Verschlüsselung personenbezogener Daten zur Umsetzung von Löschvorschriften

Ulrich Greveler[1] · Christoph Wegener[2]

[1]Labor für IT-Sicherheit, Fachhochschule Münster
greveler@fh-muenster.de

[2]Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum
christoph.wegener@rub.de

Abstract: Der nachfolgende Beitrag schlägt die Verwendung von Verschlüsselungsmethoden als Ersatz zum technischen Löschen von personenbezogenen Daten vor. Im Rahmen eines Löschkonzeptes erfolgt das eigentliche Löschen dabei durch eine Verschlüsselung in Verbindung mit einer späteren Vernichtung des verwendeten Schlüsselmaterials. In der Praxis werden entsprechende Löschvorschriften in Bezug auf personenbezogene Daten nicht selten vernachlässigt. Oft ist dies der Fall, wenn bereits während der Verarbeitung der Daten unzählige Kopien entstehen, die sich im Nachhinein nicht mehr ohne erheblichen organisatorischen bzw. technischen Aufwand durch den Löschvorgang zuverlässig erfassen lassen. Unser Ansatz ermöglicht nun auch komplexen Organisationen mit verteilten Systemen eine Umsetzung der gesetzlichen Löschvorschriften für personenbezogene Daten und kann damit entscheidend zu einem höheren Datenschutzniveau beitragen.

1 Motivation

Personenbezogene Daten müssen spätestens dann gelöscht werden, wenn der Zweck ihrer Erhebung entfallen ist oder der Betroffene eine Löschung verlangt. Für große Unternehmen mit verteilten Datenbanken und internen wie externen Backup-Lösungen stellt diese Anforderung allerdings eine nicht unerhebliche Herausforderung für den datenschutzgerechten Einsatz der verwendeten Informationstechnologie dar. Das deutsche Datenschutzrecht – hier insbesondere § 35 des Bundesdatenschutzgesetzes (BDSG) – sieht ein Löschen personenbezogener Daten stets 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 der Daten ausgeschlossen wird. 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 [HF07].

Der technische Vorgang des irreversiblen Löschens von Daten auf Speichermedien – wie

etwa Festplatten oder USB-Sticks – ist zwar keineswegs trivial[1], kann jedoch unter Nutzung etablierter Verfahren mit vertretbarem Aufwand erreicht werden [Fox09]. Der technisch-organisatorische Aufwand ist vor allem dann gering, wenn bereits im Vorfeld ein entsprechender Prozess – insbesondere zur Aussonderung von Datenträgern – geschaffen und dann mit der notwendigen Sorgfalt ausgeführt wird.

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 ein eklatanter Verstoß gegen die Datenschutzbestimmungen und kann sowohl zivil- als auch strafrechtliche Konsequenzen nach sich ziehen. In diesem Zusammenhang sind insbesondere die §§ 43 und 44 BDSG zu beachten.

1.1 Anwendungsbereiche

In diesem Beitrag wollen wir eine Möglichkeit untersuchen, das Löschen von Daten durch Nutzung kryptographischer Verfahren – in unserem 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 den damit einhergehenden erheblichen technisch-organisatorischen Aufwänden nur schwer und unzureichend umsetzen lassen, ein zuverlässige Löschen aller entsprechenden Daten erreicht werden. In diesem Zusammenhang ist die Durchsetzbarkeit von Löschvorschriften insbesondere 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?
- Betreiber von E-Mail-Archivierungssystemen
  Wie löscht man alle E-Mails eines Mitarbeiters, der ein Kunden-Unternehmen verlässt und verlangt, dass alle „seine“ E-Mails vollständig gelöscht werden?
- Betreiber großer Datenbanksysteme
  Die Administratoren lagern 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?

[1] Die Berichterstattung über Fälle restaurierter personenbezogener Daten auf gebrauchten Festplatten reißt zum Zeitpunkt der Erstellung dieses Beitrages nicht ab. [Bri08]

- Mobilfunk-, Internet- und E-Mail-Provider
  Die Datenspeicherung gemäß Vorratsdatenspeicherung nach § 113a des Telekommunikationsgesetzes (TKG) stellt eine Herausforderung dar, da hier die anfallenden Daten in der Regel innerhalb des auf die Speicherfrist folgenden Monats zu löschen sind (§ 113a, Abs. 11 TKG). Wie lässt sich dieser Prozess adäquat umsetzen?

- 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 logisch bereits gelöschte 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 eine dabei eine interessante Alternative zum (technischen) Löschen von Daten dar. Dies gilt zumindest dann, wenn dem verwendeten Krypto-Algorithmus langfristig Vertrauen entgegengebracht werden kann und das Schlüsselmanagement die Anforderungen an die Löschvorschriften für personenbezogene Daten erfüllt. Die verschlüsselten Daten können dann zu einem späteren Zeitpunkt zusätzlich noch physikalisch gelöscht werden. Dies wird vor allem regelmäßig dann der Fall sein, wenn der verwendete Krypto-Algorithmus nicht mehr als sicher betrachtet werden kann.

Die Verschlüsselung ermöglicht insbesondere 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. Das durch Vernichtung des zugehörigen Schlüssels vorgenommene Löschen erstreckt sich dann auch auf jede weitere Kopie des gespeicherten Datums. Dabei ist es völlig unerhelblich, 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 vorliegt.

Darüber hinaus lassen sich auch nahezu beliebige Mehr-Augen-Konzepte mit Hilfe kryptographischer Methoden umsetzen. Unter dem Stichwort *Secret Sharing* [Sha79] kann hier durch Aufteilen eines Schlüssels k in n Teilschlüssel k_i eine Beteiligung mehrerer, unabhängiger Parteien bei einer Dateneinsicht erzwungen werden. Dabei lässt sich auch ein Schwellenwert $m < n$ festlegen, der die Anzahl der mindestens benötigten Teilschlüssel und damit die Anzahl der benötigten Teilnehmer angibt, die zusammen spielen müssen, damit der eigentliche Datensatz entschlüsselt werden kann. Während sich diese Funktionalität bei kleinem n auch durch rein organisatorische Maßnahmen umsetzen lassen würde – etwa durch Verteilen der PIN und der zugehörigen physikalischen Smartcard auf zwei unabhängige Parteien – skaliert dieses Vorgehen bei einem $n \approx 5$ sicherlich nicht mehr. Hier bietet ein Ansatz nach Shamir dann die Möglichkeit, einen kontrollierten Zugriff auf personenbezogenen Daten zu gewährleisten.

2 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.

2.1 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. Zudem sollen alle Schlüssel mit einer festen Länge (z. B. 128 Bit) zufällig und gleichverteilt generiert werden, damit auch eine XOR-Verknüpfung von Schlüsseln zur Gewinnung 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[2]. Eine Anpassung an beliebige kürzere Zeiträume ist möglich, wobei sich allerdings 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 dessem Ablauf der Schlüssel gelöscht wird. Das genaue Löschdatum liegt dann jeweils innerhalb des angegebenen Monats.

Soll berücksichtigt werden, dass Daten aufgrund eines nicht vorherbestimmten 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 $k_{s_1}, k_{s_2}, k_{s_3}, \ldots$ 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 Schlüssel k_m bzw. k_s herangezogen bzw. zunächst ein Schlüssel $k_m \oplus k_s$ bzw. $k_m \oplus k_{s_1} \oplus k_{s_2} \oplus \ldots$ gebildet, wenn mehrere Vorschriften zutreffen. Der or-

[2] 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.

ganisatorische 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 mit geringem Aufwand durch einzelne Löschungen der Schlüssel erfolgen.

2.2 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) ebenfalls dem Löschkonzept unterworfen sind und auf keinen Fall 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, das eine Preisgabe der Schlüssel außerhalb des Moduls wirksam verhindern kann.

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 auf unverschlüsselten Daten im Speicher operieren kann, um rechenaufwändige Operationen (z. B. lesend zugreifende Queries, die einen *Join*-Operator enthalten) auszuführen. In diesem Fall wäre eine Entschlüsselung eines Teildatenbestandes für den Arbeitsspeicher einmalig nach jedem Löschvorgang vorzunehmen.

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 *Query* 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 Löschkonzeptes unter Systemleistungsgesichtspunkten.

Das Löschen des Schlüssels selbst erfolgt als nachvollziehbarer (auditierbarer) Vorgang. Alle schlüsselspeichernden Objekte innerhalb der Systemlandschaft müssen das Löschen auf Anforderung bzw. selbsttätig zu einem bestimmten Zeitpunkt jeweils unter Erzeu-

gung eines Protokolls vornehmen. Wird als Schlüsselträger beispielsweise eine Smartcard verwendet, kann die Vernichtung derselben physikalisch erfolgen, und die zerstörte Karte kann als Beweismittel für ein Datenschutzaudit archiviert werden. Ein Hardware-Sicherheitsmodul bzw. eine Trusted-Computing-Lösung als Schlüsselträger kann das Löschen des Schlüssel mit einem elektronisch signierten Protokoll bestätigen. Hierbei ist eine Auditierung der Schlüsselvernichtung auch aus der Ferne möglich. Der Nachweis gegenüber einem Datenschutzbeauftragten, der hier im Sinne der organisatorischen Eigenkontrolle tätig wird und das Protokoll überprüft, kann dann beispielsweise an einem zentralen Standort erbracht werden.

2.3 Schlüsselbackups

Ein wesentlicher Einwand gegenüber der verschlüsselten Speicherung von Daten innerhalb produktiver Systeme betrifft die Verfügbarkeit beim Verlust von Schlüsseln bzw. beim 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 $SC_i = SC_2 \dots SC_n$ 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 $SC_2 \dots SC_n$) zu vernichten. Die Backup-Smartcards $SC_2 \dots SC_n$ 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 kann zudem auch über die Vergabe der PIN bei den Backup-Smartcards oder durch die zusätzliche Verwendung von Secret Sharing organisatorisch bzw. technisch erzwungen werden.

2.4 (Sanfte) Integration in bestehende Datenbankkonzepte

Eine technische Umsetzung des Löschkonzeptes wird in der betrieblichen Praxis in den allermeisten Fällen für bereits bestehende Systeme erfolgen. Auf der anderen Seite 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 keine 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 Ziffer 0 – 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 – 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 datenformaterhaltende Verschlüsselungsverfahren Anwendung finden [BR00, Pro09]. 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 einige dieser Methoden aus kryptographischer Sicht derzeit nicht ausreichend untersucht; die Verwendung sollte sich auf solche Methoden beschränken, deren Sicherheitsniveau mit etablierten Blockchiffren vergleichbar ist.

Die beginnende Verbreitung von serviceorientierten Architekturen ermöglicht eine Rolle des SOA-Bussystems, das 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 schlüsselspeichernde Partei in der Architektur benötigt wird.

2.5 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 an einer übergreifenden juristischen Defintion 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 Landesdatenschutzgsetzen, 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 sich das Löschen – wie bereits beschrieben – auf das Unkenntlichmachen bezieht, entspricht das Sperren einer Markierung (*Datum nicht preisgeben oder verarbeiten*!) des Datums. 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 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 Defintionen um ein Löschen im rechtlichen Sinne handelt, lässt sich mit Hilfe der Defintion 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 führt 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 sollte damit zunächst auch den Anforderungen an Datenlöschungen, etwa im Sinne des Telekommunikationsgesetzes (TKG) und anderer Vorschriften, genügen.

3 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 Aufgabe. Angesichts aktueller Skandale um sogenannte Datenpannen rückt aber auch die Löschpflicht wieder in das Zentrum der Aufmerksamkeit, denn gelöschte Daten entziehen sich jedem Missbrauch, da eine zukünftige Preisgabe – fahrlässig wie vorsätzlich – ausgeschlossen ist.

Das Löschen über dem Umweg der 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 Um-

stände – 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 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. Dieser „positiven Nebenwirkung“ steht allerdings auch ein nicht zu unterschätzender Aufwand entegegen, 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.

Literatur

[BR00] J. Black und P. Rogaway. Ciphers with Arbitrary Finite Domains. *Lecture Notes In Computer Science*, 2000.

[Bri08] Volker Briegleb. Erneut Festplatte mit Daten britischer Bürger verkauft. *Heise Online vom 27. August 2008, 18:37 Uhr*, 2008.

[Fox09] Dirk Fox. Sicheres Löschen von Daten auf Festplatten. *DuD Datenschutz und Datensicherheit*, (2):110–113, 2009.

[HF07] Volker Hammer und Reinhard Fraenkel. Rechtliche Löschvorschriften. *DuD Datenschutz und Datensicherheit*, (12):899–904, 2007.

[Pro09] Thomas Probst. Verschlüsselung: Neue Ansätze und Ideen. *Datenschutzberater*, 2009.

[Sha79] Adi Shamir. How to Share a Secret. *Communications of the ACM*, (11):612–613, 1979.