DATENSCHUTZ

Rechtssichere Löschkonzepte

VON PATRICK KNITTEL
Patrick Knittel leitet die Knittel Akademie für Datenschutz & Compliance in Berlin und berät Unternehmen zu datenschutzrechtlichen und compliance-relevanten Themen. Zum externen Datenschutzbeauftragten ist er vor allem bei sozialen Trägern, Sozial- und Wohlfahrtsverbänden und Vereinen im Bereich des Paritätischen Wohlfahrtsverbandes benannt, für dessen Akademie er auch regelmäßig entsprechende Seminare veranstaltet. Zudem ist er Lehrbeauftragter an der Hochschule Technik und Wirtschaft Berlin.
www.knittel-compliance.de

Soziale Organisationen sind verpflichtet, geeignete technische und organisatorische Maßnahmen bei der Verarbeitung von personenbezogenen Daten umzusetzen. Das schließt auch Maßnahmen hinsichtlich der Löschung personenbezogener Daten ein und erfordert indirekt die Erstellung eines Löschkonzepts.

In unserer Beratungspraxis gibt es immer wieder Anfragen zu Thema Löschen im Rahmen der Erstellung eines Löschkonzepts. Prominente Fälle mit Bußgeldern wegen Nichtlöschung der Daten bei Taxiunternehmen, nicht löschfähiger Archivsysteme gegen die Deutsche Wohnen SE oder Nichtfestlegung der Speicherdauer bei Online-Schuhhändlern machen das Thema zum Dauerbrenner.

Eine Pflicht zur Erstellung eines Löschkonzepts gibt es nicht, vielmehr ergibt sie sich indirekt aus mehreren Regelungen der Datenschutz-Grundverordnung (DSGVO). Maßgebend sind hierbei die in Art. 5 DSGVO verankerten Grundsätze:

- Aus dem Grundsatz der Speicherbegrenzung folgt, dass die Speicherung personenbezogener Daten nur so lange zulässig ist, wie es für die Zwecke, für die die Daten erhoben wurden, erforderlich ist. Zudem müssen die Daten nach dem Grundsatz der Datenminimierung dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Diese maßgeblichen Grundsätze müssen Verantwortliche nicht nur ausreichend berücksichtigen und einhalten, sondern auch in der Lage sein, diese nachzuweisen.
- Zudem sind Verantwortliche dazu verpflichtet, geeignete technische und organisatorische Maßnahmen bei der Verarbeitung von personenbezogenen Daten umzusetzen. Das schließt auch Maßnahmen hinsichtlich der Löschung personenbezogener Daten ein und fordert indirekt die Erstellung eines Löschkonzepts.
- Schließlich verpflichtet Art. 17 Abs.1 DSGVO alle Verantwortlichen, eine Löschung durchzuführen, sofern die dort genannten Gründe vorliegen und beispielsweise die Rechtsgrundlage wegfällt oder der Zweck der Verarbeitung erfüllt ist.

Löschen: Eine Begriffsdefinition fehlt, jedoch schließt die Datenschutz-Grundverordnung in Art. 4 Nr. 2 auch »das Löschen oder die Vernichtung« ein. Als finale Verarbeitung stellt es das Ende eines jeden persönlichen Datums dar. Es ist als ein Prozess zu verstehen, durch den personenbezogene Daten derart verändert werden, dass sie anschließend nicht mehr vorhanden oder unkenntlich sind.

Löschen im Sinne der Datenschutz-Grundverordnung bezieht sich daher nicht zwingend auf den gespeicherten Datensatz, sondern den vorhandenen Personenbezug. Daher kann eine Löschung auch im Wege einer Anonymisierung erfolgen, sofern der Verantwortliche diese nicht mehr rückgängig machen kann.

Löschkonzept nach DIN 66398

Aufgrund fehlender gesetzlicher Vorgaben hat ein Löschkonzept unternehmensintern zu regeln, wer wann welche Daten zu löschen hat, wo die Daten abgespeichert werden und wie die Löschung

DOI: 10.5771/1613-0707-2021-3-32

vor sich gehen sollte. Bei der Erstellung hilft die Leitlinie der DIN 66398 mit folgenden Bestandteilen:

- Grundlagen des Konzepts formulieren
- Datenarten bilden und Löschfristen festlegen
- Löschklassen bilden
- Vorgaben für die Umsetzung von Löschregeln regeln
- Aufbau und Dokumentation eine Ablauforganisation konzipieren, Verantwortlichkeiten sowie Prozesse fürs Löschen benennen

Mit der DIN 66398 liegt zwar eine Leitlinie vor, dennoch zeigt die Praxis, dass diese sich für Vereine oder andere kleine Unternehmen als nicht praxistauglich erweist. Sie liefert weder konkrete Löschregeln noch Löschfristen, weil diese von den jeweils datenschutzrechtlichen Vorschriften, den einzelnen zulässigen Zwecken und weiteren gesetzlichen Normen beim jeweiligen Verantwortlichen abhängt.

Alternatives fachliches und technisches Löschkonzept

Als Grundlage für ein fachliches Löschkonzept dient als Bestandsaufnahme das Verzeichnis der Verarbeitungstätigkeiten, denn es beinhaltet eine strukturierte Erfassung aller personenbezogenen Daten im Unternehmen und die Einteilung in die dort vorgegebenen Datenkategorien, vgl. Art 30 DSGVO.

Erfassung der Speicherorte und betroffenen IT-Systeme: Um festzustellen, an welcher Stelle die Daten gelöscht werden, ist zu ermitteln, wo die und allen welchen Stellen die Daten überhaupt gespeichert sind. Hierbei kann es sich um ein oder mehrere IT-System(e), Back-up, Cache, aber auch um Handakten oder andere physische Dokumente handeln.

Bestimmung der Löschfrist: Personenbezogene Daten müssen grundsätzlich gelöscht werden, sobald der Zweck, für den sie erhoben wurden, erfüllt ist und keine Rechtsgrundlage oder gesetzliche Verpflichtung für eine weitere Speicherung vorliegt. Die Festlegung der konkreten Löschfristen erfolgt somit in zwei Stufen:

- Zunächst muss der Zeitpunkt der Zweckerfüllung bestimmt und die Frage, wann brauchen wir die Daten eigentlich nicht mehr, beantwortet werden. Dabei kommt es auf den Zweck an, für den die Daten ursprünglich erhoben wurden.
- Danach muss geprüft werden, ob es für diese Datenkategorie gesetzliche Aufbewahrungspflichten gibt und wenn ja, wie lange diese eine Speicherung der Daten vorgeben. Aufbewahrungspflichten ergeben sich bei buchhaltungsrelevanten Daten, insbesondere aus § 257 HGB und § 147 AO.

Im Personalbereich gibt es auch eine Vielzahl an gesetzlichen Vorgaben und es sind gesetzlichen Fristen zur Rechtsverfolgung zu beachten. Bewerberdaten sind daher mindestens drei Monate nach Ablehnen des Bewerbers noch aufzubewahren, weil Bewerber innerhalb von zwei Monaten Schadensersatz aus dem Allgemeinen Gleichbehandlungsgesetz fordern könnten.

Um die konkrete Löschfrist zu ermitteln, müssen der Zeitpunkt der Zweckerfüllung und die gesetzliche Aufbewahrungsfrist bzw. die Frist zur Rechtsverfolgung ins Gleichgewicht gebracht werden: Bestehen bei einer Datenkategorie keine gesetzlichen Aufbewahrungspflichten oder Fristen zur Rechtsverfolgung, ist der Zeitpunkt der Zweckerfüllung für die Löschung maßgeblich. Bestehen nach Zweckerfüllung hingegen noch (andere) gesetzliche Aufbewahrungspflichten, müssen diese vorrangig berücksichtigt werden.

Gerade bei den Betroffenenrechten zeigt sich, dass im Voraus intern festgelegt werden muss, wie im konkreten Fall zu verfahren ist, wenn ein Betroffener den Verantwortlichen auffordert, seine Daten zu löschen, jedoch gesetzliche Aufbewahrungsfristen diesem Löschbegehren entgegenstehen. Neben Möglichkeiten der Einschränkung der Verarbeitung müssen gegebenenfalls Möglichkeiten der Anonymisierung oder Pseudonymisierung vorgegeben werden.

Technisches Löschkonzept (Definition des Löschvorgangs): Nach der Festlegung welche Daten zu welchem Zeitpunkt gelöscht werden können und müssen, müssen Prozesse zu entwickelt werden, um die zuvor definierte Löschfrist für jeden Speicherort und jedes IT-System einhalten und umsetzen zu können. Bei der Analyse, wie eine Löschung der Daten vorgenommen werden kann, ist vor allem bei IT-Systemen als Speicherort die Mithilfe der IT-Abteilung gefragt. Es sind technisch und organisatorische Maßnahmen festzulegen und die Zuständigkeiten zu prüfen, ob eine Löschung automatisiert stattfinden kann oder ob die Löschung durch die Aktion eines Beschäftigten bedarf.

Beachte: Das altbekannte Argument, das eingesetzte Programm oder Archivsystem biete keine Möglichkeit Daten zu löschen, ist seit der Geltung der Datenschutz-Grundverordnung keine geeignete Strategie, um sich vom Grundsatz der Speicherbegrenzung freizusprechen – im Gegenteil: Es kann zu empfindlichen Bußgeldern führen.

Zuständigkeit für Löschung: Im technischen Konzept sollte aufgrund der Rechenschaftspflicht unbedingt festgehalten werden, wer für die Durchführung der Löschung zuständig ist. Jede Person und Abteilung mit Löschverantwortung muss dafür sorgen, dass die zugeordneten Datenkategorien einer regelmäßigen Löschung unterzogen werden. In welchen Abständen eine Löschung zu erfolgen hat, liegt maßgeblich an der Dauer der Frist und der Komplexität des Löschvorgangs. Im Gegensatz dazu ist bei automatisierten Löschungen die Frist genau einzuhalten, sodass bei komplexeren Vorgängen eine geeignete Regelmäßigkeit gewählt werden muss. Schließlich muss jede Löschung von den jeweiligen Lösch-Verantwortlichen dokumentiert werden.

Regelmäßige Kontrolle der Löschung: Im Rahmen der kontinuierlichen Verbesserung ist die Entwicklung und Umsetzung eines Löschkonzepts ein fortlaufender Prozess, der sich den stetigen Veränderungen anpassen soll. Die Verantwortlichen haben daher in regelmäßigen Abständen das Löschkonzept auf Vollständigkeit und Funktionalität zu prüfen.

Fazit

Die Erstellung und Umsetzung eines Löschkonzepts für alle personenbezogenen Daten im Unternehmen ist ein sehr komplexes Vorhaben. Bei der Umsetzung spielen neben gesetzlichen Vorgaben eine ganze Reihe unternehmensspezifischer Faktoren eine Rolle und fordern eine individualisierte Gestaltung der Löschvorgaben. Zu den größten Herausforderungen zählt neben den Löschregeln die Findung der Speicherorte und Sonderfälle. ■