. Darauf sollte man sich schon jetzt einstellen.

Vorbeugende Maßnahmen nicht vergessen!

Am besten wäre es natürlich, wenn Datenschutzverletzungen erst gar nicht vorkommen. Vielleicht nehmen Sie diesen Beitrag zum Anlass, einen genaueren Blick auf Ihren Schreibtisch zu werfen. Liegen dort Datenträger ungesichert offen herum? Und wie sieht es eigentlich mit der Passwortsicherung für den Laptop und das Smartphone aus?

Wenige Handgriffe können dafür sorgen, dass es erst gar nicht zu Problemen kommt. &

Auf dem Weg zum Digital Workspace

Digitalisierung gilt als einer der wichtigsten Trends in der deutschen Wirtschaft. Aus dem Arbeitsplatz soll ein Digital Workspace werden. Das hat auch Folgen für den Datenschutz.

© K. Borchhardt/ www.miniansichten.de

Bereits jedes vierte Unternehmen setzt auf digitalen Schriftverkehr, 40 Prozent wollen in Zukunft vermehrt auf digitale Kommunikation umstellen, so eine repräsentative Umfrage von Bitkom Research. Die Digitalisierung verändert aber nicht nur die Kommunikation. Auch die Produkte und Märkte ändern sich. Vier von zehn Unternehmen haben infolge der Digitalisierung bereits neue Produkte oder Dienste auf den Markt gebracht und 57 Prozent bestehende Angebote angepasst.

Fast alles soll digital werden

In den einzelnen Bereichen eines Unternehmens ist die Digitalisierung unterschiedlich stark ausgeprägt. Spitzenreiter ist die Produktion und Projektabwicklung, die in 74 Prozent der Unternehmen stark digitalisiert ist (mindestens zu 50 Prozent). Die Abteilungen Personal/Human Resources und Buchhaltung/Finanzen/Controlling sind jeweils in 66 Prozent der Unternehmen stark digitalisiert. Im Ranking folgen dahinter Marketing

(62 Prozent), Einkauf (54 Prozent), Logistik (53 Prozent) sowie Forschung und Produktentwicklung (30 Prozent).

Kaum eine Tätigkeit wird davon nicht betroffen sein

Noch setzen acht von zehn deutschen Unternehmen häufig das Faxgerät zur internen oder externen Kommunikation ein, 40 Prozent nutzen bereits Online- oder Videokonferenzen, 15 Prozent Soziale Netzwerke. Der klassische Büroarbeitsplatz verändert sich zunehmend. Etwa jeder zweite Mitarbeiter sitzt an einem Computer-Arbeitsplatz, jeder Dritte nutzt für die Arbeit ein Mobilgerät mit Internetzugang wie Tablet-PC oder Smartphone.

Die Möglichkeit, an jedem Ort auf das Internet zuzugreifen, verändert die Arbeitswelt, so der Bitkom-Verband. Dank Smartphone, Tablet-Computer und Laptop ist man nicht mehr auf einen Büroarbeitsplatz angewiesen, sondern kann von unterwegs oder aus dem Home Office arbeiten.

Der Arbeitsplatz wird zum Digital Workspace. Diese Veränderungen haben Auswirkungen darauf, wie wir arbeiten, wie wir Daten nutzen und schützen müssen.

So führt die Nutzung mobiler Geräte vermehrt dazu, dass Daten im Internet, in einer Cloud gespeichert werden, da so der Zugriff auf die Daten flexibel ist. Die Flexibilität erkauft man sich aber mit steigenden Gefahren für Datensicherheit und Datenschutz. Die digitalen Risiken werden nämlich unterschätzt: 86 Prozent der Top-Manager sehen in der Digitalisierung eher Chance als Risiko für ihr Unternehmen. Zehn Prozent sehen eher eine Gefahr und nur vier Prozent meinen, die Digitalisierung habe keinen Einfluss auf ihr Unternehmen.

Der Weg hin zum Digital Workspace ist doppelt gefährlich

Bei den zahlreichen Projekten zur Digitalisierung und der offensichtlichen Umstellung auf eine zunehmend digitale Kommunikation darf aber eines nicht vergessen werden: Es gibt nicht nur die Datenrisiken beim Digital Workspace, bei den Smartphones, Tablets und Clouds. Auch die ganz klassischen Arbeitsgeräte und Arbeitsplätze tragen Risiken für personenbezogene Daten in sich und können zu Datenpannen führen. Die Aktenordner im Papiermüll sind nur ein Beispiel dafür.

Wenn es also um Datenschutz im digitalen Zeitalter geht, sollten Unternehmen immer auch daran denken, dass wir erst auf dem Weg hin zum Digital Workspace sind. Es ist gut möglich, dass es den komplett digitalen Arbeitsplatz nur in Einzelfällen geben wird. Deshalb müssen alle Maßnahmen zum Schutz personenbezogener Daten immer die klassische UND die digitale Arbeitswelt umfassen. Sonst werden die klassischen Datenrisiken übersehen – und damit zu einer wachsenden Gefahr. &

Schätzen Sie digitale Gefahren richtig ein? Testen Sie sich!

Frage: Die größten Risiken für die vertrauliche Kommunikation liegen im Internet. Stimmt das?

a. Ja, denn die klassische Kommunikation wird bei Weitem nicht so stark angegriffen.
b. Nein, jede Kommunikation muss geschützt werden, auch die klassischen Formen.

Lösung: Die Antwort b. ist richtig. Tatsächlich ist es sogar so, dass bestimmte Schutzverfahren wie Verschlüsselung für papiergebundene Verfahren gar nicht verfügbar sind. Je nach Kommunikationsverfahren gibt es andere Risiken. Die Vertraulichkeit muss aber immer geschützt werden..

Frage: Die Digitalisierung bedroht den Datenschutz. Stimmen Sie dem zu?

a. Nein, nicht die Digitalisierung, sondern unzureichender Schutz und unvorsichtige Handlungen bedrohen die Daten, auch am klassischen Arbeitsplatz.
b. Ja, denn mit dem Internet kommen ganz neue Gefahren auf uns zu.

Lösung: Die Antwort a. ist richtig. Das Internet bringt zwar neue Datenrisiken mit sich, doch auch die klassischen Arbeitsverfahren können personenbezogene Daten in Gefahr bringen und Datenpannen verursachen. Der Schutzbedarf der Daten muss immer erfüllt werden, ganz gleich, ob am digitalen oder am klassischen Arbeitsplatz.

Ein ganz besonderer KFZ-Check

Mit dem Auto in den Urlaub, für viele von uns eine Selbstverständlichkeit. Vor der Abfahrt die Reifen und Bremsen sowie den Ölstand kontrollieren, das kennen und beherrschen wir. Aber, wie sieht es eigentlich mit dem KFZ-Datenschutz aus? Warum, fragen Sie sich jetzt? Weil moderne Autos jede Menge Daten über uns sammeln!

Alles was gemessen werden kann, wird auch gemessen! Das ist nicht unbedingt neu und dient vor allem zur Diagnose möglicher Mängel beim Werkstattbesuch.


© K. Borchhardt/
www.miniansichten.de

Moderne Fahrzeuge verfügen allerdings nicht nur über einige wenige Sensoren zur Überwachung von kritischen Bauteilen, die aktuellen Schaltzentralen überwachen und dokumentieren zunehmend unser gesamtes Fahrverhalten.

Welche Daten werden gesammelt?

Der ADAC untersuchte die Datensammlung einiger Fahrzeuge genauer (https://goo.gl/zlmDkb) und stellte fest, dass u.a. folgende Daten gespeichert werden:

- Anzahl der Fahrtstrecken zwischen 0 und 5, 5 und 20, 20 und 100 sowie über 100 Kilometer (erlaubt Rückschlüsse auf das Nutzungsprofil)
- Welche Straßenarten (Autobahn, Landstraße usw.) befahren wurden (erlaubt Rückschlüsse auf das Nutzungsprofil)
- Zahl der Verstellvorgänge des elektrischen Fahrersitzes (erlaubt Rückschlüsse auf Anzahl der Fahrer)
- Intermodale Verbindungspunkte (an denen in andere Verkehrsmittel wie Bus und Bahn umgestiegen wurde)

Die genannten Beispiele lassen uns nur zu gut erahnen, welches Potenzial sich den Automobilherstellern beim Erstellen solcher Nutzungsprofile eröffnet, was allerdings nicht zwingend als negativ gewertet werden muss. Sinnvolle Anwendungsbereiche, wie z.B. die Selbstreflexion oder eine konsumorientierte Nutzung müssen nicht per se ausgeschlossen werden.

Was passiert derzeit mit den Daten?

Problematisch dabei ist, dass die Daten regelmäßig nach Hause gesendet werden oder zumindest jederzeit aus der Ferne abgerufen werden können. Mit zu Hause ist aber nicht der heimische Laptop gemeint, sondern die Serverfarm des Automobilherstellers (http://goo.gl/N9UWuk). Der Autofahrer kriegt davon in der Regel nichts mit. Was danach mit den Daten passiert ist bis jetzt ebenfalls unklar.

Werden unsere KFZ-Daten womöglich mit anderen Daten verknüpft oder an andere Unternehmen übermittelt? Eine Übersicht lieferten die Automobilhersteller laut ADAC nicht. Die Möglichkeit Einfluss auf die Datensammlung- und Weitergabe zu nehmen, wurde durch den ADAC ebenfalls verneint. So ist es durchaus vorstellbar, dass wir aufgrund unseres mit dem Auto angesteuerten Reiseziels, auch mit entsprechend personalisierter Werbung im Rahmen der Internetnutzung angesprochen werden.

Es wird Zeit für Selbstdatenschutz!

Spätestens über die Fahrzeug-ID lassen sich die gesammelten Daten tatsächlich dem Fahrer oder Halter zuordnen, sodass datenschutzrechtliche Vorgaben beachtet werden müssen! Mangels transparenter Datenschutzpolitik der Automobilhersteller oder besonderen Vorgaben des Gesetzgebers, liegt es auch an uns selbst, zu kontrollieren was unser Auto eigentlich über uns weiß, wem es etwas über unser Fahrverhalten verrät und ob es dabei auch wirklich mit rechten Dingen zugeht. &

Akademie

Ausbildung Datenschutzbeauftragte
Grundlagenseminar Datenschutz
inkl. Ausblick auf die EU-Datenschutzgrundverordnung

Das Seminar vermittelt in kompakter Form das „Handwerkszeug“ für die Aufgaben eines betrieblichen Datenschutzbeauftragten auf Grundlage der aktuellen Datenschutzgesetze. Anschauliche Beispiele aus der Datenschutzpraxis vermitteln das komplette Basiswissen. In nur drei Tagen erlernen Sie so die notwendige Fachkunde.

Inhalte des Seminars

- Einführung und Sensibilisierung
- Rechtliche Grundlagen des Datenschutzes
- Grundzüge und Vergleich der Gesetze
- Rechtsstellung, Anforderungen und Aufgaben des Datenschutzbeauftragten
- Daten: Erhebung, Verarbeitung und Nutzung
- Rechte der betroffenen Personen
- Bereichsspezifischer Datenschutz
- Praktische Fallbeispiele
- Informationssicherheit
- Technische- und organisatorische Maßnahmen
- Die ersten 100 Tage des Datenschutzbeauftragten
- Aktuelle Herausforderungen (Cloud Computing, Social Media)

Termine

Ausbildung Datenschutzbeauftragte allgemein
27.–29.09.2016, Hannover
18.–20.10.2016, Düsseldorf

Ausbildung Datenschutzbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft
06.–08.09.2016, Düsseldorf
12.–14.09.2016, Hannover

Ausbildung IT-Sicherheitsbeauftragte
Grundlagenseminar Informationssicherheit
auf Basis von IT-Grundschutz und ITSVO-EKD

Das Seminar vermittelt anschaulich und praktikabel das „Handwerkszeug” für die Aufgaben eines IT-Sicherheitsbeauftragten. Die Teilnehmer eignen sich ein fundiertes aktuelles Fachwissen an, mit dem sie den professionellen Schutz ihrer Informationen und IT-Systeme gewährleisten können.

Inhalte des Seminars

- Einführung in die IT-Sicherheit
- Rechtliche Rahmenbedingungen
- Verfügbare Normen
- Organisatorische Sicherheitsmaßnahmen
- Technische Sicherheitsmaßnahmen
- Entwicklung eines IT-Sicherheitskonzeptes (BSI)
- Praxisorientierte Vorgehensweise nach BSI IT-Grundschutz
- Definition IT-Verbund, Durchführung Strukturanalyse, Schutzbedarfsfeststellung
- Pflege und Optimierung des IT-Sicherheitskonzeptes
- Rechtliche Fallstricke der IT-Sicherheit
- Besondere Themen wie (Sozial-)Datenschutz, Schweigepflicht, Fernmeldegeheimnis
- Haftung des IT-Sicherheitsbeauftragten

Termine

Ausbildung IT-Sicherheitsbeauftragte
20.–22.09.2016, Hannover
11.–13.10.2016, Düsseldorf

Ausführliche Seminarbeschreibungen und Anmeldemöglichkeiten finden Sie hier:
www.althammer-kill.de/akademie.html

Termine

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

12.09.2016, Bad Honnef
Begleitung der Fortbildung „Referent/-in Online-Fundraising“
Wir sind Dozenten für den Bereich „Recht und Datenschutz“

14.09.2016 – 15.09.2016, Soltau
Standard-Systeme Anwendertreffen
Unser Vortrag „Aktuelle Entwicklungen in den Bereichen Datenschutz, Informationssicherheit und IT-Compliance“

22.09.2016, Karl-Bröger-Zentrum, Nürnberg
Seminar Datenschutz-Praxis
Seminar Datenschutz-Praxis für IT-Abteilungen und Software-Anbieter
Anmeldung über: https://www.finsoz.de/node/864

18.10.2016, Bonifatiushaus, Fulda
Seminar IT-Notfallmanagement
Praxisorientiertes Seminar zum Einstieg in ein strukturiertes IT-Notfallmanagement
Anmeldung über: https://www.finsoz.de/node/829

26.10.2016 – 27.10.2016, Nürnberg
Messe ConSozial 2016
Wir freuen uns auf Ihren Besuch!

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

News

Aus unserem aktuellen Newsletter:

Netzwerkdrucker als Sicherheitsrisiko
https://www.althammer-kill.de/news-detail/netzwerkdrucker-als-sicherheitsrisiko.html

Datenaustauschabkommen EU-US-Privacy Shield
https://www.althammer-kill.de/news-detail/datenaustauschabkommen-eu-us-privacy-shield-tritt-in-kraft.html

Stets auskunftsfreudig: Blackberrys haarsträubender Umgang mit vertraulichen Daten
www.althammer-kill.de/news-detail/stets-auskunftsfreudig-blackberrys-haarstraeubender-umgang-mit-vertraulichen-daten.html

Störerhaftung fällt… vielleicht?!
www.althammer-kill.de/news-detail/stoererhaftung-faellt-vielleicht.html

Verbraucher informieren – Abmahnungen vermeiden!
www.althammer-kill.de/news-detail/online-streitbeilegung-verbraucher-informieren-abmahnungen-vermeiden.html

Briefpost – Verletzung des Briefgeheimnisses droht!
https://www.althammer-kill.de/news-detail/briefpost-verletzung-des-briefgeheimnisses-droht.html

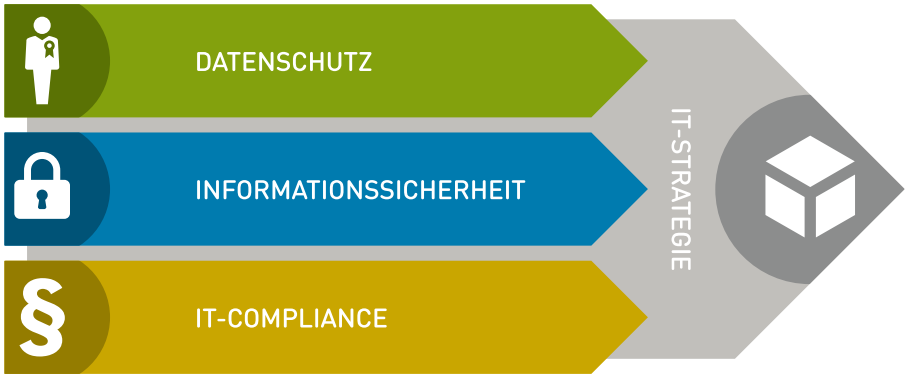
Anmeldemöglichkeiten zu unserem Newsletter finden Sie unter:
www.althammer-kill.de

12 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2016

ALTHAMMER & KILL

Althammer & Kill – Wir schützen Ihre Daten.

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



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 5139 973949-2
ta@althammer-kill.de

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

Mariusz Bucki
Berater für IT-Sicherheit u. Datenschutz
Tel. +49 211 936748-30
mb@althammer-kill.de

Lars Begerow
Berater für IT-Strategie
Tel. +49 211 936748-40
lb@althammer-kill.de

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 211 936748-0
ak@althammer-kill.de

Dr. Jan Holling
Berater für Datenschutz
Tel. +49 5139 973949-4
jh@althammer-kill.de

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

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

Althammer & Kill GmbH & Co. KG

info@althammer-kill.de
www.althammer-kill.de

Mitglied im:

FINSOZ e.V. · GDD Mitglied · BvD e.V. Mitglied

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Standort Hannover:
Buchenhain 15 · 30938 Burgwedel
Tel. +49 5139 973949-0 · Fax -9