Datenschutz bei Callcenter-Dienstleistern

Mehr als nur Papier?

Ja, das können wir – Regelungen, Gesetze, Verordnungen … Im Grunde fühlen wir uns in Deutschland aber auch genau deswegen so sicher. Alles ist geregelt, die Grenzen sind klar, jeder weiß, was erlaubt ist und was nicht. Dennoch sorgt vor allem das Thema Datenschutz immer wieder für Stress: „Als Datenschutzbeauftragter ist man wegen der vielen Bestimmungen und Verordnungen manchmal eine Art ‚Spielverderber' im Unternehmen", beschreibt Heiko Hildebrand, Datenschutzbeauftragter bei T.D.M., die Herausforderungen rund um den Datenschutz in einem Callcenter. Das macht die neue EU-Datenschutzgrundverordnung (EU-DSGVO) vermutlich auch nicht gerade einfacher. Oder, Herr Hildebrand?

SQUT: Was ändert sich für CC-Dienstleister mit der EU-DSGVO?

H. Hildebrand: Derzeit ist das deutsche Datenschutzrecht im BDSG (Bundesdatenschutzgesetz) und in weiteren einzelnen Gesetzen geregelt. Ab dem 25. Mai 2018 wird das BDSG durch die DSGVO (EU-Datenschutz-Grundverordnung) und das BDSG (neu) abgelöst. Eine Folge ist, dass der europäische Wettbewerb weiter angeglichen wird, da alle EU-Länder damit den gleichen Regelungen unterliegen. Allerdings können die Mitgliedsstaaten durch diverse Öffnungsklauseln eigene spezifische Vorschriften vorsehen, was eine Vereinheitlichung wiederum relativiert. Mit der DSGVO treten teilweise umfangreiche Änderungen in Kraft. Dies erfordert die Etablierung neuer sowie die Umstrukturierung vorhandener Prozesse. Vor allem bei den von nun an notwendigen Dokumentationen wird wesentlich mehr Aufwand anfallen.

WESENTLICH MEHR AUFWAND

Im Zuge der DSGVO wurden die Bestimmungen zur Datensicherheit und damit zu den TOM[1] überarbeitet. Diese sind nicht mehr so konkret geregelt wie zuvor. Stattdessen orientiert sich die Entscheidung, welche Art Schutz geeignet ist, nun immer an dem abzusichernden Risiko und den Anforderungen zur Aufrechterhaltung eines geeigneten Schutzniveaus nach dem aktuellen Stand der Technik. Dies geht mit erweiterten Dokumentationspflichten zu den umgesetzten Maßnahmen einher, damit sichergestellt und nachgewiesen werden kann, dass personenbezogene Daten gemäß den Vorgaben der DSGVO verarbeitet werden.

Außerdem wird das Auskunftsrecht für Betroffene weiter gestärkt. Der Zugang zu ihren Daten und zu Informationen über deren Nutzung soll erleichtert werden. Hierdurch entstehen für CC-Unternehmen erhebliche Dokumentationspflichten und zusätzliche Prozesse, um die Pflichten (das Informationsrecht, das Auskunfts- und Widerspruchsrecht sowie das Recht auf Berichtigung, Löschung und Einschränkung) ausreichend gewährleisten zu können.

Hinzu kommt, dass Unternehmen nun generell verpflichtet sind, Datenpannen jedweder Art der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Um diesen Meldepflichten fristgerecht nachkommen zu können, müssen Unternehmen mehrere Dinge berücksichtigen: Erstens muss erkannt werden, dass eine Verletzung des Schutzes von personenbezogenen Daten vorliegt. Zweitens müssen der Datenschutzbeauftragte, die zuständigen Entscheidungsträger sowie der Auftraggeber über diesen Sachverhalt informiert werden, und drittens muss eine Bewertung des Sachverhalts erfolgen.

Zudem steigen mit der neuen DSGVO die Risiken für CC-Dienstleister als Auftragsverarbeiter. Bei Verletzung der Pflichten haftet ein CC-Dienstleister nun direkt vollumfänglich für die beim Betroffenen eingetretenen immateriellen und materiellen Schäden. Zusätzlich zu dieser Haftung können Bußgelder von bis zu

1: Technische und organisatorische Maßnahmen nach § 9 Bundesdatenschutzgesetz.

4 Prozent des weltweiten Jahreseinkommens des Unternehmens verhängt werden.

Neu ist nun auch eine Risikobeurteilung in Form der sogenannten Datenschutzfolgenabschätzung, in deren Rahmen die Eigenart der betreffenden Verarbeitung, die mögliche Verletzung von Rechten etc. festgehalten werden müssen. Diese Beurteilung ist verpflichtend, wenn ein hohes Risiko für die personenbezogenen Daten bei der Verarbeitung anzunehmen ist. Daher muss von nun an vor der Implementierung jeder Verarbeitung geprüft werden, ob eine Folgenabschätzung durchzuführen und zu dokumentieren ist.

MEHRAUFWAND BEIM DATENSCHUTZ-MANAGEMENT

Infolge dieser Änderungen ist also mit erheblichem Mehraufwand beim Datenschutzmanagement zu rechnen. Um die Vorgaben der DSGVO umzusetzen, bedarf es natürlich auch Änderungen an bestehenden CRM-Systemen. Hier arbeiten wir bereits seit längerer Zeit an adäquaten Erweiterungen, um den neuen Dokumentations-, Evaluations- und Auskunftspflichten ab 25.05.2018 nachzukommen.

SQUT: Welche Qualifikation hat bzw. braucht ein Datenschutzbeauftragter (DSB) bei einem CC-Dienstleister – vor allem in Anbetracht dieser Regelungsvielfalt?

H. Hildebrand: Als DSB sollte man über umfassende Kenntnisse der internen betrieblichen Organisation und der Abläufe verfügen. Für diese Tätigkeit gibt es weder eine Berufsausbildung noch ein Studium. Jeder ist somit theoretisch berechtigt, als DSB zu fungieren. Für die Ausübung dieser Tätigkeit sind in der Praxis jedoch konkrete Fachkenntnisse und anerkannte Qualifikationen Voraussetzung. Das betrifft z. B. Kenntnisse in den Bereichen IT-Systeme und Software sowie natürlich im Datenschutzrecht. Außerdem sind bestimmte Soft Skills klar von Vorteil, beispielsweise didaktisches Know-how, Teamfähigkeit sowie die Bereitschaft, in Bezug auf seine eigenen Aufgaben konfliktfähig zu sein. Als DSB ist man schließlich wegen der vielen Bestimmungen und Verordnungen manchmal eine Art „Spielverderber“ im Unternehmen, da der direkte Weg, etwas umzusetzen, nicht immer der „datenschutzfreundlichste“ ist. Bei einem Callcenter-Dienstleister kommt im Speziellen hinzu, dass aufgrund der technischen Mittel wie Telefonanlagen, Netzwerke und Bildschirmarbeitsplätze sowie durch die Einbindung von Auftraggebern ein ständiger Austausch mit der IT stattfinden muss. Auch der Beschäftigtendatenschutz spielt eine besondere Rolle. Dies erfordert neben Kommunikationsgeschick auch ein abteilungsübergreifendes Wissen. Außerdem sollte ein DSB bei einem Callcenter-Dienstleister auch in der Lage sein, alle anderen Mitarbeiter und Agenten dafür zu sensibilisieren, wie jeder Einzelne dazu beitragen kann, Datenschutz umzusetzen.

SQUT: In welcher Form wird Datenschutz tatsächlich vom Auftraggeber nachgefragt?

H. Hildebrand: Im Grunde wird von jedem Auftraggeber die Einhaltung des Datenschutzes nachgefragt bzw. die Umsetzung der Sicherheits- und Schutzanforderungen des BDSG wird verlangt. Lediglich die Intensität der Nachfrage und die Anforderung an eine Dokumentation variieren. Wir arbeiten mit einer Vielzahl an Unternehmen zusammen, dadurch haben wir es natürlich mit sehr unterschiedlichen Branchen und entsprechend differenzierten Schutzbedürfnissen zu tun. Während beispielsweise Banken und Versicherungen ein sehr hohes Interesse an unserer Organisation des Datenschutzes zeigen und diese auch vor Ort detailliert überprüfen, steht bei kleinen und mittelständischen Unternehmen unser Datenschutzkonzept, die technische Infrastruktur und der damit einhergehende Datenschutz in der Regel nicht auf Platz eins der Prioritätenliste.

Noch vor Vertragsabschluss stehen wir intensiv mit unseren Auftraggebern im Dialog, um den Umfang des Datenschutzes und etwaige besondere Vereinbarungen zu klären. Denn auch spezifische Datenschutzmaßnahmen werden von unseren Kunden gefordert. Wir wiederum legen die TOM, unsere Übersicht mit allen technischen und organisatorischen Maßnahmen, vor. Diese zeigen auf, wie wir konkret die grundsätzlichen Rahmenbedingungen für eine sichere Datenverarbeitung in allen involvierten Unternehmensbereichen sicherstellen. Strukturell folgt diese Übersicht den obligatorischen Vorgaben des BDSG anhand verschiede-

ner Kategorien mit Nennung konkreter Maßnahmen. Es sind auch Frage- bzw. Checklisten der Auftraggeber üblich, um unsere Datenschutzmaßnahmen in kundenspezifischer Ausprägung abzufragen.

SQUT: Welche Form des Datenschutzes wird obligatorisch vom Dienstleister zur Verfügung gestellt?

H. Hildebrand: Es gibt immer den vollen Datenschutz. Grundsätzlich sind wir so aufgestellt, dass in allen organisatorischen und technischen Belangen im Hinblick auf grundlegende Schutzziele, wie z. B. Vertraulichkeit, Datensparsamkeit, Verfügbarkeit sowie Integrität und Transparenz, die IT-Struktur im Unternehmen entsprechend gestaltet ist und auf dem aktuellen Stand der Technik gehalten wird. „Vertraulichkeit" bedeutet, dass Daten nur befugten Personen zugänglich gemacht werden. Hier müssen insbesondere Sicherheitsmaßnahmen ergriffen werden, um unbefugten Zugriff zu verhindern, beispielsweise durch eingeschränkte Berechtigungen und Absicherungen durch sichere Passwörter, die nicht ausgespäht werden können. Zum Datenschutz gehört es auch, unnötige Datensammlungen zu vermeiden („Datensparsamkeit"), z. B. durch entsprechende Datenerfassungsmasken, aber auch durch die regelmäßige Sensibilisierung aller Mitarbeiter. „Verfügbarkeit" zielt auf die Möglichkeit ab, ständig auf benötigte Daten zugreifen zu können. Diese kann insbesondere durch Systemausfälle, wie beispielsweise eine Hardwarebeschädigung, beeinträchtigt werden. Solchen Beeinträchtigungen kann u. a. mittels geeigneter Back-up-Systeme vorgebeugt werden. „Integrität" meint, dass Daten unverändert von A nach B verschickt werden. Das lässt sich z. B. durch Verschlüsselung realisieren. Eine vollumfängliche Dokumentation aller Verarbeitungsprozesse ermöglicht Transparenz gegenüber Kunden, Mitarbeitern und Aufsichtsbehörden. Diese Schutzziele sind immer im Verbund zu betrachten und greifen stets ineinander.

Unter Umständen werden zusätzliche erforderliche Schutzmaßnahmen für einzelne Kundenaufträge abgestimmt. Aus diesem Grund wird bei uns rund um die Leistung von Beginn an der betriebliche DSB in Entscheidungs- und Installationsprozesse eingebunden. Regelmäßige und auftragsbezogene Schulungen vermitteln den Mitarbeitern praxisnah den Datenschutz im Umgang mit den IT-Systemen, sodass auch bei dem nicht zu vernachlässigenden Faktor „Mensch als Mitarbeiter" das Sicherheitsrisiko reduziert wird.

ES GIBT IMMER DEN VOLLEN DATENSCHUTZ

SQUT: Gibt es Spielräume?

H. Hildebrand: Der Bereich Datenschutz sollte wirklich ernst genommen werden, nicht nur im Eigeninteresse, um einer drohenden Sanktionierung zu entgehen, sondern auch im Interesse aller Kunden und Mitarbeiter. Datenschutz ist in diesem Sinne nicht dehnbar. Da sind die Auflagen des Gesetzgebers klar und deutlich. Auch mit der neuen EU-DSGVO ändert sich daran nichts. Alle Maßnahmen, um die bereits erwähnten Schutzziele zu erfüllen, sind verpflichtend.

DATENSCHUTZ IST NICHT DEHNBAR

Die Gewichtung dieser Ziele ist dabei allerdings einzelfallabhängig und kann je nach Auftraggeber und Art der Daten unterschiedlich ausfallen. So macht es je nach Kundenauftrag einen Unterschied, ob man es z. B. ausschließlich mit Kontakt- bzw. Adressdaten oder zusätzlich mit „besonderen Daten", wie Gesundheitsdaten, zu tun hat. Trotzdem, um ein ausreichendes Datenschutzniveau zu gewährleisten, führt an der Einhaltung der zuvor erwähnten Maßnahmen kein Weg vorbei.

SQUT: Gibt es „unmoralische Angebote", sprich, verlangen Auftraggeber auch die Umgehung des Datenschutzes? Wenn ja, wie gehen Sie damit um?

H. Hildebrand: Ein unmoralisches Angebot haben wir noch nie erlebt. Sollte dies passieren, würden wir auf die obligatorische Einhaltung des Datenschutzes verweisen und eine Zusammenarbeit mit dem potenziellen Auftraggeber verweigern.

Wir bei T.D.M. sehen uns als umfassenden Dienstleister, d. h., dass wir auch einen Beratungsauftrag gegen-

▸▸

fest, dass es z. B. Schwachstellen im System des Auftraggebers oder bei den beteiligten Prozessen gibt, weisen wir darauf hin und suchen gemeinsam nach einer Lösung. Unser Appell kann deswegen nur lauten, sich einen qualifizierten Dienstleistungspartner zu suchen. Denn nur mit einem ganzheitlichen Paket aus Leistung und Sicherheit entstehen Vertrauen und Erfolg. Wir freuen uns, wenn die Leser mit uns über ihre aktuellen Datenschutz-Herausforderungen in unseren Gruppen auf XING und Facebook diskutieren. ■

Diskussionsforen:

XING

Facebook

Über T.D.M.

Das 1983 gegründete Dienstleistungsunternehmen ist auf den Bereich der Dialogkommunikation für erklärungsbedürftige technische Produkte und Dienstleistungen spezialisiert. Als mittlerweile in der zweiten Familiengeneration inhabergeführtes Sarstedter Unternehmen hat es sich seit seiner Gründung in den verschiedensten Branchen etabliert. Für namhafte Unternehmen aus den Bereichen Industrie, IT, Banken, Versicherungen und Handel ist T.D.M. ein engagierter und zuverlässiger Kooperationspartner. Die Dialogkommunikation im In- und Outbound auf höchstem Niveau zeichnet die Kernkompetenzen des in allen europäischen Sprachen tätigen Dienstleisters aus.

Heiko Hildebrand

Heiko Hildebrand ist seit mehreren Jahren Datenschutzbeauftragter des Callcenter-Dienstleisters T.D.M. Telefon-Direkt-Marketing GmbH und beschäftigt sich intensiv mit Callcenter-Dienstleistungen und der gesetzlichen Entwicklung des Datenschutzes im Auftragsverarbeiterumfeld.