Reinhard Fraenkel / Volker Hammer

Erfahrungen bei der Umsetzung eines Löschkonzeptes

1 Einleitung

Die Toll Collect GmbH ist die Betreiberin des Mautsystems in Deutschland. Da es hinsichtlich der im Rahmen der Mauterhebung anfallenden Fahrt- und Kontrolldaten klare Löschgebote im Bundesfernstraßenmautgesetz (BFStrMG) gibt, waren die sich aus dem BFStrMG ergebenden Löschfristen schon seit 2005, dem Zeitpunkt des Mautstarts, erfolgreich umgesetzt. Das Löschen personenbezogener Daten war damit von Anfang an Teil der Kultur des Unternehmens.

Für andere Arten personenbezogener Daten gelten die Löschgebote des § 35 Abs. 2 Nr. 3 BDSG. Konsequenter Weise wurde das Löschkonzept daher weiterentwickelt. Jetzt sind Löschregeln auch für die anderen im normalen Geschäftsablauf der Toll Collect GmbH anfallenden Arten personenbezogener Daten festgelegt. Die zugehörigen Löschmaßnahmen wurden inzwischen für die datenhaltenden Systeme umgesetzt.

In diesem Beitrag berichten wir über Erfahrungen aus dem Umsetzungsprojekt.

2 Erforderlichkeit und Löschen

Das BDSG fordert die Löschung personenbezogener Daten, wenn die weitere Speicherung der Daten für ein Unternehmen nicht mehr erforderlich ist. Leider lässt der Gesetzgeber die wenigen Rechtsanwender, die diese Vorschrift ernst nehmen, weitgehend allein, wenn es darum geht, die Norm des § 35 Abs. 2 BDSG mit Leben zu füllen. Es wäre beispielsweise schon viel gewonnen, wenn das BDSG hinsichtlich der Löschfristen das insbesondere für die Privatwirtschaft wenig taugliche Kriterium der Erforderlichkeit mit etwas mehr Kontur füllen könnte. Leider ist es in der Regel bereichsspezifischen Datenschutzregelungen vorbehalten, Löschgebote so zu konkretisieren, dass sie auch für den Rechtsanwender umsetzbar und überprüfbar werden.

Die Unbestimmheit der Norm darf aber nicht dazu führen, sie erst gar nicht zu beachten. Das Löschgebot reflektiert nämlich in besonderer Weise das informationelle Selbstbestimmungsrecht und den Grundsatz des Verbotsgesetzes mit Erlaubnisvorbehalt. Einmal rechtmäßig erhobene personenbezogene Daten müssen gelöscht werden, wenn die weitere Speicherung der Daten für die verantwortliche Stelle nicht mehr erforderlich ist. Diesen Zeitpunkt zu bestimmen ist damit die Aufgabe der verantwortlichen Stelle.

3 Voraussetzungen für die Umsetzung

Voraussetzung für die Implementierung von Löschregeln ist, dass diese Regeln vor Beginn des Umsetzungsprojekts definiert sind. Die Fristbestimmung für die Löschung der verschiedenen Arten personenbezogener Daten, die im Geschäftablauf der Toll Collect GmbH anfallen, wurde durch das Datenschutzteam angestoßen. In Abstimmung mit den Fachbereichen des Unternehmens und unter Beachtung der Gesetze, die spezielle Aufbewahrungspflichten auch für personenbezogenen Daten vorschreiben, wie beispielsweise dem HGB oder der AO, wurden die erforderlichen Speicherfristen der Datenarten bestimmt und dementsprechend die Löschregeln festgelegt.[1] Im Falle der Toll Collect werden die Löschregeln im Dokument „Regellöschfristen“ zusammengefasst.

Durch die Festlegung von Löschregeln für Datenarten wird von konkreten IT Systemen abstrahiert. Damit gelten einheitliche Fristen für alle Bestände einer Datenart. Um die Löschregeln für die einzelnen Datenarten festzulegen, wurde ein System von Löschklassen entwickelt.[2] Dadurch kann leicht verglichen werden, ob Datenarten mit ähnlichen Zwecken auch gleich behandelt werden. Außerdem wird die Zuweisung der Löschregeln viel effizienter – ein wichtiger Erfolgsfaktor für das Löschkonzept. Durch einen umfangreichen Review-Prozess und über Workshops mit den Fachbereichen, die Daten verwenden, wurden die Löschregeln abgestimmt.

Am Ende des Prozesses stand ein von der Geschäftsführung freigegebenes Dokument „Regellöschfristen“ mit unternehmensweiter Gültigkeit. Zugleich wurde die datenschutzkonforme Löschung personenbezogener Daten in den Katalog der Unternehmensziele aufgenommen. Die Toll Collect GmbH hat damit § 35 Abs. 2 Nr. 3 BDSG erfolgreich mit Leben gefüllt. Vermutlich sind einige der Löschregeln auf andere Unternehmen übertragbar, weil viele der betrachteten Datenbestände, wie Kundenstammdaten oder Buchhaltungsdaten, auch in jedem anderen Unternehmen anfallen.

Mit der Freigabe einher ging der Beschluss der Geschäftsführung, ein Projekt zur Umsetzung der Regellöschfristen aufzusetzen. Projektanforderer war der betriebliche Datenschutzbeauftragte. Die Projektverantwortung lag beim Fachbereichsleiter Betrieb zentrale Systeme. Er ist nach den Regelungen der Toll Collect der Datenverantwortliche für die meisten Systeme und damit auch für die Umsetzung und die betriebliche Überwachung von Löschmaßnahmen verantwortlich. Er etablierte seinerseits ein kleines Projektteam, das die Anforderungen des Dokumentes „Regellöschfristen“ in für die Entwicklung der Löschprozeduren taugliche Pflichtenhefte transformierte und die weiteren Projektarbeiten koordinierte.

4 Motivation zum Löschen

Auf die gute Ausgangsbasis für das neue Löschprojekt wurde unter 1. schon hingewiesen. Die Löschung der sensiblen Maut- und Kontrolldaten im deutschen Mautsystem war schon zu Beginn des produktiven Betriebs des Mautsystems erfolgreich in die Unternehmensprozesse integriert worden. Durch die so gewachsene Löschkultur war die Notwendigkeit der Löschung personenbezogener Daten sowohl der Geschäftsführung als auch den Fachbereichen klar. Das erleichterte die Definition der Regellöschfristen wie auch der Pflichtenhefte. Lästige Grundsatzdiskussionen mussten nicht mehr geführt werden. Vielleicht bietet es sich auch für andere Unternehmen an, die Umsetzung eines Löschkonzepts mit einem „Leit-Datenbestand“ zu beginnen. Selbstverständlich war auch der Beschluss der Geschäftsführung für Umsetzung eine zentrale Voraussetzung der weitgehend reibungslosen Umsetzung.

Der Erfolg eines solchen Projektes hängt, das ist eine gewonnene Erkenntnis, ganz wesentlich an der Person des Projektleiters. Er muss teamfähig sein und offen für Argumente. Er muss unterschiedliche Standpunkte verstehen und, wo es notwendig ist, Kompromisse finden und sie den betroffenen Stakeholdern vermitteln. Er muss, um es auf einen Nenner zu bringen, den Erfolg wollen und von der Sinnhaftigkeit der Datenlöschungen überzeugt sein. Das alles ist keine Selbstverständlichkeit. All diese Vorraussetzungen waren in der Person des konkreten Projektleiters erfüllt. Da er im Bereich des Systembetriebs tätig ist, motivierten ihn – ganz unabhängig von einer datenschutzgerechten Löschung – zusätzlich die betrieblichen Vorteile einer durchgängigen Löschung der Daten. Nach der Produktivsetzung der Löschmechanismen würden in einzelnen Systemen bis ca. 30% der Datenvolumina gelöscht sein. Das würde zu einem stabileren Systembetrieb und zu verbesserter Performance der Systeme führen. Auch mit betriebwirtschaftlichen Vorteilen konnte gerechnet werden. Diese Erwartungen erwiesen sich neben der Tatsache, dass die Umsetzung des Löschkonzepts zu einem der Unternehmensziele erklärt worden war, als ein großer Motivationsschub für die Umsetzung. Sie halfen dann auch über gelegentlich aufflammende Diskussionen über das Löschen an sich oder über einzelne Löschfristen mit den anwendenden Fachbereichen hinweg.

Diese Diskussionen hatten gelegentlich, jedenfalls für das Datenschutzteam auch erheiternde Momente. Ein Beispiel sind die Diskussionen mit dem Data-Warehouse-Team. Das Team hatte Anonymisierungsstrategien für ein Data-Warehouse-System (DWS) erarbeitet. Gäbe es nur das Data Warehouse, wären diese Strategien auch ausreichend gewesen. Aber dies wäre eine verkürzte Sicht der Dinge gewesen, denn selbstverständlich hängt die Beurteilung der Frage einer hinreichenden Anonymisierung wesentlich auch von der Systemlandschaft ab, in die das DWS eingebettet ist. Da wo unternehmensweit Zusatzwissen in anderen Systemen gespeichert ist, das eine Deanonymisierung ermöglicht, müssen höhere Anforderungen an den Grad der Anonymisierung gestellt werden. Dementsprechend mussten die Anonymisierungsstrategien im DWS weiter geschärft werden. Das Datenschutz-Team beteiligte sich aktiv an diesem Prozess und konnte in der gemeinsamen Diskussion schnell die relevanten Attribute identifizieren.

Dieses Beispiel steht stellvertretend für andere ähnlich gelagerte Diskussionen. Sie sind immer der Mühe wert, denn so werden die Ansätze des Datenschutzes argumentativ in die Breite des Unternehmens getragen. Das Datenschutz-Team wird so im Unternehmen als Anreger und als Gestalter statt als Verhinderer wahrgenommen.

5 Technische Umsetzung

Ein Löschkonzept kann gut ausgearbeitet sein, es steht aber zunächst nur auf dem Papier. Durch das Konzept alleine wird kein Datensatz und keine Tabelle in einer Datenbank gelöscht. Für die Systeme müssen Löschmaßnahmen entwickelt und vor allem getestet werden.

Die Löschroutinen mussten in eine bestehende Systemlandschaft integriert werden. Insofern war die Situation der Toll Collect GmbH sicherlich vergleichbar mit der Situation vieler anderer Unternehmen. IT-Landschaften entwickeln im Laufe der Zeit eine hohe Komplexität. In den gewachsenen Strukturen gibt es immer auch Brüche oder unerwartete Abhängigkeiten zwischen Datenbeständen. Solche Abhängigkeiten können bei der Löschung von Daten zu Fehlfunktionen für einzelne Prozesse führen. Daher mussten im Umsetzungsprojekt des Löschkonzepts vom Projektteam

- einerseits die Datenarten in den Beständen der einzelnen Systeme identifiziert werden, um die Löschregeln zuweisen zu können und
- andererseits die Abhängigkeiten der Systeme untereinander genau überprüft werden und für die relevanten Datenarten jeweils ein führendes System bestimmt werden.

Beispielsweise müssen bestimmte Daten nach einiger Zeit nur noch auf Grund handels- oder steuerrechtlicher Vorschriften aufbewahrt werden. Da die Daten aber in unterschiedlichen Systemen verwendet werden, musste entschieden werden, ob es nicht genügt, die Daten dann nur noch in einem System vorzuhalten – mit der Konsequenz, dass sie in den anderen Systemen gelöscht werden können. Die Frage kann zunächst theoretisch entschieden werden, bedarf aber in jedem Fall der gründlichen praktischen Überprüfung, um unbeabsichtigte Nebeneffekte auszuschließen.

Aber auch aus anderen Gründen sollte im Rahmen der Umsetzung des Löschkonzepts die gesamte Systemlandschaft noch einmal intensiv analysiert werden. Denn auch bei einer sehr gut gepflegten, alle Changeprozesse berücksichtigenden Systemdokumentation kann es Lücken geben. Verdeckte Abhängigkeiten der Prozesse untereinander können sich im Laufe der Jahre eingeschlichen haben. Es können auch bisher unbemerkt gebliebene Datenschiefstände zwischen verschiedenen Systemen bestehen. Erkannt werden können diese Probleme, soweit sie nicht schon bekannt sind, vor allem in der Phase des Testens. Der Phase kommt daher im Rahmen eines solchen Entwicklungsprojekts sehr große Bedeutung zu. Die finale Löschung der Daten ist irreversibel. Daher muss durch die Analyse der Systemlandschaft und der Einzelsysteme sowie durch das Testen sichergestellt werden, dass durch

die Produktivsetzung der Löschroutinen die normalen Arbeitsabläufe nicht gestört werden. Die vertiefte Analyse und die intensive Phase des Testens waren Teile des Projekts bei der Toll Collect GmbH. Die dabei identifizierten Probleme konnten sowohl technisch wie datenschutzrechtlich vertretbar gelöst werden.

Spätestens an diesem Punkt bekommen viel früher getroffene Grundsatzentscheidungen hinsichtlich der eingesetzten IT-Systeme noch einmal unerwartete Relevanz. Aus der Sicht des Löschprojekts bestehen nämlich die folgenden Kernanforderungen an IT-Systeme:

- Unterstützung differenzierter Löschung im Datenbestand: Löschregeln für verschiedene Datenarten enthalten unterschiedliche Fristen. Enthält der Datenbestand eines Systems unterschiedliche Datenarten – was in der Regel der Fall ist – müssen differenzierte Löschregeln zur Anwendung kommen.
- Archivieren und Sperren: Nach Möglichkeit sollen aufbewahrungspflichtige Daten nur in einem System gespeichert werden. Spätestens im Löschprojekt muss daher entschieden werden, in welchem System aufbewahrungspflichtige Daten vorgehalten werden. Diese Daten sollen dann aber im Sinne des BDSG für die normalen Anwender gesperrt sein. Das Vorhalten der aufbewahrungspflichtigen Daten soll die produktiven Systeme möglichst wenig belasten – es ist sinnvoll, sie zu archivieren (im Sinne von auszulagern).
- Wechselwirkungen mit gelöschten Daten von führenden Systemen ausschließen: Die Systeme, in denen die Daten vor dem Ende der Aufbewahrungspflicht gelöscht werden, sollen mit den verbleibenden Daten korrekt weiterarbeiten.
- Löschmöglichkeit in Archiven: Schließlich muss auch die Löschung von archivierten Daten möglich sein.

Nicht jede der Kernanforderungen ist für jedes System relevant. Aber die Systemlandschaft insgesamt mit ihren Wechselwirkungen zwischen den Systemen muss die Anforderungen abdecken. Nur dann, wenn die relevanten Systeme über geeignete Implementierungen der Anforderungen verfügen, kann unabhängig von den eingesetzten Ausgangsprodukten entschieden werden, ob die Archivierung der Daten beispielsweise im CRM-System erfolgen soll oder im Buchhaltungssystem. Werden in einem der üblichen Kandidaten für die Archivierung, beispielsweise CRM, DMS oder Buchhaltungssystem Anforderungen nicht abgedeckt, wird der Lösungsraum des Löschprojekts eingeschränkt.

Wenn in einem System die notwendigen Funktionen zunächst gar nicht vorgesehen sind, wie dies beispielweise für Archivierung/Sperrung bei PeopleSoft-basierter CRM-Software der Fall ist, scheidet dieses System für die Archivierung in aller Regel aus. Denn schon das in diesem Fall erforderliche individuelle Customizing des Produkts würde die Kosten der Umsetzung eines Löschkonzepts erheblich in die Höhe treiben.

Noch prekärer wird die Situation natürlich dann, wenn Systeme in ihrer Ursprungskonfiguration überhaupt keine Löschfunktionalitäten vorsehen, wie dies beispielsweise lange im SAP R/3 HR der Fall war.[3] Für diesen Umstand wurde seitens SAP zunächst im Wesentlichen technische Gründe ins Feld geführt, aber auch die Auffassung der Industrie, Datenschutz dürfe kein Geld kosten. Inzwischen besteht im SAP eine deutlich besserer Ausgangssituation. Beispielsweise werden bei Toll Collect in den Modulen BWS, FI, CO und PA personenbezogene Daten mit Hilfe der Archivierungsfunktionen ausgelagert und gesperrt. Die Löschung erfolgt dann für archivierte Daten. Diese Funktionskette wird auch zum Löschen von Daten mit kurzen Fristen genutzt: Die Speicherdauer der Archivdateien ist dann auf wenige Tage reduziert. Um keinen falschen Eindruck zu bezüglich andere Software-Produkte zu erwecken: Auch PeopleSoft beispielsweise ist für durchgängiges Löschen nicht gut vorbereitet und erfordert erhebliche Customizing-Aufwände.

Die oben genannten Kernanforderungen lenken den Blick aber auf die Beschaffungsprozesse von Software. Unabhängig von der gesetzlich gebotenen Vorabkontrolle, die ja nur für bestimmte Anwendungen verpflichtend ist, muss sichergestellt werden, dass bereits im Beschaffungsprozess von Software die datenschutzrechtlichen Anforderungen an IT gestützte Verfahren berücksichtigt werden. Dazu gehört zwingend, dass zu entwickelnde Software oder Standardsoftware über die notwendigen Lösch-, Archivierungs- oder Anonymisierungsfunktionalitäten verfügen und Wechselwirkungen, die Löschen verhindern, ausgeschlossen werden.[4]

6 Lessons learned

Nach Abschluss des Projektes sind in allen dafür vorgesehen Systemen die Löschfunktionalitäten implementiert und produktiv gesetzt, unter anderem im Data-Warehouse, dem CRM-System und in SAP. Im DWS wurden bei Produktivsetzung knapp 30% des Datenbestandes gelöscht, in den SAP-Modulen 25% und im CRM-System ca. 15%.

Mit den jetzt etablierten Löschroutinen werden künftig alle Datenbestände mit Löschfristen länger als einem Jahr jährlich bereinigt, Datenbestände mit kürzeren Löschfristen meist wöchentlich. Die Performance der angepassten IT-Systeme hat sich deutlich verbessert. Zukünftig notwendige Datenmigrationen werden allein wegen der geringeren Menge vorgehaltener Daten und wegen konsistenterer Datenhaltung kostengünstiger. So wird auch der ökonomische Nutzen von Datensparsamkeit transparent.

Der Praxistest für ein übergreifendes Löschkonzept darf als gelungen betrachtet werden. Drei Elemente waren im Projekt Voraussetzung für die erfolgreiche Umsetzung.

1. Verantwortung und Unterstützung der Geschäftsführung:

Ohne einen entsprechenden Rückhalt in der Geschäftsführung ist ein Projekt „Löschkonzept“ nicht möglich. Die Geschäftsführung muss die Löschregeln und das Projektbudget freigeben. Sie muss das Projekt fördern und fordern – wozu sie gesetzlich verpflichtet ist.

2. Vollständigkeit der Regellöschfristen:

Es war sehr hilfreich für den Projektverlauf, dass die Regellöschfristen zum Start des Umsetzungsprojekts weitge-

hend vollständig und im Unternehmen abgestimmt waren. Nur so können die Anforderungsdokumente für die Umsetzung von Anfang an die richtigen Regeln vorgeben. Jede nachträglich identifizierte Datenart und jede angepasste Löschregel erfordert mindestens ein neues Review der geänderten Regellöschfristen durch die betroffenen Fachbereiche. Und erst danach können die Anforderungsdokumente fertiggestellt und freigegeben werden. Dadurch steigt die Projektkomplexität erheblich und die Motivation der Beteiligten sinkt stark.

3. Interaktion zwischen Datenschutz-Team und den weiteren Beteiligten des Unternehmens:

Selbstverständlich kann ein solch übergreifendes Projekt nicht „glatt durchgezogen“ werden. Dazu gibt es einerseits zu viele unterschiedliche Interessen im Unternehmen und andererseits zu viele Überraschungen in den technischen Zusammenhängen. Das Datenschutz-Team kann sich deshalb nicht zurücklehnen, sondern muss das Projekt aktiv begleiten. Es muss motivieren und gemeinsam mit den anderen nach Kompromissen suchen, wenn Lösungsansätze komplex, teuer oder unpraktikabel scheinen. Dafür ist es sehr hilfreich, wenn im Datenschutz-Team juristische und technische Kompetenz vertreten ist. Das Datenschutz-Team sollte sich als Technikgestalter verstehen.

7 Ausblick

Die Erstellung und Umsetzung eines Löschkonzepts ist keine einmalige Aufgabe. Die Weiterentwicklung von Geschäftsprozessen, Änderungen der Rechtsvorschriften und die Veränderungen an IT-Systemen erfordern eine kontinuierliche Fortschreibung. Zukünftige Weiterentwicklungen der IT-Systeme bei Toll Collect müssen die Anforderungen der Regellöschfristen bruchlos unterstützen. Diese Vorgaben für die technische Umsetzung und die Dokumentation der Löschmaßnahmen werden bereits in den Pflichtenheften berücksichtigt.

Mit Interesse verfolgt die Toll Collect GmbH, dass eine verallgemeinerte Beschreibung der Vorgehensweisen in der Standardisierung aufgegriffen wurde.[5] Eine ISO-Norm würde dem Thema sowohl bei Technikern in Entwicklung und Betrieb als auch in anwendenden Fachbereichen erhebliches, zusätzliches Gewicht verleihen. Wenn viele Unternehmen ein entsprechendes Löschkonzept verwenden, sind auch Synergieeffekte zu erwarten: viele Datenarten und Löschfristen sind sicher zwischen Unternehmen einer Branche übertragbar.

Diese allgemeinen Löschregeln liefern auch den Herstellern wertvolle Vorgaben: sie könnten sich nicht mehr darauf zurückziehen, dass keine Anforderungen bestünden. Vielmehr müssten sie endlich Systeme so gestalten, dass sie mit geringem Aufwand datenschutzgerecht eingesetzt werden können. Von den Aufsichtsbehörden sollten solche Entwicklungen durch klare Empfehlungen für datenschutzfreundliche Softwareprodukte unterstützt werden.

1 Zu den näheren Einzelheiten der Regellöschfristen und der Methodik der Fristbestimmungen vgl. Hammer/ Fraenkel, Löschklassen, DuD, 12/2011, S 890 ff, mit weiteren Literaturhinweisen; Hammer, Löschen nach Regeln, in diesem Heft; und ausführlich Hammer, V. / Schuler, K. 2012: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Secorvo, Karlsruhe, 2012; http://www.secorvo.de/publikationen/din-leitlinie-loesch-konzept-hammer-schuler-2012.pdf..

2 Vgl. dazu näher Hammer/ Fraenkel DuD 12/2011.

3 Erst auf Druck der Aufsichtsbehörden hat SAP Löschfunktionalitäten in SAP HR integriert. Vgl. dazu instruktiv: 23. Tätigkeitsbericht des BfDI 2009- 2010 S. 61. Vgl. zur gleichen Problematik auch 36. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (2007) Nr. 5.10.3.2; 38. Tätigkeitsbericht (2009) Nr. 4.8.3; 39. Tätigkeitsbericht (2010) Nr.4.1.5 und 40. Tätigkeitsbericht (2011) Nr. 3.10.3.

4 Die Aufsichtsbehörden könnten das Ihrige dazu tun, wenn nicht nur versteckt in Tätigkeitsberichten Hinweise auf datenschutzfreundliche Tools zu finden wären. Wünschenswert wäre ein Weißbuch, in dem datenschutzfreundliche Softwaresysteme aufgelistet wären. Eine Software, die beispielsweise keine Löschfunktionalitäten vorsieht, dürfte im Geltungsbereich des BDSG nicht vertrieben werden. Die Entwicklung bei SAP HR hat gezeigt, wie von den Aufsichtsbehörden zum Nutzen des Datenschutzes erfolgreich Druck auf Anbieter aufgebaut werden kann.

5 Siehe dazu Hammer, Löschen nach Regeln, in diesem Heft.

Cartoon