Das comTeam Kunden-Magazin.
Ausgabe Juni 2018

EF.IT
ERFOLGSFAKTOR-IT

DSGVO

Die EU-DSGVO greift - was tun, wenn man sich noch nicht darauf eingestellt hat?

Industrie 4.0 | Seite 8
Neue Lösungen gegen neue Bedrohungen durch IoT

VR-Headsets | Seite 10
Warum sich Unternehmen für Virtual Reality interessieren sollten.

Multifaktor-Authentifizierung | Seite 13
Schlüssel zu mehr Sicherheit

© Vasily Merkushev - #200491765 - Fotolia.com

WIR DIGITALISIEREN ZUKUNFT

comTeam
DAS TECHNOLOGIE-NETZWERK

© Xtravagant - #201123071 - Fotolia.com

Die EU-DSGVO greift - was tun, wenn man sich noch nicht darauf eingestellt hat?

Der Tag X ist vorbei und die Welt steht noch. Das eigene Unternehmen ist nicht wegen Datenschutzmängeln verklagt worden. Alles gut also? Kommt drauf an. Die Datenschutzgrundverordnung (DSGVO) ist seit dem 25. Mai 2018 rechtswirksam. Bei Nichtbefolgen drohen potenziell abschreckend hohe Strafen. Diejenigen, die sich auf die Verordnung vorbereitet haben, können aus gutem Grund ruhig bleiben. Diejenigen aber, die bisher nichts getan haben, um ihr Unternehmen fit zu machen für diese grundlegende europaweite Neuregelung des Datenschutzes, sollten schleunigst anfangen. Denn, dass sie bis jetzt nicht von den Aufsichtsbehörden belangt wurden, liegt im Zweifel nur daran, dass sie noch nicht an der Reihe sind.

Mit dem Datenschutz Ernst machen und zwar (EU)-europaweit einheitlich wollen die Schöpfer dieser neuen Verordnung. Betrachtet man die mediale Aufregung in den letzten Monaten so ist es ihnen sicherlich gelungen, den Schutz personenbezogener Daten in den Blick der Öffentlichkeit zu bringen. Inwieweit die Unternehmen am 25. Mai aber reagiert und ihre Hausaufgaben gemacht haben, steht auf einem anderen Blatt. Gewiss ist, dass bis zuletzt allzu oft nichts geschehen ist. So haben zum Beispiel noch Ende März 70 Prozent der Top-50-Onlineshops die Anforderungen der Verordnung nicht erfüllt. Das ergab eine Analyse von Usercentrics. Damit der Datenschutz kein Papiertiger (mehr) ist, ahnden die Aufsichtsbehörden dessen Missachtung jetzt mit abschreckend hohen Strafen von bis zu vier Prozent vom Jahresumsatz bzw. maximal einer Summe von 20 Millionen Euro. Die gute Nachricht für alle kleinen und mittelständischen Unternehmen (KMU), die noch nichts in Sachen DSGVO getan haben, ist, dass ihnen noch etwas Zeit bleibt bis die Behörden sie überprüfen. Denn die wenden sich zunächst den großen Fischen zu. *„Pragmatisch betrachtet werden die KMU, besonders die mit bis 100 Mitarbeitern, nicht so schnell in den Fokus der Aufsichtsbehörden geraten. Eher ist zu befürchten, dass Abmahnanwälte wieder zuschlagen“*, erläutert René Floitgraf, zertifizierter Datenschutzbeauftragter und Geschäftsführer des IT-Dienstleisters Spider Network Consulting GmbH, Aachen.

Vor Abmahnanwälten wird gewarnt

Abmahnanwälte haben im Zweifel schon begonnen, nach Angriffsflächen im Außenauftritt von Unternehmen zu suchen. Die Firmenwebsite muss die geforderten Datenschutzinformationen enthalten und

die Informationspflichten nach den Vorschriften der Datenschutzerklärung der DSGVO einhalten. Hier müssen alle Unternehmen, die sich noch nicht um die Datenschutzgrundverordnung gekümmert haben, als erstes aktiv werden. *„Sorgen Sie dafür, dass die Website, überall dort, wo personenbezogene Daten abgefragt werden, SSL-verschlüsselt ist"*, mahnt Floitgraf. Jedes Unternehmen, bei dem sich zehn oder mehr Mitarbeiter mit der Verarbeitung personenbezogener Daten befassen, muss einen Datenschutzbeauftragten haben. Dieser muss schleunigst nicht nur bestimmt werden, sondern auch für Außenstehende leicht erreichbar sein. Daher müssen dessen Kontaktdaten auf der Website vermerkt sein. Eine Adresse wie datenschutz@firma_xy.de gewährleistet beispielsweise, dass ein kurzer Kontaktweg zu ihm zur Verfügung steht.

Gegenüber der Aufsichtsbehörde gilt es, den kompletten Datensatz mit Namen und Anschrift des Datenschutzbeauftragten anzugeben. Ein entsprechendes Meldeformular haben die Aufsichtsbehörden zum 25.5.2018 bereitgestellt. Damit wären den Abmahnanwälten der Zahn gezogen, diese Gefahr ausgeschaltet.

Ebenfalls wichtig ist es, von Anfang an die Mitarbeiter zu sensibilisieren. Denn auch im Vertrieb ändert sich durch die neuen Informationspflichten einiges. Schon beim Erstkontakt muss der Betroffene erfahren, sei er Interessent oder Neukunde, wer seine Daten zu welchem Zweck erfasst und ob sie gegebenenfalls weitergegeben werden. Im Rahmen seiner Betroffenenrechte hat er ein jederzeitiges Auskunfts- und Beschwerderecht gegenüber der Aufsichtsbehörde, wenn er annimmt, dass mit seinen Daten unzureichend umgegangen wird.

Der Datenschutzbeauftragte kommt erneut bei der Dokumentation der Verarbeitungen im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten sowie der technischen und organisatorischen Maßnahmen, mit denen die Daten gesichert werden, ins Spiel. Hier müssen viele Details beachtet werden. Daher sollte diese Aufgabe in Zusammenarbeit mit dem Datenschutzbeauftragten erledigt werden.
Wer bis jetzt noch nichts in Sachen DSGVO getan hat, ist mit den genannten Maßnahmen *„erst einmal aus der vordersten*

René Floitgraf
Geschäftsführer der Spider Network Consulting GmbH, Aachen

Schusslinie raus" wie es Floitgraf formuliert. Das heißt aber noch lange nicht, dass damit alle Aufgaben erledigt sind und man sich beruhigt zurücklehnen kann.

Als nächstes gilt es nun, die eigenen Dienstleister auf Zulässigkeit zu prüfen. Dazu gehört, dass man eine Vereinbarung zur Auftragsvereinbarung mit den Dienstleistern schließt, sofern diese für das Unternehmen personenbezogene Daten verarbeiten. Wenn das Unternehmen selbst Daten für den Auftraggeber verarbeitet, muss ebenfalls mit dem Auftraggeber eine solche Vereinbarung geschlossen werden. Dafür sollte man vorher seine Dienstleister kennen und wissen welche Daten dort verarbeitet werden. Die Dienstleister müssen im Rahmen der Auftragsdatenverarbeitung gegenüber dem Auftraggeber benannt werden.

Die DSGVO verlangt ausdrücklich, dass Einwilligungen geprüft und verständlich formuliert werden. Sie müssen den Betroffenen unmissverständlich über den Grund der Einwilligung in die Verarbeitung seiner Daten informieren und auch darüber, dass er diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. *„Man muss tunlichst darauf achten, dass das Kopplungsverbot eingehalten wird,"* so Floitgraf. Der Widerruf darf für den Betroffenen keine negativen Rechtsfolgen, wie das Blockieren des Vertragsabschlusses, haben.

In einem weiteren Schritt muss das Unternehmen die Prozesse im Unternehmen so organisieren, dass Betroffenenrechte berücksichtigt und Datenschutzverstöße in der gesetzlich vorgeschriebenen Zeit gemeldet werden. Wenn im Unternehmen Daten manipuliert oder unrechtmäßig übermittelt wurden oder verloren gegangen sind, muss dies das Unternehmen innerhalb von 72 Stunden bei der Aufsichtsbehörde melden.

Den Betroffenen gegenüber muss das Auskunftsrecht gewahrt werden, sprich er kann jederzeit anfragen, welche Daten über ihn im Unternehmen gespeichert sind. Diese Anfrage muss in maximal vier Wochen bearbeitet sein. Die Auskunft muss vollständig geliefert werden. Dieses Auskunftsrecht ähnelt der kostenfreien Schufa-Anfrage. Dieses Recht steht jedem Betroffenen frei und man kann es nicht einschränken.

Und was hat sich jetzt verändert?

„Der größte Unterschied zum Bundesdatenschutzgesetz liegt in der Rechenschaftspflicht wie sie der Artikel 5 der DSGVO formuliert. Unternehmen müssen nachweisen, dass sie den Datenschutz befolgen. Das gab es in der Form nicht. Man muss ein Bündel an Regelungen und Richtlinien im Unternehmen etablieren und einhalten, um diesen Nachweis zu erbringen", so Floitgraf. 100 Prozent perfekter Schutz und das Einhalten aller Bestimmungen bis ins Kleinste werden dennoch nicht immer erreicht werden können. Dies liegt daran, dass das Gesetz die Verhältnismäßigkeit im Sinne der Abwägung unterschiedlicher berechtigter Interessen vorsieht. Wenn ein Unternehmen diese Regelung anwendet und die DSGVO eventuell nicht zu hundert Prozent erfüllt, bedeutet das aber noch lange nicht, dass die Aufsichtsbehörde zu der gleichen Einschätzung gelangt. Sie könnte durchaus ein Strafverfahren anstrengen, wobei sich nachvollziehbare Überlegungen des Unternehmens strafmildernd auswirken könnten.

Ebenfalls von großer Bedeutung sind die Informationspflichten, sowohl nach außen hin auf der Unternehmenswebsite als auch gegenüber von einer Datenerhebung Betroffenen. Transparenz und die Kontrolle über die eigenen personenbezogenen Daten wurden deutlich erhöht. Und das EU-weit. Da die EU-DSGVO wie

jedes große Gesetzeswerk aber dennoch Auslegungsspielräume eröffnet, wird eine wirkliche Rechtssicherheit im Zweifel erst in zwei, drei Jahren eintreten. Dann nämlich werden die ersten Gerichtsverfahren abgeschlossen und klärende Urteile gesprochen sein. Bis dahin sollte man nach bestem Wissen und Gewissen auf Basis der Erfahrungen aus dem Bundesdatenschutzgesetz arbeiten. Und die Bestimmungen der Datenschutzgrundverordnung so gut wie möglich einhalten. Damit ist Unternehmen und ihren Kunden am meisten gedient. *„Die DSGVO stellt niemanden vor unlösbare Herausforderungen. Sie gibt dem Datenschutz und der Wahrung der Privatsphäre einen großen Schub. Und das ist heute wichtiger denn je“*, resümiert Floitgraf. ■