# DATENSCHUTZKONFORMES LÖSCHEN PERSONENBEZOGENER DATEN IN KUNDEN-BEZIEHUNGSMANAGEMENTSYSTEMEN

Tugba Koc Macit, Annika Selzer

## 1. Was sind Kundenbeziehungs-managementsysteme?[1]

Ein Kundenbeziehungsmanagementsystem (kurz: CRM-System für „Customer Relationship Managementsystem") ist eine Software, die das Kundenbeziehungsmanagement unterstützt. Ein solches CRM-System kommt in nahezu jedem Unternehmen zum Einsatz – sei es in Großunternehmen, in kleinen und mittelständischen Unternehmen oder in Start-Ups. Je nach Angebotsumfang eines CRM-Systems können in diesem unter anderem

- Kundenstammdaten erfasst und verwaltet,
- Brief- und Newslettersendungen angestoßen,
- Aktivitäten des Kunden dokumentiert und
- weitestgehend vollständige Profile über die Kunden erstellt werden (wie Interessen und Wünsche, Beschwerden, Reaktionszeiten), sodass die weitere Beziehung auf die genauen Wünsche abgestimmt werden kann.[2]

Die Basis eines jeden CRM-Systems sind die Stamm- und Kontaktdaten von Kunden sowie gegebenenfalls von Interessenten (im Folgenden zusammenfassend „Kunden" genannt). Je nach konkretem Verarbeitungskontext werden zusätzlich weitere Daten bis hin zu umfangreichen Profilen verarbeitet. Bei Kunden kann es sich sowohl um Geschäftskunden als auch um Privatkunden handeln. Da in einem CRM-System häufig auch bei Geschäftskunden die Vor- und Nachnamen der inhaltlichen Ansprechpersonen inklusive einer Kurzbezeichnung ihres Tätigkeitsbereichs (wie „Leiter Vertrieb") sowie deren berufliche Kontaktdaten verarbeitet werden, ist der Anwendungsbereich der DSGVO in der Regel nicht nur für die Privatkunden, sondern auch für die Geschäftskunden eröffnet. Dies ergibt sich insbesondere aus dem Umstand, dass die erhobenen Daten


dafür geeignet sind, einen bestimmten Mitarbeiter des Geschäftskunden zu identifizieren.[3]

## 2. Was sind datenschutzrechtliche Löschpflichten?

Der Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 lit. e DSGVO regelt, dass personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist. Den Verantwortlichen trifft insofern die Pflicht, für die von ihm verarbeiteten personenbezogenen Daten Löschfristen festzulegen, die die Speicherdauer der Daten auf das erforderliche Mindestmaß beschränken und die Daten entsprechend der festgelegten Löschfristen zu löschen (oder alternativ zu anonymisieren). Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen ▸

[1] Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autoren wieder und ist keine offizielle Stellungnahme der Fraunhofer Gesellschaft und der AGOR AG.

[2] Forgó/Helfrich/ Schneider, Betrieblicher Datenschutz, Teil VII Kapitel 3 Rn. 1-4.

[3] Fischer, NZA 2018, 8, 9.

darüber hinaus, die Umsetzung der Löschpflichten durch eine entsprechende Dokumentation nachweisbar zu machen.

Der Grundsatz der Speicherbegrenzung wird durch das Betroffenenrecht auf Löschung aus Art. 17 DSGVO konkretisiert. Auch wenn der Verantwortliche bei Wegfall der Rechtsgrundlage – etwa bei Widerruf der Einwilligung oder nach erfolgreichem Widerspruch in eine Verarbeitung, bei der sich der Verantwortliche auf sein berechtigtes Interesse beruft – grundsätzlich auch ohne Antrag der betroffenen Person dazu verpflichtet ist, zu überprüfen, ob und wann die Daten zu löschen sind, ermöglicht Art. 17 DSGVO den betroffenen Personen die Löschung ihrer personenbezogenen Daten „aktiv", also auf ihren Antrag hin, löschen zu lassen, wenn sie beispielsweise ihre Einwilligung widerrufen haben und kein Ausnahmetatbestand gem. Art. 17 Abs. 3 DSGVO vorliegt.

Ein Ausnahmetatbestand liegt unter anderem dann vor, wenn der Verantwortliche gesetzlichen Aufbewahrungspflichten unterliegt.

## 3. Was sind gesetzliche Aufbewahrungspflichten?

Entgegen der grundsätzlichen Pflichten zur Löschung personenbezogener Daten, wenn diese für den Verarbeitungszweck nicht mehr erforderlich sind, können Gesetze die Pflicht zur Aufbewahrung für einen bestimmten Zeitraum vorschreiben. Beispiele hierfür sind § 147 AO, §§ 238, 257 HGB für

- empfangene Handels- und Geschäftsbriefe (Aufbewahrungspflicht 6 Jahre)
- Inventare, Jahresabschlüsse, Buchungsbelege (Aufbewahrungspflicht 10 Jahre).

Vor der Löschung personenbezogener Daten ist daher zu prüfen, ob der Löschung gesetzliche Aufbewahrungspflichten entgegenstehen. Sollten für ein personenbezogenes Datum mehrere gesetzliche Aufbewahrungsfristen einschlägig sein, so ist das Datum solange zu speichern (oder aufzubewahren), bis die längste gesetzliche Aufbewahrungsfrist verstrichen ist.[4]

Auch mögliche einschlägige Verjährungsfristen, wie die regelmäßige Verjährungsfrist von drei Jahren nach § 195 BGB, sollten in diesem Zusammenhang Berücksichtigung finden.[5]

## 4. Warum ist die Löschung in CRM-Systemen schwierig?

Die Umsetzung der dargestellten Lösch- und Aufbewahrungspflichten ist insbesondere in komplexen Datenverarbeitungssystemen, zu denen auch CRM-Systeme gehören, mit großen Herausforderungen verbunden. Die Herausforderungen ergeben sich unter anderem dadurch, dass in komplexen Datenverarbeitungssystemen personenbezogene Daten nicht oder nur zum Teil strukturiert vorliegen und eine vollautomatische Löschung häufig nicht unterstützt wird.

Nicht selten kommen in Unternehmen gleich mehrerer solcher komplexen Datenverarbeitungssysteme zum Einsatz, was die Umsetzung der Lösch- und Aufbewahrungspflichten zusätzlich erschwert, weil jeweils auch die speziellen technischen und organisatorischen Systemgegebenheiten zu berücksichtigen sind.[6]

## 5. Wie kann die Löschung in CRM-Systemen umgesetzt werden?

Um die rechtlichen Lösch- und Aufbewahrungspflichten einzuhalten, hat der Verantwortliche ein Löschkonzept zu erstellen, zu pflegen und umzusetzen. In einem Löschkonzept werden für alle vom Verantwortlichen verarbeiteten personenbezogene Daten Löschregeln definiert, Zuständigkeiten festgeschrieben und – womöglich system- oder anwendungsabhängig – die Umsetzung und Protokollierung der Löschung beschrieben. Ein Löschkonzept stellt eine organisatorische Maßnahme i.S.d. Art. 24, 25 DSGVO dar.

### 5.1 Was sind Löschregeln und wie werden sie gebildet?

Die DIN 66398 beschreibt eine Vorgehensweise zur Entwicklung von Löschregeln. Löschregeln nach DIN 66398 werden grundsätzlich technikunabhängig beschrieben. Ihr (einziger) Zweck ist es, den rechtskonformen Löschzeitpunkt von Daten festzulegen. Die Beschreibung der anwendungsspezifischen technischen und organisatorischen Umsetzung erfolgt in einem weiteren Schritt.[7]

Für die Entwicklung von Löschregeln wird der Datenbestand eines Verantwortlichen zunächst in sogenannte Datenarten unterteilt. Hierbei sollen die Rechtsgrundlagen und Verwendungszwecke der Verarbeitung, aber auch die Sensibilität der perso-

[4] Enzmann/Selzer/Spychalski, EDPL 2018, S. 416, 417.
[5] Grothe, in Säcker/ Rixecker/ Oetker/ Limperg, Münchener Kommentar zum BGB, §195 Rn.4.
[6] Stummer/Selzer, BvD-News 3/19, S. 26.
[7] Hammer, in Jandt/Steidle, Datenschutz im Internet, S.420.

nenbezogenen Daten und bestehende Aufbewahrungspflichten berücksichtigt werden.[8]

Für jede Datenart wird sodann eine Löschregel definiert, die sowohl den datenschutzrechtlich erforderlichen Verarbeitungszeitraum und mögliche gesetzliche Aufbewahrungspflichten als auch die datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung nach Ablauf der beiden vorgenannten Zeiträume berücksichtigt.[9]

Das Erstellen von Löschregeln stellt viele Verantwortliche vor große Herausforderungen. Um eine erste Orientierung zu geben, wie Löschregeln für ein CRM-System aussehen können, werden daher im Folgenden exemplarische Löschregeln für ein CRM-System definiert. Hierfür wird ein CRM-System mit einem geringen Verarbeitungsumfang betrachtet, im Rahmen dessen lediglich Kundenstammdaten (Name, Anschrift, E-Mail-Adresse, Telefonnummer) sowie Interessensgebiete der Kunden in Bezug auf Informationsveranstaltungen für Start-Ups erfragt werden.

Zusätzlich enthält das CRM-System eine Kopie aller an den Kunden versandten Anschreiben und Rechnungen. Die Aufnahme der Kundendaten im CRM-System erfolgt hierbei

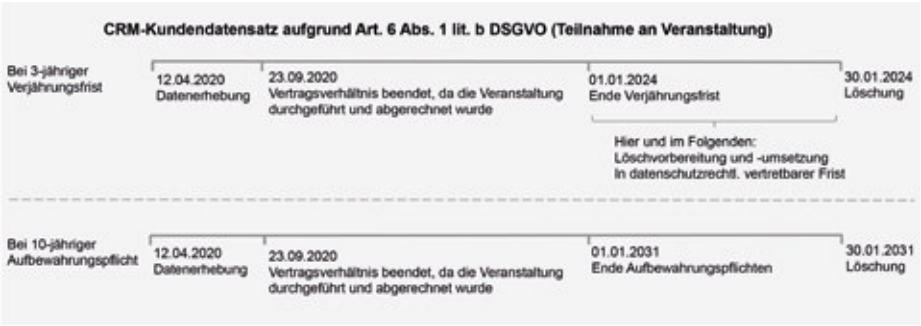
- auf Basis einer Einwilligung (beim Kundenwunsch, über zukünftige Veranstaltungen informiert zu werden) oder
- zur Erfüllung eines Vertrages (bei der Teilnahme an kostenpflichtigen Veranstaltungen) oder
- auf Basis des berechtigten Interesses (beim Speichern von Funktionsträgern bei Geschäftskunden sowie früheren Projektpartnern zur erneuten Kontaktaufnahme).

## 5.2 Wie könnten Löschregeln für ein CRM-Systemen aussehen?

Im oben dargestellten CRM-System werden keine personenbezogenen Daten besonderer Art gespeichert. Dementsprechend sollte sich die Definition der Datenarten, für die Löschregeln zu definieren sind, insbesondere an den Rechtsgrundlagen, Verwendungszwecken und Aufbewahrungspflichten orientieren, um der DIN 66398 zu entsprechen.

Für Kundendatensätze, die auf Basis einer Einwilligung oder auf Basis des berechtigen Interesses zur Information von Interessenten und zur erneuten Kontaktaufnahme verarbeitet werden, gilt, dass die Daten grundsätzlich dauerhaft im Wirkbetrieb des CRM-Systems verarbeitet werden dürfen:


Bei Kundendatensätzen, die hingegen auf der Grundlage eines Vertrags verarbeitet werden, ist das Ziel, die Teilnahme an einer Veranstaltung umsetzen zu können. Hierbei wäre der Zweck der Datenverarbeitung regelmäßig nach Durchführung und Abrechnung der Veranstaltung vollständig erbracht und die Datenverarbeitung im CRM-System könnte nicht länger auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden.[10] Je nachdem, ob für den Veranstaltungskontext „nur" die dreijährige Verjährungsfrist (BGB) oder zusätzlich die zehnjährige Aufbewahrungspflicht (HGB, AO) einschlägig ist, könnten folgende zwei Datenarten und Löschregeln unterschieden werden:




Um den Fall abzudecken, dass in den oben beschriebenen Beispielen im Laufe der Verarbeitung der Zweck oder die Rechtsgrundlage entfällt – etwa bei Widerruf einer Einwilligung, bei Wegfall des berechtigten Interesses oder nach erfolgreichem Widerspruch gegen die Verarbeitung – oder eine betroffene Person von ihrem Recht auf Löschung Gebrauch machen möchte, könnten – je nach Anwendbarkeit von Verjährungsfristen und Aufbewahrungspflichten – zusätzlich folgende drei Datenarten und Löschregeln unterschieden werden:


[8] DIN-Norm 66398.
[9] Weiterführende Informationen: Stummer/Selzer, BvD-News 3/19, Seiten 26 u. 29.
[10] Für den Einzelfall kann jedoch geprüft werden, ob sich eine Weiterverarbeitung auf Art. 6 Abs. 1 lit. f DSGVO stützen kann, um den Veranstaltungsteilnehmer zur Folgeveranstaltung im nächsten Jahr einladen zu können. Auch wenn man davon ausgeht, dass sich ein Teilnehmer in einem Jahr wegen Terminkollisionen nicht (wieder) zu einer Veranstaltung anmeldet, sollte jedoch spätestens im zweiten ohne Teilnahme das Weiterbestehen des berechtigten Interesses neu geprüft werden. Die Datenlöschung bei Wegfall des berechtigten Interesses richtet sich sodann nach den drei Datenarten und Löschfristen „Zweck- und/oder Rechtsgrundlagenwegfall, Löschersuch".

Bei allen hier vorgeschlagenen Löschregeln gilt es mitunter, zusätzlich sogenannte „Sonderlöschfristen" zu beachten. Sonderlöschfristen gelten unter anderem bei offenen Streitfällen, die über Gerichtverfahren geklärt werden müssen. In diesem Fall muss der betroffene Datensatz in der Regel aus Beweisgründen bis zum (rechtskräftigen) Abschluss des Gerichtsverfahrens aufbewahrt werden. Insofern besteht die Notwendigkeit, einen Datensatz (technisch oder organisatorisch) zu kennzeichnen, um diesen von der Löschung auszuschließen.[11]

### 5.3 Wie kann die Löschung in CRM-Systemen angemessen umgesetzt werden?

Die Löschung personenbezogener Daten wird durch technische und organisatorische Maßnahmen i.S.d. Art. 24, 25 DSGVO umgesetzt, die grundsätzlich in Bezug auf die im konkreten Verarbeitungskontext bestehenden Risiken für die betroffenen Personen, die Implementierungskosten und den Stand der Technik angemessen umzusetzen sind. Der Verarbeitungskontext im oben beschriebenen CRM-System birgt grundsätzlich höchstens ein geringes Risiko.[12] Dieser Umstand darf in die konkrete Umsetzung der Löschung einfließen. Aufgrund des geringen Risikos der im oben beschrieben CRM-System verarbeiteten Daten könnten die oben definierten Löschregeln turnusmäßig zum Beispiel monatlich oder vierteljährlich durch händisches Löschen erfüllt werden, sofern das CRM-System keine automatisierte Löschung unterstützt. In diesem Fall sollte es – ebenfalls aufgrund des geringen Risikos – angemessen sein, einen Kundendatensatz als Ganzes zu betrachten und die Löschung des gesamten Kundendatensatzes zum Ende der längstens für den Kundendatensatz relevanten Aufbewahrungspflicht zu löschen. Unterstützt ein CRM-System die Definition von Löschregeln sowie die automatisierte Löschung und Protokollierung, so könnte die systemseitige, turnusmäßige Löschung – je nachdem, ob die Löschung noch händisch zu bestätigen ist oder nicht – in kürzeren wöchentlichen oder monatlichen Intervallen erfolgen. Auch könnten in einem Kundendatensatz in diesem Fall Teillöschungen stattfinden. So könnten die Interessensgebiete des Kunden direkt nach Wegfall des Zwecks oder der Rechtsgrundlage oder nach einem Antrag auf Löschung gelöscht werden, währenddessen eine an den Kunden ausgestellte Rechnung erst nach Ende des aufbewahrungspflichtigen Zeitraums gelöscht würde.

Grundsätzlich kann jedem Verantwortlichen vor der Neubeschaffung eines CRM-Systems dazu geraten werden, für seinen konkreten Verarbeitungskontext zu bewerten, ob das neue System die (teil)automatisierte Löschung unterstützen soll, um Ressourcen im Unternehmen zu schonen.

### 5.4 Wie können die Dokumentationspflichten erfüllt werden?

Durch die Definition der Löschregeln, das Festlegen von Zuständigkeiten und der Beschreibung der technischen/organisatorischen Umsetzung der Löschung im Löschkonzept stellt dieses bereits einen Großteil der Dokumentation dar. Zusätzlich ist i.d.R. die Umsetzung der Löschung zu protokollieren. Die Protokolle selbst sollen keine (der gelöschten) personenbezogenen Daten enthalten, sondern lediglich Auskunft über das Löschdatum und der Anzahl an gelöschten Datensätzen geben. Sofern das jeweilige System eine derartige Protokollierung unterstützt, kann die Protokollierung technisch erfolgen. Andernfalls ist zu empfehlen, ein händisches Löschprotokoll fortzuschreiben, um den Aufwand für die Protokollierung angemessen zu halten.[13]

[11] Koglin, in Koreng/Lachmann, Formularhandbuch Datenschutzrecht, S. 398.

[12] Es bleibt zu betonen, dass das Risiko jedoch für den konkreten Verarbeitungskontext zu bewerten ist. Wird beispielsweise ein CRM-System im oben beschriebenen Umfang genutzt, jedoch statt des Interesses an Informationsveranstaltungen für Start-Ups das Interesse an Informationsveranstaltungen für Süchtige oder Krebserkrankte abgefragt, so wird im Gesamtergebnis der Risikobewertung i.d.R. kein geringes Risiko bestehen, so dass ggf. auch höhere Anforderung an die Löschung bestehen.

[13] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_6o_L%C3%B6schen_V1.0_uagsdmbs_final.pdf.

Über den Autorinnen

**Tugba Koc Macit**
ist Junior Consultant Datenschutz, AGOR AG Frankfurt.
tkoc@agor-ag.com

**Annika Selzer**
ist Wissenschaftlerin am Fraunhofer SIT, Darmstadt.
annika.selzer@sit.fraunhofer.de

▶ www.sit.fraunhofer.de

Fraunhofer SIT