# Datenschutzrechtliche Anforderungen an ein CRM-System

Zusammenfassung:
In einem CRM-System werden personenbezogene Daten gespeichert. Deshalb sind bei der Einrichtung und dem Betrieb eine Reihe von datenschutzrechtlichen Voraussetzungen einzuhalten.

In einem System für das Customer-Management-Relationship (CRM) werden eine Vielzahl von personenbezogenen Daten gespeichert – nicht nur die von Kunden, sondern auch über Mitarbeiter, die das System bedienen.
Deshalb muss der Datenschutz bei der Auswahl eines geeigneten Systems, bei der Einrichtung und der Nutzung beachtet werden.
Insbesondere kommt es auf folgende Punkte an:

- **Zugangsberechtigungen**
  Es sollen sich nur diejenigen Mitarbeiter in das CRM einloggen können, welche die darin gespeicherten Daten für ihre Arbeit benötigen.
  → *Der Zugang zum System darf nur durch ein personenbezogenes Login möglich sein. Zudem sollten, soweit möglich, Richtlinien für eine sichere Passwortwahl eingestellt sein.*

- **Abgesicherter mobiler Zugriff**
  Sofern auch von unterwegs auf das CRM zugegriffen werden soll, muss sichergestellt sein, dass die Daten während ihres Transportes nicht unbefugt eingesehen oder abgegriffen werden können.
  → *Ein Zugriff von unterwegs sollte nur über eine verschlüsselte Datenleitung möglich sein (z.B. per https oder eine VPN-Verbindung).*

- **Berechtigungskonzept**
  Für jeden Nutzer des CRM muss definiert sein, auf welche Bereiche er zugreifen darf (beispielsweise nur auf bestimmte Kundengruppen oder auf bestimmte Auswertungsmöglichkeiten).
  → *Es müssen Benutzerrechte innerhalb des CRM vergeben werden, die sich an der Aufgabe der jeweiligen Benutzergruppe ausrichten.*

- **Zweckbindung**
  Alle personenbezogenen Daten dürfen primär nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erhoben wurden. Andere Zwecke dürfen nicht verfolgt werden.
  → *Die Möglichkeit zu Auswertungen und Analysen sind zu beschränken (konkrete Abfragen zu anderen als den üblichen Zwecken müssen vorab datenschutzrechtlich geklärt werden).*

- **Löschfristen bestimmen**
  Alle personenbezogenen Daten dürfen nur so lange gespeichert und verwendet werden, wie ihre Kenntnisname tatsächlich erforderlich ist. Das heißt, es muss eine Standardfrist bestimmt und schriftlich festgehalten werden (u.a. in den Datenschutz-Informationen für die Betroffenen und im Verzeichnis der Verarbeitungstätigkeiten). Manchmal sehen auch Gesetze eine Aufbewahrungsfrist vor. Nach Ablauf der Frist müssen die Daten gelöscht werden.
  → *Daten müssen nach bestimmten Kriterien gelöscht werden können (Beispiel: zu löschen sind alle Adress-Datensätze, deren Vertrag vor 10 Jahren und länger ausgelaufen ist).*

- **Dokumentation von Herkunft und Weiterleitungen von Daten**
  Die Betroffenen besitzen ein Recht auf Auskunft, woher ihre Daten stammen (z.B. aus einer Anmiete bei einem Adresshändler oder von einem Vertragsschluss) und an welche externen Stellen ihre Daten weiterübermittelt werden (z.B. bei einem Weiterverkauf oder bei der Einschaltung von anderen Dienstleistern).
  → *In den Datensätzen müssen Felder für die Herkunft der Daten und für Übermittlungen an Dritte gepflegt werden (Datum, Grund, erhaltene/übermittelte Datenkategorien, Herkunft/Empfänger).*

- **Vereinbarung zur Auftragsverarbeitung mit Dienstleistern**
  Wenn Dienstleister eingebunden werden und diese Einblick in die im CRM gespeicherten Daten erhalten können (z.B. Ersteinrichtung, Wartung und Support, Cloud-Dienstleister), muss mit ihnen eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen werden.
  → *Prüfen Sie, ob eine Auftragsvereinbarung vorliegt und schließen Sie ggf. eine entsprechende Vereinbarung ab.*

- **Datenschutz-Informationen ergänzen**
  Immer, wenn personenbezogene Daten erstmals erhoben werden, müssen die Betroffenen darüber informiert werden. Unter Umständen müssen in diesem Dokument Angaben ergänzt werden, dass auch das CRM darin korrekt abgebildet wird (z.B. Empfänger von Daten bzw. Dienstleister, Löschfristen u.a.).
  → *Prüfen Sie, ob die Datenschutz-Informationen aktualisiert werden müssen.*

- **Dokumentation von Einwilligung und Widerspruch**
  Hat ein Kunde seine Einwilligung in Werbung oder eine andere Datenverwendung gegeben, muss dies dokumentiert werden (Achtung: Auch die Original-Einwilligung sollte zu Beweiszwecken archiviert werden).
  Wenn er Widerspruch gegen Werbung eingelegt hat, muss dies ebenfalls dokumentiert und bei der weiteren Verwendung entsprechend berücksichtigt werden.
  → *Die Datensätze müssen Felder für Einwilligungen und für Werbe-Widersprüche enthalten. Es muss möglich sein, Adressen auszufiltern, die einen Werbewiderspruch enthalten.*

- **Zwecktrennungsgebot:**
  Jeder Datensatz muss eindeutig einem Zweck zugeordnet sein. Es ist nicht zulässig, z.B. die Adressen von Kunden und Zulieferern gemeinsam so zu speichern, dass nicht mehr klar ist, wer zu welcher Gruppe gehört.
  → *Die Datensätze müssen sich logisch unterscheiden lassen, beispielsweise durch Zuordnung zu bestimmten Gruppen.*

- **Sicherungskonzept**
  Die im CRM-System gespeicherten Daten müssen gesichert werden können (Sicherungskopie, Backup). Die Sicherung muss regelmäßig durchgeführt werden, am besten automatisch, um Datenverlusten vorzubeugen. Die Sicherungen müssen auch wieder nahtlos in das Produktivsystem eingespielt werden können.
  → *Daten müssen exportiert und importiert werden können oder es muss eine andere Möglichkeit der Datensicherung bestehen. Die Datensicherung sollte automatisiert erfolgen und das Datensicherungskonzept nachvollziehbar dokumentiert sein.*

- **Sperren von Daten**
  Wenn Daten nicht mehr benötigt werden, aber noch nicht gelöscht werden dürfen (weil zum Beispiel die Aufbewahrungsfrist noch nicht abgelaufen ist), sind Datensätze zu sperren. Dasselbe gilt, wenn eine Löschung nur mit unverhältnismäßig hohem Aufwand durchgeführt werden könnte oder wenn durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.
  → *Adressdatensätze müssen gesperrt werden können. Dies kann beispielsweise durch eine spezielle Markierung, besser noch durch eine Ausblendung aus dem aktiven Datenbestand geschehen.*

- **Datenschutzgerechte Protokollierung**
  Die Benutzung des CRM-Systems muss protokolliert werden. Dieses Protokoll muss datenschutzgerecht ausgestaltet sein.
  Das heißt auch, dass das Logfile vor unberechtigter Nutzung und Veränderung zu schützen ist.
  Zudem ist eine Löschfrist für das Protokoll zu definieren und umzusetzen.
  → *Ein Logfile über die Benutzung des CRM muss nach datenschutzkonformen Grundsätzen erfolgen.*

**Weiterer Hinweis: Trennung von Test- und Produktivsystem**
Wenn Sie ein CRM-System testen, spielen Sie bitte keine echten Daten ein. Dies widerspricht dem Trennungsgebot. Zulässig wäre es stattdessen, Musterdaten zu verwenden oder zumindest die echten Daten so zu verändern oder zu anonymisieren, dass kein Personenbezug zu den dahinterstehenden „echten“ Menschen mehr möglich ist (beispielsweise durch ein Vermixen und Verfremden von Namen, Anschriften und Geburtsdaten).

Diese Liste ist nicht abschließend, sondern dient Ihrer Orientierung zum Thema CRM.
Binden Sie bitte möglichst vor der Einführung eines CRM-Systems Ihren Datenschutzbeauftragten ein – am besten schon in der Planungsphase. So können spätere datenschutzrechtliche Korrekturen von vornherein vermieden werden.