

IT – Info Kundendaten

Kundendaten

– Grundregeln für ein rechtskonformes Customer Data Management

Der Trend zum Ausbau vorhandener Kundeninformationssysteme und zum individualisierten Marketing verstärkt sich.

Aber allein schon eine „datenschutzrechtliche Nutzungsänderung“ aus der Zusammenführung vorhandener operativer Datenbestände kann grundlegenden Probleme aufwerfen.

Die folgenden Ausführungen sollen Ihnen dabei helfen, bei der Konzeption und beim Einsatz ihrer Kundendatenbanken manche rechtlichen Stolpersteine zu erkennen und passende Massnahmen einzuleiten.

Der rechtliche Rahmen im Überblick:

Nach **Datenschutzrecht** gilt auch für Kundendaten (personenbezogene Daten) das Verbot mit Erlaubnisvorbehalt, d.h. Verarbeitung ist erlaubt bei entsprechender Rechtsvorschrift, im Rahmen eines Vertragsverhältnisses oder mit Einwilligung. Der Kunde ist in vielen Fällen zu unterrichten und kann Auskunft über alle über ihn gespeicherten Daten verlangen.

- Check: Wie kann ein Widerspruch zur Werbung erfasst und gespeichert werden ?

Handels-, gewerberechtliche und steuerrechtliche Normen verpflichten und berechtigen den Unternehmer, Geschäftsvorgänge personenbezogen zu erfassen, zu archivieren und für Kontrollorgane bereit zu stellen.

- Check: Wie können Angebots-, und Debitorendaten entsprechend GDPdU-Norm der Steuerprüfung zur Verfügung gestellt werden ?

Datenschutz, Betriebs-, und Geschäftsgeheimnis erfordern Massnahmen zum Schutz und zur Sicherheit der Kundendaten. Nicht geschützte Informationen unterliegen i.d.R. nicht dem Betriebs-, und Geschäftsgeheimnis.

- Check: Sind alle vertraulichen Daten mit einem wirksamen Zugriffs-, und Autorisierungsverfahren geschützt ? Wird der Standard „Need to Know“ eingehalten ?

Das **Unlautere Wettbewerbsgesetz (UWG)** und das Datenschutzgesetz beschränkt die Nutzung von Daten für Werbezwecke.

Urteile bestätigen: Voraussetzung für Telefon-, und E-Mail-Marketing ist oftmals die Einwilligung.

- Check: Wie kann das Einverständnis zur Nutzung konkreter Daten erfasst und gespeichert werden ?

Teledienste-, und Telekommunikationsgesetze regeln Umfang und Nutzungsmöglichkeiten der Telekommunikationsdaten und Onlinedaten (Internetanwendungen).

- Check: Wann gilt das „Fernmeldegeheimnis“ ? In welchem Umfang dürfen Verbindungsdaten gespeichert werden ?

Risikomanagement

Kundendaten sind in aller Regel Unternehmensressourcen mit hohem Unternehmenswert. Ein wirksames Risikomanagement erfordert Massnahmen zur Minimierung der Risiken aus Nichtbeachtung rechtlicher Anforderungen, Imageschäden oder unbefugter Weitergabe von Kundendaten an die Konkurrenz.

- Check: Sind Ihre Kundendaten nach Schutzbedarf und Risiko klassifiziert und sind entsprechende Sicherheitsmassnahmen festgelegt ?

IT – Info Kundendaten

Checkliste mit Fragen zu Technik, Sicherheit und Organisation/ Management

ausgewählte Fragen ohne Anspruch auf Vollständigkeit !

Datenerhebung

- Direkterhebung Sind die Kriterien Information des Kunden (Verarbeitungszweck, Datenweitergaben) , Widerspruchsrecht, Einverständniserklärung abgeklärt u. berücksichtigt ?
Können die Kundenangaben zum Widerspruch oder zur Einwilligung den einzelnen Datensegmenten ausreichend zugeordnet werden ?
Ist ggf. eine Sperrdatei zur Speicherung der Widersprüche zur Werbung sinnvoll und notwendig?
- Wird dem Kunden eine sichere Übertragung seiner Daten ermöglicht, z.B. mit https ?
Sind die Verarbeitungs- und Nutzungszwecke, Datenweitergaben und ggf. besondere Datenverarbeitungen verbindlich festgelegt und dem Kunden bekannt, z.B. über AGB oder Datenschutzpolicy ?
- externe Quellen Wie wird die Herkunft der Daten in den Datensegmenten nachvollziehbar gespeichert ? (z.B. für spätere Widerspruchs-, oder Auskunftsabwicklung)

Operative Datenverarbeitung

- Wird gewährleistet, dass Kundendaten nach Vertragsbeendigung für die weitere Nutzung nur noch eingeschränkt verarbeitet und genutzt werden dürfen ? Sind die Kriterien hierfür bekannt ?
Wie wird eine fristgerechte Löschung der Daten gewährleistet ?
Gibt es Datenbankfelder für Sperr-, und Löschkennzeichnung ?
Wie kann bei Auskunftsanfragen nach BDSG die Auskunft über alle gespeicherten Daten erteilt werden ?
Existiert ein Verzeichnisse nach BDSG für Kundendaten ?
Werden Nutzerzugriffe entsprechend "Need to Know" eingeschränkt ?
Wird das "Kopieren" von Kundendatenbeständen überwacht und restriktiv gehandhabt, z.B. Übernahme auf Laptops ?

Datenintegration

- Wurde eine Analyse und Festlegung der zu übernehmenden Daten im Hinblick auf Qualität (Richtigkeit) und Rechtmässigkeit (keine Vorratsspeicherung, Interessensabwägung und Einwilligung des Kunden) vorgenommen ?
Wurden die Möglichkeiten zur Anonymisierung/ Pseudonymisierung von Daten abgeklärt ? Erfolgt entsprechende Verfahrensfestlegungen?

Data Ware House

- Wird gewährleistet, dass Kundendaten nach Vertragsbeendigung für die weitere Nutzung nur noch eingeschränkt verarbeitet und genutzt werden dürfen ? Sind die Kriterien hierfür bekannt ?
Wie wird eine fristgerechte Löschung der Daten gewährleistet ?
Gibt es Datenbankfelder für Sperr- und Löschkennzeichnung ?
Wie kann bei Auskunftsanfragen nach BDSG die Auskunft erteilt werden ?
Existiert ein Verzeichnisse nach BDSG für Kundendaten ?
Werden Nutzerzugriffe entsprechend "Need to Know" eingeschränkt ?
Wird das "Kopieren" von Kundendatenbeständen überwacht und restriktiv gehandhabt, z.B. Übernahme auf Laptops ?

IT – Info Kundendaten

Datenanalyse

Werden automatisiert Kundeneinstellungen und Segmentierungen vorgenommen ?
Wurde hierfür der Analysezweck definiert und liegt die Einwilligung des Kunden vor ?
Sind die vorhandenen Autorisierungskonzepte ausreichend ? Need to Know -
Wie wird die Qualität (Richtigkeit, Legalität) erstellter Kundenprofile gewährleistet ?
Entsprechen alle Funktionalitäten der Analysewerkzeuge auch den nationalen
Datenschutzbestimmungen oder sind Beschränkungen erforderlich ?

Datennutzung

Werbung Kann bei Widerspruch des Kunden / Interessenten zur Nutzung seiner Daten für
Werbemaßnahmen dies auch gewährleistet werden ?
Ist eine Sperrdatei erforderlich ? Gibt es entsprechend auswertbare Datenfelder ?
Wie wurde das Einverständnis eingeholt ? Wie dokumentiert, wie abgespeichert ?
Sind die Datenschutzkriterien für Marketing-, und vertriebsunterstützende Aktionen
im Zusammenhang mit der Nutzung von Kunden und Interessentendaten bekannt ?
u. a. Zustimmung, Information, Einschränkungen für Telefon und E-Mailwerbung

Datenweitergabe

Wird gewährleistet, dass sensible Kundendaten (z.B. Kontendaten) auf dem
Übertragungswege gegen unbefugte Einsichtnahme geschützt sind ?
Wird bei Weitergabe und Verarbeitung von Kundendaten durch Dritte die Information
des Kunden und ggf das Einverständnis des Kunden gewährleistet ?
Wie kann das Einverständnis in den entsprechenden Datensegmenten
nachvollziehbar gespeichert werden ?
Werden in Verträgen mit Dritten u. a. Verantwortlichkeiten, Datengeheimnis,
Sicherheitsmaßnahmen und Weiterleitung von Kundendaten an andere
Gesellschaften vertraglich festgelegt ?
Ist die Erlaubnis zur Datenweitergabe und der organisatorische/ technische Rahmen
datenschutzrechtlich abgeklärt ?

Rechtliche Hinweise an Unternehmen

– erstellt vom unabhängigen Landeszentrum für Datenschutz Schleswig Holstein

Den Gesamttext finden Sie als pdf-download unter:
http://www.datenschutzzentrum.de/download/BDSG_Handbuch.pdf

Hier einige Auszüge:

Erhebung von personenbezogenen Daten

Prüfen Sie vor der Gestaltung von Vertragsformularen, welche Informationen Ihrer Kunden Sie wirklich benötigen! Beachten Sie, dass der Zweck der Datenverarbeitung **konkret festzulegen** ist (Zweckbindung) - Kennzeichnen Sie freiwillige Angaben – Fairness gegenüber den Kunden zahlt sich aus.

Festlegung von Verarbeitungszwecken

Grundsätzlich ist es schon aus Beweiszwecken zu empfehlen, Verarbeitungszwecke schriftlich festzulegen. Verarbeiten Sie eine Vielzahl von gleich gearteten Datenkategorien, kann dies auch in der Verfahrensübersicht nach § 4e BDSG geschehen.

IT – Info Kundendaten

Gruppenzugehörigkeit bei Werbeansprache

Die E-Mailadresse, die Telefonnummer, die Telefaxnummer und das genaue Geburtsdatum unterliegen nicht dem Listenprivileg des § 28 Abs. 3 Nr. 3 BDSG! Eine Gruppenzugehörigkeit liegt nicht vor, wenn Sie mehrere Eigenschaften in einen Sammelbegriff zu verknüpfen suchen.

Widerspruch gegen Werbung bereits bei Vertragsschluss

Ermöglichen Sie Ihren Kunden **bereits bei Vertragsschluss**, der Verwendung ihrer Daten zu Werbezwecken zu widersprechen. Hierzu bedarf es lediglich einer Textzeile und eines Ankreuzkästchens, z.B. „Falls Sie unsere Werbung wünschen, kreuzen Sie bitte das nebenstehende Kästchen an.“

Benachrichtigungspflicht nach § 33 BDSG

Werden erstmals personenbezogene Daten für eigene Zwecke **ohne Kenntnis des Betroffenen** gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung und der Identität der verantwortlichen Stelle zu benachrichtigen

Verändert sich der Verarbeitungszweck wesentlich, so löst dies ebenfalls eine Benachrichtigungspflicht aus.

Eine Benachrichtigungspflicht entfällt insbesondere, wenn eine Speicherung ausdrücklich gesetzlich vorgesehen ist. Das gilt auch für gesetzliche Aufbewahrungspflichten (z.B. steuerrelevante Daten).

Auskunftserteilung

Das Auskunftsrecht soll den Betroffenen unter anderem in die Lage versetzen zu beurteilen, ob alle über ihn gespeicherten Daten rechtmäßig gespeichert sind. Sie müssen daher die konkret gespeicherten Daten mitteilen.

Einwilligungsklauseln für die Nutzung zu Werbezwecken

Ist für eine bestimmte Datenverarbeitung oder Nutzung zu Kundenbindungszwecken die Einwilligung des betroffenen Kunden erforderlich, genügt es nach der Rechtsprechung in der Regel nicht immer, eine Streichoption anzubieten (Unzulässigkeit eines bloßen opt-out). Die Rechtsprechung billigt hingegen regelmäßig nur Erklärungen, bei denen Sie Werbefaxe oder Werbeanrufe ausdrücklich wünschen.

Was tun, wenn Kunden über ihre Zufriedenheit befragt werden sollen (Kundenzufriedenheitsbefragung), z.B. durch Call Center?

Nach der Rechtsprechung ist die telefonische Kontaktaufnahme mit Endverbrauchern ohne deren ausdrücklichen Einwilligung (Opt-in) regelmäßig unzulässig, Überlassen Sie es dem Kunden zu entscheiden, ob er Ihnen eine Rückmeldung über Ihren Service geben will! Formulieren Sie eine Einwilligungserklärung, bei der der Kunde sich für oder gegen eine Kundenzufriedenheitsbefragung entscheiden kann. Erfahrungsgemäß trägt dies erheblich zur Akzeptanz der Befragung bei.

Automatisierte Einzelentscheidung/Scoringverfahren

Bei **negativen Entscheidungen** müssen nach § 6a Abs. 2 Nr. 2 BDSG geeignete Maßnahmen gewährleisten, dass die **berechtigten Interessen des Betroffenen** gewahrt werden. Eine Interessenwahrung liegt insbesondere vor, wenn der Betroffene die Möglichkeit hat, seinen Standpunkt geltend zu machen und die verantwortliche Stelle ihre Entscheidung daraufhin erneut überprüft. Es können auch Aspekte vorgetragen werden, die in dem automatisierten Verfahren nicht berücksichtigt wurden. Nach § 6a Abs. 3 hat der Betroffene das Recht auf Auskunft bezüglich des logischen Aufbaus der automatisierten Verarbeitung der ihn betreffenden Daten. Die verantwortliche Stelle ist allerdings nicht verpflichtet, Angaben zur Gewichtung der gesicherten Daten sowie ihrer wechselseitigen Abhängigkeit weil sie eine erhebliche Beeinträchtigung der Privatsphäre bedeutet.

Erstellung von Kundenprofilen – Data Warehouse – Data Mining

Führen die Auswertungen des Kundenverhaltens und der durch Scoring oder soziodemografische Bewertungen gewonnenen Erkenntnisse dazu, den Kunden nicht nur einer bestimmten Zielgruppe zuzuordnen sondern in seinem über das konkrete bzw. vermutete Konsumverhalten hinausgreifenden Persönlichkeitsprofil abzubilden, besteht ein Konflikt mit datenschutzrechtlichen Grundsätzen.

Die Zusammenführung von verschiedenen Kundendatenbeständen, die auf einer Vielzahl unterschiedlicher Zweckbestimmungen basieren, in einem Datenpool zwecks möglicher

IT – Info Kundendaten

Personalisierung und gezielter Werbeansprache ist mit der jeweiligen ursprünglichen Zweckbestimmung nicht vereinbar.

Nach herrschender Meinung sind der Aufbau von Data Warehouses und die darauf aufsetzende Personalisierungstechnik des Data Mining nur mit Einwilligung des Betroffenen erlaubt. Etwas anderes gilt, wenn es sich um anonymisierte Daten handelt.

Soziodemografische Adressbewertungen (Daten über soziale Struktur in Wohnbereichen)
Die Zulässigkeit der Bewertung des Kunden hiermit hängt davon ab, dass nur solide Aussagen und nicht zur Diskriminierung bestimmter Bevölkerung- und Wohngebietsgruppen führende Daten Verwendung finden.

Kundenbindungssysteme (Bonuskarten)

Soweit die Verarbeitung personenbezogener Daten der Abwicklung des Rabattvertrages dient, ist dies datenschutzrechtlich legitimiert.

Die Speicherung und Verarbeitung von weiteren personenbezogenen Daten und die Verwendung dieser Daten zu Werbezwecken ist nach Auffassung der Datenschutzaufsichtsbehörden nur mit Einwilligung der Betroffenen erlaubt.

Weitergehende und recht umfassende Informationen zum Thema Kundendatenschutz finden Sie in der neuen Broschüre (5. 2006) :

Kundendatenschutz – Leitfaden für die Praxis

Herausgegeben von der Gesellschaft für Datenschutz und Datensicherheit

<https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/kundendatenschutz-leitfaden-fur-die-praxis>

und dem Zentralverband der deutschen Werbewirtschaft

Die besondere Qualität des neuen Leitfadens liegt in der kompakten und verständlichen Darstellungsweise. Durch zahlreiche Musterformulierungen und Beispiele können nicht nur die Datenschutzpraktiker in den Unternehmen, sondern alle, die Marketing- und Vertriebsmaßnahmen unter Verwendung von Kunden- und Interessentendaten entwickeln, einen unmittelbaren Nutzwert für ihre tägliche Arbeit generieren. Der Leitfaden stellt die erste umfassende Praxishilfe zum Kundendatenschutz dar.

Für konkrete Fragen stehe ich Ihnen als Datenschutzberater und IT-Revisor gerne zur Verfügung.

Georg Osner

IT-Revisor und Datenschutzberater

Tel: 0871-2760004

E-Mail: Georg.Osner@onlinehome.de