DuD
Datenschutz und Datensicherheit

Löschkonzept

Volker Hammer, Reinhard Fraenkel

Personenbezogene Daten müssen gelöscht werden, wenn ihre Erforderlichkeit nicht mehr gegeben ist. In Organisationen mit komplexen Geschäftsprozessen stellt dies eine Herausforderung für die datenschutzgerechte Technikgestaltung dar. Der Beitrag zeigt am Beispiel der Toll Collect GmbH, wie diese Aufgabe mit einem durchgängigen Löschkonzept bewältigt werden kann. Die Effekte außerhalb des Datenschutzes können dabei zu einem echten Return of Investment und positiven Effekten für Geschäftsprozesse führen.

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

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

Einleitung

Gemäß den rechtlichen Vorgaben des § 35 BDSG sind personenbezogene Daten zu löschen, wenn sie nicht mehr erforderlich sind.[1] Damit wird nicht nur dem Grundsatz der Erforderlichkeit, sondern auch dem der Zweckbindung und der Datensparsamkeit Rechnung getragen Die konkrete Umsetzung dieser Vorgaben muss unternehmensspezifisch erfolgen – bei komplexen Geschäftsprozessen oder IT-Anwendungen keine einfache Aufgabe.

Für das deutsche Mautsystem, für dessen Erstellung und Betrieb die Toll Collect GmbH vertraglich verantwortlich ist, war die Erfüllung dieser Aufgabe gegenüber dem Auftraggeber des Mautsystems, dem Bundesamt für Güterverkehr (BAG), nachzuweisen. Der Nachweis war vor der Aufnahme des eigentlichen Mautbetriebs als eine der Voraussetzungen zur Erlangung der Betriebserlaubnis zu erbringen und damit ein kritisches Teilprojekt.

Als erschwerende Rahmenbedingung war zu berücksichtigen, dass – anders als das BDSG – das Autobahnmautgesetzes (ABMG) abstrakt kurze Löschfristen für die spezifischen Bewegungs- und Kontrolldaten, die beim Betrieb des Mautsystems anfallen, festlegt. Daher stand die Toll Collect GmbH vor der Herausforderung, zum Start des Wirkbetriebs produktiv wirksame Löschfunktionen zu implementieren, um den Nachweis eines den Anforderungen des ABMG entsprechenden Datenschutzkonzeptes führen zu können. Für die nach dem ABMG verarbeiteten Daten gab es zu diesem Zeitpunkt allerdings nur die abstrakten Regelungen des ABMG hinsichtlich der Löschpflichten des Betreibers und des BAG. Da die Löschfunktionen vor der Aufnahme des Mautbetriebes implementiert werden mussten, konnte auch hinsichtlich der Geschäfts- und IT-Prozesse nicht auf praktische Erfahrungen zurückgegriffen werden.

Das Projekt stand daher zunächst vor der Aufgabe, eine praktikable Methode für die Erstellung eines unternehmensweiten Löschkonzepts zu entwickeln. Anschließend musste diese Methode so angewandt werden, dass die relevanten Datenbestände des Unternehmens vollständig abgedeckt wurden. Zum Einen waren daher die Löschregeln für Toll Collect festzulegen und zum Anderen für jedes relevante System nachzuweisen, dass Löschfunktionen für den Betrieb auch tatsächlich bereitstehen.

Der Beitrag stellt den methodischen Ansatz vor, beschreibt wichtige Aspekte der Umsetzung und fasst die Erfahrungen aus zweieinhalb Jahren praktischen Einsatzes bei Toll Collect zusammen.

2 Methodischer Ansatz

Ein datenschutzrechtliches Löschkonzept umfasst die organisatorischen und technischen Vorgaben, die eine unternehmensweite Löschung personenbezogener Daten sicherstellen. Für ein effizientes Vorgehen müssen eine strukturierte Vorgehensweise und abgrenzbare Arbeitspakete bestimmt werden. In Anlehnung an die Methode der normativen Anforderungsanalyse[2] können für ein Löschkonzept zwei grundsätzliche Ebenen identifiziert werden:

- Einerseits werden aus den abstrakten rechtlichen Vorgaben die konkreten Löschfristen für die Organisation (hier Toll Collect) abgeleitet.[3] Sie legen die Obergrenzen der Verarbeitungszeiträume der verschiedenen Datenarten fest. Die Ergebnisse der dazu notwendigen Analysen werden in einem Dokument erster Ordnung „**Regellöschfristen**“ festgehalten.
- Andererseits muss für jeden relevanten Datenbestand sichergestellt werden, dass dort Löschfunktionen realisiert sind, die spätestens zum Fristende auch die Löschung durchführen. Da die Löschung

[1] Zu den datenschutzrechtlichen Grundlagen des Löschgebots siehe *Fraenkel / Hammer 2007*.

[2] *Hammer, 1999,* 337 mwN.

[3] Siehe dazu auch *Fraenkel / Hammer 2007.*

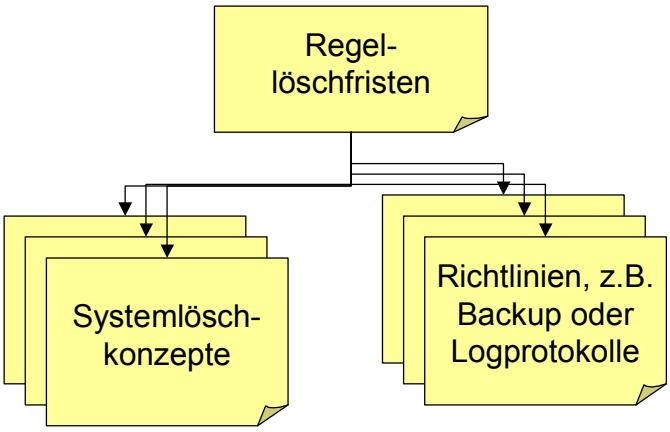

Abb. 1: Dokumentenstruktur des Löschkonzepts

personenbezogener Daten systemspezifisch durchgeführt wird, ist es sinnvoll, für jedes relevante System ein **Systemlöschkonzept** (SLK) zu erarbeiten, ein Dokument zweiter Ordnung, in dem die Vorgaben des Dokuments erster Ordnung systemspezifisch umgesetzt werden.

Voraussetzung zur Bearbeitung der Ebene der Systemlöschkonzepte ist die **Identifikation aller Bestände personenbezogener Daten** in den Systemen des Unternehmens. Für diese Analyse müssen drei Fragestellungen miteinander kombiniert werden:

- Welche unterstützenden Funktionen für die Geschäftsprozesse der Organisation sind auf welchem System implementiert und welche personenbezogenen Daten werden dazu verarbeitet?
- Wie sind die Datenflüsse der personenbezogenen Daten im Gesamtsystem spezifiziert?
- Welche Schnittstellen haben die als relevant erkannten Systeme und wie werden die Daten an diesen Schnittstellen übergeben?

Die Ergebnisse der drei Ansätze werden abgeglichen und zusammengeführt. Systeme, die keine personenbezogenen Daten enthalten, können unbeachtet bleiben.

3 Umsetzung

Im diesem Abschnitt werden die Inhalte der Regellöschfristen, Systemlöschkonzepte und Richtlinien dargestellt.

3.1 Regellöschfristen

Aus den teilweise abstrakten rechtlichen Vorgaben müssen die konkreten Löschfristen abgeleitet werden, die von Toll Collect einzuhalten sind. Diese Löschfristen unterscheiden sich je nach Datenart. Beispielsweise gelten für die im ABMG geregelten fahrtbezogenen Daten und Kontrolldaten andere Löschfristen als für Handelsbriefe, Buchhaltungsdaten oder Stammdaten der Benutzer des Mautsystems. Zweck des Dokuments Regellöschfristen ist es, die verschiedenen Datenarten zu identifizieren und für sie Löschfristen festzulegen.

Je Datenart sind dafür die spezifische Zulässigkeit und die Erforderlichkeit der Verarbeitung festzustellen. Die jeweilige Löschfrist ergibt sich dann aus der Konkretisierung der rechtlichen Randbedingungen unter Berücksichtigung der Geschäftsprozesse bei Toll Collect.[4] Um die jeweils abgeleitete Frist nachvollziehbar zu machen, werden auch die Faktoren und Argumente für die Fristentscheidung für jede Datenart dokumentiert. Das jeweilige Kapitel in den Regellöschfristen gibt in knapper Form Auskunft über:

- Datenquellen,
- Nutzungszwecke,
- Attribute, die typischerweise unter die Datenart fallen,
- Rechtsgrundlage für die Verarbeitung,
- Löschvorgaben und Aufbewahrungspflichten aus rechtlichen Regelungen sowie
- die abgeleitete Löschfrist und den Beginn des Fristlaufs, gegebenenfalls mit erläuternden Hinweisen.

Insbesondere im Bereich der ABMG-Daten waren die Löschfristen an den engen Verarbeitungsvorgaben des Gesetzes zu orientieren und ggf. die Geschäftsprozesse daran auszurichten. Unter anderem waren die bereichsspezifischen Anforderungen, die das ABMG stellt, abzugrenzen gegen andere rechtliche Regelungen, die sich beispielsweise aus dem HGB, der AO, dem subsidiär mitgeltenden BDSG oder dem Betreibervertrag ergeben.

Die Ableitung der Regellöschfrist für die fahrtbezogenen Daten soll hier als Beispiel skizziert werden. Rechtsgrundlage für die Verarbeitung ist § 4 Abs. 2 ABMG, der die relevanten fahrtbezogenen Daten bestimmt. Aus § 9 ABMG und § 10 Lkw-MautV ergibt sich die Löschvorgabe mit Bezug zur Reklamationsfrist. Danach sind die Daten dann zu löschen, wenn ein Mauterstattungsverlangen nicht mehr gestellt werden kann oder das Reklamationsverfahren abgeschlossen ist. Für die Regellöschfrist der fahrtbezogenen Daten muss Toll Collect daher prüfen, wie lange es im ungünstigsten Fall dauert, bis eine Reklamation bei Toll Collect eingegangen ist und die betroffenen Daten geeignet gekennzeichnet wurden. Als Ausgangspunkt wird der Versandtermin der Mautaufstellung an den Halter des Fahrzeugs verwendet. Danach ist die maximale internationale Postlaufzeit zum Halter zu fingieren, die eigentliche Reklamationsfrist von 2 Monaten zu berücksichtigen und die Bearbeitungszeit bei Toll Collect unter ungünstigen Bedingungen anzunehmen. Insgesamt ergibt sich so eine Frist von 120 Tagen. Daten zu Mautaufstellungen, die reklamiert wurden, werden nach dieser Frist je nach Fallkonstellation länger gespeichert, während alle anderen fahrtbezogenen Daten gelöscht werden. Den engen Vorgaben des ABMG wird mit dieser Fristbestimmung Rechnung getragen. Entsprechende Ableitungen sind auch für alle anderen Arten personenbezogener Daten vorzunehmen.

Wir empfehlen, dass die Geschäftsführung des Unternehmens die Regellöschfristen als verbindlich für das Unternehmen freigibt. Dies ist bei Toll Collect geschehen. Soweit gesetzliche Spielräume bestehen, trifft das Unternehmen dadurch eine Selbstbindung, die für alle Geschäftsprozesse gilt.

Die Regellöschfristen sind damit die intern verbindliche Referenzvorgabe für die Löschung personenbezogener Daten. Abweichungen davon sind nur in begrenzten und begründeten Ausnahmefällen (z.B. zur Fehleranalyse oder -behebung oder im Falle eines Releasewechsels) zulässig, soweit der rechtliche Rahmen Spielräume eröffnet.[5]

[4] Hinweise zur Ableitung von Löschfristen gibt *Fraenkel / Hammer 2007,* Abschnitt 3.1.

[5] Wenn der Gesetzgeber harte Fristvorgaben trifft, erscheint es deshalb sinnvoll, die Geschäftsprozesse so zu organisieren, dass die Regellöschfrist kürzer als die gesetzlichen Vorgabe festgelegt wird. Dadurch bestehen dann in

Die Regellöschfristen leiten die Obergrenzen der Löschfristen unternehmensspezifisch für Toll Collect her. Damit ist aber noch nicht gewährleistet, dass diese Fristen in den einzelnen Prozessen auch eingehalten werden. Die Umsetzung der Fristvorgaben wird deshalb über die sogenannten Systemlöschkonzepte und Richtlinien sicher gestellt.

3.2 Systemlöschkonzepte

Welche Löschfristen für ein bestimmtes System gelten, hängt von seiner spezifischen Funktion im Geschäftsprozess ab. Außerdem musste Toll Collect zum Betriebsstart für die relevanten Systeme auch nachweisen, dass die Löschfunktionen realisiert waren.

Aufgabe eines Systemlöschkonzepts (SLK) ist es deshalb, die Löschfristen für die Datenbestände in einem bestimmten System zu konkretisieren und die Löschmechanismen darzustellen. Im Ergebnis kann durchaus eine Löschung in einem speziellen System deutlich vor dem Erreichen der Regelfrist erfolgen, z. B. weil die Daten im betreffenden System nur einer Vorverarbeitung unterliegen und anschließend an andere Systeme weitergereicht werden. Als Nachweis für einen Löschmechanismus ist es ausreichend, wenn die implementierten Funktionen benannt werden und ihre Konfiguration vorgegeben wird. Die Überprüfung, ob die Löschfunktionen auch korrekt arbeiten, ist dagegen Gegenstand von Abnahmetests, fachlichen Prüfungen und Audits.

Die Inhalte eines SLK müssen in sich geschlossen verständlich sein, so dass ein Außenstehender, bspw. die Aufsichtsbehörde oder das BAG, die Löschmaßnahme bewerten kann. Ein SLK enthält daher die folgenden Informationen:

- eine knappe Information zum Zweck des Systems.
- eine kurze Übersicht der Datenarten, die im System gespeichert werden. Um diesen Datenbestand vollständig zu erfassen, müssen auch die Schnittstellen des Systems benannt sein. Die ein- und ausgehenden Datenströme können so auf Konsistenz mit den Datenarten und dem Datenmodell des Systems geprüft werden.
- eine Darstellung der Löschregeln und -mechanismen für die im System verarbeiteten Datenarten.

Oft ist es sinnvoll, die Darstellung der Löschmechanismen nach Datenarten zu unterscheiden, weil innerhalb des Systems entweder unterschiedliche Fristen angewendet werden sollen oder verschiedene Funktionen die Löschung der jeweiligen Datenart übernehmen. Ein solches Kapitel zu einer Datenart enthält einen standardisierten Katalog von Informationen.

Zunächst wird der Lifecycle der jeweiligen Datenart im System dargestellt. Dazu gehören auch die Abhängigkeiten innerhalb des Systems und zu externen Systemen, die vor einer Löschung beachtet werden müssen. Durch diese Information kann vermieden werden, dass die Löschung erfolgt, bevor alle Prozessschritte abgeschlossen sind. Insgesamt lässt sich aus diesen Informationen ableiten, ob im System die Regellöschfrist ausgenutzt werden muss oder ob es möglich ist, die Daten bereits früher zu löschen und so den Prinzipien von Erforderlichkeit und Datensparsamkeit konsequent zu entsprechen.

In einem zweiten Schritt werden die Speicherorte identifiziert, an denen die Datenart auf dem System abgelegt wird. Häufig handelt es sich dabei um Datenbanktabellen. Je nach Implementierung können dies aber auch Dateien, E-Mails oder andere Datenstrukturen sein. Für jeden der Speicherorte muss ein Löschmechanismus greifen. Beispielsweise ist im Falle einer Schnittstelle, an der Daten per Datei übergeben werden, sicherzustellen, dass die Dateien an allen potentiellen Speicherorten gelöscht werden (z. B. Quellsystem, Empfangssystem, ggf. Übertragungsstationen)

Die Löschmechanismen sind schließlich im Einzelnen mit den folgenden Angaben nachzuweisen:

- Name des Löschprozesses
- Wie und wie häufig wird der Löschprozess ausgelöst? (Löschperiode; z. B. automatisch täglich per Jobkette oder manuell durch einen Administrator am Wochenende.)
- Welcher Mitarbeiter ist für die Überwachung der Funktion verantwortlich? In der Regel ist dafür die Angabe der zuständigen fachlichen Rolle in einem Fachbereich ausreichend.
- Welche Parameter sind wie zu konfigurieren? Bei der Festlegung dieser Werte ist die Löschperiode so zu berücksichtigen, dass die für dieses System festgelegte Löschfrist nicht überschritten wird.
- Außerdem wird aufgeführt, ob für das System besondere Maßnahmen für die Löschung von Backups und Archivbeständen oder im Fall von Recoverys erforderlich sind.

Da diese sehr konkreten Angaben durch den Systemverantwortlichen bzw. den RZ-Betrieb bestätigt werden müssen, kann davon ausgegangen werden, dass die Löschfunktion für die Produktion zur Verfügung steht. Soweit beim Erstellen eines SLK Handlungsbedarf für die Löschung identifiziert wird, führt dies zu einem entsprechenden Change Request für die Entwickler oder einer Anpassung der Konfiguration durch die verantwortlichen Systemadministratoren. [6]

Für jedes im Rahmen der Datenflussanalyse als relevant identifizierte System ist vom jeweiligen Systemverantwortlichen ein SLK zu erstellen.

3.3 Richtlinien

Oft wird übersehen, dass auch Backups, Logprotokolle oder Datenabzüge personenbezogene Daten enthalten und sie deshalb ebenfalls Löschfristen unterliegen müssen. Ein durchgängiges Löschkonzept muss daher neben den Geschäftsprozessen auch die Prozesse des IT-Betriebs einbeziehen. Bei Toll Collect sind die Regellöschfristen für diese betrieblichen Querschnittsthemen in Datenschutz-Richtlinien festgelegt.

Die Richtlinie für die Speicherung von **Logprotokollen** mit personenbezogenen Daten stellt sicher, dass diese Daten nicht länger aufbewahrt werden, als dies für die Daten in produktiven Beständen der Fall ist. Für Analysezwecke im Fall von Unregelmäßigkeiten sind längere Fristen zulässig. Allerdings ist dann auch eine schrittweise Ausdünnung der Logs auf die relevanten Datensätze gefordert.

Datenabzüge mit personenbezogenen Daten können aus verschiedenen betrieblichen und fachlichen Gründen erforderlich sein. So kann es notwendig werden, Datenbestände unterschiedlicher Systeme abzugleichen. Auch zu Zwecken der Analyse

Sondersituationen entsprechende Spielräume zur zeitweisen Fristverlängerung.

[6] Bei der Implementierung von Löschfunktionen muss darauf geachtet werden, dass die Löschfrist konfigurierbar ist. Dadurch wird gewährleistet. dass im Falle von Anpassungsbedarf, z. B. durch Änderung der Rechtslage oder Rückwirkungen aus Geschäftsprozessen, die notwendige technische Flexibilität besteht.

eines Geschäftsprozesses kann es notwendig sein, Daten zeitweise außerhalb eines produktiven Systems zu verarbeiten. Betriebliche Notwendigkeiten für Datenabzüge können sich aus Fehleranalysen, zur Fehlerbereinigung oder für die Migration bei Releasewechseln ergeben. In einem Datenabzug sind regelmäßig Daten enthalten, die die Löschfrist im jeweiligen System demnächst erreichen. Im Rahmen der Richtlinie wird daher festgelegt, unter welchen Bedingungen welche Fristüberschreitungen für Datenabzüge zulässig sind. Insbesondere muss immer auch ein Verantwortlicher benannt werden, der die Einhaltung der erweiterten Fristen überwacht.

Backups sind erforderlich, um im Falle von Störungen oder Fehlern ein Recovery durchführen zu können. Die Vorhaltefrist der Backups muss allerdings im Verhältnis zur regulären Speicherfrist der im System gehaltenen Daten stehen. Im Falle von Toll Collect unterscheidet die Richtlinie daher zwischen Vorhaltefristen für Backups von Systemen, in denen ABMG-Daten verarbeitet werden (wenige Wochen) und solchen, die nur andere personenbezogene Daten verarbeiten (mehrere Monate).

Eine weitere Gruppe von „Richtlinien zur datenschutzrechtlichen Steuerung von Vertragspartnern“ unterstützt die Systemverantwortlichen darin, die Löschpflichten von Toll Collect bei Dienstleistern sicherzustellen, die für Toll Collect **Auftragsdatenverarbeitung** durchführen. Die Richtlinien unterscheiden sich nach allgemeinen Aspekten und spezifischen Aufgabenbereichen. Die Richtlinien konkretisieren die datenschutzrechtlichen Pflichten und werden den Dienstleistern als Anlage zum Vertrag übergeben.

4 Praxis und Erfahrungen

Das Löschkonzept der Toll Collect GmbH hat sich inzwischen in mehr als zweieinhalb Jahren Wirkbetrieb bewährt. In diesem Abschnitt wollen wir die wichtigsten Erfahrungen aus dem betrieblichen Alltag darstellen.

4.1 Umsetzung

Der Einstieg in das Projekt „Löschkonzept“ war zunächst mit einem Kraftakt verbunden: Neben den methodischen Vorüberlegungen und Verbesserungen mussten im Projekt auch gleichzeitig die erste Version der Regellöschfristen und die initialen Systemlöschkonzepte für knapp 30 verschiedene Systeme erstellt werden. Grundsätzlich ist allerdings auch eine iterative Vorgehensweise sowohl für die Datenarten als auch für einzelne Systemlöschkonzepte denkbar. Dadurch kann der initiale Aufwand über einen größeren Zeitraum verteilt werden.

Durch die Präsentation der Vorgehensweise und die Begründung der abgeleiteten Löschpflichten konnten die Prozess- und Systemverantwortlichen schnell überzeugt und eingebunden werden. Alle notwendigen Systemlöschkonzepte lagen zum Start des Wirkbetriebs vor und es war sichergestellt, dass die erforderlichen Löschfunktionen rechtzeitig ihre Arbeit aufnehmen konnten.

Inzwischen sind Regellöschfristen, Richtlinien zur Löschung und insbesondere die Systemlöschkonzepte fester Bestandteil der Unternehmenskultur bei Toll Collect.

4.2 Verantwortung, Change-Management und Awareness

In der Zweiteilung der Dokumentation – einerseits die Regellöschfristen und andererseits Systemlöschkonzepte und Richtlinien – spiegeln sich zugleich unterschiedliche Verantwortungsebenen.

Die Ableitung der Regellöschfristen aus den einzelnen gesetzlichen Vorgaben gehört zur klassischen Beratungstätigkeit des bDSB. Die **Regellöschfristen** werden vom bDSB nach Bedarf fortgeschrieben, beispielsweise im Falle neuer Erkenntnisse zu Geschäftsprozessen oder Änderungen der Rechtslage. Neue Fassungen legt der bDSB der Geschäftsführung als Entscheidungsvorlage vor.

In der betrieblichen Praxis zeigt es sich schnell, dass eine gute Motivation und nachhaltige Vermittlung der Löschregeln nur möglich ist, wenn sie eine relativ einfache Struktur aufweisen. Andernfalls wird ihre technische Implementierung, die betriebliche Umsetzung und die Überwachung der Einhaltung der Fristen in der Praxis scheitern. Änderungen werden daher immer auch an der Vorgabe „Keep it Simple“ überprüft. Wo dies datenschutzrechtlich vertretbar ist, werden derzeit auch Datenarten zusammengefasst, um die Komplexität zu reduzieren.

Dagegen liegt die Erstellung der **Systemlöschkonzepte** grundsätzlich in der Verantwortung der jeweiligen Systemverantwortlichen. Sie, und nicht der bDSB, sind die fachlich Verantwortlichen für die einzelnen Systeme. Sie müssen die normativen Vorgaben[7] der Regellöschfristen für ihre jeweiligen Systeme umsetzen.

Eine Aktualisierung kann vom Systemverantwortlichen selbst vorgenommen oder durch das Datenschutz-Team angestoßen werden. Für den bDSB können Auslöser einer solchen Aufforderung die Freigabe von Pflichtenheften für die Systementwicklung oder Audit-Ergebnisse sein. Auch eine periodische Überprüfungsaufforderungen ist sinnvoll.

Der Aktualisierungsvorschlag für ein SLK wird bei Toll Collect vom Systemverantwortlichen beim Datenschutz-Team eingereicht, ggf. nach vorheriger Diskussion. Der bDSB überprüft bei neuen oder aktualisierten SLKs die Einhaltung der Regellöschfristen und gibt sie frei.[8] Im Rahmen der oben angesprochenen Verankerung in einer Datenschutz-Policy sind die SLKs dann normativ für den Systembetrieb.

Die technische und operative Umsetzung der Löschmaßnahmen wird dementsprechend auch von den Systemverantwortlichen veranlasst. Sie bringen die notwendigen Anforderungen in den allgemeinen Systementwicklungsprozess ein und steuern über den üblichen Change-Prozess die Anpassung von Konfigurationsparametern durch die Administrationsteams im Rechenzentrum, wenn dies erforderlich ist.

Die unternehmensweit kommunizierte Verantwortlichkeit erhöht bei den Systemverantwortlichen die **Awareness** für Datenschutz-Aspekte. Durch die Löschmaßnahmen wird ein Ergebnis von Datenschutz auch im Arbeitsalltag erlebt. Die Löschfristen sind bei vielen, die mit entsprechenden Fragestellungen in Berührung kommen, verankert. Die Mitarbeiter gehen oft schon

[7] Normativ im Sinne der Datenschutz-Policy von Toll Collect (vgl. oben).

[8] Denkbar ist auch eine Aufgabenteilung, in dem das Datenschutz-Team als Dienstleister für die Systemverantwortlichen auftritt und quasi als Profit-Center die Systemlöschkonzepte pflegt. Dies kann für beide beteiligte Parteien effizienter sein. Voraussetzung ist, dass entweder das Datenschutz-Team entsprechend ausgestattet ist oder durch die Systemverantwortlichen die notwendigen Mittel bereitgestellt werden. Allerdings verringern sich in diesem Modell die Berührungspunkte der Mitarbeiter in den Fachbereichen zum Datenschutz. Außerdem wird die Review-Funktion des Datenschutz-Teams schwieriger, weil die Dokumente ja von ihm selbst gepflegt wurden.

mit ersten Überlegungen zur Weiterentwicklung von Verfahren auf das Datenschutz-Team zu, um die datenschutzrechtliche Zulässigkeit und die einzuhaltenden Randbedingungen zu klären. Das Datenschutz-Team kann deshalb auch über die Diskussion der Löschkonzepte an der Gestaltung der Prozesse und Systeme mitwirken. Es unterstützt bei der Suche nach datenschutzfreundlichen Lösungen. In den Fachbereichen mit Verantwortung für personenbezogene Daten wird durch diese Prozesse die Awareness für Datenschutz-Fragen spürbar gestärkt. Ergänzend wird ein fachbereichsübergreifender Erfahrungsaustausch zu Löschaspekten in Workshops gepflegt.

Durch die Abnahme beschäftigt sich das Datenschutzteam mit allen SLKs und baut Detailwissen über alle im Unternehmen eingesetzten Systeme auf, in denen personenbezogene Daten verarbeitet werden. Gleichzeitig erhält und bewahrt das Datenschutz-Team auch den Überblick über alle entsprechenden Verarbeitungsprozesse. Durch dieses Know How kann das Datenschutz-Team wichtige Hinweise geben und aktiv an der Lösung von Problemen mitwirken. Es wird zu einem geschätzten und gleichberechtigten Partner der Verantwortlichen bei der Fortentwicklung der Systeme.

4.3 Teil des Verfahrensverzeichnisses

Systemlöschkonzepte sind mit den oben genannten Inhalten ein wichtiger Bestandteil des internen Verfahrensverzeichnisses (vgl. § 4e BDSG). Für viele Fragestellungen bieten sie einen schnellen Zugriff auf Informationen zu Datenbeständen und Verarbeitungsschritten. Wie oben beschrieben, werden SLKs aus verschiedenen Anlässen heraus aktualisiert. Implizit wird dadurch dieser Teil des Verfahrensverzeichnisses fortgeschrieben.

4.4 Datenschutzaudits

Durch die Inhalte der Systemlöschkonzepte können System-Audits vom bDSB sehr effizient vorbereitet werden, soweit es darum geht, die Löschfunktionen eines Systems nachzuweisen.

Die Angaben zu Speicherorten und Löschprozessen identifizieren für die Audit-Pläne die Stellen, an denen zu prüfen ist. Sie bieten außerdem die Möglichkeit, einen Abgleich beispielsweise mit einem produktiven Schema-Abzug einer Datenbank vorzunehmen. Die systemspezifischen Frist- und Konfigurationsvorgaben definieren den Sollzustand für die Prüfpunkte. Gleichzeitig stehen damit auch für die Systemverantwortlichen alle Informationen zur Verfügung, die sie zur Vorbereitung eines Audits benötigen. Von der Tragfähigkeit der SLKs für Audits konnte sich auch der BfDI überzeugen.[9]

Befunde im Audit können in der Regel leicht aufgeklärt werden. Bei Fehlern in der Löschfunktion wird ein Fehlerticket eröffnet, im Falle von Konfigurationsfehlern eine entsprechende Anweisung an das Administrationsteam gestellt und bei Unklarheiten oder falscher Darstellung im Systemlöschkonzept eine Aktualisierung des SLKs angestoßen. Die systematische Dokumentation der Vorgaben in den SLKs und die klare Zuweisung von Verantwortlichkeiten schafft sehr gute Voraussetzungen für die betriebliche Umsetzung.

4.5 Außendarstellung

Toll Collect genießt die Aufmerksamkeit des BfDI als gesetzlicher Aufsichtsbehörde. Auch das BAG als auftraggebende Behörde überwacht, neben vielen anderen Aspekten, die Einhaltung von datenschutzrechtlichen Vorgaben.

Durch die Bereitstellung des Dokuments „Regellöschfristen“ sowie der Systemlöschkonzepte sind für beide Behörden die abgeleiteten Fristen ebenso nachvollziehbar dokumentiert, wie die daraus resultierenden Löschregeln der einzelnen Systeme. Auf Basis der Dokumentenlage können sich Auftraggeber wie Aufsichtsbehörde auf Vor-Ort-Termine bei Toll Collect vorbereiten. Sie nehmen informiert an Audits teil und können sich dabei von der praktischen Umsetzung der dokumentierten Mechanismen überzeugen.

4.6 Return on Investment

Für die Entwicklung und Pflege eines durchgängigen, unternehmensweiten und dokumentierten Löschkonzepts müssen Ressourcen aufgebracht werden. Mit der Umsetzung stellt sich jedoch vielfältiger Nutzen ein.

Zu aller erst gewinnt das Unternehmen: Sein Datenschutz-Profil wird nach innen wie außen wesentlich geschärft. Natürlich profitiert auch das Datenschutz-Team des jeweiligen Unternehmens in großem Umfang von der des Löschkonzepts einhergehenden Systematisierung. Auch die oben beschriebene Verankerung des Themas Löschen ist ein großer Gewinn für die Datenschutz-Awareness im Unternehmen. Dadurch lassen sich auch andere Themen des Datenschutzes nachhaltiger vermitteln.

Aber auch über diese primär datenschutzbezogenen Verbesserungen hinaus ergeben sich an vielen Stellen Vorteile für das Unternehmen – bis hin zu echtem monetären Return on Investment. Die wichtigsten dieser Gewinne sollen im Folgenden kurz angesprochen werden:

- Durch die Forderung nach Datenlöschung sind die Verantwortlichen gezwungen, sich intensiv mit der Prozess- und Systemgestaltung auseinander zu setzen. Sie bauen Prozesskompetenz und Wissen über die Systeme auf.
- Es wird kritischer hinterfragt, welche Datenbestände wirklich gebraucht werden und wie ein Zweck schnell und effizient mit kleinen Datenbeständen erreicht werden kann. Weil die Geschäftsprozesse terminiert werden müssen, um die Daten löschen zu können, werden die Prozesse klarer strukturiert und häufig in ihren zeitlichen Abläufen gestrafft.
- Die datenschutzrechtliche Löschforderung zwingt die Prozessverantwortlichen, sich stärker mit der Zulässigkeitsfrage der Datenverarbeitung auseinander zu setzen. In der Diskussion mit dem Datenschutzteam wird deshalb früh entschieden, ob ein Entwicklungsprojekt umgesetzt, modifiziert oder doch nicht weiterverfolgt wird. Die Kosten für rechtlich unzulässige Systeme oder funktionale Ergänzungen werden vermieden.
- Verbindliche Löschfristen führen in den meisten Fällen zu einer Reduzierung und Konsolidierung von Datenbeständen. Gerade im Bereich der Massendatenverarbeitung können dadurch große Volumina an Speicherplatz „aufgeräumt“ werden. Über die Kosten pro operativ betriebenem Gigabyte Speicher inklusive aller Nebenkosten wie Notfall-Redundanz und Backups können die monetären Einsparungen einfach berechnet und den Projektkosten gegenübergestellt werden. Bei Toll Collect dürfte die Kostenerspar-

[9] Der BfDI nahm einen Besuch im Herbst 2006 bei der Toll Collect GmbH zum Anlass, das interne Überwachungssystem der Toll Collect GmbH speziell auf die Einhaltung der spezifischen Datenschutzvorgaben aus dem ABMG zu überprüfen, vgl. *BfDI 2007*, *124*.

nis über den Aufwendungen für den Datenschutz liegen.

Fazit

Die Erfahrungen bei Toll Collect zeigen, dass ein praxisgerechtes Löschkonzept unternehmensweit erstellt und gelebt werden kann. Voraussetzungen für ein erfolgreiches Projekt sind die Unterstützung durch die Unternehmensleitung sowie eine klare Strukturierung der Dokumentation und die Regelungen der Verantwortlichkeiten. Sinnvoll sind außerdem wenige, einheitliche Löschfristen, weil sie die Vermittlung und Umsetzung des Löschkonzepts wesentlich erleichtern.

Das Datenschutz-Team muss ggf. mit interner oder externer Unterstützung eine Anfangsinvestition für die Prozessanalyse und die Definition der Regellöschfristen erbringen. Außerdem müssen die anfänglichen Hürden gegen ein solches Projekt in den Köpfen der Mitarbeiter überwunden werden. Danach kann eine effiziente Arbeitsteilung zwischen dem Datenschutz-Team und den Systemverantwortlichen für die Fortschreibung und Umsetzung des Löschkonzepts einsetzen.

Das Unternehmen kann aus einem Löschkonzept vielfältigen Nutzen ziehen – neben der verbesserten Verankerung des Datenschutzes sind auch andere positive interne Effekte zu erwarten – bis hin zu einem echten Return on Investment für die Projektkosten.

Abkürzungen

ABMG	Autobahnmautgesetz (http://bundesrecht.juris.de /bundesrecht/abmg/gesamt.pdf)
ABMG-Daten	Daten nach §§ 4 Abs. 2 (fahrtbezogene Daten) und 7 Abs. 2 ABMG (Kontrolldaten)
BAG	Bundesamt für Güterverkehr
bDSB	betrieblicher Datenschutzbeauftragter
RZ	Rechenzentrum
SLK	Systemlöschkonzept

Literatur

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Tätigkeitsbericht 2005-2006 – 21. Tätigkeitsbericht. (http://www.bfdi.de/)

Fraenkel, R./ Hammer V. (2007): Rechtliche Löschvorschriften, DuD, in diesem Heft

Hammer, V. (1999): Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig/ Wiesbaden, 1999.