Datenschutz im Service

von Dirk Zimmermann

Hintergrund

Im Mai letzten Jahres ist die neue europäische Datenschutzrichtlinie mit der Bezeichnung Datenschutz-Grundverordnung (DSGVO) inkraftgetreten. Diese Regulierung betrifft die Datenschutzgesetze vor Ort in allen Ländern der EU und des EWR.

Sie gilt für alle Unternehmen, die Produkte und Dienstleistungen an europäische Bürger verkaufen und deren personenbezogene Daten speichern, einschließlich Firmen auf anderen Kontinenten. Die neue Richtlinie gibt EU- und EWR-Bürgern mehr Kontrolle über ihre personenbezogenen Daten und stellt sicher, daß ihre Informationen europaweit geschützt sind.

Gemäß der DSGVO sind personenbezogene Daten alle Daten zu einer Person, wie Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge in den Social Media, Angaben zum Wohnort, medizinische Daten oder IP-Adressen.

Es wird nicht unterschieden zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person – es geht immer um die Person selbst. Auch im B2B-Bereich geht es immer um Einzelpersonen, die Informationen mit- und übereinander austauschen.

Kunden in B2B-Märkten sind natürlich Unternehmen, doch die Geschäftsbeziehungen werden von einzelnen Personen gepflegt.

Anforderungen

Mit der Einführung der neuen Datenschutzgrundverordnung (EU-DSGVO) kommen auch auf Dienstleistungs- und Serviceunternehmen zusätzliche Anforderungen zu. Gerade in Dienstleistung und Service ist es nahezu selbstverständlich geworden, ständig und überall Kundendaten zu sammeln. Zu wissen, was im Umgang mit personenbezogenen Daten genau zu beachten ist und welche einzelnen Maßnahmen zum Schutz ergriffen werden müssen, wird für Unternehmen zur Pflicht.

Ein erster wichtiger Schritt betrifft die Kommunikation und Sensibilisierung aller in einem Dienstleistungs- und Serviceunternehmen. Entscheidungsträger sollten sich der Auswirkungen der neuen Datenschutzgrundverordnung bewußt sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet und die Mitarbeiter sollten dafür sensibilisiert werden, was sich damit genau ändert.

Um einen Änderungsbedarf im Umgang mit personenbezogenen Daten identifizieren zu können, sollte auch Dienstleistungs- und Serviceunternehmen eine Bestandsaufnahme der aktuell bestehenden Prozesse durchführen, in denen personenbezogene Daten verarbeitet werden. Dabei wird zunächst den Soll-Zustand ermittelt und im Anschluß daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchgeführt.

Bei der Überprüfung der Prozesse geht es auch um Angelegenheiten, die Verträge und Regularien betreffen, z.B. Auftragsdatenverarbeitung in Dienstleistungsbeziehungen. Zudem sollte sich der Blick nach innen richten: Bestehende Geschäftsprozesse, Regularien, Richtlinien oder auch Handbücher und Dienstvereinbarungen, sollten daraufhin überprüft werden, ob sie mit den Anforderungen der neuen Datenschutzgrundverordnung vereinbar sind.

Pflichten

Dienstleistungs- und Serviceanbieter dürfen die Daten zu ihren Kunden erfassen, die sie zur Angebotserstellung, Lieferung und Rechnungsstellung brauchen. Auch Angaben, die zur Beantwortung von Support-Anfragen und Reklamationen benötigen werden, dürfen gesammelt und gespeichert werden.

Zu den personenbezogenen Daten gehört auch die IP-Adresse des Computers. Hier wird es interessant: Denn manche Live-Chat-Software oder Plattform für die sozialen Medien speichert sie, ebenso wie die Browser-Version und die Betriebssystem-Version. Das sind Informationen, die Unternehmen im Service nahezu nie benötigen werden. Nach dem Grundsatz der Datensparsamkeit dürften Unternehmen sie nicht sammeln.

Richtigkeit

Unternehmen müssen sicherstellen, da die vorhandenen Daten aktuell und korrekt sind. Fehlerhafte Angaben sollten berichtigt oder gelöscht werden. Das ist im Service eine Herausforderung, den in ERP- und CRM-Systemen sammeln sich über die Zeit falsche Daten an: Tippfehler in den Anschriften, veraltete Telefonnummern, ungültige E-Mail Adressen. Auch doppelte und dreifache Datensätze sind häufig. Es ist eine umfangreiche Aufgabe, nachlässig gepflegte Datenbanken mit tausenden von Einträgen zu berichtigen. Eine weitere Herausforderung stellen nicht verknüpfte Systeme dar, in denen die gleichen Kunden erfaßt sind. Solche Datensätze bewegen sich zwangsläufig auseinander. In beiden Datenbanken häufen sich unterschiedliche Fehler an.

Vertraulichkeit

Unternehmen müssen mit geeigneten Paßwörtern, Firewalls und Virenschutz sicherstellen, daß die Datenbanken nicht von Unbefugten geöffnet werden können. Doch auch die Serviceverantwortlichen sind gefragt. Denn dort werden zunehmend Software as a Service-Lösungen genutzt. Oft lagert man CRM-Daten aus, aber sogar ERP-Systeme wandern zunehmend in die Wolke. Das heißt, Kundendaten werden an ein anderes Unternehmen weitergegeben. Server solcher Dienste stehen oft in den USA, wo Datenschutz geringer geachtet wird, als in Europa. Bei der Auswahl der Software sollte deshalb in Zukunft darauf geachtet werden, daß die Anbieter das europäische Datenschutz-Niveau beachten und einhalten. Die Weitergabe von Daten innerhalb eines Konzerns, wenn zum Beispiel Standorte in verschiedenen Ländern mit der gleichen Datenbank arbeiten, sind einfacher. Wichtig ist hier, daß im Konzern durch einen Code of Conduct oder durch Verträge geregelt wird, wie die Daten geschützt sind.

Informationspflicht

Jeder Kunde darf in Zukunft Auskunft verlangen, welche Informationen ein Unternehmen über ihn gesammelt hat. Solche Anfragen müssen innerhalb von 4 Wochen beantwortet werden. Bei einem Unternehmen mit vielen Niederlassungen und dem einen oder anderen Shared Services Center ist diese Zeit knapp. Eine fehlende Auskunft kann teuer werden!

Datenlöschung

Jeder Kunde hat in Zukunft das Recht auf einen unbelasteten Neubeginn. Kunden und Interessenten dürfen von Unternehmen verlangen, daß sie ihre Daten löschen, soweit Sie nicht durch Gesetze daran gehindert werden. Unternehmen müssen also weiterhin alle Angaben, die für die erstellten Rechnungen relevant sind, für 10 Jahre aufbewahren. Andere Informationen, wie die Themen, für die sich ein Kunde interessiert, oder die IP-Adresse seines Rechners, müssen Unternehmen bei einer entsprechenden Anfrage löschen. Zur Löschung und Bestätigung an den Kunden haben Unternehmen maximal 4 Wochen Zeit.

Dokumentation

Die Datenschutz-Beauftragten der Unternehmen müssen ein Verzeichnis der Verarbeitungstätigkeiten erstellen. Dafür brauchen sie die Informationen auch aus dem Servicebereich. Könnten die gesammelten Informationen mißbraucht werden, wenn sie den Falschen in die Hände geraten, so muß Ihr Unternehmen außerdem eine Datenschutz-Folgenabschätzung erstellen. Das betrifft zum Beispiel Gesundheitsdaten oder biometrische Daten.

Maßnahmen

Zur Einhaltung der DSGVO müssen auch Unternehmen im Dienstleistungs- und Servicebereich mehrere Maßnahmen ergreifen. Dazu gehören insbesondere die folgenden ersten Schritte:

1. Erstellung einer Übersicht

Unternehmen müssen eine Übersicht der personenbezogenen Daten erstellen und dokumentieren, wie mit diesen Daten umgegangen wird. Zudem muß ermittelt werden, wo diese Daten gespeichert werden, wer darauf zugreifen kann und ob die Daten Risiken ausgesetzt sind.

2. Ermittlung der Daten

Unternehmen sollten nicht mehr Informationen als erforderlich speichern und alle Daten löschen, die nicht verwendet werden. Wenn Unternehmen viele Daten ohne einen wirklichen Nutzen sammeln, müsse sie dies mit der neuen DSGVO ändern. Die DSGVO erfordert einen disziplinierten Umgang mit personenbezogenen Daten.

Bei der Datenbereinigung sollten folgende Fragen gestellt werden:

- Warum genau archivieren wir diese Daten, anstatt sie zu löschen?
- Warum speichern wir all diese Daten?
- Was bezwecken wir mit dem Erfassen verschiedener Kategorien personenbezogener Informationen?
- Ist der finanzielle Vorteil größer, wenn wir diese Informationen löschen anstatt sie zu verschlüsseln?

3. Ergreifen von Sicherheitsmaßnahmen

Zudem sollten Unternehmen für die gesamte Infrastruktur Schutzmaßnahmen entwickeln und implementieren, die die Verletzung der Datensicherheit verhindern. Das bedeutet die Implementierung von Sicherheitsmaßnahmen, die die Daten schützen, und das Ergreifen schneller Maßnahmen zur Benachrichtigung von Einzelpersonen und Behörden, falls es zu einer Verletzung der Datensicherheit gekommen ist. Auch die Verfahren von Partnern und Lieferanten müssen geprüft werden. Das Outsourcing befreit nicht von den Verpflichtungen. Unternehmen müssen sicherstellen, daß auch ihre Partner und Lieferanten geeignete Sicherheitsvorkehrungen getroffen haben.

4. Prüfen der Dokumentation

Nach der DSGVO müssen Einzelpersonen der Erfassung und Verarbeitung ihrer Daten ausdrücklich zustimmen. Vorab angekreuzte Kästchen und stillschweigende Zustimmung sind nicht mehr zulässig. Deshalb müssen Unternehmen alle ihre Erklärungen und Angaben zum Datenschutz überprüfen und sie gegebenenfalls anpassen.

5. Festlegen von Verfahren zur Bearbeitung personenbezogener Daten

Wie bereits erwähnt haben Einzelpersonen nach der DSGVO acht grundlegende Rechte. Unternehmen müssen daher Richtlinien und Verfahren für den Umgang mit den einzelnen Punkten festlegen.

Zum Beispiel:

a) Wie können Kunden und Interessenten ihre Zustimmung ordnungsgemäß erteilen?
b) Welcher Prozeß wird angewendet, wenn ein Kunde oder Interessent verlangt, daß seine Daten gelöscht werden?
c) Wie stellen sie als Unternehmen sicher, daß die Daten wirklich aus allen Systemen gelöscht werden?
d) Wie gehen sie als Unternehmen vor, wenn Kunde oder Interessent seine Daten übertragen möchte?
e) Wie wird die Identität des Kunden oder Interessenten geprüft, der den Antrag auf Datenübertragung gestellt hat?
f) Welchen Kommunikationsplan existiert im Unternehmen im Falle einer Datenschutzverletzung?