MM TITEL-INHALT

DATENSCHUTZ-REGELUNGEN

MM TITEL

KOMMT DIE EU-DSGVO ZU SPÄT?

Am 25. Mai endet die Übergangsfrist für die Europäische Datenschutz-Grundverordnung (EU-DSGVO) und **Datenschutzverstöße** werden mit hohen Strafen belegt. Kurz vor diesem Stichtag herrscht helle Aufregung um die Facebook-Datenpanne. Ob unter den 50 Mio. betroffenen Kunden auch EU-Bürger sind, ist noch unklar. Doch schon jetzt kann man aus dem Facebook-Debakel zweierlei lernen: Erstens, wie man es nicht macht. Zweitens, wie man es selbst besser macht.

Esther Niederhammer

Facebook – gefällt mir nicht mehr! Wie sehr diese Umkehrung des weltweit erfolgreichen Slogans den Facebook-Gründer schmerzen muss, ist kaum auszudenken. Der Stolperstein: eine missglückte Datenschutzstrategie, die mit Datensammlung und Datennutzung begann und mit Datenhandel, Datenvernachlässigung, Datenmissbrauch und Vertrauensverlust zu enden scheint. Natürlich gilt auch hier, wie bei jeder klassischen Tragödie: je höher der Status, desto tiefer der Fall.

Noch weiß man nicht, wie diese Geschichte ausgehen wird, doch dass die britische Datenanalysefirma Cambridge Analytica Zugriff auf Daten von 50 Mio. Facebook-Nutzern hatte, sorgte für ein PR-Debakel und ein finanzielles Desaster. Facebook verlor an der Börse binnen drei Tagen ab Bekanntwerden dieser Informationen bis zu 50 Mrd. US-Dollar an Unternehmenswert. Die Süddeutsche Zeitung titelte zu diesem Zeitpunkt sogar „Der blaue Riese wankt". Und mit jedem weiteren Detail, das ans Licht kam, geriet das Unternehmen mehr ins Schleudern, denn es gab ohne Zustimmung der Nutzer offenbar besonders heikle Formen der Datennutzung, möglicherweise sogar eine Beeinflussung des US-Wahlkampfes.

MM INFO

EU-DSGVO AUF DEN PUNKT GEBRACHT

- Stichtag 25. Mai 2018
- DSGVO löst EU-Richtlinie 95/46/EG ab
- Datenschutzregeln europaweit vereinheitlicht und für alle Länder verbindlich
- Verstöße werden mit Bußgeldern bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes geahndet
- Marktortprinzip löst Standortprinzip ab, das heißt, die EU-DSGVO gilt auch für Unternehmen mit Firmenhauptsitz außerhalb der EU, sofern Angebote an Kunden in der EU gerichtet sind
- Informations- und Auskunftspflicht deutlich erweitert, lückenlose Dokumentation vorgeschrieben
- Produkte und Programme müssen nach dem Prinzip „privacy by design" / „privacy by default" gestaltet werden, das heißt, datenschutzfreundlich und DSGVO-konform voreingestellt sein (aktueller Stand der Technik ist relevant)
- Für Datenschutzpannen mit hohen Risiken für persönliche Rechte gilt eine Meldepflicht binnen 72 h
- Kunden haben Recht auf „Vergessenwerden" / Löschung
- Kunden haben ein Recht auf Datenübertragbarkeit / Datenportabilität
- Betriebliche Datenschutzbeauftragte müssen jetzt die Einhaltung der DSGVO auch überwachen (erweiterte Haftung)
- Outsourcing von Daten führt nicht automatisch zur Auslagerung der Haftung
- Unternehmen mit besonders hohen Datenaufkommen beziehungsweise mit besonders sensiblen Daten oder Angebote mit Profiling-Absichten sind zu einer Datenschutz-Folgenabschätzung verpflichtet

maschinenmarkt.de Suche „EU-DSGVO"

DATENPANNEN PASSIEREN TÄGLICH UND ÜBERALL

Dass langjährige Facebook-Gegner jetzt zur Schadenfreude neigen, ist einerseits verständlich. Sich aber ausschließlich an Facebook festzubeißen oder sich auf dieser Seite des großen Teiches sicherer zu fühlen, ist weder sinnvoll noch angebracht. Datenverlust und Datenklau sind in allen Branchen und Ländern an der Tagesordnung. Der IT- und Telekommunikationsnachrichtendienst Heise.de – ein guter Gradmesser, da dort neben technischen Neuerungen und Produkttests auch Technikpannen und Datenschutzpleiten zusammengetragen und verarbeitet werden – wies im März 2018 auf einen Trojaner hin, der auf 40 günstigen Android-Smartphones aus Asien schon vorinstalliert ist und so unbemerkt in die Taschen und Leben der Smartphonenutzer wandert, inklusive Update der Malware. Ebenfalls in den letzten Monaten betroffen: der Fahrdienstleister Uber (Beute: persönliche Daten von 57 Mio. Fahrgästen und 7 Mio. Fahrern), das 4G-LTE-Netz (Forscher entdeckten gefährliche Schwachstellen), Apple (Unlock-Software ermöglicht Auslesen von I-Phones vom Typ iOS 10 und 11) und Regierungen mehrerer Staaten (weltweiter Hackerangriff auf Regierungsnetze, darunter 17 Rechner der Bundesregierung). Die Liste ließe sich endlos fortsetzen.

Natürlich kann Datenprotektionismus jetzt nicht die Lösung sein. Ohne Daten läuft weltweit nichts mehr. Personenbezogene Daten werden benötigt für die Auftragsabwicklung, die gezielte Werbeansprache, für Neukundenakquise und Kundenbindung. „Datenprotektionismus, wie man ihn früher oder auch vor zehn Jahren noch verstanden hat, ist nicht mehr möglich", sagt auch Nicolas Woltmann, Diplom-Jurist und wissenschaftlicher Mitarbeiter an der Forschungsstelle Robot-Recht der Universität Würzburg. „Die Verarbeitung von Daten wird immer wichtiger und immer mehr Unternehmen setzen darauf, weil sie wichtige Informationen für ihr Unternehmen erhalten, zum Beispiel wie man Produkte und Dienstleistungen verbessern kann." Natürlich stehen Facebook, Google, Amazon für eine besondere Datensammelwut. Doch auch von Unternehmen, an die man in diesem Zusammenhang nicht unbedingt denkt, werden immer mehr Daten gesammelt. „Das hat eine Eigendynamik entwickelt, die auch das Datenschutzrecht komplett überholt hat. Und je mehr von diesen persönlichen Daten gesammelt werden, desto größer wird die Gefahr, dass es auch zu Lecks oder Cyberangriffen kommt, wo große Datensätze erbeutet werden", sagt Woltmann. „Hier versucht das Regelwerk der EU-DSGVO anzusetzen. Es schafft Rahmenbedingungen, um den Missbrauch von Daten einzudämmen."

UNFREIWILLIGE DATENSCHUTZ-LEKTIONEN DURCH FACEBOOK

Die Debatte über Facebook wirkt wie ein Weckruf für die Umsetzung der EU-DSGVO. Sie spielt Datenschützern und kritischen Konsumenten in die Hände. Daher ist die große Öffentlichkeit jetzt ebenso schmerzhaft wie gut. Die Industrie sollte also das Facebook-Debakel zum Anlass nehmen, um zu lernen. Und es selbst besser zu machen.

Was haben Facebook und Uber also falsch gemacht? Auf den ersten Blick fast alles. Zunächst war man sich seiner Sache offenbar allzu sicher, hat sich auf Vermarktungsstrategien konzentriert und auf Erfolgen des eigenen Geschäftsmodells ausgeruht. Dabei sind wesentliche, kritische Aufgaben im Alltagsgeschäft vergessen oder halbherzig bis schlampig erledigt worden. Oder gar nicht. Auch das passiert allen und überall täglich; es ist zutiefst

MM FAZIT

NICHT NUR BUSSGELDER SIND FÜR UNTERNEHMEN SCHMERZHAFT, WIE DAS BEISPIEL FACEBOOK ZEIGT.

Stéphane Itasse, Redakteur

MM INFO

SO REDUZIEREN SIE DAS RISIKO FÜR DATENVERLUST IN IHREM BETRIEB

- Halten Sie sich ganz strikt an das Grundprinzip der Datenminimierung: Daten, die Sie nicht erheben und speichern, können auch nicht verloren gehen oder missbraucht werden.
- Sichern Sie die für den Betrieb unbedingt notwendigen personenbezogenen Daten durch ein konsequentes Datenschutzkonzept.
- Formulieren Sie Datenschutzauflagen so klar und so einfach wie möglich. Es darf keinen Interpretationsspielraum in Ihren internen Anweisungen geben.
- Trennen Sie, wo immer möglich, Maschinendaten und personenbezogene Daten.
- Anonymisieren und verschlüsseln Sie Daten so früh wie möglich. Damit werden Daten für bestimmte kriminelle Gruppen sofort unbrauchbar.
- Beschränken Sie den Zugriff auf personenbezogene Daten auf wenige und besonders geschulte und geeignete Personen in Ihrem Betrieb.
- Automatisieren Sie Prozesse innerhalb der Datenschutzabläufe, um menschliche Fehleinschätzungen oder Nachlässigkeiten im Umgang mit Daten auf ein Mindestmaß zu reduzieren.
- Nutzen Sie externes Know-how (zum Beispiel Beratung und Audits), um Schwachstellen in Ihrem Datenschutzkonzept zu identifizieren und ein Notfallkonzept für Datenpannen zu definieren.
- Installieren Sie technische Sperren und automatische Löschung von nicht mehr benötigten Daten, um versehentlichen oder missbräuchlichen Zugriff auf sensible Daten zu unterbinden.
- Nehmen Sie interne Kritik am Unternehmen ernst. Unzufriedene Mitarbeiter stellen ein hohes Risiko für Datenabfluss und -missbrauch dar.

menschlich. Facebook steht vielleicht wie kein anderes Unternehmen im Fokus der Kritik, weil man diesen Technik- und Innovationsfreaks aus dem Silicon Valley die notwendigen technischen Fähigkeiten und auch die hohe Priorisierung des Datenschutzes zutraute und sie auch besonders erwartete.

Trotz Warnungen und langjähriger Kritik von Datenschützern hat Facebook die Dringlichkeit und auch das Risiko des eigenen Datengeschäfts nicht verstanden oder nicht ernst genug genommen. In diesem Zusammenhang ist Facebook nicht einfach Opfer von kriminellen Machenschaften geworden, auch wenn Zuckerberg in einer Pressemitteilung äußert: „Das ganze Unternehmen ist entsetzt darüber, dass wir hintergangen wurden". Man hat die vorhandenen Daten nicht effizient genug und nach Stand der Technik geschützt. Zu viele unterschiedliche Menschen hatten Zugriff auf zu viele Daten. Das Unternehmen hatte keine ausreichenden technischen oder vertraglichen Hürden, die Datenmissbrauch in dieser Form unterbunden hätten. Auch gab es keine verlässlichen Warnsysteme, die den Abfluss von Daten an interne oder externe Datenschutzstellen gemeldet hätten. Die Strukturen und Prozesse sind offenbar zusätzlich so ungegliedert oder schlecht dokumentiert, dass Facebook-Gründer Mark Zuckerberg nach erstem Schweigen und sicher intensiven Beratungen durch Juristen im Hintergrund vor der Presse formulieren musste: „Es ist schwer zu sagen, was wir finden werden."

Um nun selbst nicht nur über Facebook zu schwadronieren: In fast allen Datenschutzskandalen geht es um die gleichen Nachlässigkeiten und Fehler im Umgang mit personenbezogenen Daten. Uber, ein weiteres Schwergewicht mit einer großen Erfolgsgeschichte, hat einen zusätzlichen Kapitalfehler begangen: Statt ab dem Tag X transparent mit der eigenen Datenpanne umzugehen und den Verlust von Kfz-Kennzeichen von rund 600.000 US-Fahrern zu melden sowie die Kunden vor weiteren Schädigungen zu bewahren, zahlte Uber den Tätern 100.000 Dollar, um den Vorfall zu vertuschen. „Das ist die schlechtestmögliche Art, mit sowas umzugehen", sagt Woltmann. „Es wird ja häufig von der Salamitaktik gesprochen, dass man genau so viel nach außen preisgibt, wie unbedingt nötig ist. Das scheint ein Grundsymptom zu sein bei großen Unternehmen."

WIE STEHT ES UM DIE DSGVO-VORBEREITUNGEN IN DEUTSCHLAND?

Zurück nach Deutschland, zurück zur Industrie im Zusammenhang mit dem Datenschutz. Eine Nachfrage von MM bei verschiedenen, auch renommierten Industrieunternehmen im August letzten Jahres anlässlich des ersten Schwerpunktartikels über die

MM INFO

SO VERMEIDEN SIE HOHE GELDBUSSEN IM FALLE EINER DATENPANNE

- Sorgen Sie für eine aktualisierte, eindeutige und unmittelbar zugängliche Aufklärung darüber, wann welche Daten von Ihnen wozu und wie lange erhoben, gespeichert und gegebenenfalls weitergegeben werden (erweiterte Informationspflicht der DSGVO).
- Gewährleisten Sie eine lückenlose und jederzeit abrufbare Dokumentation aller datenschutzrelevanten Prozesse (erweiterte Dokumentationspflicht der DSGVO).
- Investieren Sie nachweislich in die Datenschutzkompetenz Ihrer Beschäftigten (zum Beispiel durch Schulungen, wiederholte Audits, Prämien für interne Hinweise auf Datenschutzlücken).
- Anonymisieren und verschlüsseln Sie Daten ab dem frühestmöglichen Zeitpunkt, insbesondere wenn Sie Daten an Dritte übermitteln (zum Beispiel in eine Cloud). Wenn Ihr Geschäftspartner gehackt wird oder auch pleite geht, haben Sie Ihre Auflagen für den Datenschutz dennoch erfüllt und können hohe Bußgelder für Ihren eigenen Betrieb vermeiden.
- Definieren Sie eine klare Anlaufstelle für Datenschutzbelange und schulen Sie diese Stelle nachweislich für alle möglichen Datenschutzanfragen von Kunden und Aufsichtsbehörden.
- Erarbeiten und üben Sie einen Notfallplan für den Fall einer Datenpanne. Ein unmittelbares Umsetzen dieses Planes begrenzt im Ernstfall weiteren Schaden und dient den Behörden als Nachweis für die Ernsthaftigkeit und Professionalität des betrieblichen Datenschutzkonzepts.
- Schaffen Sie – im Gegensatz zu Facebook und Uber – unverzüglich Transparenz, wenn es zu Datenschutzpannen in Ihrem Unternehmen gekommen ist (Meldepflicht der DSGVO). Auch dies gehört zu einer konsequenten Datenschutzstrategie und kann im Ernstfall sogar eine vertrauensstärkende Maßnahme für Ihre Kunden bedeuten.
- Nehmen Sie die DSGVO auch nach dem Stichtag noch ernst und bleiben Sie am Thema dran! Ein veralteter Datenschutz unterhalb des Standes der Technik wird laut DSGVO schnell wie ein gar nicht vorhandener Datenschutz gewertet.

MM INTERVIEW

INTERVIEW MIT NICOLAS WOLTMANN

Diplom-Jurist und wissenschaftlicher Mitarbeiter an der Forschungsstelle Robot-Recht, Lehrstuhl Prof. Dr. Dr. Eric Hilgendorf, Universität Würzburg

Bild: Nicolas Woltmann

„Das Problem an Daten ist ja, dass sie sich derartig leicht vervielfältigen lassen, dass man ab dem Zeitpunkt, an dem man die Daten abgibt, eigentlich keine Kontrolle mehr darüber hat", sagt Nicolas Woltmann von der Forschungsstelle Robot-Recht.

Hat Facebook alles falsch gemacht?
Das ist im Augenblick nicht eindeutig zu sagen. Schwierig ist, dass Facebook Dritten ermöglicht hat, über Apps auf derartig viele Daten und Nutzerkonten zuzugreifen, wobei das gleichzeitig das Geschäftsmodell von Facebook und den App-Anbietern ist. Wenn man sich die Einwilligung von den Kunden holt, dann ist es schwer, hier von unternehmerischem Versagen zu sprechen. Wirklich problematisch ist, dass vorhandene Daten rechtswidrig, ohne Einwilligung der Nutzer, anderweitig genutzt wurden. Facebook behauptet, das sei ein Betrug des Dritt-Unternehmens Cambridge Analytica, wobei hier die Frage ist, inwieweit Facebook in der Lage gewesen wäre, dies zu unterbinden. Wo ich aber definitiv ein Versagen sehen würde, ist beim Krisenmanagement. Facebook ist seit 2015 bekannt gewesen, dass es ein Leck gibt, doch das wurde nicht offengelegt. Nach der neuen Datenschutzgrundverordnung wäre das nötig gewesen. Es besteht die ausdrückliche Pflicht, solche Vorfälle der Aufsichtsbehörde zu melden, in schweren Fällen auch den Betroffenen.

Kommt die EU-DSGVO für betroffene Facebook-Kunden zu spät?
Noch weiß man nicht, ob EU-Kunden betroffen sind. Wenn dem aber so ist, wäre der Vorfall ein grober Verstoß gegen die DSGVO und zumindest Teile der Datenpanne haben sich nach Inkrafttreten der Verordnung 2016 und innerhalb der Umsetzungsfrist ereignet. Welches Strafmaß hier folgt, ist noch unklar. Interessant für mich ist, dass der Vorfall einige Wochen vor dem Stichtag des 25. Mai 2018 publik wurde. Ich kann da aus meiner Position heraus schlecht Absicht unterstellen, aber für mich ist das zumindest ein lustiger Zufall.

Was ist für deutsche Unternehmen die größte Herausforderung der DSGVO?
Da die EU-DSGVO zu einem erheblichen Teil auf dem alten Bundesdatenschutzrecht aufsetzt, sind deutsche Unternehmen im europäischen Vergleich gut bedient. Die größte Herausforderung ist der organisatorische Mehraufwand durch die erweiterte Dokumentationspflicht. Ich muss als Unternehmer jetzt ständig in der Lage sein, nachzuweisen, was ich wann und warum erhoben und verarbeitet habe und wer darauf Zugriff hat. Gerade für mittelständische Betriebe ist das aufwendig. Doch die Qualität und Schlüssigkeit der Dokumentation wird am Ende den Ausschlag geben darüber, wie meine Verantwortung bewertet wird und welche Bußgelder auf Verstöße folgen.

Wem gehören Daten, die in der Cloud gespeichert werden?
Das ist derzeit sehr umstritten. Es gibt Leute, die sagen, wenn der Cloud-Anbieter die Daten empfängt und bei sich speichert, dann hat er darüber auch ein Verfügungsrecht. Aber es gibt kein Dateneigentum, wie man ein Eigentum an einem Stuhl, einem Handy oder ähnlich physischen Dingen hat. Das Problem an Daten ist ja, dass sie sich derartig leicht vervielfältigen lassen, dass man ab dem Zeitpunkt, an dem man die Daten abgibt, eigentlich keine Kontrolle mehr darüber hat.

Wie kann man diese Daten dennoch schützen?
Es ist wichtig, dass man eine eigene Weiternutzung von Daten, außerhalb des Auftragsrahmens, vertraglich ausschließt. Zwar habe ich auch dann keine Möglichkeiten, zu verhindern, dass ein Auftragsverarbeiter mit den Daten schaltet und waltet, wie er will. Aber juristisch gesehen, habe ich mich abgesichert. Zusätzlich kann ich die Daten durch Verschlüsselung zumindest teilweise unbrauchbar machen und damit die Persönlichkeitsrechte meiner Kunden zusätzlich schützen. Besonders wirksam ist es, Daten zu anonymisieren oder zu pseudonymisieren. Selbst wenn solche Daten in falsche Hände geraten, kann man auf der anderen Seite nicht so viel damit anfangen, da der Personenbezug fehlt. Und um eine Verschlüsselung zu umgehen, müsste man selbst eine Straftat begehen.

EU-DSGVO ergab – nichts (siehe MM 38/2017). Betriebliche Datenschutz-Mailadressen liefen ins Leere, telefonische und schriftliche Anfragen zum Stand oder Aufwand der aktuellen Umsetzung der DSGVO wurden nicht beantwortet oder abgelehnt. Einige Monate später? Dasselbe Ergebnis. Desinteresse? Überforderung? Datenprotektionismus? Eingeständnis eines mangelnden Datenschutzes? Keine Zeit wegen fieberhafter Hintergrundarbeiten im Zusammenhang mit der DSGVO? All dies ist unklar. Natürlich waren dies nur Stichproben und die vorbildlichen Unternehmen in puncto Datenschutz gibt es auch. Dennoch sei die Frage erlaubt: Wie viel Facebook steckt ehrlicherweise in der täglichen Datenerhebung und -nutzung deutscher Unternehmen? Und ist es nicht Zeit, die Speicherung von personenbezogenen Daten zur Chefsache zu machen?

Die EU-DSGVO stellt die Weichen und es führt kein Weg an besserem Datenschutz vorbei. Natürlich bedeutet die Umsetzung der Maßnahmen einen erheblichen Aufwand, sowohl organisatorisch wie finanziell. Doch die massiven Datenpannen der letzten Tage, Monate und Jahre zeigen auch, dass der Datenschutz noch ernster genommen werden muss als bisher. Die neue Verordnung kann auch eine Chance sein, nämlich dann, wenn sie zum hilfreichen Antreiber gemacht wird, um sich selbst, persönlich, im eigenen Unternehmen oder als betrieblicher Datenschutzbeauftragter endlich um das gefürchtete oder immer wieder verschobene Thema Datenschutz zu kümmern.

Ein professionelles Datenschutzkonzept gehört in unserer vernetzten Welt zu einem Paket von unverzichtbaren unternehmerischen Maßnahmen, um den eigenen Standort und die Position innerhalb der Industrie zu sichern und dem Verlust der Kunden und Finanzmittel vorzubeugen, die jeder großen Datenpanne folgen. Damit Ihnen dies leichter fällt, sind die wichtigsten Punkte der Verordnung noch einmal für Sie zusammengefasst. MM