

## **Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Un- ternehmen**

Bremerhaven, 16.05.2007

Unser Zeichen: 10-500-03.06/1#4

Version 1.0 vom 16. Mai 2007

Am Ende der Produktionskette bei öffentlichen wie bei nichtöffentlichen Stellen steht das Löschen von Datenträgern mit personenbezogenen Daten und deren Entsorgung. Hierbei kann es sich z. B. um einzelne Ausdrucke, geheftete Vorgänge, Akten oder ganze Aktensammlungen in Papierform oder aber auch um elektronische Datenträger verschiedener Art handeln. Leider wird gerade die Löschung, dabei insbesondere die Vernichtung des Datenträgers, oft nicht als eine Phase der Datenverarbeitung erkannt (§ 2 Abs. 2 Nr. 6 BremDSG, § 3 Abs. 4 BDSG) und werden die gesetzlichen Anforderungen des Datenschutzes häufig vernachlässigt. So fehlen bei öffentlichen und nichtöffentlichen Stellen gerade für die „letzte Phase“ der Datenverarbeitung oft geeignete Regelungen, die einen unzulässigen Umgang mit personenbezogenen Daten vermeiden helfen.

Es empfiehlt sich daher, dass die für die Datenverarbeitung verantwortlichen Stellen Konzepte für eine datenschutzgerechte Löschung und Entsorgung erstellen, die erforderlichenfalls an die Löschfristen anknüpfen und präzise Regelungen für die Löschung und Entsorgung von nicht mehr benötigten Datenträgern mit personenbezogenen Inhalten enthalten. In diesen Konzepten sind technische und/oder organisatorische Maßnahmen festzulegen, die in das übergreifende Datenschutz- bzw. Sicherheitskonzept integriert werden und eine sichere Löschung von Daten bei Verkauf oder Vermietung, Aussonderung, Rückgabe, Reparatur, Wartung und letztendlicher Vernichtung von Datenträgern gewährleisten.

Wichtig für das sichere Löschen von Daten ist darüber hinaus die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers durch geeignete Information und Schulung. Es müssen Maßnahmen festgelegt werden, die ein datenschutzgerechtes Verfahren

regeln. Um Mängel bei der Datenträgerentsorgung zu vermeiden, sollten auf der Basis des jeweiligen Konzeptes Anordnungen an die Mitarbeiter erlassen werden.

Die Erstellung eines geeigneten und angemessenen Konzeptes zur Löschung und Entsorgung von Datenträgern erfordert nach einer fachlichen Analyse detaillierte Festlegungen zu folgenden Punkten:

### **Feststellung der in der Behörde/dem Unternehmen anfallenden Datenträger und der dort aufbewahrten bzw. gespeicherten Daten**

In allen öffentlichen und nichtöffentlichen Stellen gibt es eine Vielzahl von Daten, die auf ganz unterschiedlichen Datenträgern verarbeitet werden. Als Datenträger finden u. a. Papier, Akten, Festplatten, CD, DVD, Disketten, Speicherkarten, ZIP-, Audio-, Videokassetten, Tonbänder, Mikrofilme, Folien, Farbbänder und Stempel Verwendung. Zunächst sollte daher analysiert werden, welche Daten auf welchen Datenträgern verarbeitet werden. Die Fortentwicklung der Technik und andere Gründe können im Laufe der Zeit dazu führen, dass bisherige Datenträger nicht mehr zum Einsatz gelangen und andere Datenträger verwendet werden. Die aufbewahrten bzw. gespeicherten Daten unterliegen in der Regel unterschiedlichen Sicherheitsanforderungen. Es sollte daher auch eine „Klassifikation“ der Daten vorgenommen werden. Geprüft werden sollte grundlegend, ob es sich um personenbezogene oder nicht personenbezogene Daten handelt. Darüber hinaus können die Daten unterschiedlichen Schutz- und Vertraulichkeitsbedürfnissen unterliegen, z. B. offen, intern, vertraulich, streng vertraulich und geheim. Auf bzw. in einem Datenträger können unterschiedlich schutzbedürftige Daten verarbeitet werden. Häufig wird die Sensibilität der Daten unterschätzt, so dass eine präzise „Klassifikation“ sämtlicher verarbeiteter Daten erforderlich ist. Die Analyse der in einer öffentlichen oder nichtöffentlichen Stelle vorhandenen Datenträger und der Schutz- und Vertraulichkeitsbedürfnisse der auf oder in ihnen gespeicherten Daten ist maßgeblich für die für die Entsorgung zu treffenden Regelungen. Das Analyseergebnis sollte im Entsorgungskonzept aufgeführt werden, das aufgrund möglicher Veränderungen einer steten Überprüfung seiner Richtigkeit und ggf. Aktualisierung bedarf.

## **Datenschutzgerechte Löschung optischer und magnetischer Datenträger**

Soweit personenbezogene Daten, die auf magnetischen Datenträgern wie Magnetbändern, Magnetbandkassetten, Disketten, Fest- oder Wechselplatten oder USB-Sticks gespeichert werden, gelöscht werden sollen, ohne dass der Datenträger vernichtet wird, empfiehlt es sich nicht, die Daten mit der Lösch- oder Formatierungsfunktion des Betriebssystems zu löschen. Beim Löschen mit der Betriebssystemfunktion werden die auf dem Datenträger gespeicherten Daten nicht wirklich gelöscht oder überschrieben, sondern meistens lediglich im Inhaltsverzeichnis des Datenträgers gelöscht und der zugehörige Datenbereich als frei markiert. Die Daten selbst sind in diesen Bereichen jedoch noch unversehrt solange vorhanden bis sie - eher zufällig und meist auch nicht vollständig - mit neuen Daten überschrieben werden. Solange die Daten nicht überschrieben sind, lassen sie sich mit frei im Internet verfügbaren Softwarewerkzeugen problemlos wieder herstellen.

Daten, die irreversibel gelöscht werden sollen, müssen entweder durch geeignete physikalische Maßnahmen wie mechanische oder thermische Zerstörung (Verbrennen, Einschmelzen) oder magnetische Durchflutung des Datenträgers vernichtet werden. Durch mehrmaliges Überschreiben der Daten kann deren Rekonstruktion ebenfalls ausgeschlossen werden.

Die durchzuführenden Maßnahmen müssen jeweils den Schutzbedarf der zu löschenden Daten berücksichtigen sowie Aufwand und Kosten für eine mögliche Datenwiederherstellung.

Eine wirksame Löschungsfunktion ist z. B. das Löschen des Datenträgers mit einem Löschgerät mit einem Magnetfeld, das auch spezialisierte Entsorgungsfirmen als Verfahren verwenden. Für die Löschung von Daten mit Hilfe eines Löschgeräts ergeben sich aus der DIN 33858 zwei Anforderungsstufen:

### **Stufe A**

Löschdämpfung mind. 45 db. Eine Reproduktion der gespeicherten Daten ist bei erheblichem Aufwand (Personal, Zeit und nicht handelsübliche Einrichtungen) nicht auszuschließen. Je nach Art der Datenträger sind unterschiedlich hohe Feldstärken zu gewährleisten; innerhalb der Anforderungsstufen wird dies durch die Stufen A1 bis A3 angegeben.

In die Stufe A eingruppierte Löscheräte tragen eine entsprechende Bezeichnung:  
Löscherät DIN 33858-A1 (Magnetbänder), DIN 33858-A2 (Magnetbandkassetten,  
Disketten)

### Stufe B

Löscherdämpfung mind. 90 db. Eine Reproduktion ist nach dem Stand der Technik unmöglich. Je nach Art des Datenträgers sind unterschiedliche Feldstärken zu gewährleisten; innerhalb der Anforderungsstufe wird dies durch die Stufen B1 bis B3 angegeben.

In die Stufe B eingruppierte Löscheräte tragen eine Bezeichnung, aus der die erfüllten Anforderungsstufen hervorgehen, z. B. Löscherät DIN 33858 – A2 B1. Daten auf intakten Datenträgern können durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen gelöscht werden. Dazu sind geeignete Softwarewerkzeuge verfügbar. Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Beim Löschen personenbezogener Daten niedriger oder mittlerer Schutzstufe sollten mindestens sieben Überschreibzyklen ausgeführt werden. Personenbezogene Daten hoher Schutzstufe sollten mit mindestens 33 Überschreibzyklen gelöscht werden. Diese Form der Wiederaufbereitung sichert die weitere Verwendbarkeit des entsprechenden Datenträgers. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ erarbeitet, in der weiterführende Informationen zu finden sind. Die Orientierungshilfe kann unter folgendem Link heruntergeladen werden:

[http://www.datenschutz-bremen.de/pdf/oh\\_sicheres\\_loeschen.pdf](http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf)

Optische Datenträger wie CD oder DVD können in der Regel nicht überschrieben oder durch magnetische Durchflutung zerstört werden. Die Daten sind für Spezialisten selbst dann noch rekonstruierbar, wenn z. B. eine CD zerbrochen oder zerstückelt worden ist. In Abhängigkeit vom Schutzbedarf der dort gespeicherten Daten sind daher geeignete Maßnahmen für eine datenschutzgerechte Vernichtung und Entsorgung der entsprechenden Datenträger zu treffen wie thermische Behandlung oder Schreddern oder Schmelzen der Datenträger. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert bei der Vernichtung von optischen Datenträgern ergänzend zur DIN 32757 bei mittleren Sicherheitsanforderungen eine maximale Partikelgröße von 20 mm<sup>2</sup>, bei

hohen Sicherheitsanforderungen eine maximale Partikelgröße von  $10\text{mm}^2$  (Diagonale  $\leq 5\text{ mm}$ ), entsprechend der Sicherheitsstufen 4 und 5 der DIN 32757.

### **Festlegung von Entsorgungswegen**

Sollen Datenträger mit personenbezogenen Daten entsorgt werden, so ist zunächst festzulegen, welche Entsorgungswege hierfür genutzt werden. Häufig kommen verschiedene Entsorgungswege für einen Datenträger in Frage. Ausschlaggebend für die Auswahl des am ehesten passenden Entsorgungsweges sind neben der Schutzbedürftigkeit der mit dem Datenträger verarbeiteten Daten u. a. die Masse der anfallenden Daten, die örtlichen Gegebenheiten und die wirtschaftlichen Möglichkeiten der für die Datenverarbeitung verantwortlichen Stelle. Soll der betreffende Datenträger innerhalb oder außerhalb der verantwortlichen Stelle, z. B. durch ein Dienstleistungsunternehmen, vernichtet werden? Sind auf einem Datenträger Daten mit unterschiedlichen Schutz- und Vertraulichkeitsbedürfnissen, so ist ein Entsorgungsweg festzulegen, der den Sicherheitsbedürfnissen der sensibelsten verarbeiteten Daten entspricht. Keinesfalls gewählt werden darf ein Entsorgungsweg, der mit den Schutz- und Vertraulichkeitsbedürfnissen des Datenträgers nicht zu vereinbaren ist. Nicht selten wird aber der vermeintlich einfachere Weg der Entsorgung gewählt. Die zu entsorgenden Datenträger werden z. B. dem normalen Hausmüll zugeführt oder ohne Rücksicht auf die verarbeiteten Daten an ein Entsorgungsunternehmen abgegeben. Die festgelegten Entsorgungswege sind im Entsorgungskonzept zu dokumentieren.

### **Vernichtung von Datenträgern mit personenbezogenem Inhalt in der verantwortlichen Stelle selbst**

Im Hinblick auf die Vernichtung von Datenträgern mit personenbezogenem Inhalt in der verantwortlichen Stelle selbst bedarf es konkreter Festlegungen hinsichtlich der Frage, wie die Sammlung und Vernichtung von Datenträgern intern erfolgt, insbesondere welche Sammelpunkte gewählt werden, welche Geräte zum Einsatz gelangen sollen und wo diese aufgestellt werden sollen. Fragen, die bei einer internen Vernichtung zu klären sind, wären z. B., ob die Vernichtung abteilungsintern erfolgen muss oder ob es ausreicht, lediglich einen festen geeigneten Platz zu haben, an dem die Vernichtung

stattfindet. Maßgeblich für die Beantwortung der Frage, ob die Vernichtung abteilungsintern erfolgen muss, können z. B. besondere Sicherheitsanforderungen der in einer Abteilung verarbeiteten Daten sein. Daneben sind auch für die Beantwortung dieser Frage die Masse der anfallenden Datenträger und die örtlichen Gegebenheiten in der verantwortlichen Stelle von größerer Bedeutung. Wichtigstes Kriterium, dem nicht zuwider gehandelt werden darf, müssen aber auch hier die Schutz- und Vertraulichkeitsbedürfnisse der auf dem jeweiligen Datenträger aufbewahrten bzw. gespeicherten Daten sein. Soll eine Sammlung erfolgen und deshalb ein fester Sammelpunkt eingerichtet werden, ist dieser so zu wählen, dass unbefugte Personen zu dem Sammelpunkt keinen Zutritt haben und nicht unberechtigt Einblick in Datenträger mit zu schützenden Daten nehmen oder diese entwenden können. Sammelpunkt sollten daher z. B. nicht in unverschlossenen Behältnissen auf allgemein zugänglichen Fluren eingerichtet werden. Zu treffen sind angemessene technische und organisatorische Sicherungsmaßnahmen (§ 7 Abs. 4 Satz 2 BremDSG, § 9 BDSG), insbesondere Zutritts- und Zugangsmaßnahmen. Falls der Ort der vorhergehenden Verarbeitung vom Ort der Vernichtung abweicht, sind auch Maßnahmen der Transportkontrolle (sowohl bis zum Abtransport als auch während des Transports der Datenträger) erforderlich. Um die Akzeptanz bei den Mitarbeiterinnen und Mitarbeitern zu erhöhen, ist es wichtig, sie bei der Auswahl eines geeigneten Sammelpunktes zu beteiligen.

Die für die Vernichtung eingesetzten Geräte wie z. B. Schredder sollten für die Mitarbeiterinnen und Mitarbeiter der öffentlichen/nichtöffentlichen Stelle handhabbar sein. Wer 20 Minuten nur Einzelblätter vernichtet, ist geeignet, unkontrollierte Wege der Entsorgung einzuschlagen. Häufig sind die Herstellerangaben zu den Geräten Optimalangaben, die sich nur unter bestimmten Bedingungen erreichen lassen. In der Regel haben Schredder schon bei einer normalen Nutzung einen geringeren Durchsatz als er vom Hersteller angegeben wird. Auch bei der Auswahl der Geräte, die für die Vernichtung verwendet werden sollen, muss aber die Sicherheitsbedürftigkeit ausschlaggebend sein. Zur Wahrung der erforderlichen Schutz- und Vertraulichkeitsbedürftigkeit sind in der DIN 32757 fünf Sicherheitsstufen definiert, nach denen z. B. Papier von 12 mm breiten Streifen (Sicherheitsstufe 1) bis praktisch zu „Pulver“ (Sicherheitsstufe 5) zu verkleinern ist. Die Sicherheitsstufen haben im Einzelnen folgende Bedeutung:

#### Stufe 1

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen ohne besondere Hilfsmittel und ohne Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand, möglich ist.

Papiere und Filme in Originalgröße: Materialteilchenfläche max. 1.000 mm<sup>2</sup>, Streifenbreite max. 12 mm.

#### Stufe 2

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen mit Hilfsmitteln und nur mit besonderem Zeitaufwand möglich ist.

Papiere und Filme in Originalgröße: Materialteilchenfläche max. 400 mm<sup>2</sup>, Streifenbreite bis max. 6 mm.

#### Stufe 3

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist.

Papiere und Filme in Originalgröße: Materialteilchenlänge max. 60 mm, Materialteilchenbreite bis max. 4 mm und Streifenbreite max. 2 mm.

Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 1 mm<sup>2</sup>.

#### Stufe 4

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, die im Falle kleiner Auflagen sehr aufwändig sind, möglich ist.

Papiere und Filme in Originalgröße: Materialteilchenlänge max. 15 mm, Materialteilchenbreite bis max. 2 mm als Preßling.

Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 0,5 mm<sup>2</sup>.

#### Stufe 5

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass es nach dem Stand der Technik unmöglich ist, auf ihnen wiedergegebene Informationen zu reproduzieren

Papiere und Filme in Originalgröße: Asche zerkleinert, Lösung, Suspension oder Faser. Materialteilchenbreite max. 0,8 mm, Materialteilchenlänge max. 15 mm.

Kunststoff wie Identifikationskarte oder Mikrofilm: Materialteilchenfläche max. 0,2 mm<sup>2</sup>.

### **Festlegung von Verantwortlichkeiten für die Löschung und Vernichtung**

Die festgelegten Löschverfahren und Entsorgungswege führen zu unterschiedlichen Verantwortlichkeiten. Auch diese sollten im Konzept festgelegt werden. Die Verpflichtung zur Wahrung des Datengeheimnisses gilt für die Mitarbeiter auch im Hinblick auf die Löschung personenbezogener Daten. Darüber hinaus sind gelegentliche Kontrollen, ob die vorgegebenen Entsorgungswege eingehalten werden, sinnvoll.

## **Entsorgung von Datenträgern mit personenbezogenem Inhalt durch ein Dienstleistungsunternehmen**

Lässt eine öffentliche oder eine nichtöffentliche Stelle Datenträger mit personenbezogenem Inhalt durch ein Dienstleistungsunternehmen entsorgen, so liegt eine Auftragsdatenverarbeitung vor, deren Durchführung sich nach § 9 BremDSG bzw. § 11 BDSG richtet. Nach § 9 BremDSG bzw. § 11 BDSG trägt für die Datenverarbeitung durch den Auftragnehmer bei einem Auftragsdatenverarbeitungsverhältnis auch weiterhin der Auftraggeber die Verantwortung. Der Abschluss eines Entsorgungsvertrages entbindet den Auftraggeber von seinen Pflichten nicht (§ 2 Abs. 3 Nr. 1 BremDSG, § 3 Abs. 7 BDSG). Die Auswahl und die Beauftragung des Auftragnehmers erfolgen unter Beachtung der in § 9 BremDSG bzw. § 11 BDSG aufgeführten Anforderungen. Danach ist der Auftragnehmer sorgfältig unter besonderer Berücksichtigung der vom Auftraggeber getroffenen technischen und organisatorischen Maßnahmen, wie angemessenen Zugangs-, und Zutritts-, und Transportkontrollmaßnahmen auszuwählen. Der Auftraggeber kann sich hierfür z. B. ein Sicherheitskonzept vorlegen oder Referenzpartner angeben lassen oder auf eine Zertifizierung nach ISO 9001:2000 oder nach der Entsorgungsfachbetriebsverordnung oder ein Datenschutzaudit Gütesiegel abstellen. In dem schriftlich zu erteilenden Auftrag sind auch die Datenverarbeitung, die zu ergreifenden technischen und organisatorischen Sicherungsmaßnahmen und etwaige Unterauftragsverhältnisse festzulegen. Der Auftraggeber hat sich im Rahmen der Auftragskontrolle (§ 7 Abs. 4 Satz 2 Nr. 6 BremDSG, Nr. 6 der Anlage zu § 9 BDSG) von der Einhaltung der zu treffenden technischen und organisatorischen Maßnahmen zu überzeugen. Häufig wird im Laufe der Zeit von den vertraglichen Festlegungen abgewichen, so dass eine regelmäßige Überprüfung, z. B. einmal im Jahr, durchgeführt werden sollte. Die Erstellung von Übergabe- und Vernichtungsprotokollen ist sinnvoll. Beauftragt eine nach dem BremDSG personenbezogene Daten verarbeitende Stelle ein Dienstleistungsunternehmen mit der Entsorgung, so hat sich der Auftragnehmer den Bestimmungen des Landesdatenschutzgesetzes zu unterwerfen, sofern er diesem nicht bereits unterliegt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist über die Beauftragung durch die verantwortliche öffentliche Stelle zu unterrichten. Bestimmte Amts- oder Berufsgeheimnisse oder andere besondere Geheimhaltungsvorschriften (§ 203 StGB) können die Vergabe eines Entsorgungsauftrags an ein Dienstleistungsunternehmen verhindern.