Das Titelfoto: Jürgen Frank, neuer Marketingleiter beim Einkaufswagen-Weltmarktführer Wanzl.

KUNDENMAGAZIN • HEFT 4 • MAI 2016

3m5. <script>

Champions auf ganzer Linie

Losziehen und die Welt erobern: 3m5. begleitet Global Player auf ihrem Weg zum Erfolg. Wie Wanzl, einen Weltmarktführer mit Bodenhaftung.

Schlaue Köpfe on- und offline

Was wird aus der sozialen Marktwirtschaft? Das Frankfurter Allgemeine Forum eröffnet Denkräume – mit 3m5.

Wie spricht die Industrie 4.0?

Produktionsanlagen tun sich schwer mit der schnellen Welt im Web. Das geht bei der Sprache los, hat 3m5. evaluiert.

Global Player, **Global Data?**

Wer sich als internationales Unternehmen mit Social Media sowie Datenschutz und -sicherheit befasst, muss viel beachten, sagt Jurist ***Dr. Karsten Kinast***

Einige Global Player sind zögerlich im Umgang mit Social Media. Was sollten sie aus juristischer Sicht beachten?

Social Media ist ein weiter Begriff. Meist assoziiert man Themen wie Fanpage oder Like-Buttons. Tatsächlich geht es aber um jede dem Unternehmen zurechenbare Äußerung auf Foren, in Netzwerken oder sonstigen Umgebungen des Web 2.0. Oft setzen Unternehmen Mitarbeiter als *Botschafter* ein, etwa indem diese einen Twitter-Account für das Unternehmen eröffnen oder auf Facebook einen privaten Account eröffnen, den die Firma dann nutzt. In diesem Fall müssen die Rahmenbedingungen vorher eindeutig geklärt sein: Es gilt, Urheber- und Nutzungsrechte der Bilder und Texte zu klären, damit keine Rechte Dritter verletzt werden. Außerdem ist es problematisch, wenn der Mitarbeiter – auch über seine Beschäftigung beim Unternehmen hinaus – solche Rechte hält. Das könnte für das Unternehmen unangenehme Folgen haben, bis hin zum Verlust oder Missbrauch des Accounts. Wir raten dringend zu Social-Media-Guidelines und Schulungen der Mitarbeiter.

Welche Folgen hat die EU-Datenschutz-Grundverordnung (DSGVO), die ab Mitte 2018 in Kraft tritt, für Unternehmen?

Entgegen anders lautender Gerüchte dürfte der Datenschutz restriktiver, strenger werden als bisher unter dem Bundesdatenschutzgesetz. Dazu zählt die Pflicht zu datenschutzfreundlichen Voreinstellungen von IT-Systemen (Privacy by Design), welche hohe Anforderungen an die Produktimplementierung stellt. Unternehmen haben danach technische und organisatorische Maßnahmen zu treffen, die eine Einhaltung der Datenschutzvorschriften durch IT-Systeme schon durch deren Funktionsweise und nicht nur durch deren Einstellungen gewährleisten. Systeme, die keine Daten löschen können, dürften kritischer sein als bisher.

»Ich bin perplex, dass es Unternehmen gibt, die dem Thema Sicherheit weder strategisch noch im Alltag den erforderlichen Stellenwert einräumen.«

Die ebenfalls neu eingeführte Plicht zur Datenschutz-Folgenabschätzung (Privacy Impact Assessment, PIA) entspricht im Grunde der bisherigen Pflicht zur Vorabkontrolle. Nur dass man nun, wenn man kritische Anwendungen erkennt, die Aufsichtsbehörde zu konsultieren hat.

Auch an die Meldepflicht von Datenschutzverstößen stellt die DSGVO erhöhte Anforderungen. Ein Unternehmen muss den Verstoß bereits dann melden, wenn der Schutz irgendwelcher Daten – also nicht nur besonders sensibler – betroffen ist. Und zwar innerhalb von 72 Stunden nach Kenntniserlangung.

Außerdem erhöhen sich die Anforderungen an die datenschutzrechtliche Einwilligung, und es wird eine strengere Zweckbindung geben. Wer Ja zur Datenverarbeitung sagt, muss also umfassend informiert sein und natürlich auch verstanden haben, was genau mit seinen Daten dann passiert.

Insgesamt stehen Unternehmen verstärkt in der Pflicht, die Anforderungen der DSGVO angemessen umzusetzen. Tun sie es nicht, wird es teurer als bisher: Die Bußgelder steigen auf bis zu 10 Millionen Euro (2 Prozent des weltweiten Jahresumsatzes) bei Nichteinhaltung der Pflichten. Werden Rechte Betroffener verletzt, sind bis zu 20 Millionen Euro (4 Prozent des weltweiten Jahresumsatzes) fällig.

Welche Auswirkungen hat das neue Safe-Harbor-Urteil auf die Datenübermittlungen in die USA für deutsche und europäische Unternehmen?

Der EuGH hat im Oktober 2015 die Safe-Harbor-Entscheidung 2009/529 der EU-Kommission, auf deren Basis ein Datentransfer europäischer personenbezogener Daten in die USA unter bestimmten Voraussetzungen zulässig war, für nichtig erklärt. Daten aus der EU seien nicht ausreichend vor dem Zugriff durch US-Geheimdienste geschützt. Anfang 2016 präsentierte die EU-Kommission das Nachfolgeabkommen für Safe Harbor, das sogenannte EU-/U.S. Privacy Shield. Dieses soll zukünftig die Legitimationsgrundlage für einen rechtmäßigen Datenaustausch mit den USA darstellen. Doch auch das bringt für Unternehmen vorerst nicht die erhoffte Rechtssicherheit. Aktuell ist zu erwarten, dass das EU-/U.S. Privacy Shield nicht geeignet ist, den Anforderungen des EuGH gerecht zu werden. Eine Datenübermittlung in die USA auf Grundlage dieses Abkommens könnte sich also erneut als rechtswidrig herausstellen, oder das Abkommen könnte nicht in Kraft treten oder zu einem späteren Zeitpunkt gekippt werden.

Die deutschen Datenschutzbehörden wollen auch die anderen rechtlichen Möglichkeiten zur Übertragung personenbezogener Daten in nichteuropäische Länder prüfen, etwa die aktuell häufig verwendeten Standardvertragsklauseln. Würden auch diese wegfallen, würde Firmen bis auf die Einwilligung kein legaler Weg zum Datentransfer in die USA offenstehen.

ZUR PERSON

Dr. Karsten Kinast
Partner in seiner Kanzlei in Köln, spezialisiert auf Datenschutzrecht, IT-Recht, Urheberrecht und Medienrecht. Zertifizierter Datenschutzbeauftragter und Lehrbeauftragter an der Hochschule Fresenius mit Vorlesungen zum Zivil- und Medienrecht. Hält im In- und Ausland Vorträge und ist Autor verschiedener juristischer Fachpublikationen.

Welche Schwierigkeiten sind bei der Auswahl nichteuropäischer Dienstleister, zum Beispiel eines Cloud-Anbieters, nach dem Safe-Harbor-Urteil zu erwarten?

US-amerikanische Cloud-Anbieter haben bereits vor dem EuGH-Urteil erkannt, dass viele Unternehmenskunden aufgrund der unsicheren Rechtsgrundlage eine Speicherung der Daten innerhalb der EU präferieren. So hat Microsoft mithilfe einer europäischen Tochtergesellschaft sein Cloud-Produkt Azure bei Verträgen mit europäischen Kunden bereits sowohl auf EU-Standardvertragsklauseln als auch auf das Safe-Harbor-Abkommen gestützt.

Weiterhin besteht die Möglichkeit, die Daten von Microsoft oder auch Amazon Web Services (AWS) ausschließlich auf Servern innerhalb der EU zu hosten. Doch dürfte die Möglichkeit, den Vertrag mit einer europäischen Tochtergesellschaft einer amerikanischen Mutter zu schließen, aus datenschutzrechtlicher Sicht nicht als ausreichend zu bewerten sein. Denn laut dem Patriot Act können US-Behörden Daten von einer in der EU ansässigen Tochtergesellschaft beschaffen. Es bestehen also bei der europäischen Tochtergesellschaft die gleichen Zugriffsmöglichkeiten durch US-Behörden wie beim in den USA ansässigen Unternehmen selbst.

Sicher erscheint eine Konstruktion, bei der der amerikanische Cloud-Anbieter einen Dritten einbindet, der in Europa sitzt und gerade nicht gesellschaftsrechtlich mit dem Cloud-Anbieter verbunden ist, so wie etwa T-Systems für Microsoft. Denn so weit greift der US-amerikanische juristische Arm dann doch nicht.

Global agierende Unternehmen haben oft Angst um die Sicherheit ihrer Daten – was raten Sie diesen?

Ich bin manches Mal perplex, dass es exponierte Unternehmen gibt, die dem Thema Sicherheit weder strategisch noch im Alltag den erforderlichen Stellenwert einräumen. Oder meinen, dass sich die diversen Dienstleister für das jeweilige Tool schon um die Sicherheit kümmern werden – und dabei einen ganzheitlichen Ansatz völlig vermissen lassen. Oft gibt es nicht einmal einen Informationssicherheitsbeauftragten. In solchen Fällen kann ich die von Ihnen erwähnte Angst sehr gut nachvollziehen.

Wir raten, etwas gegen diese Angst zu tun, indem Transparenz über den eigenen Schutzbedarf hergestellt und dann über die passenden Maßnahmen entschieden wird. Dann habe ich als Unternehmer Gewissheit darüber, ob ich in gewissen Fragen ein kleineres, mittleres oder höheres Risiko eingehen möchte. Selbst wenn sich die Kosten für eine höhere Sicherheit nicht rechnen, kann ich vorher ein Datensicherheitsrisiko realisieren, Eintrittswahrscheinlichkeit und Schadensumfang kalkulieren und einen Notfallplan entwickeln, der trotz nicht perfekter Primärmaßnahmen im Schadensfall dann sehr gut greift.

Auch rechtliche Rahmenbedingungen fangen bezüglich der Datensicherheit an, eine größere Rolle zu spielen. Wichtig sind neben dem neuen IT-Sicherheitsgesetz vor allem internationale Vorgaben wie die Ende vergangenen Jahres beschlossene Richtlinie zur Netz- und Informationssicherheit (NIS) der EU. Diese wird weniger diskutiert als die Datenschutz-Grundverordnung, dürfte aber eine ähnliche Relevanz für die Praxis haben. Oder die Frage, ob gewisse Security Tools rechtlich akzeptabel sind. So sollte ich genau überlegen, ob ich SSL-Verschlüsselungen in der Kommunikation der Mitarbeiter aufbreche, wenn ich gleichzeitig die private Nutzung der betrieblichen Kommunikationsmittel erlaube. Der Zweck heiligt eben nicht immer die Mittel.