funkschau

business.technology.strategy

funkschau.de

IfKom Ingenieure für Kommunikation

MANAGED SERVICES
Vom Techniker zum IT-Koordinator

ARBEITSPLATZ DER ZUKUNFT
Fundamentaler Wandel – große Chance

VIRTUAL REALITY
Herausforderung B2B

WLAN
Netzwerkmanagement aus der Cloud

8
2017
28. April
€ 6,00 sfr 10,00

RICHTIGES KUNDEN-DATENMANAGEMENT NACH DER EU-DSGVO

Die EU-Datenschutzgrundverordnung stärkt die Rechte von Betroffenen und bringt mehr Pflichten für Unternehmen sowie höhere Strafen bei Verstößen mit sich. Vorsicht ist besonders bei Big Data-Analysen geboten, da die Datenverarbeitung künftig von berechtigtem Interesse sein muss. Um weiterhin von Daten profitieren zu können, und damit Umsatz zu steigern, sowie Kosten und Risiken zu minimieren, bleibt Unternehmen noch ein Jahr Zeit, ihr Kundendatenmanagement für die neue Verordnung zu rüsten.

Autoren: Holger Stelz und Thorsten Schremmer **Redaktion: Axel Pomper**

➤ Der Wunsch vieler Betreiber von Online- und Social Network-Plattformen, möglichst viele Daten ihrer Nutzer und Kunden zu erfassen und auszuwerten, steht im Gegensatz zum „Recht auf informationelle Selbstbestimmung“. Die neue Datenschutz-Grundverordnung der EU soll die Grundlage für einen einheitlichen Datenschutz in allen 28 EU-Staaten bilden. Im März soll die erste deutsche Fassung erarbeitet werden, bevor sie ab dem 25. Mai 2018 angewendet wird.

Mehr Pflichten und höhere Anforderungen

Die EU-DSGVO dient dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Das bedeutet unter anderem, dass Betroffene von Unternehmen ab sofort über Art, Umfang, Grund und Zweck der Datenerhebung sowie über ihre Rechte (Widerspruch, Beschwerde) informiert werden müssen. Zudem muss die Datenverarbeitung von „berechtigtem Interesse“ sein. Allerdings ist die Rechtslage hier noch sehr unsicher. Denn der Rahmen und die Grenzen zwischen dem Interesse an der Datenverarbeitung in einem CRM-System und dem Interesse des Kunden am Datenschutz sind noch nicht abgesteckt.

Doch es kommen noch weitere Pflichten auf die Unternehmen zu, die sich besonders auf das Kundendatenmanagement auswirken und neue Anforderungen an die Datenanalyse stellen:

Dokumentationspflicht: Alle Vorgänge in Zusammenhang mit Kundendaten müssen künftig genau dokumentiert werden – angefangen bei der Einwilligung des Kunden: Dieser muss nun aktiv zustimmen, dem Unternehmen seine Daten zur Verfügung zu stellen. Ein per Default gesetzter „Ich akzeptiere die Bestimmungen“-Haken ist nicht mehr rechtsgültig. Ideal ist ein „Double-Opt-In“-Verfahren, bei dem der Kunde erst aktiv einen Haken unter die Bestimmungen setzt und anschließend seine Willenserklärung durch den Klick auf einen Bestätigungslink in einer separaten Mail bekräftigt. Es ist empfehlenswert, den Zeitpunkt und den Kanal der Einwilligung zu dokumentieren, um im Falle von Streitigkeiten belastbare Nachweise erbringen zu können. Ebenso sollten der Widerruf und Änderungen an den Bestimmungen festgehalten werden.

➤ **Pflicht zur Löschung der Daten:** Unternehmen müssen bald in der Lage sein, im Falle eines Widerrufs die Daten zu löschen oder zu maskieren, ohne damit die Integrität der Daten aufzuheben. Ist ein Browserverlauf Teil des zu löschenden Datenbestandes, muss er entfernt werden können, ohne dass der verbleibende Kundendatensatz dadurch inkonsistent wird. Hinzu kommt die Vorgabe, die Daten zu löschen, wenn ihre Speicherung nicht mehr notwendig ist, die Daten unrechtmäßig verarbeitet wurden oder eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht. Im Einzelfall ist zu entscheiden, welche Attribute, also Strukturinformationen der Daten, bewahrungswürdig sind. Dies hängt vom Geschäftsmodell des Unternehmens und der Art der Kundenbeziehung ab. Besonders im Onlinebereich zieht dies notwendige technische Änderungen nach sich, da die Oberflächen vieler Customer-Facing-Systeme und auch vieler Apps auf mobilen Endgeräten nicht auf diesen Anwendungsfall ausgelegt sind.

➤ **Überwachungsaufgabe für betriebliche Datenschutzbeauftragte:** Die im Unternehmen eingesetzten betrieblichen Datenschutzbeauftragten erhalten zusätzlich zu ihren bisherigen Aufgaben – Sicherstel-

Bild: fs Quelle: fotolia

lung und Hinwirkung von Datenschutz – nun auch den Überwachungsauftrag, dass im Unternehmen alle Vorgaben und Regelungen eingehalten werden. Das hat zur Folge, dass Unternehmer und Beauftragte zukünftig persönlich bei Verstößen haften. Durch diese Änderung wird dem Zuständigen eine deutliche gewichtigere Rolle zuteil. Besonders bei externen Datenschutzbeauftragten bedeutet dies eine engere Verflechtung in die regulären Prozesse und die täglichen Aufgaben – so werden sie häufiger bei der Planung von Direktmarketingmaßnahmen konsultiert.

Zentraler Datenstamm und 360-Grad-Sicht

Die neuen Pflichten fordern von Unternehmen an vielen Stellen, ihre bestehenden Systeme umzustellen. Auf jeden Fall sollten sich auch Marketing- und Vertriebsverantwortliche darüber informieren, was sie künftig im Umgang mit Daten beachten müssen, um nicht gegen die neuen Regelungen der EU-DSGVO zu verstoßen.

So müssen Unternehmen in der Lage sein, die Daten in den verschiedenen Systemen, die sie zur Datenverarbeitung nutzen, mit dem entsprechenden Kunden in Verbindung zu setzen. Das erfordert eine eindeutige Zuordnung von Kundendaten über Systemgrenzen hinweg. Idealerweise erfolgt diese Maßnahme über einen unternehmensweiten, zentralen Pool, der alle Systeme versorgt und die Verteilung der Daten in den einzelnen Datensenken protokolliert. Sind Kundendaten noch in Silos organisiert, wird es deutlich schwieriger, die neuen rechtlichen Anforderungen zu erfüllen. Oftmals werden Informationen nach dem „Gießkannenprinzip“ in die Silos verteilt und alle über einen Kunden verfügbaren Daten in vielen verschiedenen Systemen, wie ERP, CRM sowie Marketing-Automation, redundant gehalten und teilweise verändert. Das ist nicht nur hochgradig ineffizient, es erschwert zukünftig, Daten nachzuvollziehen, zu korrigieren oder zu löschen. Um Datensilos zu vermeiden, sollte ein zentraler Datenstamm – zum Beispiel mithilfe eines Master-Data-Management-Systems – geschaffen werden. Nur so können Unternehmen sicherstellen, dass im Falle einer vom Endverbraucher angeforderten Löschung alle Instanzen eines Attributes auch in allen Systemen entfernt wurden. Sie müssen sich darüber bewusst sein, dass bei Nichteinhaltung die persönliche Haftung von Geschäftsleitung und Datenschutzbeauftragten drastische persönliche und finanzielle Folgen nach sich ziehen kann.

Ziel sollte es sein, eine 360-Grad-Sicht auf den Kunden zu gewährleisten. Das ist nicht nur notwendig, um der Dokumentationspflicht nachzukommen, sondern auch, um Fremdverstöße innerhalb kürzester Zeit melden zu können. Sind erst noch alle Daten umständlich zusammenzusuchen, besteht die Gefahr, dass nicht wirklich alle Informationen miteinbezogen werden – oder zu viel Zeit benötigt wird. Um schnell reagieren und den Kunden über Art, Umfang, Grund und Zweck der Datenerhebung informieren zu können, muss außerdem sichergestellt sein, dass seine Kontaktdaten korrekt sind. Das gelingt zum Beispiel durch eine Validierung für E-Mail-Adressen, einer postalischen Validierung oder einer korrekten Zuordnung. Braucht das Unternehmen zu lange, den Kunden diese Informationen mitzuteilen oder versäumt es komplett, drohen empfindliche Bußgelder. Konkret müssen Unternehmen zukünftig in der Lage sein, innerhalb einer engen Frist von maximal drei Monaten auf entsprechende Auskunftsanfragen zu reagieren. Datenschutz ist also nicht länger ein „nice to have“, sondern wird zu einem wichtigen, durchgängigen und nachhaltigen Prozess, bei dessen Scheitern unter Umständen sogar der Fortbestand des Unternehmens gefährdet sein kann.

Anonymisierung und Pseudonymisierung

Unternehmen können ebenso Einbußen erleiden, wenn sie ihre Daten nicht wie gewohnt auswerten können. Denn von Big Data-Analysen hängen oft Konzepte oder sogar ganze Geschäftsmodelle ab. Die EU-DSGVO schränkt in dieser Hinsicht ein. Daten können plötzlich gelöscht werden, es gibt weniger Freiheiten bei der Datenauswertung und Prozesse werden aufwändiger. Vielen Unternehmen stellt sich die Frage, wie sie weiterhin von ihren Daten profitieren können, ohne gegen die neuen Regelungen zu verstoßen oder etwa einen Datenmissbrauch zu riskieren. Zwei mögliche Lösungen sind die Anonymisierung und Pseudonymisierung.

Auf der sicheren Seite sind Unternehmen, wenn sie ihre Daten anonymisieren. Dabei wird sichergestellt, dass eine Zuordnung von Datenbeständen zu einer bestimmten Person nicht mehr oder nur mit extrem hohem Aufwand möglich ist. Diese Methode eignet sich beispielsweise, um Verhaltensweisen der Kunden oder Trends zu analysieren – ohne die Ergebnisse für personenbezogene Maßnahmen zu verwenden, da der jeweilige Kunde nach der Anonymisierung nicht mehr identifizierbar ist. Es können allerdings immer noch Maßnahmen für bestimmte Segmente oder Kundengruppen mit bestimmten Eigenschaften wie Alter, Interessen oder Standort einer Person abgeleitet werden. Außerdem muss man anonymisierte Datensätze nicht löschen, da keine individuellen Informationen mehr in ihnen vorhanden sind – ganz egal, ob der Kunde seine Einwilligung widerrufen hat oder eine Speicherung aus anderen Gründen nicht mehr notwendig ist.

Die Pseudonymisierung hingegen erlaubt es, Rückschlüsse und Auswertungen von Big Data-Analysen für zielgerichtete Maßnahmen wie zum Beispiel eine individuelle Kundenansprache oder personalisierte Angebote zu nutzen. Bei dieser Methode wird lediglich die Identität des Kunden verschleiert. und der Name beispielsweise durch eine ID ersetzt. Die pseudonymisierten Daten darf das Unternehmen für Analysen verwenden. Allerdings kann die ID mittels Mappingtabellen wieder den ursprünglichen Kundendaten zugeordnet werden. Entsteht ein Datenleck, ist hier die Gefahr größer, dass sich die Daten über das System doch wieder dem jeweiligen Kunden zuordnen lassen. Deswegen ist eine Anonymisierung empfehlenswerter.

Beide Lösungen zeigen: Big-Data-Analysen werden für Unternehmen mit der neuen EU-DSGVO durchaus aufwändiger – aber nicht unmöglich. Wenn Unternehmen ihre Systeme rechtzeitig umstellen, sich einen Überblick über ihre Daten verschaffen und ihr Kundendatenmanagement für die neuen Änderungen rüsten, können sie auch weiterhin von der Datenverarbeitung profitieren.

Holger Stelz ist Director Marketing & Business Development bei Uniserv
Thorsten Schremmer ist Solution- & Product Management bei Uniserv