



Lohnender Aufwand

Datenschutz ist im Kundenservice keine Kür, sondern Pflicht: Die Vorstände eines Unternehmens können ihren Job verlieren, wenn sie Outsourcing-Partner wählen, die das Thema Datenschutz nicht ernst nehmen. Data Security ist daher Chefsache – und kostet Geld.

Das Thema Datenschutz ist nahezu ausschließlich mit Negativmeldungen in den Schlagzeilen vertreten: Aktuelle Fälle von Datenschutzverletzungen lassen die Verbraucher aufhorchen, stets aufs neue geraten personenbezogene Daten in falsche Hände und werden im Internet einer breiten Masse zugänglich gemacht. Nur wenn der Schaden bereits eingetreten ist, werden Rufe nach strengeren Regelungen laut. Doch was bedeutet Datenschutz überhaupt?

Der Datenschutz schützt persönliche Daten. Personenbezogene Daten sind Informationen, die in Zusammenhang mit einer bestimmten Person stehen. Dazu gehören nicht nur die Kreditkartennummer eines bestimmten Verbrauchers oder dessen Fernsehgewohnheiten sondern einfach jede Information in Verbindung mit seinem Namen, also beispielsweise Adresse, Hautfarbe, Schuhgröße, Automarke oder die Lieblingspeise. Der Datenschutz steht außerdem für

das Recht auf informationelle Selbstbestimmung: Jeder Mensch soll und darf grundsätzlich selbst entscheiden, wem er wann, welche seiner persönlichen Daten zugänglich macht und wem welche nicht. Dieses Prinzip steht in krassem Widerspruch zum Phänomen Social Media. Bürger werden zunehmend transparent, die Datenweitergabe auf globaler Ebene funktioniert ohne Probleme und kann nur schwer eingegrenzt werden. Und dort, wo Menschen aus eigenem Antrieb Informationen über sich oder andere ins Netz stellen, etwa auf Facebook, versagt der Datenschutz völlig. Wer seine Daten aber nicht preisgeben möchte, dem bietet das Bundesdatenschutzgesetz (BDSG) weitreichende Sicherheit.

Rechtliche Grundlagen

In der EU gelten die weltweit strengsten Datenschutzgesetze. Mit der so genannten Datenschutzrichtlinie 95/46/EG hat die EU für alle Mitgliedsstaaten den Mindeststandard festgeschrieben. Die Richtlinie erläutert explizit, unter welchen Voraussetzungen die

Verarbeitung personenbezogener Daten rechtmäßig, und welche Art der Verarbeitung untersagt ist. Diese Richtlinie gibt die Rahmenbedingungen vor, an denen sich die Mitgliedsstaaten mit ihren eigenen Gesetzen zu orientieren haben und messen lassen müssen. Auf dieser Grundlage wurde beispielsweise in Österreich das Datenschutzgesetz 2000 (DSG 2000), und in Deutschland das BDSG novelliert. In diesen Gesetzen wird vor allem die Handhabung von personenbezogenen Daten geregelt. Für Call Center, die datenschutzkonform agieren, bedeuten die Gesetze grundsätzlich, dass Kunden- und auch Mitarbeiterdaten vertraulich behandelt, nicht an Dritte weitergegeben und nach entsprechender Zeit gelöscht werden. Diese gesetzlichen Vorgaben nehmen manche Outsourcer sehr genau, andere weniger genau.

Datenschutz im Call Center

Die eigene Kundendatenbank stellt für viele Unternehmen einen wesentlichen Vermögenswert dar. Betreut aber ein Contact Center beispielsweise die Kundenhotline eines Energieversorgers, so hat der Dienstleister Zugriff auf dessen Kundendaten. Dabei handelt es sich um personenbezogene Daten, aus denen sich auch ergibt, welchen Stromverbrauch der Kunde A hat, welches Nutzungsprofil er aufweist und wie hoch seine monatlichen Rechnungen sind. Alle diese Kundendaten unterliegen dem BDSG und sind daher grundsätzlich vor einer Weitergabe an Dritte geschützt. Verwendet ein Call Center diese Kundendaten daher für ein anderes Projekt, etwa für den Verkauf von Zeitungsabonnements, stellt dies eindeutig eine Datenschutzverletzung dar. Gleiches gilt, wenn einzelne Kundendaten öffentlich zugänglich gemacht werden, zum Beispiel im Internet, oder schlicht gestohlen werden, indem ein Call Center-Mitarbeiter beispielsweise Kundendaten auf einem Datenstick speichert. Der Schutz der eigenen Kundendaten ist daher oberstes Prinzip. Viele Unternehmen stellen sich deswegen die Frage, warum sie Kundendaten überhaupt einem Outsourcing-Partner überlassen sollten. Zudem sind die Auftraggeber mittlerweile gesetzlich laut BDSG verpflichtet, sich von der Eignung des ausgewählten Call Centers im Hinblick auf die Daten-

schutzmaßnahmen zu überzeugen. Im BDSG heißt es: „Der Auftragnehmer (hier: Call Center) ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.“ Das ist keine Lappalie, denn werden vom Dienstleister Kundendaten missbräuchlich verwendet, drohen dem Auftraggeber im Fall einer nicht ausreichenden Prüfung des Dienstleisters nicht nur negative Presseberichte, sondern ein erheblicher Kundenverlust, der eigene Jobverlust und ein Bußgeld von bis zu 250.000 Euro.

BRANCHE IN DER PFLICHT

Datenschutz ist keine freiwillige Übung sondern gesetzliche Pflicht. Call Center, die nicht datenschutzkonform agieren, begehen eine Datenschutzverletzung. Sie können durch weniger Aufwand beim Datenschutz ihre Leistung zwar günstiger anbieten als andere Wettbewerber, handeln jedoch gesetzwidrig und gefährden damit den Ruf ihrer Auftraggeber. Informationssicherheit und Datenschutz im Call Center sind daher eine Investition für die erfolgreiche Zukunft der gesamten Branche. Infos und der Text der EU Richtlinie zum Datenschutz finden sich unter: <http://eur-lex.europa.eu>

Die rechtlichen Rahmenbedingungen zu kennen ist eine Sache, den Datenschutz und die Datensicherheit im Call Center praktisch umzusetzen, eine ganz andere. Die Herausforderung dabei ist, die gesamte Organisation für das Thema zu sensibilisieren. Das gelingt nicht von heute auf morgen, sondern braucht eine Vielzahl von organisatorischen und technischen Maßnahmen, wie etwa spezielle Trainings, Policies, Audits und Tests. All diese Maßnahmen sind mit erheblichen Kosten und mit Aufwand für den Contact Center-Dienstleister verbunden. Grundsätzlich von Vorteil ist es dabei immer, einen Verantwortlichen für Informationssicherheit als so genannten IS-Officer zu benennen, alle Besuche zu vermerken und Besucherkarten zu vergeben.

Umsetzung im Servicecenter

Konkret kann die Datensicherheit im Call Center mit verschiedenen Methoden um-

gesetzt werden, etwa durch biometrische Zugangskontrollen beim Eingang, zusätzliche biometrische Zugangskontrollen für autorisierte Personen zu Projekten mit besonders hohen Datenschutzerfordernissen sowie ID Cards (Badges), auf denen die Zugangsberechtigungen und der Name des einzelnen Mitarbeiters ausgewiesen sind.

Ebenfalls hilfreich ist eine so genannte Clean Desk Policy, die festlegt, dass es keine handschriftlichen Notizen oder persönlichen Dokumente am Arbeitsplatz gibt. Persönliche Gegenstände wie Handtaschen, Jacken und Mobiltelefone sollten zudem in dafür vorgesehenen, individuellen Schließfächern verstaut werden. Der uneingeschränkte Internetzugang für die Agents ist idealerweise nur an eigens dafür vorgesehenen PCs möglich, die in den Pausen genutzt werden können. Auch sollten Richtlinien für sehr sichere Passwörter eingehalten werden. Des Weiteren sind Einschulungen und regelmäßige Trainings der Mitarbeiter zum Thema Datensicherheit nötig, hinzu kommen regelmäßige Tests zur Informationssicherheit, regelmäßige Audits durch interne Mitarbeiter, Partner und externe Organisationen sowie monatliche Reports über den aktuellen Status und die möglichen Verbesserungen. Ein solches Reporting kann nicht in kurzer Zeit erstellt werden.

Vielmehr dauert die Implementierung hoher Sicherheitsstandards, die Schaffung eines Bewusstseins für Datenschutz viele Monate, wenn nicht gar Jahre.

Sind Unternehmen auf der Suche nach einem geeigneten Dienstleister, der den Datenschutz ernst nimmt, lässt sich das übrigens recht schnell feststellen: Das Unternehmen fordert den potenziellen Auftragnehmer einfach dazu auf, ihm die Berichte zu den letzten drei Datenschutz-Audits zu übermitteln – kann der Dienstleister das nicht innerhalb weniger Minuten erfüllen, ist er kaum die richtige Wahl.

Katrin Albrecht



Katrin Albrecht ist Datenschutzbeauftragte von Competence Call Center an den Standorten Leipzig und Berlin.

katrin.albrecht@yourccc.com