DuD
Datenschutz und Datensicherheit

Rechtliche Löschvorschriften

Reinhard Fraenkel, Volker Hammer

Personenbezogene Daten müssen gelöscht werden, wenn sie für die weiteren Geschäftprozesse der Unternehmen nicht mehr erforderlich sind und auch gesetzliche Aufbewahrungsfristen der Löschung nicht im Wege stehen. In der Praxis wird dieser Löschpflicht allerdings nur zurückhaltend Rechnung getragen. Der Beitrag begründet das Erfordernis konsequenten Löschens und will dazu motivieren, den gesetzlich vorgegebenen Löschpflichten durch ein Löschkonzept Rechnung zu tragen.

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

Einleitung

Das BDSG ist – gelegentlich ist es notwendig, daran zu erinnern – ein Verbotsgesetz mit Erlaubnisvorbehalt. Das bedeutet, dass die Erhebung, und Verwendung von personenbezogenen Daten zwar in den gesetzlich geregelten Fällen zulässig ist, grundsätzlich aber eine „regelwidrige“ Ausnahme darstellt.

Zwar ist diese Ausnahmesituation in vielen Fällen notwendig. Das politische, wirtschaftliche und soziale Gefüge der Gesellschaft wäre überhaupt nicht vorstellbar und organisierbar, gäbe es nicht die Möglichkeit, personenbezogene Daten zu erheben und zu verwenden. Diese Tatsache aber darf nicht den Blick dafür verstellen, dass es in der Logik des Datenschutzrechts liegt, einmal erhobene Daten auch wieder zu löschen, wenn der Zweck zu dem die Daten erhoben wurden, weggefallen ist. Der Regelfall, nämlich die Situation, dass über den Betroffenen keine Daten gespeichert werden, muss wieder hergestellt werden. Dies wird durch die Löschung vormals erhobener und verwendeter Daten bewirkt. Der Löschung von Daten kommt daher rechtsdogmatisch eine eminente Bedeutung zu. Daher ist es überraschend, wie wenig Aufmerksamkeit in Literatur und im BDSG selbst der Verpflichtung zur Löschung von Daten tatsächlich eingeräumt wird.[1]

Wir diskutieren im Folgenden kurz die Löschregel des BDSG, suchen nach Ursachen für Löschdefizite in der Praxis, begründen das Erfordernis konsequenten Löschens und motivieren, der Löschpflichten durch ein Löschkonzept Rechnung zu tragen.

1 Löschregeln im BDSG

Nachfolgend werden die Löschregeln für personenbezogene Daten betrachtet, die private Unternehmen zur Erfüllung eigener Geschäftszwecke erheben und verwenden. Zentrale Norm ist § 35 Abs. 2 Nr. 3 BDSG. Sind, so bestimmt es § 35 Abs. 2 Nr. 3, die für eigene Zwecke verarbeiteten personenbezogenen Daten für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich, sind diese Daten zu löschen. Diese gesetzliche Vorschrift ist unmittelbarer Ausfluss des im Zusammenhang mit den nachfolgenden Erörterungen nicht weiter diskutierten dogmatischen Ansatzes des Gesetzes als Verbotsgesetz mit Erlaubnisvorbehalt.[2] Grundlegende Annahme für die weitere Diskussion ist selbstverständlich, dass die personenbezogenen Daten in zulässiger Weise gespeichert wurden. Sollte nämlich die Speicherung unzulässig sein, sind die Daten gemäß § 34 Abs. 2 Nr. 1 BDSG ohnehin unverzüglich zu löschen.

1.1 Zur Zweckbindung und Erforderlichkeit

Die verantwortlichen Stellen, die Daten erheben und verwenden, müssen gemäß § 28 Abs. 2 BDSG bereits zum Zeitpunkt der Erhebung personenbezogener Daten die Zwecke konkret festlegen, für die die Daten verarbeitet oder genutzt werden sollen. Das Kriterium der Zweckbindung fordert ergänzend, dass die verantwortliche Stelle diese Daten nur für den Zweck verwendet, zu dem sie erhoben wurden. In gleicher Weise werden der Umfang und die Speicherdauer rechtmäßig erhobener Daten durch das Kriterium der Erforderlichkeit begrenzt. Die erhobenen oder verwendeten Daten müssen für den Zweck, für den sie verwendet werden, erforderlich sein.

Es bedarf keiner besonderen Erörterung, dass beispielsweise ein Versandhandelsunternehmen die für die Abwicklung eines

[1] Siehe dazu näher 1.2

[2] Unerörtert bleibt also die Frage, ob der Ansatz des Gesetzgebers das Datenschutzrecht als Verbotsgesetzes mit Erlaubnisvorbehalt zu konstruieren richtig ist. Zweifel sind durchaus angebracht. § 29 BDSG jedenfalls ist so weit gefasst, dass der Verbotscharakter der Erhebung und Verwendung von personenbezogenen Daten weitgehend in den Hintergrund tritt.

Geschäftes im Fernabsatz alle für die Abwicklung erforderlichen personenbezogenen Daten seines Kunden erheben und verwenden muss. Die mögliche Speicherdauer dieser Daten richtet sich unter anderem nach den gesetzlichen Gewährleistungsregeln. Daraus lassen sich ohne weiteres Speicherfristen von bis zu 4 Jahren ableiten.[3] Hingegen gibt es für den mit der Auslieferung der Ware beauftragten Spediteur keinen Grund, die ihm vom Versandhändler rechtmäßig übermittelten Daten ebenfalls so lange zu speichern. Nach der Auslieferung ist für den Spediteur die Kenntnis der Adressdaten des Empfängers der Ware nicht mehr erforderlich.

Ausgehend vom zulässigen Zweck der Verarbeitung begrenzt die Analyse der Erforderlichkeit einerseits die Menge der zu erhebenden und zu verwendenden Daten. Andererseits leitet sich aus der Analyse zugleich auch die Frist ab, nach der diese Daten zu löschen sind. Werden die Daten über diese Frist hinaus ohne Notwendigkeit gespeichert, ist darin regelmäßig eine Datenspeicherung auf Vorrat zu sehen, die gegen das datenschutzrechtliche Erforderlichkeitsprinzip verstößt.[4]

Die Löschung von Daten stellt endgültig sicher, dass sie nicht zweckfremd verwendet werden können. Das Prinzip der Datensparsamkeit, das ein Gebot für den gesamten Prozess der Datenverarbeitung darstellt, unterstreicht die Löschforderungen im BDSG. Gemäß den datenschutzrechtlichen Prinzipien Zweckbindung, Erforderlichkeit und Datensparsamkeit ist daher eine möglichst frühe Löschung personenbezogener Daten geboten.

1.2 Gebot einer Regellöschfrist

Da die zulässige Speicherung einmal erhobener personenbezogener Daten durch die Begriffe Zweckbindung und Erforderlichkeit markiert werden, ist es konsequent, dass der Gesetzgeber Regellöschfristen unterstellt. Daher müssen gemäß § 4 d Abs. 1 BDSG Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde gemeldet werden. Inhalt der Meldung ist gem. § 4 e Abs. 1 Nr. 7 regelmäßig auch eine Regelfrist für die Löschung der Daten.

Diesem Gebot wird in der Kommentarliteratur teilweise nur wenig Aufmerksamkeit entgegengebracht. So heißt es beispielsweise bei Schaffland/Wiltfang in der Kommentierung zu § 4 e Nr. 7: „Wegen der Aufbewahrungspflichten (Nr. 7) wird regelmäßig 10 Jahre einzutragen sein.“[5] Zwar vermag Petri der Vorschrift auch keine normative Wirkung in dem Sinne zu entnehmen, dass gleichsam hausinterne Fristenregelungen geschaffen werden müssten. Immerhin räumt er aber der Norm insofern Bedeutung ein, da anhand dieser Meldung die Behörde in die Lage versetzt werden muss, zu überprüfen, ob gesetzliche Regellöschfristen eingehalten werden.[6]

Demgegenüber muss betont werden, dass die verantwortliche Stelle bereits bei der Festlegung der Verarbeitungszwecke Regelfristen für die Löschung zu treffen hat: „Entfällt das die Verarbeitung rechtfertigende Verarbeitungsinteresse, sind die Daten regelmäßig zu löschen, es sei denn, gesetzliche Aufbewahrungspflichten stehen dem entgegen.“[7] Dieser den Interessen der Betroffenen gerecht werdenden Auffassung ist zuzustimmen. Der Anspruch auf Löschung personenbezogener Daten aus Dateien ist im BDSG abschließend geregelt. Mögliche andere, das Persönichkeitsrecht schützende zivilrechtliche Normen, z.B. §§ 823 Abs. 2 oder 1004 BGB, finden keine Anwendung. Darauf hat der BGH ausdrücklich hingewiesen. Soweit spezielle Rechte der Betroffenen nach dem BDSG bestünden, könne keine Anwendung der für die Eingriffe in das allgemeine Persönlichkeitsrecht entwickelten Rechtsgrundsätze stattfinden.[8]

Wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat, entfällt zwar die Meldepflicht gemäß § 4 d Abs. 2 BDSG: Die gleichen Angaben muss sie dann aber ihrem Beauftragten zur Verfügung stellen (§ 4 g Abs. 2 BDSG). Stellt die verantwortliche Stelle dem betrieblichen Datenschutzbeauftragten die notwendigen Informationen zur Löschung nicht zur Verfügung, ist es seine Aufgabe, darauf hinzuwirken, dass sie Löschregeln erstellt und einhält.

> Insoweit kann festgehalten werden, dass das BDSG für jeden Fall der automatisierten Verarbeitung personenbezogener Daten die Erstellung eindeutiger Löschregeln fordert.

2 Löschdefizite in der Praxis

Langjährige Erfahrungen der Autoren zeigen, dass die Löschung von personenbezogenen Daten eine Verpflichtung ist, die, wenn überhaupt, nur äußerst ungern eingehalten wird. Dies mag vielfältige Gründe haben, auch psychologische oder landsmannschaftliche, wie sie in der Aussage „Ein Ostwestfale löscht keine Daten“ deutlich werden. Jedenfalls ist es eine nicht hinweg zu diskutierende Tatsache, dass beispielsweise die Mehrzahl der deutschen Versicherungen Kundendaten auch dann nicht löschen, wenn Versicherungsverträge gekündigt werden, obwohl alle Leistungen wechselseitig erbracht wurden. Branchenüblich spricht man vornehm von „stornierten Verträgen“ Auch im Versandhandel ist es durchaus üblich, einmal gespeicherte Kundendaten nicht mehr zu löschen, auch wenn die letzte Bestellung mehr als 2 Jahre zurückliegt und es auch keine offenen Forderungen mehr gibt. So sammeln sich sogenannte „Kellerbestände“ an, die für gelegentliche Werbeaktionen vorgehalten werden und die sich nicht selten aus Daten ehemaliger Kunden speisen, die 10 oder noch mehr Jahre alt sind. Die Beispiele lassen sich beliebig vermehren, denkt man beispielsweise an Lotterieeinnehmer oder die sich etablierenden Rabattvereine.

2.1 Ursachen im BDSG

Eine der Ursachen für diesen Missstand liegt in der Struktur des BDSG selbst begründet. Die nachfolgend vorrangig zu diskutierende Löschnorm des § 35 Abs. 2 Nr. 3 muss zwar zwingend von allen verantwortlichen Stellen umgesetzt werden. Diese Umsetzung kann aber in der Praxis auf Schwierigkeiten stoßen, weil Löschfristen gerade nicht zeitlich konkret festgelegt werden. Da kann es gelegentlich für einen betrieblichen Datenschutzbeauftragten schon schwer werden, bei der Geschäftsleitung seines Unternehmens die notwendige Sensibilität dafür zu wecken, einmal erho-

[3] Der einmalige Kauf im Versandhandel rechtfertigt aber keine dauerhafte Speicherung der Kundendaten. Diese sind vielmehr nach der Abwicklung des Vertrages zulöschen. Vgl Achtzehnter Datenschutz und Informationsfreiheitsbericht NRW, Seite 72.

[4] In diesem Sinne auch von v. Zezschwitz in *Roßnagel 2003* Seite 239.

[5] Siehe *Schaffland/Wiltfang* § 4e Rdnr. 7.

[6] Vgl. Petri in *Simitis* § 4e, Rdnr. 11.

[7] *Gola/Schomerus* § 4e, Rdnr. 9.

[8] Vgl. BGH in NJW 1986, 2205, 2206/07, vgl. im Übrigen in diesem Sinne auch und weiterführend *Bergmann/Möhrle/Herb* § 35, Rdnr. 78 ff.

bene personenbezogenen Daten auch wieder zu löschen. Es lässt sich ja trefflich darüber diskutieren, wann der Zeitpunkt eingetreten ist, ab dem die Kenntnis der einmal erhobenen Daten für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Dies gilt umso mehr, als ja zumindest in gewissen Grenzen auch eine zweckändernde Nutzung der Daten im Rahmen von § 28 Abs. 2 BDSG zulässig ist.

Eine potentielle künftige Zweckänderung kann aber keinesfalls ein hinreichender Grund dafür sein, um von einer Löschung abzusehen. Voraussetzung für jede zweckändernde Nutzung ist, dass die Daten noch rechtmäßig verwendet werden dürfen. Personenbezogene Daten bloß deshalb noch zu speichern, weil möglicherweise eine zweckändernde Nutzung in der Zukunft in Frage kommt, wäre rechtswidrig. Diese bloße Vorratsspeicherung würde dazu führen, dass die Speicherung der ehemals rechtmäßig erhobenen und verwandten Daten nunmehr unzulässig wäre und diese damit entsprechend § 35 Abs. 2 Nr. 1 gelöscht werden müssten.

2.2 Wegfall der Meldung, Mangelnde Aufsicht

Auch die Tatsache, dass gemäß § 4 d BDSG die Meldepflicht von Regellöschfristen dann entfällt, wenn die verantwortliche Stelle einen Beauftragten für Datenschutz bestellt hat, fördert nicht die Bereitschaft der Unternehmen, Löschfristen zu definieren. Durch die fehlenden Meldungen haben die Aufsichtsbehörden heute faktisch keinen Überblick mehr darüber, ob und inwieweit die Unternehmen ihrer Verpflichtung zur Löschung von Daten nachkommen.

Hinzu kommt, dass eine spezielle Prüfung seitens der Aufsichtsbehörden bei einzelnen Unternehmen, ob Regelfristen für die Löschung festgelegt bzw. eingehalten werden, kaum stattzufinden scheint. In den Jahresberichten der Aufsichtsbehörden findet man zwar eine Fülle von Fällen, in denen man Einzelbeschwerden nachgegangen ist. Aussagen darüber aber, ob ein Unternehmen durchgängig Löschfristen festgelegt hat und ob diese auch eingehalten werden, finden sich in den Berichten kaum. Wenn das Problem von Regellöschfristen problematisiert wird, wird es bezogen auf Missstände im öffentlichen Bereich thematisiert.[9]

Dass die Aufsichtsbehörden der Überprüfung der Einhaltung von Regellöschfristen offenbar so geringe Aufmerksamkeit schenken ist insbesondere deswegen schade, weil eine entsprechende Prüfung relativ einfach durchführbar ist, auch bei ansonsten hoch komplexen IT-Prozessen oder Datenbankstrukturen.[10]

2.3 Schwierige Entscheidungen

Der auf Grund der Struktur des BDSG sinnvolle Verzicht auf die Festlegung konkreter Löschfristen ist teilweise dafür verantwortlich, dass datenschutzgerechtes Löschen nicht im tatsächlich erforderlichen Maß von den verantwortlichen Stellen durchgeführt wird. Hinzu kommt aber oft auch eine große Unsicherheiten auf der Seite der Unternehmen, da mit jeder Löschung von Daten auch ihr irreversibler „Verlust“ verbunden ist. Da das Löschen von Daten oft auch noch mehr oder weniger als notwendiges Übel wahrgenommen wird, unterbleibt es vielfach ganz oder erfolgt nicht in dem vom BDSG geforderten Umfang. Mittelbare Vorteile des Unternehmens, abgesehen davon, dass man eine abstrakte Rechtsnorm erfüllt, werden kaum wahrgenommen. Insoweit fehlt es auch in vielen Unternehmen an der notwendigen Motivation, Löschfristen zu definieren und dann auch einzuhalten. Hinzu kommt, wie gesagt, die Endgültigkeit des Vorgangs, die Unsicherheit auslöst. Der „Ostwestfale“ löscht ja nicht etwa deswegen keine Daten, weil er Spaß an einem bewussten Rechtsverstoß hat. Vielmehr ist diese Haltung Ausdruck einer prinzipiellen Unsicherheit, ob die Daten nicht doch noch benötigt werden könnten.

Trotz dieser durchaus nachvollziehbaren Befindlichkeiten kommt die verantwortliche Stelle nicht darum herum, konkrete Fristen für die Löschung personenbezogener Daten festzulegen. Die nachfolgenden Voraussetzungen erleichtern diese komplizierte Festlegung:

- Die verantwortliche Stelle muss ihre Geschäftsprozesse so genau kennen, dass sie entscheiden kann, wann diese im Regelablauf und bei Sonderfällen beendet sind.
- Die verantwortliche Stelle muss die rechtlichen Randbedingungen der Geschäftsprozesse so gut kennen, dass sie die Einwendungsmöglichkeiten der Kunden gegen Leistungen und ihre anderen rechtlichen Pflichten überblickt und hinsichtlich der Notwendigkeit, auf personenbezogene Daten zurückzugreifen, bewerten kann.
- Es muss Entscheidungsträger geben, die die vorgenannten Faktoren überblicken und die Fristfestlegung treffen.

2.4 Dokumentationspflichten

Schließlich darf auch nicht verkannt werden, dass die Löschung personenbezogener Daten allein deswegen nicht trivial ist, weil beispielsweise nach Abschluss eines Geschäftsvorgangs nicht einfach alle Daten gelöscht werden dürfen. Vielmehr ist es häufig so, dass ein bestimmter Kranz von Daten auf Grund von handels- und/oder steuerrechtlichen Vorschriften auch nach Abwicklung des eigentlichen Geschäftsvorfalles weiter gespeichert werden, weil die verantwortliche Stelle gesetzlichen Dokumentationspflichten unterliegt. Beispielsweise müssen Handelsbriefe oder Buchhaltungsdaten nach AO und HGB oder Personaldaten[11] regelmäßig über die Dauer der eigentlichen Abwicklung eines Geschäftsvorfalls hinaus zur Prüfung durch Externe vorgehalten werden. Der Zweck der Speicherung ist dann nur noch wegen der gesetzlichen Dokumentationspflichten begründet. Dieser Zweck ist mit dem Ablauf der längsten Dokumentationspflicht erfüllt. Auch für diese Daten besteht dann die Löschpflicht gemäß BDSG.

Im Übrigen müssen auch Daten, die nur noch zu Dokumentationszwecken gespeichert werden, aus dem Prozess der normalen Datenverarbeitung ausgesondert und gemäß § 35 Abs. 3 Nr. 1 gesperrt werden. Nimmt man die grundrechtssichernde Intention des Datenschutzes ernst, verbietet sich

[9] Vgl. beispielhaft 18. Tätigkeitsbericht LfD Saarland, Seite 110/111 in Bezug auf Datenbeihilfe berechtigter Patienten für psychotherapeutische Behandlung bzw. 19. Tätigkeitsbericht des LfD Baden-Württemberg in Bezug auf die Berufsakademie Stuttgart, vgl. Teil 6 Gliederungspunkt 2.1.5.

[10] Vgl. dazu *Hammer/Fraenkel* in diesem Heft.

[11] Zu den differenzierten Aufbewahrungsfristen vgl. z.B. die umfassende Darstellung in *Bolten/Putte 2007*.

für so gesperrte Daten auch die oben schon angesprochene nachträgliche Zweckänderung nach § 28 Abs. 2 BDSG.

> Die vorstehende Analyse zeigt, dass sowohl die ergebnisoffenen Formulierungen des BDSG als auch die Unsicherheiten in den Unternehmen bezüglich der die Daten verwendenden Prozesse wesentlich zum oben beklagte Löschdefizit beitragen.

3 Konsequentes Löschen

Auch wenn die Umsetzung des Löschgebotes des BDSG kompliziert ist und für die Unternehmen vermeintlich risikobehaftet ist, rechtfertigen diese Hürden jedoch keinen Gesetzesverstoß. Jede verantwortliche Stelle, die personenbezogene Daten verarbeitet, ist deshalb gehalten, auch die fristgerechte Löschung dieser Daten sicherzustellen. Vor der Umsetzung der Löschvorgaben stellen sich allerdings einige Fragen, die hier kurz skizziert werden sollen:

3.1 Ableitung von Löschfristen

Nach Schaffland/Wiltfang ist ja eine differenzierte Ableitung von Löschfristen nicht erforderlich.[12] So holzschnittartig geht es allerdings nicht. Unter Kapitel 2.4 wurde bereits auf spezifische, sich einstellende Einzelprobleme hingewiesen. Ihre Beachtung im Rahmen einer Ableitung von Löschfristen führt zur Bildung von Gruppen von Datenbeständen, die hinsichtlich ihrer Löschfristen gleichartig zu behandeln sind. Im Folgenden unterscheiden wir daher nach Datenarten. Beispiele für Datenarten können sein: Stammdaten, Kontaktdaten, Buchhaltungsdaten, Bestelldaten oder Personaldaten. Für die Löschung ist dabei nicht wesentlich, ob in einem ja in der Regel nach technischen Gesichtspunkten gebildeten Datensatz nur Attribute einer Datenart enthalten sind. Vielmehr müssen in einem Datensatz ggf. auch einzelne Attribute gelöscht werden, wenn sich dies aus der Löschregel für die Datenart ergibt.

Die Ableitung der Löschfristen setzt eine genaue Analyse der Geschäftsprozesse voraus, in denen die verschiedenen Datenarten erhoben und verwendet werden. Dies ist im Wesentlichen eine juristische Analyse der Prozessschritte: In diese Analyse müssen neben den datenschutzrechtlichen und gegebenenfalls vertraglichen Löschgeboten bzw. Löschpflichten auch gesetzliche Regelungen mit einbezogen werden, die die Aufbewahrung bestimmter Daten vorschreiben, insbesondere also steuerrechtliche Regelungen und die Regelungen des HGB.

In Abhängigkeit z. B. vom jeweiligen Einzelvertrag[13] muss bestimmt werden,

- wann die jeweilige Leistungserfüllung erbracht ist,
- wann mögliche Ansprüche verjährt sind,
- inwieweit Dokumentationspflichten des HGB bzw. der AO oder anderer Rechtsvorschriften zu erfüllen sind,
- unter welchen Bedingungen für den Regelprozess und für Sonderfälle die Erforderlichkeit entfällt und damit das datenschutzrechtliche Löschgebot greift, sowie
- ob gegebenenfalls engere spezialgesetzliche Löschfirsten (vgl. unten 3.2) zu berücksichtigen sind und deshalb der Geschäftsprozess anzupassen ist.

Soweit AGB-Regelungen relevant sind, muss darauf hingewiesen werden, dass sich die verantwortliche Stelle in den AGB von Löschpflichten des BDSG nicht dispensieren kann. Regelungen in den AGB, die die Löschgebote des BDSG außer Kraft setzen wollen, sind stets unwirksam.

Die geforderte Analyse nach Datenarten muss auch die besonders sensiblen Daten gemäß § 3 Abs. 9 BDSG detektieren. Soweit irgend möglich, sind für diesen Kranz der Daten kürzest mögliche Löschfristen zu etablieren.

Nach dem Wortlaut des Gesetzes bleibt der speichernden Stelle nach dem Ende des letzten Verarbeitungszwecks noch ein gewisser zeitlicher Spielraum, bis sie die Daten Löschen muss. Der eigentliche Löschlauf kann so möglicherweise in geeignete, vielleicht schon bestehende andere organisatorische und technische Abläufe eingebaut werden. Allerdings muss der genutzte Spielraum im Verhältnis zur Speicherdauer und Sensitivität der Daten stehen.

In bestimmten Fällen gelten aber auch bereichsspezifische Rechtsvorgaben für die Ableitung der Löschfrist.

3.2 Bereichspezifische Löschfristen

Bereichsspezifische Datenschutzregelungen unterscheiden sich gelegentlich vom BDSG dadurch, dass sie den diese Daten verarbeitenden Unternehmen konkrete Löschfristen vorgeben oder einen so engen Rahmen stecken, dass die Interpretationsspielräume, die dieser Rahmen zulässt, begrenzt sind. Solche Fristen können auch als Orientierungshilfe für die Ableitung von Fristen in anderen Bereichen mit vergleichbaren Datenbeständen dienen. Beispiele für bereichspezifische Fristen sind:

- § 7 Postdienstdatenschutzverordnung (PDSV): Gemäß dieser Regelung müssen Adressdaten, die im Rahmen eines Nachsendeauftrages von Postdienstunternehmen erhoben wurden, spätestens 2 Jahre nach ihrer Erhebung gelöscht werden.
- Ähnlich eindeutig ist das Telekommunikationsgesetz (TKG), das in seinem § 90 bezüglich der Verkehrsdaten festhält, dass diese 6 Monate nach Versand der Rechnung zu löschen sind.[14] Auch das neue Telemediengesetz (TMG) schreibt in § 15 Nr. 7 vor, dass Abrechnungsdaten, die für die Erfüllung von Einzelnachweisen benötigt werden, höchstens bis zum Ablauf des 6. Monats nach Versand der Rechnung gespeichert werden dürfen.
- Nicht ganz so eindeutig, sondern in einem gewissen Umfang interpretationsoffener sind die Regelungen des Autobahnmautgesetzes (ABMG). Die im Rahmen dieses Gesetzes erhobenen fahrtbezogenen Daten muss der Betreiber gem. § 9 ABMG unverzüglich löschen, wenn ein Mauterstattungsverlangen nicht fristgerecht gestellt worden ist. Andernfalls sind die Daten unverzüglich nach Abschluss eines entsprechenden Reklamationsverfahrens zu löschen.
- Auch da, wo das BDSG selbst konkrete Fristen vorgibt, sind diese selbstverständlich einzuhalten. Insoweit statuiert § 35 Abs. 2 Nr. 4 BDSG für die Unternehmen, die gemäß § 29 BDSG geschäftsmäßig Daten zu Übermittlungszwecken speichern, die unbedingte Pflicht, jeweils am Ende des vierten Kalenderjahres zu prüfen, ob eine länger währende Speicherung einstmals erho-

[12] Siehe Fußnote 5.

[13] Für Datenbestände, die auf der Basis einer Einwilligung des Betroffenen oder auf gesetzlicher Grundlage verarbeitet werden, sind die Löschfristen entsprechend abzuleiten.

[14] Die Probleme mit der Richtlinie zur Vorratsdatenspeicherung werden im Rahmen dieser Erörterung nicht weiter behandelt.

bener Daten noch erforderlich ist. Stellt sich bei dieser Einzelfallprüfung beispielsweise heraus, dass ein Adresshändler die gespeicherten Daten einer bestimmten Person während der vorangegangenen 4-Jahres-Frist keinmal für Werbezwecke vermietet hat, erscheint eine entsprechende Löschung geboten.

Vorgegebene gesetzliche Fristen für die Löschung muss die verantwortliche Stelle einhalten. Eine Ausweitung der Speicherung aus anderen Gründen ist unzulässig. Die verantwortliche Stelle muss daher ihre Geschäftsprozesse und technischen wie organisatorischen Abläufe so anpassen, dass die fristgerechte Löschung erreicht wird. Im Bereich der Telekommunikationsrechnungen wie auch bei der Mautabrechnung wird dies bspw. dadurch erreicht, dass die eigentlichen Abrechnungsbelege unabhängig von den Einzelverbindungsnachweisen bzw. Einzelfahrtnachweisen gestaltet sind. Die sensitiven Detaildaten können daher früh gelöscht werden, ohne gegen die Vorgaben von HGB und AO zu verstoßen.

Für Anwendungsbereiche ohne konkrete rechtliche Fristvorgaben gilt damit aber nicht, dass die Speicherung beliebig ausgedehnt werden kann. Vielmehr bedeutet der Rückgriff auf die allgemeine Regelung des § 35 Abs. 2 BDSG, dass spezifische Löschfristen rechtlich abgeleitet werden müssen.

3.3 Besondere Art der Speicherung

Gemäß § 35 Abs. 3 Nr. 3 BDSG tritt an die Stelle der Löschung die Sperrung von Daten, wenn wegen der besonderen Art der Speicherung die Löschung nur mit unverhältnismäßig hohem Aufwand möglich ist. Diese Regelung bezieht sich auf die Fälle, in denen personenbezogene Daten auf nicht wieder beschreibbare Datenträger, beispielsweise CD-ROMs, ausgelagert sind.[15] Überall da aber, wo Daten in Datenbanken vorgehalten werden, kann eine Löschung unter Verweis auf § 35 Abs. 3 Nr. 3 nicht vermieden werden.[16] Auch ansonsten können unverhältnismäßige organisatorische oder technische Aufwände nicht von den verantwortlichen Stellen gegen die Löschung ins Feld geführt werden. Die Löschung ist, wie eingangs bereits erwähnt, die Wiederherstellung des vom Gesetzgeber gewünschten Zustandes, dass nämlich über natürliche Personen keine personenbezogenen bzw. personenbeziehbaren Daten gespeichert werden sollen.

4 Umsetzung der Löschvorschrift

Normadressat der Löschpflicht ist die verantwortliche Stelle. Die Geschäftsführung muss dieser Verantwortung nachkommen und für ihre Organisation sicherstellen, dass Zuständigkeiten geklärt sind und Anweisungen zur Löschung erteilt werden. Versäumt es die verantwortliche Stelle, die notwendigen Maßnahmen zu ergreifen, trägt sie die volle Organisationsverantwortung. Und es ist die Pflicht des bDSB, seine Geschäftsführung auf entsprechende Versäumnisse hinzuweisen.

4.1 Löschkonzept

Um nachzuweisen, dass die verantwortliche Stelle ihre Löschpflichten im geforderten Umfang wahrgenommen hat, muss sie die Analysen und die Umsetzung der Löschmaßnahmen dokumentieren. Vollständigkeit kann erreicht werden, wenn eine systematische Vorgehensweise gewählt wird – zu empfehlen ist daher ein durchgängiges Löschkonzept mit folgenden Inhalten:

- Regelung der Verantwortlichkeiten: Abgrenzung zwischen den Aufgaben des Datenschutz-Teams und denen der System- oder Informationsverantwortlichen bis hin zur Verantwortung für das Monitoring von Löschfunktionen,
- Identifikation der personenbezogenen Datenbestände ,
- Festlegung der Regellöschfristen für die verschiedenen Datenarten auf der Basis der oben skizzierten Faktoren,
- organisatorische und technische Maßnahmen, die im Einzelnen zur Löschung in den produktiven Prozessen ergriffen werden,
- Steuerung von Auftragnehmern, soweit personenbezogene Daten im Auftrag verarbeitet werden.

Da sich Unternehmen und Geschäftsprozesse kontinuierlich verändern, unterliegen auch die Löschprozesse einem stetigen Wandel. Soll ein Löschkonzept nicht nur die Augenblickskizze eines Unternehmens wiedergeben, sondern als dauerhafter Prozess gelebt werden, ist es schließlich erforderlich, die Anpassung des Löschkonzepts als einen Teil des allgemeinen Change-Managements aufzufassen. Der bDSB wie die anderen Verantwortlichen müssen an diesem Anpassungsprozess mitwirken.

Die Erstellung eines Löschkonzepts erfordert die konzeptionelle und inhaltliche Zusammenarbeit zwischen dem bDSB, der Rechtsabteilung und den IT-Verantwortlichen eines Unternehmens. Die Erstellung eines Löschkonzepts ist also ein interdisziplinäres Projekt, dessen Erfolg wesentlich davon abhängt, dass die Notwendigkeit des Löschkonzepts den Akteuren vermittelt wird. Dies kann gelingen, wenn deutlich wird, dass die Erstellung des Löschkonzepts nicht Selbstzweck ist, sondern vielfältige Vorteile für das Unternehmen erschließt.

4.2 Motivationen für ein Löschkonzept

Das Löschkonzept stellt primär sicher, dass das Unternehmen seinen rechtlichen Verpflichtungen nachkommt, personenbezogene Daten zu löschen (Compliance). Die Löschung nicht mehr erforderlicher personenbezogener Daten verhindert eine unzulässige Vorratsdatenspeicherung. Insoweit wird durch die rechtzeitige Löschung von Daten auch das Risiko vom Bußgeldverfahren minimiert. Dieses Risiko sollte nicht unterschätzt werden, denn je nach Schwere des Verstoßes können Verletzungen des BDSG mit bis zu 25.000,00 € bzw. 250.000,00 € geahndet werden.[17] Insofern sind die Unternehmen gut beraten, die notwendigen Kosten für die Festlegung und Umsetzung von Löschregeln aufzuwenden. Auch einen möglicherweise hohen Gesamtaufwand für die Festlegung und Umsetzung von Löschregeln kann die verantwortliche Stelle nicht als Argument gegen eine Löschung anführen Es geht schließlich um die Einhaltung einer gesetzlichen Pflicht, der im Rahmen der Struktur eines Verbotsgesetzes mit Erlaubnisvorbehalt besondere Bedeutung zukommt.

Organisationsrechtlich bringt insbesondere ein sauber aufgesetzter Change-Prozess den weiteren Vorteil mit sich, dass durch die Einbeziehung eines Datenschutzbeauftragten die gemäß § 4 d BDSG notwendige Vorabkontrolle bei Verfahren automatisierter Verarbeitungen gewährleistet ist. Dadurch wird das Löschkonzept

[15] Vgl. dazu *Gola/Schomerus* § 35, Rdnr. 17.
[16] Wie hier auch: *Gola/Schomerus*, aaO.
[17] Vgl. für den ersten Fall § 43 Abs. 1 Nr. 1 für den Fall einer nicht richtigen Meldung an die Aufsichtsbehörde und für den zweiten Fall § 43 Abs. 2 für den Fall einer zweckändernden Nutzung der Daten durch Weitergabe an Dritte.

gleichzeitig auch ein wesentlicher Bestandteil des Verfahrensverzeichnisses und zum unerlässlichen Hilfsinstrument des betrieblichen Datenschutzbeauftragten. Auch das Datenschutz-Management kann durch die Systematik des Löschkonzepts ggf. verbessert werden.

Ein großer Vorteil des Löschkonzepts liegt darin, dass das Unternehmen mehr Transparenz über seine internen wie auch die im Rahmen der Auftragsdatenverarbeitung ausgelagerten Teile der Geschäftsprozesse gewinnt. Ein lückenlos erstelltes Löschkonzept deckt auf, wo überall personenbezogene Daten verarbeitet werden. Die Transparenz bezieht sich deshalb auch auf entsprechende Geschäftsrisiken. Insoweit ergänzen sich Löschkonzept und Informationssicherheitskonzept, Risikomanagement und Controlling. Das Löschkonzept sichert darüber hinaus – soweit nicht anderweitig erfolgt – dass Verantwortlichkeiten für Prozesse, Informationsbestände und Systeme geregelt werden.

Das Löschkonzept vermag weitere positive Effekte hervorzurufen.[18] Beispielsweise muss klar zwischen Archivbeständen und Backups unterschieden werden, soweit dies noch nicht der Fall ist. Während die Archivsysteme längerfristige Dokumentationen für ausgewählte Datenbestände sicherstellen sollen, muss mit den Backup-Maßnahmen ein Recovery von Systemen unterstützt werden. Für letzteres ist allerdings nur ein kurzer Vorhaltezeitraum erforderlich. Im Löschkonzept werden daher die Bestände in Backups und in Archiven unterschiedlich zu behandeln sein. Als „Nebeneffekt" werden die Aufgaben Backup und Archivierung, ggf. auch über personenbezogene Daten hinaus, zum Vorteil des Unternehmens klarer strukturiert. Die klarere Struktur von Backup und Archivierung sowie auch weitere Prozessoptimierungen in der Folge des Löschkonzepts führen häufig dazu, dass Speicherplatz in nennenswertem Umfang oder Verarbeitungskapazitäten eingespart werden. Durch die Einsparungen kann sogar ein *Return on Invest* bezüglich der Kosten für die Erstellung und Umsetzung des Löschkonzepts erzielt werden.

Schließlich kann das Unternehmen, das sich der Mühe unterzogen hat, ein durchgängiges Löschkonzept zu erstellen, daraus auch in der Außendarstellung insbesondere gegenüber Kunden Vorteile und Nutzen ziehen.

[18] Vgl. dazu auch die Details in *Hammer/ Fraenkel* in diesem Heft.

Fazit

Die fristoffene Regelung des § 35 Abs. 2 Nr. 3 BDSG zwingt Unternehmen zwar einerseits dazu, ein Löschkonzept zu erstellen, andererseits kann nur so die notwenige Flexibilität für die jeweils spezifischen Abläufe erreicht werden. In dem vorstehend ausgeführten Verständnis erweist sich das „hässliche Entlein" Datenlöschung als möglicher Königsweg einer strukturierten und an den Normen des Datenschutzes orientierten Datenverarbeitung. Da der Verarbeitungsprozess von seinem Ende her gedacht wird, werden Optimierungsansätze schneller erkannt bzw. mögliche Fehlentwicklungen von vornherein vermieden. Letztere wären später nur mit wesentlich höherem finanziellen Aufwand zu korrigieren.

Ein durchgängiges Löschkonzept stellt durch organisatorische und technische Maßnahmen sicher, dass zum Ende des Verarbeitungszwecks der datenschutzrechtlich geforderter Zustand hergestellt wird. Es erweist sich auch als notwendige Voraussetzung und wesentlicher Bestandteil des so viel beschworenen Systemdatenschutzes.[19] So trägt ein Löschkonzept im Sinne des Verbotsgrundsatzes des BDSG zugleich dem hohen Schutzgut des Persönlichkeitsrechts der Betroffenen und der Optimierung betrieblicher Abläufe adäquat Rechnung.

Nichts überzeugt im Übrigen mehr als das praktische Beispiel. Dass ein durchgängiges Löschkonzept entwickelt und umgesetzt werden kann, zeigt – am Beispiel von Toll Collect – der folgende Beitrag in diesem Heft.

Literatur

Bolten, R. / Putte, P : Aufbewahrungsnormen und -fristen im Personalbereich, 6. Auflage, Frechen, 2007.

Hammer, V. / Fraenkel, R: Löschkonzept, Beitrag in diesem Heft.

Roßnagel, A.: Handbuch Datenschutzrecht München 2003.

Schaffland, H.-J. / Wiltfang, N.: Bundesdatenschutzgesetz, Berlin, Lieferung 3/2006

Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, München, 6. Auflage 2006

Gola P. / Schomerus, R.: BDSG – Bundesdatenschutzkommentar, 9. Aufl., München, 2007

Bergmann, L. / Möhrle, R. / Herb, A.: Datenschutzrecht, Stuttgart, 33. Ergänzungslieferung August 2006

[19] Statt aller: Dix in *Roßnagel 2003*, S.363 ff.