Ulrich Greveler, Christoph Wegener

Ein Ansatz zur Umsetzung von Löschvorschriften mittels Verschlüsselung

Der Beitrag beschreibt die Verwendung von Verschlüsselungsmethoden zum Löschen von personenbezogenen Daten. Im Rahmen eines Löschkonzeptes erfolgt das eigentliche Löschen dabei durch eine Verschlüsselung in Verbindung mit einer späteren, möglicherweise automatisierten, Vernichtung des verwendeten Schlüsselmaterials. Der hier beschriebene Ansatz könnte dadurch auch komplexeren Organisationen mit verteilten Systemen eine Umsetzung der gesetzlichen Löschvorschriften für personenbezogene Daten ermöglichen und zudem auch zum Schutz der Vorratsdaten im Rahmen der zu erwartenden gesetzlichen Neuregelung der technischen Durchführungsvorschriften bzgl. der Vorratsdatenspeicherung beitragen.

1 Einleitung

In der Praxis werden Löschvorschriften in Bezug auf personenbezogene Daten noch immer vernachlässigt. Der unzureichende Schutz gespeicherter Vorratsdaten war schließlich auch einer der Gründe, die das Bundesverfassungsgericht bewog, die gesetzliche Regelung zur Speicherung der Vorratsdaten zu kippen. Wir stellen in diesem Beitrag einen kryptographisch-technischen Ansatz vor, mit dem Löschverpflichtungen zuverlässig durchgesetzt werden können.

Prof. Dr.-Ing. Ulrich Greveler

lehrt seit 2006 Informatik mit den Schwerpunkten IT-Sicherheit und technischer Datenschutz an der Fachhochschule Münster.
E-Mail: greveler@fh-muenster.de

Dr. Christoph Wegener

CISA, CISM und CBP, ist promovierter Physiker und seit 1999 freiberuflich mit der wecon.it-consulting in den Themen IT-Sicherheit, Datenschutz und Open Source unterwegs. Darüber hinaus ist er als Projektleiter und Berater am Horst Görtz Institut für IT-Sicherheit (HGI) bzw. am Lehrstuhl für Netz- und Datensicherheit der Ruhr-Universität Bochum tätig.
E-Mail: wegener@wecon.net

Personenbezogene Daten müssen spätestens immer dann gelöscht werden, wenn der Zweck ihrer Erhebung entfallen ist oder der Betroffene eine Löschung verlangt. Das deutsche Datenschutzrecht, hier insbesondere der § 35 des Bundesdatenschutzgesetzes (BDSG)[1], sieht ein Löschen personenbezogener Daten immer dann vor, wenn die Speicherung nicht mehr erforderlich ist bzw. wenn die betroffene Person ihr Recht wahrnimmt, auf sie bezogene Daten löschen zu lassen, und keine andere rechtliche Norm diesem Löschvorgang entgegensteht. Ein Löschen von Daten soll dabei zuverlässig sicher stellen, dass ein zukünftiger Missbrauch ausgeschlossen werden kann. In der Praxis bestehen beim Löschen von Daten jedoch immer noch erhebliche Defizite, und die Löschverpflichtung wird aus technisch-organisatorischen und psychologischen Gründen oft nur unzureichend umgesetzt[2]: Vor allem für große Unternehmen mit verteilten Datenbanken und internen wie externen Backup-Lösungen stellen diese Anforderung eine nicht unerhebliche Herausforderung für den datenschutzgerechten Einsatz der verwendeten Informationstechnologie dar.

Die Entscheidung[3] des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung legt zudem fest, dass für die Daten aus der Vorratsdatenspeicherung „*hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes*“ vorliegen müssen, um eine verfassungskonforme Regelung zu treffen. Detailliert wird dies zusätzlich mit der Maßgabe: „*Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben.*“

Der eigentliche Vorgang des irreversiblen Löschens von Daten auf Speichermedien ist zwar keineswegs trivial[4], kann jedoch unter Nutzung etablierter Verfahren mit vertretbarem Aufwand erreicht werden[5]. Der technisch-organisatorische Aufwand ist vor allem dann gering, wenn bereits im Vorfeld ein entsprechender Prozess – insbesondere zur Aussonderung von Datenträgern – geschaffen und dann

1 Im Falle der öffentlichen Stellen der Länder tritt an die Stelle der Anwendung des BDSG natürlich die Anwendung des jeweiligen Landesdatenschutzgesetzes (LDSG). Der Einfachheit halber verzichten wir im Laufe dieses Beitrags aber auf die weitere Unterscheidung zwischen diesen beiden Anwendungsfällen.

2 Siehe beispielsweise *Hammer* und *Fraenkel* in DuD 12/2007, 905 ff

3 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 – 345), online abrufbar unter: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html

4 Die Berichterstattung über Fälle restaurierter personenbezogener Daten auf gebrauchten Festplatten reißt zum Zeitpunkt der Erstellung dieses Beitrages nicht ab.

5 So etwa *Fox* in DuD 2/2009, 110 ff.

mit der notwendigen Sorgfalt ausgeführt wird. Anstelle eines Löschens der eigentlichen Daten auf dem Datenträger kommt dabei oft auch eine mechanische Zerstörung des Datenträgers in Betracht. Mit der DIN EN 15713[6] besteht dabei seit August 2009 auch eine konkrete Vorgabe, wie diese mechanische Zerstörung in Abhängigkeit der Klassifizierung der zu löschenden Daten vorzunehmen ist. Ein Löschen durch mechanisches Zerstören ist auch immer dann notwendig, wenn der Datenträger aufgrund einer Beschädigung nicht mehr in allen Datenbereichen „schreibbar" ist und der Datenbestand damit nicht vollständig durch „Überschreiben" gelöscht werden kann.

Die geeignete Aussonderung veralteter oder beschädigter Datenträger stellt allerdings keinen Ersatz für das ordnungsgemäße Löschen im Sinne des BDSG dar. Dies gilt vor allem dann, wenn Daten regelmäßig zwischen Datenträgern kopiert und damit im Gesamtdatenbestand gehalten werden. Auch unter der zusätzlichen Annahme, dass aufgrund bestehender organisatorischer Maßnahmen mit der Aussonderung von Datenträgern alle betreffenden Daten gelöscht sind, ist die Missachtung von Löschfristen unter Umständen ein Verstoß gegen die Datenschutzbestimmungen und kann durch die §§ 43 und 44 BDSG sowohl zivil- als auch strafrechtliche Konsequenzen haben.

2 Mögliche Anwendungsbereiche

In diesem Beitrag wollen wir eine Möglichkeit vorstellen, das Löschen von Daten durch Nutzung kryptographischer Verfahren – in diesem Fall durch Verschlüsselung in Verbindung mit einem entsprechenden Key-Management – durchzusetzen. Dadurch könnte auch in den Bereichen, die ein Löschen von personenbezogenen Daten aufgrund der Komplexität der beteiligten Systeme und dem damit einhergehenden erheblichen technisch-organisatorischen Aufwand nur schwer und unzureichend umsetzen lassen, ein zuverlässiges Löschen aller entsprechenden Daten erreicht werden. Technische Details des Verfahrens wurden bereits von den Autoren publiziert.[7] Zugleich bietet die Verschlüsselung aller Daten eines Datenträgers auch einen gewissen Schutz bei Verlust des Datenträgers – etwa in Bezug auf mögliche Folgen durch § 42a BDSG[8].

Insbesondere die Diskussion um geeignete Löschmechanismen zur Umsetzung der Vorgaben in Bezug auf die Speicherung von Vorratsdaten kann durch das vorgestellte Verfahren bereichert werden. Neben dem aktuellen Aspekt der Vorratsdatenspeicherung ist die Durchsetzbarkeit von Löschvorschriften zudem für die folgenden, nach BDSG verantwortlichen, Stellen eine große Herausforderung:

- **Betreiber von Archivierungssystemen**
  Wie lässt sich mit vertretbarem Aufwand ein Datum, das „in der Tiefe" des Bandroboters „begraben" liegt, löschen, ohne die möglicherweise bestehenden Speicherfristen für andere archivierte Daten zu verletzen? Wie lassen sich Daten ohne Referenzliste im System sperren?
- **Betreiber von E-Mail-Archivierungssystemen**
  Wie löscht man alle E-Mails eines Mitarbeiters, der ein Unternehmen verlässt und verlangt, dass alle „seine" E-Mails vollständig gelöscht werden?
- **Betreiber großer Datenbanksysteme**
  Die Administratoren lagern sog. Datenbank-Dumps gemäß der gängigen Praxis häufig für längere Zeiträume. Wie löst man die Probleme, die dadurch entstehen, dass die einzelnen Datenfelder zum Teil unterschiedlichen Löschvorschriften unterliegen?
- **Nutzer serviceorientierter Architekturen (SOA)**
  Serviceorientierte Architekturen sehen oft eine Kommunikation verteilter Systeme über den sogenannten SOA-Bus vor, der die Nachrichten für alle Dienste archiviert. Aus diesem Archiv lassen sich aber die bereits in den Datenbanken gelöschten Daten rekonstruieren. Wie kann man nun ein vollständiges Löschen gewährleisten, bei dem sich der entsprechende Löschvorgang immer auch auf einzeln eingebettete Datenfelder der archivierten SOA-Messages erstrecken muss?

Die in diesem Beitrag vorgeschlagene Methode, das Löschen der Daten durch eine Verschlüsselung und die entsprechende Vernichtung der Schlüssel zu ersetzen, stellt dabei eine Alternative zum (technischen) Löschen von Daten dar. Dies gilt zumindest dann, wenn dem verwendeten Krypto-Algorithmus langfristig Vertrauen entgegengebracht werden kann[9] und das Schlüsselmanagement die Anforderungen an die Löschvorschriften für personenbezogene Daten erfüllt. Die verschlüsselten Daten sollten aber über die Löschung des Schlüsselmaterials hinaus zu einem späteren, organisatorisch gut geeignetem Zeitpunkt zusätzlich noch physisch gelöscht werden. Dies wird vor allem vor dem Hintergrund gefordert, dass verwendete Krypto-Algorithmen nicht mehr über mehrere Jahrzehnte hinweg als sicher betrachtet werden können, eine Umverschlüsselung verteilt gespeicherter Daten viele Organisationen jedoch überfordern dürfte.

Die Verschlüsselung ermöglicht insbesondere auch ein gezieltes Löschen einzelner Datenfelder (z. B. Spalten einer Tabelle innerhalb einer relationalen Datenbank) oder Felder von Datensätzen, die vor einem bestimmen Zeitpunkt erfasst wurden (vgl. Speicherungsdauer von sechs Monaten bei der gesetzlichen Regelung zur Vorratsdatenspeicherung). Das durch Vernichtung des zugehörigen Schlüssels vorgenommene Löschen erstreckt sich dann auch auf jede weitere Kopie des gespeicherten Datums. Dabei ist es völlig unerheblich, ob dieses als Kopie im produktiven Datenbankmanagementsystem (DBMS) selbst oder innerhalb eines Abbildes, etwa als Datenbank-Dump, als Archivdatei, als vergessene „temporäre" Kopie oder als Datenfragment auf einer ausgesonderten RAID-Platte[10] vorliegt.

Darüber hinaus lassen sich auch nahezu beliebige Mehr-Augen-Konzepte mit Hilfe kryptographischer Methoden umset-

6 Zu den Details siehe beispielsweise: http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=113162714&bcrumblevel=2&languageid=de

7 *Greveler und Wegener*: „Verschlüsselung personenbezogener Daten zur Umsetzung von Löschvorschriften". Workshop Sicherer Umgang mit sensiblen Daten. „Informatik 2009", Lecture Notes in Informatics P-154

8 Vgl. dazu BT-Drs. 16/12011, S. 52; a. A. *Ernst* in DuD 7/2010, 472

9 Ist langfristige Sicherheit erwünscht, sollte eine simultane Verschlüsselung unter Anwendung mehrerer kryptographischer Algorithmen auf Basis unterschiedlicher mathematischer Verfahren in Betracht gezogen werden.

10 Die weit verbreiteten RAID-Lösungen sehen eine redundante Anordnung unabhängiger physischer Festplatten vor, wobei der Ausfall einzelner Festplatten ohne Datenverlust vom System kompensiert wird. Unzuverlässige Platten können dabei meist im laufenden Betrieb durch neue Platten ersetzt und entsorgt werden. Abhängig vom verwendeten RAID-System enthalten die entsorgten Platten dabei nicht selten den gesamten Datenbestand.

zen[11]. Unter dem Stichwort *Secret Sharing*[12] kann hier durch Aufteilen eines Schlüssels in Teilschlüssel eine Beteiligung mehrerer, unabhängiger Parteien bei einer Dateneinsicht erzwungen werden. Dabei lässt sich auch ein Schwellenwert festlegen, der die Anzahl der mindestens benötigten Teilschlüssel und damit die Anzahl der benötigten Teilnehmer angibt, die kooperieren müssen, damit der eigentliche Datensatz entschlüsselt werden kann. Während sich diese Funktionalität bei nur wenigen Teilschlüsseln (z. B. zwei) auch durch rein organisatorische Maßnahmen umsetzen lassen würde – etwa durch Verteilen der PIN und der zugehörigen physischen Smartcard auf zwei unabhängige Parteien – stößt dieser Lösungsansatz ab etwa vier Teilschlüsseln an seine Grenzen. Hier bietet ein kryptographischer Ansatz die Möglichkeit, einen kontrollierten Zugriff auf personenbezogenen Daten zu gewährleisten.

3 Implementierung und Schlüsselmanagement

Als wichtige Kriterien sind zunächst die Erzeugung und anschließende Verwaltung der zur Verschlüsselung genutzten kryptographischen Schlüssel zu betrachten. Eine Realisierung von Löschvorschriften mittels Verschlüsselung setzt allerdings ein angepasstes Schlüsselmanagement voraus, das die Zuordnung von personenbezogenen Daten zu Löschzeitpunkten und nicht zeitlich festgelegten, aber möglichen Anlässen über die Wahl eines jeweils eindeutigen symmetrischen Schlüssels vornimmt. Soll das Löschen bereits erfolgen, wenn eine von mehreren Bedingungen zutrifft, kann dies durch Verschlüsselung mit einem aus mehreren Schlüsseln zusammengesetzten Schlüssel erfolgen, etwa um eine mehrfache Verschlüsselung und damit potentielle Engpässe der Systemleistung zu vermeiden.

3.1 Generierung der Schlüssel

Wir gehen im Folgenden davon aus, dass zur Verschlüsselung ein etabliertes symmetrisches Verfahren (z. B. nach dem *Advanced Encryption Standard* (AES)) verwendet wird[13]. Zudem sollen alle Schlüssel mit einer festen Länge (z. B. 128 Bit) zufällig und gleichverteilt generiert werden, damit auch eine einfache Verknüpfung[14] von Schlüsseln zur Erzeugung weiterer, abgeleiteter Schlüssel möglich ist. Ohne uns im allgemeinen Fall zu beschränken, setzen wir zudem voraus, dass ein monatliches Löschen der Daten erfolgt, d. h. es wird toleriert, dass zu löschende Daten erst bis zu einem Monat nach dem vorgegebenen Löschzeitpunkt gelöscht werden[15]. Eine Anpassung an kürzere Zeiträume ist natürlich ohne Probleme möglich, wobei sich ein Trade-Off in Bezug auf die Zahl der jeweils benötigten Schlüssel ergibt. Personenbezogene Daten, die nach Ablauf einer Frist gelöscht werden sollen, werden nun vor der Speicherung mit einem *Monatsschlüssel* k_m verschlüsselt, wobei *m* für den Monat steht, mit dessen Ablauf der Schlüssel gelöscht wird. Das genaue Löschdatum liegt dann jeweils innerhalb des angegebenen Monats.

Soll berücksichtigt werden, dass Daten aufgrund eines nicht vorher bestimmten Anlasses gelöscht werden müssen, z. B. weil das Subjekt ein Recht ausübt, Daten löschen zu lassen, die das Subjekt betreffen, kann ein zusätzlicher *Subjektschlüssel* k_s generiert werden, der für diesen Anlass eindeutig ist. Im einfachen Fall genießt das Subjekt *s* dabei ein Löschrecht, bei Existenz mehrerer Löschrechte kann der Schlüssel aber auch in mehrere Subjektschlüssel k_{s1}, k_{s2}, k_{s3}, … untergliedert werden, um mehrere Rechte desselben Subjektes abzubilden.

Die Verschlüsselung der Daten erfolgt zwingend immer vor der erstmaligen Speicherung des Datums. Das Löschkonzept muss daher in jedem Fall bereits zum Zeitpunkt der Datenerfassung festlegen, welche Löschvorschriften zu beachten sind. Zum Verschlüsseln wird dann der ermittelte bzw. berechnete Schlüssel herangezogen. Der organisatorische und technische Aufwand für die Umsetzung der Löschvorschriften mittels Verschlüsselung entsteht hier vor allem bei der Erstellung des Löschkonzeptes selbst und der anschließenden Anpassung der Systemlandschaft. Zur Laufzeit kann das Löschen im produktiven System aber durch gezieltes Löschen einzelner Schlüssel und damit mit sehr geringem Aufwand erfolgen.

3.2 Zugriff auf die Schlüssel und Löschen der Schlüssel

Der Zugriff auf die Schlüssel, die im Rahmen des Löschkonzeptes verwendet werden, muss für die datenerfassende Partei und bei einem das Datum betreffenden Verarbeitungsschritt für die verarbeitende Partei unmittelbar möglich sein. Schlüssel können dabei wahlfrei im Arbeitsspeicher eines IT-Systems gehalten werden, wenn zu jedem Zeitpunkt sichergestellt ist, dass Abbilder des Arbeitsspeichers (z. B. automatisch generierte Speicherauszüge bei Fehlfunktionen) nicht existieren oder zumindest ebenfalls dem Löschkonzept unterworfen sind und auf keinen Fall im Klartext archiviert werden. Sind die Anforderungen an die Zuverlässigkeit des späteren Löschens sehr hoch, ist gegebenenfalls die Verwendung eines Hardware-Sicherheitsmoduls (HSM) oder einer Smartcard in Betracht zu ziehen, so dass eine Preisgabe der Schlüssel außerhalb des Moduls technisch wirksam verhindert werden kann[16].

Zur Laufzeit des Systems erfolgt die Entschlüsselung für die Datenverarbeitungskomponenten transparent, dazu ermöglicht eine vor- und nachgeschaltete Komponente die Entschlüsselung beim Lesen bzw. die Verschlüsselung beim Schreiben. Die Prozessorleistung heutiger IT-Systeme ist auch bei der Verarbeitung großer Datenmengen ausreichend, um eine spürbare Latenz bei einzelnen Ver- und Entschlüsselungsvorgängen zu vermeiden. Problematisch wird es jedoch in den Fällen, die einen Abgleich großer Datenmengen bzw. komplexe relationale Operationen auf verschlüsselten Daten erfordern. In diesen Fällen ist zu prüfen, ob das DBMS selbst ohne Verletzung der Löschvorschriften

11 Vgl. dazu auch die Forderungen des BVerfG in 1 BvR 256/08, Rn. 225.

12 Grundlage dazu ist der Beitrag von *Shamir* „How to Share a Secret", Communications of the ACM, 11/1979, 612-613.

13 Das BSI gibt in seiner technischen Richtlinie BSI-TR 02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" entsprechende Empfehlungen, die aktuelle Fassung (Stand Juni 2008) findet sich online unter: https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30924/BSI-TR-02102_V1_0_pdf.pdf

14 Hierzu kann dann beispielsweise eine bitweise Addition (sog. *XOR-Verknüpfung*) herangezogen werden.

15 Dies entspricht beispielsweise den Regelungen zur Vorratsdatenspeicherung nach dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung", das am 1. Januar 2008 in Kraft trat und in § 113a, Abs. 11 TKG ein Löschen innerhalb eines Monats nach Ablauf der Speicherpflicht vorsieht.

16 Wenn man die technische Sicherheit des verwendeten Sicherheitsmoduls (Smartcard oder HSM) voraussetzt, lässt sich die Preisgabe des Schlüssels auch bei Verlust des Schlüsselträgers wirksam verhindern, wenn dieser etwa mittels einer zufälligen, nicht auf dem Modul vermerkten, PIN geschützt ist.

auf unverschlüsselten Daten im Speicher operieren kann, um rechenaufwändige Operationen auszuführen.

Ist dies nicht möglich bzw. aus konzeptionellen Erwägungen heraus nicht gewünscht, kann die Operation auch so durchgeführt werden, dass bei jedem Zugriff auf ein einzelnes Datum die Ent- bzw. Verschlüsselung erfolgt, was jedoch eine Vielzahl von Krypto-Operationen bei Ausführung einer einzelnen Abfrage erforderlich macht. Hier muss eine Abschätzung der maximalen Anzahl erforderlicher Krypto-Operationen während der Planungsphase erfolgen, um Leistungsengpässe im produktiven Betrieb auszuschließen. Bei der technischen Umsetzung ist daher die Art der Datennutzung zu berücksichtigen, Änderungen der Nutzung (z. B. Einführung neuer datenbankbasierter Dienste) erfordern eine Überprüfung des Lösch- und damit des Verschlüsselungskonzeptes unter Systemleistungsgesichtspunkten.

Das Löschen des Schlüssels selbst erfolgt als nachvollziehbarer Vorgang (eine sog. „revisionssichere Protokollierung" wird ermöglicht). Alle Schlüssel-speichernden Objekte innerhalb der Systemlandschaft müssen das Löschen auf Anforderung bzw. selbsttätig zu einem bestimmten Zeitpunkt jeweils unter Erzeugung eines Protokolleintrags vornehmen. Wird als Schlüsselträger beispielsweise eine Smartcard verwendet, kann die Vernichtung derselben anhand der DIN EN 15713[17] physisch erfolgen, und die zerstörte Karte kann als Beweismittel für ein späteres Datenschutzaudit archiviert werden. Ein Hardware-Sicherheitsmodul (HSM) bzw. eine Lösung auf Basis vertrauenswürdiger Hardware als Schlüsselträger würde das Löschen der Schlüssel mit einem elektronisch signierten Protokoll bestätigen. Hierbei ist über den Weg der Signaturüberprüfung auch eine Auditierung der Schlüsselvernichtung aus der Ferne möglich. Der Nachweis gegenüber einem Datenschutzbeauftragten, der hier im Sinne der organisatorischen Kontrolle tätig wird und das Protokoll überprüft, kann dann an einem zentralen Standort erbracht werden, auch wenn die Systeme verteilt und ggf. weit entfernt betrieben werden.

17 Vgl. Fn. 6

3.3 Schlüsselbackups

Ein wesentlicher Einwand gegenüber der verschlüsselten Speicherung von Daten innerhalb produktiver Systeme betrifft die Verfügbarkeit beim Verlust von Schlüsseln bzw. bei Verlust oder Fehlfunktion einer Smartcard bzw. eines HSM als Schlüsselträger. Um die Verfügbarkeit auch bei vorzeitigem Verlust eines Schlüssel(träger)s sicherstellen zu können, ist das Löschkonzept in jedem Fall um eine Beschreibung eines Schlüsselbackups und entsprechender organisatorischer Maßnahmen zum Umgang mit den Schlüsselkopien zu erweitern.

Schlüssel, die auf einer Smartcard generiert und gespeichert werden, können unter Nutzung kryptographischer Protokolle dupliziert werden. Dann existiert nach Generierung und Duplizierung der Schlüssel eine Menge $SC_i = SC_2 \ldots SC_n$ vom Smartcards, die als Backup für die Smartcard SC_1, die im Produktivsystem eingesetzt wird, zur Verfügung stehen. Zum Löschzeitpunkt sind dann neben der produktiven Smartcard auch alle Backup-Schlüssel (= Smartcards $SC_2 \ldots SC_n$) zu vernichten. Die Backup-Smartcards sind bei dieser Vorgehensweise während der Lebenszeit der darauf gespeicherten Schlüssel in einem besonders geschützten Bereich – etwa dem Tresor des Datenschutzbeauftragten – aufzubewahren, so dass ein Zugriff bzw. ein Kartenaustausch dokumentiert und protokolliert wird und ein unbefugtes Verwenden der Backup-Smartcards ausgeschlossen ist. Die Einbeziehung des Datenschutzbeauftragten oder anderer (externer) Personen kann zudem auch über die Vergabe der PIN bei den Backup-Smartcards technisch erzwungen werden.

3.4 Integration in bestehende Datenbankkonzepte

Eine technische Umsetzung des Löschkonzeptes wird in der betrieblichen Praxis in den meisten Fällen für bereits bestehende Systeme erfolgen. Zudem werden Systemkomponenten, die für eine Datenhaltung verschlüsselter Daten bisher nicht vorgesehen waren, in neue datenschutzfreundliche Systeme zu integrieren sein. Eine wesentliche Problematik stellt hierbei die Tatsache dar, dass verschlüsselte Daten keine syntaktische Struktur mehr aufweisen. Anhand des Chiffrats ist somit nicht erkennbar, um welche Art von Daten es sich handelt bzw. welche Datenformate den Klartextdaten zu Grunde liegen. Während dies aus Sicherheitsbetrachtungen heraus durchaus eine gewünschte und notwendige Eigenschaft darstellt – aus verschlüsselten Daten soll schließlich keinerlei Information über die Klartextdaten zu ermitteln sein – führt dies bei der Datenhaltung immer dann zu Problemen, wenn einzelne Systemkomponenten eine Syntax von Datensätzen (etwa zur Speicherung in Datenbanken) voraussetzen.

Eine Verschlüsselung einer Kreditkartennummer, die als Byte-Folge (jede Ziffer entspricht einem Byte, das die ASCII-Kodierung der Ziffern 0 bis 9 enthält) innerhalb eines Datensatzes vorliegt, führt beispielsweise immer zu einer Chiffrat-Bytefolge, die sämtliche Werte eines Bytes aufweisen kann, d. h. insbesondere nicht auf die Ziffern 0 bis 9 beschränkt ist. Der Versuch, dieses Datum verschlüsselt in derselben Datenbank mit unveränderter Attribut-Definition zu speichern, schlägt dann regelmäßig fehl, weil syntaktische Nebenbedingungen verletzt werden. Die Integration bestehender Systeme ist jedoch ohne Änderungen der Datendefinitionen – und damit ohne Anpassung der bestehenden Komponenten – möglich, wenn Datenformat-erhaltende Verschlüsselungsverfahren Anwendung finden[18] [19]. Diese Verfahren sehen eine Modifikation der Ver- und Entschlüsselung in der Art und Weise vor, dass der syntaktische Aufbau der Datensätze im Zuge der Verschlüsselung nicht zerstört wird. Allerdings sind diese Methoden aus kryptographischer Sicht zum jetzigen Zeitpunkt noch nicht ausreichend in der Praxis untersucht und sollten daher mit besonderer Vorsicht eingesetzt werden. Darüber hinaus gibt es mit der sog. *homomorphen Verschlüsselung* einen weiteren Ansatz, der in der Forschung aktuell untersucht wird[20], jedoch noch nicht das Stadium der Integration in Produkte und Lösungen erreicht hat.

Die beginnende Verbreitung von serviceorientierten Architekturen ermöglicht eine Rolle des SOA-Bussystems, das

18 *Black* und *Rogaway* in Lecture Notes In Computer Science, 2271 (2000)

19 *Probst* in Datenschutzberater, 3 (2009); Details zum dort angesprochenen Verfahren unter: http://www.voltage.com/technology/format-preserving-encryption.htm

20 Beispielsweise *Gantry* "Fully homomorphic encryption using ideal lattices" in Proceedings of the 41st annual ACM symposium on Theory of computing, 2009, 169-178.

die Nachrichten der einzelnen verteilten Systeme entgegennimmt und weiterreicht, als kryptographischer Dienstleister. Daten können hier nach ihrer Erfassung verschlüsselt werden, das erfassende System gibt diese an den SOA-Bus weiter, der Bus reicht das Datum dann verschlüsselt zur Speicherung an das DBMS weiter. Eine Änderung ist bei Anwendung unseres Verfahrens bei beiden Komponenten nicht erforderlich. Bei Anforderung eines verschlüsselt vorliegenden Datums kann der SOA-Bus transparent die Entschlüsselung vornehmen, so dass keine weitere Schlüssel-speichernde Partei in der Architektur benötigt wird.

4 Abgrenzung der rechtlichen Begriffe: Verschlüsseln statt Löschen bzw. Sperren

Rechtlich ist der Aspekt des Löschens von personenbezogenen Daten nicht so zu fassen, dass eine technische Realisierung des Löschens in jedem Falle als zulässig oder unzulässig betrachtet werden kann. Hier mangelt es nach Meinung der Autoren an einer übergreifenden juristischen Definition für genau diesen Sachverhalt. Hilfreich ist in diesem Punkt aber das Bundesdatenschutzgesetz (BDSG), das in § 3, Abs. 4, Nummer 5 eine Definition für das Löschen von Daten gibt: „*Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.*“

Die Interpretation, dass ein entsprechendes Datum so verändert wird, dass der eigentliche Inhalt nicht mehr kenntlich ist, was durch eine Verschlüsselung und Vernichtung des Schlüssels zuverlässig erreicht werden kann, erscheint hier juristisch nachvollziehbar. Den Autoren ist jedoch bisher keine richterliche Entscheidung zu dieser Interpretation bekannt geworden. In der Papierwelt lässt sich die Forderung gemäß anerkannter Vorgehensweisen durch das Schwärzen von entsprechenden Daten umsetzen, in der elektronischen Welt könnte man Löschen etwa durch Überschreiben mit nicht interpretierbaren Daten (= pseudozufälligen Bits) erzielen. Ähnliche Definitionen finden sich auch in den entsprechenden Landesdatenschutzgesetzen, beispielsweise dem Landesdatenschutzgesetz NRW (DSG NRW), hier in § 3, Abs. 2, Nummer 6: „*Löschen (Löschung) – das Unkenntlichmachen gespeicherter Daten.*“

Wichtig ist in diesem Zusammenhang noch die Abgrenzung zum *Sperren* von Daten, vgl. hierzu auch § 3, Abs. 4, Nummer 4 BDSG: „*Sperren – das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.*“ Während es beim Löschen wie bereits beschrieben um das Unkenntlichmachen geht, lässt sich das Sperren eher mit einer Markierung (*Datum nicht preisgeben oder verarbeiten!*) vergleichen. Die Verschlüsselung könnte bereits als Sperrung im Sinne des BDSG betrachtet werden, wenn über den Schlüssel nicht mehr frei verfügt werden kann (der Schlüssel also selbst einer *Sperrung* unterliegt). Das Löschen des Schlüssels geht jedoch über die Anforderungen der Sperrung, die bereits als Ersatzhandlung bei unangemessenen Löschaufwänden vorgesehen ist, hinaus.

Die Frage, ob es sich bei der oben beschriebenen Methode nun um ein Löschen von Daten im Sinne des BDSG bzw. der DSG NRW und damit mangels weiterer juristischer Definitionen um ein Löschen im rechtlichen Sinne handelt, ließe sich mit Hilfe der Definition aus dem BDSG beantworten. Ein Datum, das durch einen modernen, allgemein akzeptierten kryptographischen Algorithmus (etwa AES-128) verschlüsselt wurde, ist damit für denjenigen unkenntlich gemacht, der nicht im Besitz des passenden Schlüssels ist. Somit führte die Vernichtung des passenden Schlüssels in jedem Fall dazu, dass dieses Datum unkenntlich gemacht wurde, und damit zu einer Löschung im Sinne des BDSG. Dies könnte damit auch den Anforderungen an Datenlöschungen, etwa im Sinne des Telekommunikationsgesetzes (TKG) und anderer Vorschriften, genügen, sofern entsprechende Begleitverordnungen einer gesetzlichen Neuregelung den hier beschriebenen Ansatz zulassen und der vom Bundesverfassungsgericht geforderte „besonders hohe Standard der Datensicherheit“ beim Löschen der Daten[21] damit erfüllt wäre.

5 Fazit

Die unzureichende Umsetzung von Löschvorschriften in der betrieblichen Praxis ist u. a. der Komplexität verteilter Anwendungen geschuldet. Das zuverlässige Löschen personenbezogener Daten, das in einem Spannungsfeld zur – meist als vorrangig empfundenen – Aufbewahrungspflicht kaufmännisch relevanter Vorgänge steht, ist keine triviale technische und organisatorische Aufgabe.

Angesichts der Skandale um sogenannte Datenpannen rückte aber auch die Löschpflicht wieder in das Zentrum der Aufmerksamkeit – noch bevor das Bundesverfassungsgericht sein Urteil zur Unzulässigkeit der Vorratsdatenspeicherung fällte. Denn gelöschte Daten entziehen sich jedem Missbrauch, da eine zukünftige Preisgabe – fahrlässig wie vorsätzlich – ausgeschlossen ist.

Das Löschen über dem Umweg einer Verschlüsselung im Vorfeld in Verbindung mit der späteren Vernichtung des verwendeten Schlüssels stellt sich nur auf den ersten Blick als Verkomplizierung eines einfachen Vorgangs dar. Nach Berücksichtigung tatsächlicher Umstände – der Überblick über existierende Kopien personenbezogener Daten innerhalb einer Organisation ist oft nicht gegeben – wird dadurch jedoch überhaupt erst ein realistischer Prozess ermöglicht, Löschvorschriften umzusetzen, die sonst in existierenden betrieblichen Abläufen schlicht ignoriert werden.

Über den Aspekt der Löschpflicht hinaus bewirkt eine Verschlüsselung aller personenbezogenen Daten zudem einen Gewinn an technischem Datenschutz, da Möglichkeiten einer missbräuchlichen Weitergabe (z. B. über ausgesonderte Datenträger) eingeschränkt werden. So hat auch das Bundesverfassungsgericht für die Daten bzgl. der Vorratsdatenspeicherung eine Verschlüsselung in Verbindung mit einem Mehr-Augen-Prinzip gefordert, um den Zugriff auf diese sensiblen Daten kontrollieren zu können.

Dieser „positiven Nebenwirkung“ steht allerdings auch ein nicht zu unterschätzender Aufwand entgegen, die Ver- und Entschlüsselungsoperationen in die technischen betrieblichen Abläufe störungsfrei zu integrieren. Nutzt man dazu moderne serviceorientierte Strukturen und Möglichkeiten der sanften Integration von Alt-Systemen, ist der Aufwand aber beherrschbar, und die Organisation kann ihren Verpflichtungen in Bezug auf die Speicherung und Verarbeitung personenbezogener Daten nachkommen.

21 Vgl. Rn. 221 und 222 des Urteils BvR 256/08 vom 2.3.2010.