Volker Hammer, Reinhard Fraenkel

Löschklassen

Standardisierte Fristen für die Löschung personenbezogener Daten

Personenbezogene Daten werden häufig in komplexen Geschäftsprozessen verwendet, oft auch für mehrere miteinander verzahnte. Das BDSG bestimmt zwar, dass diese Daten auch zu löschen sind – in der Festlegung von Löschregeln und –fristen ist der Rechtsanwender aber weitgehend auf sich allein gestellt. Schon am Aufwand für die Abstimmung entsprechender Regeln kann die Umsetzung eines Löschkonzepts scheitern. Diese Herausforderung muss der bDSB meistern – z. B. durch gezielten Einsatz von Prozessanalysen einerseits und die Verwendung standardisierter Fristen andererseits. Der Beitrag stellt den Konkretisierungsrahmen des § 35 Abs. 2 BDSG und die Ausgestaltung in Form von 12 Löschklassen bei Toll Collect vor. Dieses Konzept eignet sich auch für die Übertragung auf andere Unternehmen.

Einleitung

Personenbezogene Daten müssen gelöscht werden. Da der Gesetzgeber nur selten konkrete Fristen für die Löschung vorgibt, bleibt die Festlegung konkreter Löschfristen meist den verantwortlichen Stellen überlassen. Die Festlegung dieser Fristen ist allerdings Voraussetzung dafür, dass ein Löschkonzept überhaupt umgesetzt werden kann.

Da die Löschfristen nach den Vorgaben des Datenschutzes bestimmt werden müssen, ist der betriebliche oder behördliche Datenschutzbeauftragte (bDSB) vielfach gefordert, Daten und ihre Verwendung zu bewerten. Angesichts vielfältiger und oft dynamischer Geschäfts- und IT-Prozesse stößt der bDSB bei detaillierten Analysen schnell an die Grenzen seiner Ressourcen – was die Realisierung eines Löschkonzepts insgesamt gefährdet. Die Aufgabe kann nur bewältigt werden, wenn Löschfristen mit einer einfachen Methode festgelegt werden können. Die Autoren stellen den bei Toll Collect gewählten Ansatz vor.

Reinhard Fraenkel

ist nach verschiedenen Tätigkeiten in der Industrie seit 1994 als Rechtsanwalt in Gütersloh tätig. Zu seinen Arbeitsschwerpunkten zählt das Datenschutzrecht. Seit August 2004 ist er externer Datenschutzbeauftragter der Toll Collect GmbH.
E-Mail: post@kanzlei-fraenkel.de

Dr. Volker Hammer

ist Consultant der Secorvo GmbH. Seit Mitte 2003 unterstützt er die Toll Collect GmbH in verschiedenen Datenschutz-Projekten. Weitere Arbeitsschwerpunkte sind Public Key Infrastrukturen und kritische IT-Infrastrukturen
E-Mail: volker.hammer@secorvo.de

1 Löschvorgaben des BDSG

Im BDSG wird die Löschung der Daten, die der eigennützige Datenverarbeiter in zulässiger Weise auf der Basis von § 28 BDSG erhebt, in § 35 Abs. 2 Nr. 3 BDSG geregelt: *„Sie sind zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist“*, heißt es dort.

Nach § 4e Nr. 4 in Verbindung mit § 4g Abs. 2 BDSG muss die verantwortliche Stelle *„Regelfristen für die Löschung der Daten“* festlegen. Dabei lässt der Gesetzgeber die verantwortliche Stelle oft allein – denn konkrete Löschfristen finden sich im BDSG bisher nicht und auch in spezialgesetzlichen Regelungen nur selten.

Durch das Gesetz zur Regelung des Beschäftigtendatenschutzes, das in einer Entwurfsfassung vorliegt und nach den Vorstellungen des Gesetzgebers in das BDSG eingegliedert werden soll,[1] gerät unter anderem die Frage der Löschung personenbezogener Daten in Unternehmen wieder stärker in den Blickpunkt. So enthält der Entwurf zum Beschäftigtendatenschutzgesetz eine Fülle konkreter Löschgebote. Dies haben jüngst Isabell Conrad und Dominik Hansen zum Anlass genommen, sich mit der Frage der datenschutzgerechten Löschung personenbezogener Daten auseinander zu setzen.[2]

2 Löschkonzept ohne Fristen?

Der Aufsatz ist interessant und auch lesenswert, weil er nicht nur die zu erwar-

1 Vgl. Bundestagsdrucksache 17/4230 vom 15.12.2010.

2 Conrad/Hansen ITRB 2011

tenden Löschregelungen im Gesetzentwurf zum Beschäftigtendatenschutz darstellt. Er macht auch die Komplexität von Löschprozessen insofern transparent, als er vor allem die technischen Prozesse und auch die Systeme in den Blick nimmt, in und auf denen Löschmechanismen zu etablieren sind. Eine umfangreiche Checkliste für ein „Löschkonzept" erhöht den Praxisbezug und auch den Nutzen dieser Ausarbeitung für den Anwender.[3]

Gleichwohl bleibt eine wesentliche Frage offen. Die Autoren sagen nämlich nichts zu den zu etablierenden Löschfristen. Nicht einmal in der Checkliste findet sich ein entsprechender Platzhalter. Das ist insofern überraschend, weil sich die zentrale Löschvorschrift zur Löschung personenbezogener Daten für eigennützige Datenverarbeiter, § 35 Abs. 2 Nr. 3 BDSG, ja gerade nicht von selbst versteht, sondern besonders ausfüllungsbedürftig ist.

Wenn man sich aber mit der Frage datenschutzgerechter Löschung personenbezogener Daten auseinandersetzt, kann man die Frage, wann denn eigentlich die vorher erfassten und dann verwendeten Daten wieder zu löschen sind, nur dann ausblenden, wenn sich die Antwort darauf eindeutig aus dem Gesetz ergibt. Entsprechende Vorschriften gibt es in bestimmten bereichsspezifischen Datenschutzregelungen. Erinnert sei in diesem Zusammenhang an § 13 Abs. 4 Nr. 2 TMG hinsichtlich des Löschgebots von Nutzungsdaten, die bei der Inanspruchnahme von Telemedien anfallen. Auch das Bundesfernstraßenmautgesetz (BFStrMG) kennt ähnlich eindeutige Löschgebote.

Dies aber ist, wie gesagt, die Ausnahme. In der Regel gilt § 35 Abs. 2 Nr. 3 BDSG das Tatbestandsmerkmal „nicht mehr erforderlich". Dieses ist ausfüllungsbedürftig! Ein Löschkonzept aber, das keine praxistauglichen Fristen für die verschiedenen Arten personenbezogener Daten bestimmt, bleibt inhaltsleer und nur formal.

Zum Tatbestandsmerkmal „erforderlich"

Versucht man das Tatbestandsmerkmal „nicht mehr erforderlich" zu konkretisieren, stellt man zweierlei fest: Das Adjektiv „erforderlich" ist einer der zentralen Begriffe des BDSG – angesichts der häufigen Verwendung wird er in der Fachliteratur aber nur sehr sparsam kommentiert. Nicht weniger als 62-mal taucht der Begriff im BDSG in unterschiedlichen Kontexten auf, z. B. im Zusammenhang mit der Erhebung von Daten (§ 4Abs. 2 Nr. 2a BDSG), hinsichtlich spezifischer Aufklärungserfordernisse der verantwortlichen Stelle gegenüber einem Betroffenen (§ 4 Abs. 3 S. 3 BDSG) oder der Notwendigkeit technischer und organisatorischer Maßnahmen datenverarbeitender Stellen (§ 9 BDSG). Zentral ist seine Bedeutung aber insbesondere auch für den Umfang von Datenbeständen und deren Verwendung.

Dem Maßstab der Erforderlichkeit kommt sowohl im Abschnitt für den öffentlichen Bereich als auch in dem für den privaten Bereich zentrale Bedeutung zu – er soll schlechthin sowohl die die Datenerhebung als auch die den gesamten Prozess der Datenverwendung limitierende Maxime sein. Beispielhaft sei § 28 Abs. 1 BDSG zitiert: *„Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist."*

Der Maßstab der Erforderlichkeit macht die Datenerhebung und -verwendung zulässig. Dieses Kriterium, das in besonderer Weise den Ausnahmecharakter der ja grundsätzlich verbotenen Erhebung personenbezogener Daten unterstreicht, konkretisiert einerseits den in § 3a BDSG normierten Grundsatz der Datenvermeidung und Datensparsamkeit, verleiht aber andererseits auch dem Gebot der Zweckbindung normative Wirkung. Beide Aspekte sind in § 28 Abs. 1 Nr. 1 verknüpft.

Angesichts der offensichtlichen Relevanz des Merkmals „erforderlich" bzw. „Erforderlichkeit" ist es überraschend, dass in der Kommentarliteratur zum BDSG kaum etwas zu finden ist, was den interpretationsbedürftigen Begriff „erforderlich" besonders im Hinblick auf seine Tauglichkeit als trennscharfes Kriterium der Datenverarbeitung im privaten Bereich näher erläutert bzw. untersucht. Mit Verweis auf den Maßstab der Erforderlichkeit, den das BVerfG in seiner berühmten Volkszählungsentscheidung von 1983[4] entwickelt habe, versuchen die Autoren Bergmann, Möhrle Herb in ihrem Kommentar der Norm auch für den privaten Bereich Konturen zu verleihen.[5]

„Erforderlichkeit" im öffentlichen Bereich

Im Bereich der öffentlichen Verwaltung ist der Begriff der Erforderlichkeit für den Datenschutz weitgehend tragfähig. Dort nämlich, im Bereich der gesetzesgebundenen Verwaltung, gibt es das Korrektiv, das dem Tatbestandsmerkmal „erforderlich" seine Konkretion verleiht und damit auch seine limitierende Wirkung: das Gesetz.

Das Gesetz definiert die Aufgabe der Verwaltung und schafft damit auch den gerichtlich überprüfbaren Handlungsrahmen der Verwaltung. Welche Anforderungen diesbezüglich an die Normenklarheit zu stellen sind, das lehrt eindrücklich das Volkszählungsurteil.[6] Gerade aber diese Ausführungen machen nachdrücklich deutlich, dass es in dieser Entscheidung in aller erster Linie um Verwaltungshandeln ging – um den Datenschutz in der öffentlichen Verwaltung. Daher ist bei einer Übertragung der in der Entscheidung entwickelten Grundsätze der Erforderlichkeit in die Sphäre der Privatwirtschaft Vorsicht geboten.

„Erforderlichkeit" im privaten Bereich

Die Parteien in der vom Grundsatz der Privatautonomie geprägten Sphäre vereinbaren einen großen Teil ihrer Regeln selbst. Sie sind eben nicht durch gesetzesgebundene Aufgaben bestimmt, wie die Verwaltung. Vielmehr definieren Gesetze im privaten Bereich nur Rahmenbedingungen für die Handlungen der Akteure. Insofern verliert das Tatbestandsmerkmal der Erforderlichkeit auch einen großen Teil der Konkretion, die ihm durch die Gesetzesregeln für das Verwaltungshandeln verliehen werden.[7]

Die Weite beispielsweise von Vertragsinhalten bestimmen die Parteien selbst.

3 Conrad/Hansen, ITRB 2011, S.39

4 vgl. Urteil des BVerfG vom 15.12.1983, Az./BvR 209, 269 (BVerfGE 65,1ff)

5 Vgl. *Bergmann, Möhrle, Herb 2009,* § 35 Rd-Nrn 61 ff.

6 BVerfGE 65, S. 44 ff.

7 Die Einführung des Tatbestandsmerkmals „erforderlich" in das BDSG ist hinsichtlich des Verwaltungshandelns konsequent. In ihm spiegelt sich noch das Pathos eines negatorischen Abwehrrechts. Das Kriterium der Erforderlichkeit ist Ausfluss des *Prinzips des geringst möglichen Eingriffs* (in die Rechte der Bürger). Es ist Bestandteil jeder Prüfung der Verletzung von Grundrechten. (Vgl. dazu näher: *Manssen 1995,* RdNrn 629 ff.)

Von diesen Inhalten aber wird der Kranz zu erhebender bzw. zu verwendender personenbezogener Daten wesentlich bestimmt. Manches um ein simples Verkaufsgeschäft herum konstellierte zusätzliche Dienstleistungsangebot dient vielleicht nur der Erhebung weiterer Daten zur Festigung der Kundenbindung. Erinnert sei in diesem Zusammenhang nur an die vielen Prämienprogramme. Die Liste dieser Beispiele ließe sich beliebig fortführen. Sie soll illustrieren, dass es in der Sphäre der Privatautonomie unternehmerische Entscheidungen gibt, die der eigentlichen Datenerhebung und -verwendung vorgelagert sind – die sie aber ganz wesentlich determinieren und damit zugleich das Tatbestandsmerkmal „erforderlich" unterminieren können. Es verliert so die Trennschärfe, die es in der gesetzesgebundenen Verwaltung haben sollte und trägt daher im privaten Bereich nicht in gleicher Weise.

Diese Schwierigkeiten dürfen aber im Hinblick auf das Löschgebot des § 35 Abs. 2 Nr. 3 BDSG nicht dazu führen, dass auf eine Konkretion der „Erforderlichkeit" verzichtet wird. Das Ziel, Löschfristen zu bestimmen, muss in einem Löschkonzept trotzdem geleistet werden – andernfalls wird das Konzept im rein Formalen verharren und für eine praktische Umsetzung kaum tauglich sein.

3 Methoden der Fristbestimmung

In Geschäftsprozessen werden unterschiedliche Arten personenbezogener Daten (Datenarten) verwendet, z. B. im Telekommunikationsbereich Nutzungsdaten, Verbindungsdaten und Stammdaten oder im Kontext des Mautsystems u. a. Fahrtdaten, Kontrolldaten und ebenfalls Stammdaten. Diese verschiedenen Datenarten werden für verschiedene Zwecke und in unterschiedlichen Geschäftsprozessen eingesetzt. Das eine Definition von Löschfristen für verschiedene Datenarten gelingen kann und welche Methoden sich zur Bestimmung der Fristen anbieten, soll nachfolgend am Beispiel des Löschkonzepts der Toll Collect GmbH dargestellt werden.[8]

Auf Grund der konkreten Erfahrungen, die die Autoren bei der Erarbeitung und Etablierung eines umfassenden Löschkonzepts bei der Toll Collect GmbH gemacht haben, ergeben sich drei Verfahrensweisen zur Bestimmung von Löschfristen :

- die Fristdefinition aus Rechtsvorgaben
- die Prozessanalyse oder
- die Festlegung von organisationsweiten Standardfristen.

Diese drei Verfahrensweisen sind allerdings nicht unabhängig voneinander. So wird eine Prozessanalyse oft die rechtlichen Rahmenbedingungen konkretisieren. Gegebenenfalls sind in diesem Zusammenhang auch Geschäftsprozesse an rechtliche Vorgaben anzupassen. Als Standardfristen werden sinnvoller Weise auch solche Fristen herangezogen, die sich aus Rechtsvorgaben oder Prozessanalysen ergeben.

3.1 Fristdefinition aus Rechtsvorgaben

Auch wenn sie selten zu finden sind – gelegentlich legt der Gesetzgeber Löschfristen fest. Solche Fristen gehen als normative Vorgabe in ein Löschkonzept ein. Sie lassen der Organisation auch keine Spielräume zu einer Verzögerung der Löschung. Vielmehr müssen Prozesse gegebenenfalls so gestaltet werden, dass die Fristen eingehalten werden.

Beispiele für Fristdefinitionen in Rechtsregeln sind für die Frist „sofort" das TMG[9] und das BFStrMG[10]. Auch das TKG enthält in § 97 Abs. 3 hinsichtlich der bei Telekommunikationsprozessen anfallenden Verkehrsdaten eindeutige fristgebundene Löschgebote.

3.2 Prozessanalyse

Ein zweiter Ansatz, um zu bestimmen, wann Daten nicht mehr erforderlich sind, ist die Prozessanalyse. Die Idee dieses Ansatzes ist, dass die meisten Daten eines Bestandes innerhalb eines regulären Geschäftsprozesses verwendet werden. Ist dieser Regelablauf mit allen seinen Schritten abgeschlossen, sind auch die personenbezogenen Daten nicht mehr erforderlich und können gelöscht werden.[11]

Verschiedene Datenarten werden in unterschiedlichen Geschäftsprozessen für verschiedene Zwecke verwendet. Daher endet auch die Erforderlichkeit ihrer weiteren Verwendung nach verschiedenen Zeiträumen. Diese zu bestimmen ist die zentrale Voraussetzung für die Umsetzung eines Löschkonzepts.

Wann ist der Prozess zu Ende?

Für einfache Geschäftsprozesse lässt sich häufig leicht bestimmen, wann der Geschäftsprozess als abgeschlossen angesehen werden kann. Dazu wird die jeweils maximale Dauer der einzelnen Prozessschritte festgestellt. Beispielsweise können die monatliche Fakturierung, Postlaufzeiten bis zu einem fingierten Zugang und eine Reklamationsfrist für Einzelverbindungsnachweise (Telekommunikation) oder Einzelfahrtennachweise (Autobahnmaut) relevante Zeiträume zur Bestimmung einer konkreten Löschfrist liefern. Die Summe der Teilfristen ergibt die Gesamtdauer des Regelprozesses: die Regellöschfrist. Als Beispiel sei hier die Fristanalyse für die Fahrtdaten nach BFStrMG angeführt: Aus der Prozessanalyse ergibt sich eine Regellöschfrist von 120 Tagen für Fahrtdaten, die nicht reklamiert wurden.[12]

Allerdings besteht auch in solchen Fällen oft Unsicherheit darüber, ob noch Sonderfälle eintreten können, für die einzelne Daten doch noch benötigt werden könnten. Wenn dies wenige Fälle sind, bietet es sich an, die entsprechenden Datenbestände zu kennzeichnen, und nur für die gekennzeichneten Bestände die Löschung auszusetzen. Ist die Zahl der Sonderfälle vergleichsweise hoch, kann geprüft werden, ob es verhältnismäßig ist, den Gesamtbestand länger zu speichern und die Regelfrist zu verlängern. So bestimmte Regellöschfristen sind maßgeschneiderte Fristen für die entsprechenden Datenbestände.

8 Für weitere Details zum Löschkonzept von Toll Collect siehe Fraenkel/Hammer 2007 und Hammer/Fraenkel DuD 2007

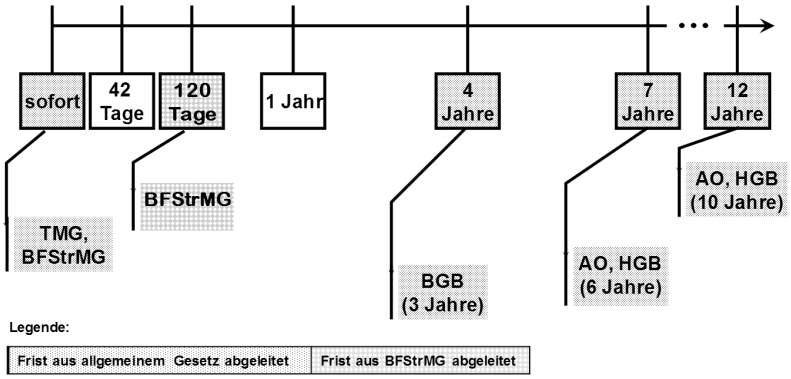
9 Für Nutzungsdaten nach dem Ende der Nutzung.

10 Für Kontrolldaten, sobald feststeht, dass es sich um ein nicht-mautpflichtiges Fahrzeuge handelt.

11 Je nach Datenart und Geschäftsprozess kann am Ende die Erfüllung von Aufbewahrungspflichten stehen.

12 Vgl. auch die Hinweise zur Prozessanalyse in *Hammer/Fraenkel, DuD 2007.*

Abbildung 1 | Standardfristen im Löschkonzept von Toll Collect



Dynamik: Prozessanalyse oder Löschen?

Für viele Datenbestände gilt heute allerdings, dass sie von mehreren – ggf. miteinander verzahnten – Geschäftsprozessen, verwendet werden. Und: Die heute üblichen Geschäftsprozesse sind oft so komplex oder dynamisch, dass das Wissen um die Verwendungsregeln auf viele Köpfe verteilt ist. Dann wissen zwar viele Einiges, aber der Überblick über die Prozesse und Zusammenhänge ist nur schwer zu erlangen. Oft unterliegen die Prozesse auch einer so starken Dynamik, dass das scheinbare Ende einer Analyse dann nur der Anfang der nächsten ist.

Diese Randbedingungen wären wenig problematisch, wenn die Analyse auf einfache Weise delegiert werden könnte. Da es aber um die Ausfüllung des Tatbestandsmerkmals der Erforderlichkeit geht, also um die Konkretion des § 35 Abs. 2 Nr. 3 BDSG oder vergleichbarer bereichsspezifischer Regelungen, kann die Analyse in sinnvoller Weise nur in enger Kooperation mit dem bDSB durchgeführt werden. Dieser muss das datenschutzrechtliche Fachwissen entweder persönlich einbringen oder dafür sorgen, dass dies durch Dritte beigesteuert wird. Damit wird die Prozess-Analyse für den bDSB aufwändig und bindet viele personelle Ressourcen.

Gleichzeitig soll der bDSB aber sein Tagesgeschäft erledigen, also u. a. auditieren, schulen, Verfahren in ihrer Entwicklung begleiten oder dem Leiter der verantwortlichen Stelle Bericht erstatten. Ressourcen-Probleme sind vorprogrammiert. Für den bDSB ergibt sich damit ein Dilemma: Er kann entweder mit hohem Aufwand die Analyse von Geschäftsprozessen vorantreiben, , kommt dann aber nicht zur Umsetzung des Löschkonzepts oder er versucht, Löschregeln zu etablieren, scheitert dann aber in Diskussionen mit den Fachabteilungen daran, dass nicht oder nur vage bestimmt ist, wie lange die Daten tatsächlich benötigt werden.

Das Erstellen eines Löschkonzepts und seine Umsetzung können also schon daran scheitern, dass es aufwändig und schwierig ist, differenzierte Löschregeln für die verschiedenen Arten personenbezogener Daten festzulegen. So sinnvoll die Prozessanalyse nicht zuletzt auch für das Verständnis der eigenen Prozesse ist, so sehr trägt sie wegen ihrer Komplexität auch den Kern des Scheiterns in sich. Sie taugt insofern nicht als allgemeines Instrument zur Konkretisierung des Tatbestandsmerkmals „nicht mehr erforderlich". Wenn aber die Komplexität der Prozessanalyse sich als eines ihrer Kernprobleme herausstellt, stellt sich die Frage, ob und wie im Unternehmen einfache Löschregeln möglichst ohne detaillierte Prozessanalyse festgelegt werden können.

Einen erfolgreichen Ansatz zur Lösung dieses Problems konnten die Autoren bei Toll Collect entwickeln. Dabei kann davon ausgegangen werden, dass die Vorgehensweise mit geringem Aufwand auf andere Organisationen bzw. Unternehmen übertragbar ist.

3.3 Standardfristen

Nach den oben beschriebenen Erfahrungen war es das zentrale Ziel, die Bildung von Löschregeln soweit wie möglich zu vereinfachen. Da eine differenzierte Prozessanalyse für die meisten Datenarten ausschied, nahm das Datenschutz-Team einen Perspektivenwechsel vor: Zunächst wurde nach einheitlichen Löschfristen gesucht. In einem zweiten Schritt sollten die verschiedenen Datenarten diesen Löschfristen zugeordnet werden.

Für Toll Collect konnten sieben Standardfristen identifiziert werden (vgl. Abb. 1), für deren Wahl die folgenden Vorgaben und Überlegungen ausschlaggebend waren. Vier der Fristen begründen sich aus unmittelbaren Rechtspflichten:

- **Sofort:** Diese Frist ergibt sich aus Regelungen des § 9 Abs. 5 BFStrMG für nicht-mautpflichtige Fahrzeuge und aus den §§ 13 Abs. 4 Nr. 2 1. Alt., 15 Abs. 4 TMG für die angefallen Daten über den Zugriff oder sonstige Nutzung von Telemediendiensten.
- **120 Tage:** In der Regelverarbeitung endet die Erforderlichkeit der Speicherung fahrtbezogener Daten und für Kontrolldaten nach 120 Tagen.[13]
- **7 Jahre:** Nach § 257 Abs. 1 Nr. 2 und 3 i.V.m. Abs. 4 HGB und § 147 Abs. 1 Nr. 2 i.V.m. Abs. 3 und 4 AO sind Handelsbriefe sechs Jahre aufzubewahren. Die Frist beginnt am Ende des Kalenderjahres, in dem der Handelsbrief abgesandt oder empfangen wurde. Um das Entstehungsjahr auf einfache Weise abzudecken, wird die gesetzliche Vorgabe um ein Jahr verlängert.
- **12 Jahre:** Buchhaltungsunterlagen, wie buchungsbegründende Unterlagen oder Handelsbücher, sind nach § 257 Abs. 1 Nr. 4 i.V.m. Abs. 4 HGB und § 147 Abs. 1 Nr. 4 AO für zehn Jahre aufzubewahren. Die Frist beginnt mit dem Entstehen des Belegs oder der letzten Eintragung in ein Buch. Aus diesem Grund wurde die Regellöschfrist gegenüber der Aufbewahrungsvorgabe um ein Jahr verlängert – wie für Handelsbriefe. Da das Geschäftsjahr bei Toll Collect allerdings am 31. August endet, müssen auch Buchungen aus dem Vorjahr berücksichtigt werden. Daher wurde die Regellöschfrist um ein weiteres Jahr verlängert und auf 12 Jahre festgelegt.[14]

Die vorgenannten Fristen sind unmittelbar aus gesetzlichen Vorgaben abgeleitet. Die Abstände zwischen „sofort" und 120 Tagen und von da wiederum zu 7 Jahren sind allerdings so groß, dass eine Unterteilung notwendig ist. Denn es erscheint

13 Vgl. auch die Hinweise zur Prozessanalyse oben.

14 Die Löschung muss allerdings für das jeweilige Jahr freigegeben werden, weil nach AO außerdem die Festsetzungsfrist für die Steuer des entsprechenden Jahres abgelaufen sein muss. Für diese können verschiedene Verzögerungen oder Unterbrechungen eintreten, die nicht sinnvoll in einer automatischen Regelfrist abgebildet werden können.

bsp. kaum vertretbar, dass alle personenbezogenen Daten, die länger als 120 Tage benötigt werden, gleich mindestens sieben Jahre vorgehalten werden. Aus dem datenschutzrechtlichen Prinzip der Erforderlichkeit in Verbindung den fachlichen Anforderungen war es sinnvoll, drei weitere Fristen einzuführen:

- **42 Tage:** In einigen Systemen werden sensitive Daten erhoben oder verwendet, die ein Mal monatlich ausgewertet werden. Dies ist beispielsweise ist für die Protokolle von Viren-Scannern, Intrusion-Detection-Systemen oder internen Firewalls der Fall. Alle Daten ohne Befund können nach der Auswertung gelöscht werden. Da die Auswertung monatlich erfolgt, bietet eine Standardfrist von 42 Tagen (sechs Wochen) einen Spielraum von zwei Wochen, um die Auswertung durchzuführen.
- **1 Jahr:** Viele Vorgänge sollen länger als 120 Tage nachvollziehbar sein, eine Vorhaltefrist der Daten und Dokumente für ein Jahr erscheint jedoch ausreichend. Soweit das Unternehmen keine Aufbewahrungspflichten treffen, können die Daten dann gelöscht werden.
- **4 Jahre:** Andere Vorgänge können Einfluss auf die Entscheidung in Reklamationen haben oder als Hintergrundmaterial zur Begründung von offenen Forderungen dienen. Die Verjährungsfrist für Forderungen beträgt nach § 195 i drei Jahre. Fristbeginn ist gemäß § 199 BGB am Schluss des Jahres, in dem der Anspruch entstand. Entsprechend der Vorgehensweise für Handelsbriefe und Buchhaltungsdaten wird daher eine Regellöschfrist von 4 Jahren festgelegt.

Standardfristen, Sonderfälle und Spielräume

Damit ergeben sich die sieben Fristen, die in der Abbildung 1 aufgeführt sind. Diese Standardfristen bilden den Rahmen, in den alle Datenarten von Toll Collect eingeordnet werden. Bereits an dieser Stelle sei darauf hingewiesen, dass nur eine der Fristen aus einer Rechtsvorschrift abgeleitet wurde, die spezifisch für das Mautsystem gilt und nur diese Frist aus dem Ergebnis der Prozessanalyse übernommen wurde. Alle anderen Fristen ergeben sich aus allgemein gültigen rechtlichen Regelungen denen alle Unternehmen unterworfen sind oder aus praktischen Erwägungen. Aber auch die spezifische Frist für Toll Collect von 120 Tagen muss nicht ausschließlich für Mautdaten verwendet werden. Sie kann auch für die Löschung anderer Datenarten herangezogen werden.

Abbildung 2 | Grundstruktur der 12 Löschklassen der Toll Collect GmbH*

	Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Ab Entstehung			Mautdaten	Mautdaten mit bes. Analysebedarf			
Ab Ende Vorgang	nmF, Web-Logs	Kurzzeit-Doku., Betriebs-Logs	voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Rekla- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
Ab Ende De-Reg.				ergänzende Stammdaten		Verträge (> 7 Jahre, >=1 Jahr nach De-Reg.)	Kernstammdaten.

Legende: Frist aus allgemeinem Gesetz abgeleitet | Frist aus BFStrMG abgeleitet

* Ohne Mitarbeiterdaten

Die Anwendung von gegebenenfalls großzügigen Standardfristen geht von der Überlegung aus, dass eine weitergehende Differenzierung für die Praxis nicht zielführend ist. Die Ausdifferenzierung von Untergruppen einzelner Datenarten, um „genauer" zu löschen, scheitert an der Prozesskomplexität. Auch die dynamische Veränderung von Geschäftsprozessen lässt eine feinere Granularität der Löschfristen unsinnig erscheinen. Und schließlich können nur einfache Regeln im Unternehmen kommuniziert werden und so Teil der Unternehmenskultur werden. Nur dadurch können die Fachabteilungen konstruktiv an der Umsetzung der Löschregeln mitwirken. Komplexe Regeln dagegen erfordern zusätzliches Spezialistentum, führen zu langen Abstimmungsprozessen und Entscheidungswegen und können so die Löschung personenbezogener Daten erschweren oder ganz verhindern.

Daher erscheint es zweckmäßig, im Einzelfall die Spielräume des Datenschutzrechts, die sich gerade im nicht-öffentlichen Bereich ergeben, zu nutzen und eine Regellöschfrist großzügig anzusetzen. Der datenschutzrechtliche Gewinn - eine Abdeckung aller relevanten Daten mit Löschregeln - sollte dies in aller Regel rechtfertigen. Nur für besonders sensitive Datenbestände sollte gesondert geprüft werden, ob eine spezifische Löschfrist festzulegen ist.

4 Anwendung der Standardfristen

Eine Frist alleine bildet noch keine Löschregel. Es muss auch festgelegt werden, ab welchem Zeitpunkt der Fristlauf beginnt. Mit Hilfe dieser beiden Parameter können Löschklassen gebildet werden, in die dann die verschieden Datenarten eingeordnet werden.

4.1 Startzeitpunkte

Für die Vorgehensweise bei Toll Collect bewährte es sich, zwischen drei Typen von Starzeitpunkten zu unterscheiden:

- **Ab Entstehung:** Der Fristlauf beginnt, sobald die Daten erhoben wurden. Dies ist beispielsweise für die Fahrtdaten der Fall, soweit sie nicht in Abrechnungssystemen verwendet werden.
- **Ab dem Ende eines Vorgangs:** In vielen Fällen muss ein Vorgang beendet sein, damit der Lauf der Regellöschfrist beginnen kann. So ist es beispielsweise sinnvoll, Anfragen von Kunden, die keiner Dokumentationspflicht unterliegen, noch ein Jahr vorzuhalten, nachdem sie beantwortet wurden. Welcher Vorgang abgeschlossen sein muss und durch welche Bedingung dieser Tatbestand geprüft wird, hängt von der jeweiligen Datenart ab. Der Startzeitpunkt „Ende des Vorgangs" verdeutlicht aber für alle Beteiligten - Fachabteilung, Entwickler, Administratoren und Datenschutz-Team -, dass diese Bedingung identifiziert und operationalisiert werden muss.

- **Ab dem Ende der De-Registrierung:** Die De-Registrierung eines Lkws oder eines Benutzers des Mautsystems[15] löst besondere Vorgänge aus und beeinflusst die Vertragsbeziehung zwischen Toll Collect und dem Benutzer. Sie ist abgeschlossen, wenn sämtliche Forderungen zum entsprechenden Objekt ausgeglichen sind. Wegen dieser Besonderheiten wurde das Ende der De-Registrierung als spezifischer Startzeitpunkt eingeführt.

Mit den Bausteinen der Standardfristen und der Startzeitpunkte können nun Löschklassen gebildet werden.

4.2 12 Löschklassen bei Toll Collect

Einer Löschklasse werden alle Datenarten zugeordnet, die der gleichen Löschfrist und dem gleichen Typ von Startzeitpunkt unterliegen. Durch die Zuordnung der Datenarten zu den Löschklassen kann auch leicht festgestellt werden, ob Datenarten mit vergleichbaren Zwecken hinsichtlich der Löschung gleich behandelt werden. Dadurch werden einerseits die Löschregeln konsistenter, andererseits fällt die Zuordnung von Datenarten leicht.

Sieben Standardfristen kombiniert mit drei Typen von Startzeitpunkten ergeben 21 Löschklassen – davon werden bei Toll Collect allerdings nur 12 benötigt. Diese sind in der Abb. 2 dargestellt.

Handlungsfähigkeit im Löschkonzept

Die Löschklassen erlauben es, vergleichbar der modernen Mülltrennung vorzugehen: Gefragt ist nicht mehr eine differenzierte Analyse von Prozessen, Datenflüssen und Abhängigkeiten – die Zuordnung von Datenarten zu Löschklassen ist ausreichend. Der Klassifikationsprozess mit den Fachanwendern gelingt um ein vielfaches schneller als eine differenzierte Prozessanalyse. Die geänderte Vorgehensweise stellt die Handlungsfähigkeit des bDSB in Sachen Datenlöschung wieder her.

Systemspezifische Anpassungen

Gleichwohl bedeutet diese Vorgehensweise nicht zwangsläufig, dass alle Daten einer Datenart in allen am Prozess beteiligten Systemen bis zum Ende der Regellöschfrist gespeichert werden müssen. Die Regellöschfrist bildet die Obergrenze für die Datenhaltung im Regelprozess. Wird erkannt, dass die Daten in einem System nur für einen kürzeren Zeitraum benötigt werden, können sie dort auch früher gelöscht werden. Die gesetzlichen Aufbewahrungsfristen des HGB und der AO bedeuten ja nicht, die entsprechenden Daten in all den Systemen entsprechend lange vorzuhalten, sondern nur dort, wo sie tatsächlich so lange benötigt werden.[16]

5 Übertragbarkeit

Wie oben bereits erwähnt, sind sechs der der Standardlöschfristen bzw. zehn der zwölf Löschklassen aus Rechtsregeln und Überlegungen motiviert, die nicht nur für Toll Collect, sondern für alle Unternehmen gelten. Insofern könnten sie als universelle Löschklassen verstanden werden.

Ob eine Frist zwischen 42 Tagen und einem Jahr benötigt wird, hängt von den spezifischen Datenarten des jeweiligen Unternehmens ab. Ergänzungen um weitere Löschklassen scheinen nur dann erforderlich, wenn entweder für die personenbezogenen Daten bereichspezifische Löschvorgaben mit abweichenden Fristen bestehen oder Arten personenbezogener Daten verarbeitet werden, für die eine spezifische Fristanalyse datenschutzrechtlich geboten erscheint. Im einen oder anderen Fall könnte es dann aber auch sinnvoll sein, nicht eine zusätzliche Frist einzuführen, sondern die Standardfristen anzupassen. So könnten sich für Dienstleister im Bereich Telekommunikation beispielsweise sechs Monate für Verkehrsdaten, die für Abrechnungszwecke benötigt werden, ergeben – an Stelle der 120 Tage für die Einzelfahrtennachweise bei Toll Collect.

Für medizinisch tätige Unternehmen könnte dagegen eine zusätzliche Löschklasse mit einer Standardfrist von 30 Jahren notwendig sein, die sich aus Dokumentationspflichten für medizinische Unterlagen ergibt.

Dies aber sind Einzelfragen, die sich je nach der besonderen Eigenart eines Unternehmens stellen können und ggf. durch Anpassung der hier vorgestellten Struktur von Löschklassen gelöst werden könnten.

Fazit

Mit Hilfe von Prozessanalysen und Standardfristen, ist es möglich, Löschklassen für eine Organisation zu bestimmen. Dabei kann die differenzierte Prozessanalyse auf Bereiche beschränkt werden, in denen spezielle gesetzliche Vorgaben zu erfüllen sind oder besonders sensitive personenbezogene Daten verwendet werden. Löschklassen wiederum bieten dem bDSB die Möglichkeit, in effizienter Weise mit den Fachanwendern die Löschregeln für verschiedene Datenarten festzulegen.

Die hier vorgestellten methodischen Ansätze sind geeignet, in angemessener Weise das Tatbestandsmerkmal „nicht mehr erforderlich“ so zu konkretisieren, dass es hinsichtlich des Löschgebots des § 35 Abs. 2 Nr. 3 BDSG in der Praxis technisch und betrieblich umgesetzt werden kann.

Literatur

Bergmann, Möhrle, Herb (2009): Datenschutzrecht, 40. Ergänzungslieferung 2009

BFStrMG (2011): Gesetz über die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen und Bundesstraßen, BGBl. I S. 1378. Das BFStrMG löst das Autobahnmautgesetz (ABMG) ab.

Conrad, I. / Hansen, D. (2011): Datenschutzgerechte Löschung personenbezogener Daten, ITRB 2011, S.35ff.

Manssen, G. (1995): Staatsrecht I – Grundrechtsdogmatik. München, 1995

Fraenkel, R. / Hammer, V. (2007): Rechtliche Löschvorschriften, DuD 12/2007, 899 ff.

Hammer, V. / Fraenkel, R. (2007): Löschkonzept, DuD 12/2007, 905 ff.

15 Die Mautschuldner nach § 2 BFStrMG werden hier als Benutzer des Mautsystems bezeichnet. Dies sind der Halter des Fahrzeugs oder Personen, die über seinen Gebrauch bestimmen z. B. die Fahrer ggf. auch die Mieter. In der Regel ist der registrierte Benutzer der Halter des Lkw.

16 Dort sind solche Daten gemäß § 35 Abs. 3 Nr. 1 nach einer geeigneten Frist zu sperren.