Vergiss mich wieder!

Datenschutzkonformes Löschen in Kanzleien

StB Sigune Vahnauer, Neubrandenburg

Die erweiterten Löschpflichten stellen viele Kanzleiverantwortliche vor große Probleme. Die Komplexität moderner IT – Systeme führt häufig dazu, dass die Speicherorte personenbezogener Daten nur noch schwer zu eruieren sind. Wo liegen die Daten überhaupt? Welche Löschfristen gelten? Was mache ich mit Daten, die keiner gesetzlichen Aufbewahrungsfrist unterliegen, wie z.B. Bewerberdaten?

Neu ist das Thema Löschpflichten nicht. Durch das Wirksamwerden der europäischen Datenschutzgrundverordnung (DSGVO) vor knapp zwei Jahren ist das Löschen jedoch auf ein neues Niveau gebracht worden. Das fehlende Bewusstsein hat seinen Ursprung im vorher anzuwendenden Bundesdatenschutzgesetz (BDSG) und den bislang zu vernachlässigenden Sanktionen in diesem Bereich. Die damals gern genutzte „Ausweichmöglichkeit“ der Sperrung statt der Löschung kann nach aktueller Rechtslage jedoch nicht mehr angewendet werden. Handlungsempfehlungen erhalten Sie beispielsweise auf der Webseite des Deutschen Steuerberaterverbandes (Rubrik Praxistipps) Empfehlenswert ist es, das Löschkonzept mit dem zuständigen Datenschutzbeauftragten zu besprechen. In Zusammenarbeit mit dem Datenschutzbeauftragten Andrè Weinert a von der Wirtschaftskontor Weinert GmbH sind wir folgenden Fragen nachgegangen:

Warum muss ich löschen?

Zuerst einmal gibt es gesetzliche Verpflichtungen. Diese zwingen Kanzleien unter anderem zur sogenannten Speicherbegrenzung. Nach Artikel 5 der DSGVO ist eine Verarbeitung nur gestattet, solange ein Zweck dies erforderlich macht. Ein solcher Zweck ist ein Mandatsverhältnis.

Doch wie verhält sich der Steuerberater, wenn ein Mandatswechsel stattfindet? Neben der Herausgabepflicht gemäß § 66 StBerG wird im Abs. 1 Satz 2 auch die Aufbewahrungspflicht von 10 Jahren definiert. Diese Verpflichtung erlischt mit der Übergabe der Handakten an den Auftraggeber, spätestens jedoch binnen sechs Monaten, nachdem der Auftraggeber die Aufforderung des Steuerberaters oder Steuerbevollmächtigten erhalten hat, die Handakten in Empfang zu nehmen.

Jedoch zählen zu den Handakten nicht zwingend der elektronische Schriftverkehr zwischen Steuerberater und Mandanten. Auch interne Arbeitsunterlagen, wie Gesprächsvorbereitungen oder Honorarkalkulationen fallen nicht unter diesen Begriff. Hier ist eine Löschung nach Zweckentfall nach Artikel 17 Abs. 1 lit. a. der DSGVO vorgeschrieben.

Spannend wird das Thema Löschen bei jahrzehntelangen Bestandsmandaten. Grundsätzlich sind die Daten für die Dauer von 10 Jahren nach Auftragsbeendigung aufzubewahren. Ein Sicherheitszuschlag von maximal 4 Jahren wegen möglicher Ablaufhemmung ist jedoch empfehlenswert und nach aktueller Rechtslage zulässig. Somit wird aber eine Löschung nach 14 Jahren der Auftragsbeendigung verpflichtend. Lediglich bei einem legitimen Grund, wie z.B. Pensionszusagen oder der Absicherung der Verfolgung titulierter Vergütungsansprüche, ist eine längere Speicherung zulässig.

Hier liegen im Alltag als Beratungsunternehmen im Bereich Datenschutz die größten Herausforderungen. IT-Systeme waren in der Vergangenheit technisch nicht ausreichend vorbereitet, Daten in Regelprozessen zu löschen. Gleichzeitig besteht häufig die Angst einer Prozessstörung oder Inkonsistenz der Daten in den IT-Systemen. Und tatsächlich können solche Probleme bei nicht sorgfältig vorbereiteten Löschungen eintreten. Der technische Fortschritt im Bereich Speicherkapazitäten tat sein Übriges. Notwendige Speichererweiterungen spielen in der Kostenbetrachtung quasi keine Rolle mehr. Ergebnis ist häufig eine durchgehende Speicherung personenbezogener Daten „ohne Ende“ und eine Mammutaufgabe für die verantwortlichen Unternehmenslenker. Eine Ablösung solcher

IT-Systeme ist unabdingbar. Moderne Branchensoftware-Anbieter stellen seit einigen Jahren Module und Umsetzungsprozesse für Löschungen zur Verfügung.

In den gesetzlichen Verpflichtungen beim Thema Löschen stehen vor allem die Rechte natürlicher Personen im Vordergrund. Diese Rechte wurden durch die Einführung der DSGVO noch einmal deutlich gestärkt. Danach hat jede natürliche Person nach Artikel 17 der DSGVO das „Recht auf Vergessenwerden“. Das bedeutet, dass auch ohne Löschbegehren eines Betroffenen seine Daten nach Zweckerfüllung und Einhaltung aller weiteren gesetzlichen Normen, wie z.B. § 147 AO, zwingend zu löschen sind.

Nicht zuletzt droht ein sehr großes Sanktions- und Haftungsrisiko. Das zeigt vor allem der Fall des Immobilienkonzerns „Deutsche Wohnen“ aus Berlin aus dem Jahr 2019 deutlich. Über ein aktuell verhängtes Bußgeld in Höhe von 14,5 Millionen Euro streiten sich nunmehr Gerichte. Was war passiert? Persönliche Daten von Mietern und ehemaligen Mietern, etwa Sozial- und Krankenversicherungsdaten, Arbeitsverträge oder Informationen über ihre finanziellen Verhältnisse wurden über viele Jahre in einem Archiv gesammelt und nicht gelöscht.

Was bedeutet eigentlich löschen?

Löschen im Sinne der DSGVO bedeutet die unwiderrufliche Entfernung eines Personenbezugs ohne Rückschlussmöglichkeit auf eine natürliche Person. Die DSGVO spricht in Art. 4 Absatz 2 von „Löschen oder die Vernichtung“. Demnach sind Löschen und Vernichtung nach dem Verständnis der DSGVO alternative Maßnahmen.

Ein fehlender Personenbezug kann somit unter Umständen auch durch eine Anonymisierung der Daten erreicht werden. Begründbar wird dies ebenfalls mit dem Erwägungsgrund 26 der DSGVO, der besagt, dass die gesetzlichen Vorgaben keine Anwendung auf anonymisierte Daten finden.

Somit gelten Daten, deren Personenbezug unwiderruflich entfernt ist, im Sinne der DSGVO als gelöscht. Das bedeutet im Umkehrschluss, dass eine technische Vernichtung der Daten nicht zwingend erforderlich ist.

Tipp: Verschlüsselte personenbezogene Daten können unter Umständen auch als gelöscht gelten, wenn der Schlüssel unwiderruflich vernichtet ist und eine Wiederherstellung des Schlüssels nicht möglich ist.

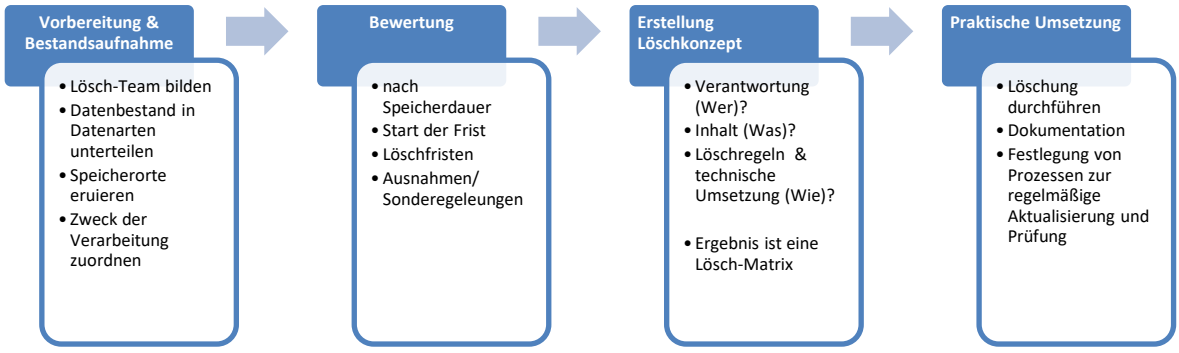
Doch wie im Steuerrecht auch, gelten im Datenschutz umfangreiche Rechenschafts- und Nachweispflichten. Diese machen eine Dokumentation des rechtskonformen Löschens unerlässlich.

Wie kann man dieses Thema systematisch und datenschutzkonform umsetzen?

Eine sinnvolle Lösung ist die Etablierung eines Löschkonzeptes. Die Ziele eines solchen Konzeptes sind neben der gesetzlichen Verpflichtung zum Löschen vor allem der Schutz der Rechte der Betroffenen nach dem Grundsatz des „Rechtes auf das Vergessenwerden“. Ergebnis muss auch sein, dass in der Kanzlei oder im Unternehmen ein Prozessbewusstsein und eine Sensibilisierung der Beschäftigten entstehen. Damit einher geht neben der Prozessoptimierung das „Platz schaffen“ durch Vernichten und das Senken der Kosten im IT-Bereich. Zuallerletzt wird das Erfüllen von Prüfnormen für Zertifizierungen und Audits eine entscheidende Rolle spielen.

Als Grundlage dienen die empfohlenen Standards nach der DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“. Sie beinhaltet Vorgaben zur Entwicklung und Etablierung eines Löschkonzeptes, gibt Empfehlungen zum Inhalt, Aufbau und den Verantwortlichkeiten und beschreibt die Vorgehensweisen, Löschfristen und Löschregeln.

Zur Vereinfachung soll das nachfolgende Schaubild helfen.



Aller Anfang ist schwer!

Lassen Sie sich nicht vom Umfang abschrecken und sehen Sie ein Löschkonzept als Chance. Beginnen Sie mit einem Teilprojekt in der Kanzlei, wie z.B. dem Personalbereich. Dieser scheint im ersten Moment überschaubar. Dabei lernen Sie, wie der Aufbau eines Löschkonzeptes funktionieren kann. Aber auch hier werden Sie erste Herausforderungen und Sonderfälle kennenlernen, wie z.B. den Umgang mit Bewerberdaten, die ja

bekanntermaßen keiner gesetzlichen Aufbewahrungsfrist unterliegen, aber durchaus sensible Daten enthalten.

Tipp: Bewerbungsunterlagen werden in der Regel an die Entscheider in einem Bewerbungsprozess verteilt und liegen häufig „für immer“ im jeweiligen Mailpostfach. Das ist aber von gewisser Brisanz, da nach aktueller Rechtsprechung Bewerberdaten von Bewerbern, die nicht genommen werden, ohne Einwilligung des Bewerbers spätestens nach 3 - 6 Monaten gelöscht werden müssen. Hier ist der Zweck der Speicherung nicht mehr gegeben, um die Daten weiter zu speichern. Die Daten dürfen für den genannten Zeitraum gespeichert werden, falls ein Bewerber eine Klage z.B. nach dem Gleichstellungsgesetz anstrebt und sich ggf. benachteiligt fühlt. Um eine Vorbereitung auf ein solches Verfahren machen zu können, dürfen die Daten zu diesem Zweck so lange gespeichert werden.

In der Praxis hat sich bewährt, dass in einem solchen Fall die Daten nur einmal zentral abgelegt werden und in der Mail an die Entscheider nur noch ein Link zu diesen Unterlagen gesendet wird. Wenn später die Löschung der digitalen Unterlagen nach dem Löschkonzept durchgeführt wird und jemand trotzdem den Link der Mail klickt, führt dieser ins „Daten-Nirvana“ und Sie haben diese Hürde charmant gemeistert.

Fazit

Dass das datenschutzkonforme Löschen von personenbezogenen Daten ein wesentliches Aufgabengebiet Ihrer Kanzlei-Compliance ist, sollte jeder Kanzleileitung bewusst sein. Wenn Sie den Anforderungen an eine moderne Kanzleiorganisation gerecht werden wollen und die Sanktions- und Haftungsrisiken reduzieren möchten, werden Sie um das Thema Löschen nicht herumkommen. Nutzen Sie einfach dieses Thema, um Geschäftsprozesse zu präzisieren, transparente IT-Prozesse zu etablieren und Datenbestände zu konsolidieren.