Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema

Datenträgerentsorgung

Orientierungshilfe

14.02.2014

Hausanschrift
Wagmüllerstr. 18
80538 München

Postanschrift
Postfach 221219
80502 München

Tel. 089 . 21 26 72 - 0
Fax 089 . 21 26 72 - 50

www.datenschutz-bayern.de
poststelle@datenschutz-bayern.de

Inhaltsverzeichnis

Orientierungshilfe Datenträgerentsorgung 4

1 Allgemeines 5

2 Gesetzliche Verpflichtung zur Datenlöschung 6

3 Beachtung von Normen 8

a) DIN 66399 9

aa) Schutzklassen 10

bb) Sicherheitsstufen 11

cc) Zuordnung der Sicherheitsstufen zu den Schutzklassen 16

dd) Kennzeichnung der Datenträgerarten 17

ee) Varianten der Datenträgervernichtung 17

ff) Bestandteile der ordnungsgemäßen Datenträgervernichtung 18

gg) Verantwortlichkeit der speichernden Stelle 18

b) DIN EN 15713 18

4 Entsorgungskonzept 21

a) Erstellung eines Entsorgungskonzeptes 21

b) Bestandteile des Entsorgungskonzeptes 21

c) Feststellung der anfallenden Datenträger und der darauf gespeicherten Daten 22

d) Festlegung der Entsorgungsart 23

e) Regelung der Zuständig- und Verantwortlichkeiten 23

f) (Zwischen)Lagerung des Entsorgungsguts 24

g) Transport der Datenträger 24

h) Geeignetheit des Entsorgungskonzepts 25

i) Sensibilisierung und Unterrichtung der Mitarbeiter 25

j) Dokumentation des Entsorgungsablaufs 25

5 Datenträgervernichtung in Eigenregie 26

a) Regelungsbedarf 26

b) Festlegungen 26
c) Geeignetheit der eingesetzten Geräte 27
d) Vernichtung von Papierunterlagen 28
e) Physikalische Löschung von magnetischen Datenträgern 28
f) Logisches Löschen 29
g) Überschreiben von Dateien 29
h) Entmagnetisieren von magnetischen Datenträgern 31
i) Vernichtung optischer Datenträger 32
j) Rückgabe von geleasten Festplatten 32
k) Vernichtung von Mikrofilmen und -fiches 32
l) Checkliste zur Datenträgerentsorgung in Eigenregie 33

6 Vernichtung von Datenträgern in Form einer Auftragsdatenverarbeitung 35
a) Arten der Datenträgerentsorgung im Auftrag 35
b) Gefahren 35
c) Verantwortung für die Einhaltung des Datenschutzes 36
d) Sorgfältige Auswahl des Auftragnehmers 36
e) Vertragsgestaltung 36
f) Überprüfung der Einhaltung der technisch-organisatorischen Sicherheitsmaßnahmen 38
g) Mustervertrag über die Vernichtung von Datenträgern 38
h) Checkliste zur Vernichtung von Datenträgern in Form einer Auftragsdatenverarbeitung 39

Orientierungshilfe Datenträgerentsorgung

Im Zusammenhang mit der Entsorgung von Datenträgern, die personenbezogene oder sonstige schutzbedürftige Daten enthalten, ergeben sich in der Praxis immer wieder Fragen wie:

- Welche Möglichkeiten der Entsorgung vertraulicher Unterlagen bestehen, und welche davon kommen für die Behörde in Betracht?
- Ist dabei Eigen- oder Fremdentsorgung vorzuziehen?
- Welche Sicherheitsstufe ist bei der Vernichtung der Datenträger angemessen?
- Welche Kriterien sind bei der Auswahl von Geräten, Verfahren und - bei externer Entsorgung - Entsorgungsunternehmen zu beachten?
- Wie ist das „Drumherum“ zu organisieren?

1 Allgemeines

Vielen öffentlichen Stellen ist es zwar bewusst, dass sie ihre nicht mehr benötigten vertraulichen Unterlagen datenschutzgerecht entsorgen müssen, allerdings ist es ihnen häufig unklar, wie sie dabei vorgehen müssen. Auch achten sie oft nicht darauf, ein entsprechendes Entsorgungskonzept zu entwickeln. Dementsprechend kommt es immer wieder bei diesen Behörden nicht nur zu Pannen bei der Entsorgung selbst, sondern bereits in den vorgelagerten Phasen.

Es muss jeder verantwortlichen Stelle bewusst sein, dass sich die zu ergreifenden Maßnahmen nicht nur auf die Vernichtung der Datenträger beschränken dürfen, sondern sie müssen auch Sammlung und Lagerung (einschl. der ggfs. notwendigen Zwischenlagerung), Transport, Organisation sowie bei externer Entsorgung die Vertragsgestaltung einbeziehen und damit den gesamten Entsorgungsvorgang und seine Vorphasen angemessen berücksichtigen. Ziel aller Maßnahmen muss die Gewährleistung eines gleichbleibend hohen Sicherheitsniveaus in allen Phasen der Entsorgung sein. Das setzt voraus, dass jede Daten verarbeitende Stelle sowohl die Vertraulichkeit der Daten als auch die Funktionalität in allen Phasen der Entsorgung sicherstellt. Dabei sind Maßnahmen für den Fall menschlichen Versagens ebenso vorzusehen wie solche für den Fall von Funktionsstörungen technischer Systeme.

Unabhängig davon, ob eine Behörde die Entsorgung von Datenträgern in eigener Regie durchführt oder ob sie damit ein darauf spezialisiertes fremdes Unternehmen beauftragt, ist die Datenträgerentsorgung wie jeder betriebliche Prozess zunächst organisatorisch auszugestalten. Voraussetzung dafür ist, dass bei den Verantwortlichen Klarheit über die Menge und Art der regelmäßig zu entsorgenden Datenträger und die Schutzbedürftigkeit der darauf aufbewahrten Daten besteht. Hat eine öffentliche Stelle erstmal die zu beachtende Sicherheitsstufe festgelegt, so kann sie ein geeignetes Vernichtungsverfahren und entsprechende Sicherheitsmaßnahmen in allen Phasen festlegen. Das Ziel muss dabei sein, ein gleichmäßig hohes Sicherheitsniveau zu erreichen, das der festgelegten Sicherheitsstufe entspricht. Der organisatorische Ablauf ist in einer Entsorgungsrichtlinie festzuschreiben.

2 Gesetzliche Verpflichtung zur Datenlöschung

Es besteht eine Reihe von gesetzlichen Vorschriften, die zur Löschung personenbezogener Daten (und damit auch deren Datenträger) verpflichten. So sind beispielsweise gemäß Art. 12 Absatz 1 BayDSG personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Ähnliche Bestimmungen enthalten die anderen Landesdatenschutzgesetze und die §§ 20 Absatz 2 (für die Bundesverwaltung) bzw. 35 Absatz 2 Satz 2 BDSG (für die Privatwirtschaft).

Das **Löschen** von personenbezogenen Daten stellt gemäß Art. 4 Absatz 6 Nr. 5 BayDSG eine Form der Verarbeitung dar, wobei das Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten ist.

Häufig (z. B. in der früheren DIN 44300) wird „Löschen“ auch als „Daten auf einem Datenträger oder Daten in einem Speicher vernichten“ definiert.

Grundgedanke beider Erläuterungen ist, dass durch die Datenlöschung die Kenntnisnahme der auf Datenträgern gespeicherten Daten für jedermann zu jeder Zeit tatsächlich unmöglich ist.

Eine Löschung von Daten kann natürlich auch durch die **Vernichtung von Datenträgern** erfolgen. Bei diesen Datenträgern kann es sich sowohl um Papierunterlagen als auch um Festplatten, Magnetbänder, USB-Sticks, CD-ROMs, DVDs, optische Speicher, Filme und dergleichen handeln.

Ein **Datenträger** ist ein Mittel, auf dem Daten aufbewahrt werden können. Er wird mitunter auch als Informationsträger bezeichnet, vor allem dann, wenn Daten zusammen mit ihrem Kontext auf dem Datenträger enthalten sind.

Gemäß dem Vorwort der neuen DIN SPEC 66399-3 bezeichnet der Begriff „**Sichere Vernichtung**“ das Vernichten von schutzwürdigen Informationen auf Datenträgern in der Art, dass ihre Reproduktion der auf ihnen wiedergegebenen Informationen unmöglich ist oder weitgehend erschwert wird. Die Vernichtung erfolgt in der Regel durch Zerkleinerung oder Stoffumwandlung. Die im Rahmen der Entsorgung zur Vernichtung vor-

gesehenen Datenträger werden als Vernichtungsgut und das (vollständig) vernichtete Vernichtungsgut als Abfallgut bezeichnet.

Werden Datenträger nicht mehr benötigt, z.B. nach Ablauf der Aufbewahrungsfrist oder wegen eingeschränkter Reproduktionsfähigkeit der darauf aufbewahrten Daten, so sind sie datenschutzgerecht zu vernichten. Die Art der Vernichtung hängt dabei von der Art der Datenträger ab. Außerdem muss natürlich auch bei der Datenträgervernichtung eine Kosten-Nutzen-Analyse durchgeführt werden. Dies bedeutet, dass die zu ergreifenden Maßnahmen in einem angemessenen Verhältnis zur Schutzbedürftigkeit der Daten stehen (Art. 7 Abs. 1 Satz 2 BayDSG). Je sensibler die zu vernichtenden Daten sind, desto höhere Anforderungen sind an die technisch-organisatorischen Maßnahmen zur Datenträgervernichtung zu stellen.

3 Beachtung von Normen

Bei der Entsorgung von Datenträgern ist zu beachten, dass die Anforderungen an technische und organisatorische Maßnahmen bei der Vernichtung von Datenträgern umso höher sein müssen, je höher die Sensibilität der Daten ist.

Zur Festlegung der für die einzelnen Daten erforderlichen Maßnahmen und Anforderungen an die Entsorgungsgeräte, wurde daher bereits im Jahre 1985 die **DIN 32757-1** erlassen, die zwischen fünf verschiedenen Sicherheitsstufen (in Abhängig von der Sensibilität der Daten) unterschied.

Im August 2009 wurde eine europäische Norm (**EN 15713:2009** - („Secure destruction of confidential material“) veröffentlicht, die in Deutschland unter der Bezeichnung **DIN EN 15713** „Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln“ Gültigkeit erlangt hat. Diese DIN-Norm beinhaltet ebenfalls eine Tabelle bezüglich der Anforderungen an Vernichtungsgeräte (z. B. Aktenvernichter), in der der Begriff Sicherheitsstufe der DIN 32757 durch die europaweite Bezeichnung Zerkleinerungsstufe ersetzt wurde. Außerdem beinhaltet sie auch erstmals die erforderlichen technisch-organisatorischen Maßnahmen für die Vernichtung von Informationsdatenträgern.

Aufgrund der neu erschienenen DIN EN 15713 beschloss der zuständige Arbeitsausschuss NA 043-01-51 AA „Vernichtung von Informationsträgern“ im „Normenausschuss Informationstechnik und Anwendungen (NIA)“ im DIN e.V. seine Arbeit zum 24.11.2009 mit einer konstituierenden Sitzung wieder aufzunehmen und die DIN 32757 mit der neuen europäischen Norm abzustimmen, da es durch die Veröffentlichung der DIN EN 15713 notwendig geworden war, „die in der DIN 32757 festgelegten Sicherheitsstufen und die in der EN 15713 empfohlenen Zerkleinerungsnummern aufeinander abzustimmen. Da eine der europäischen Normung entgegenstehende nationale Normung nicht zulässig ist, kann die DIN 32757 nicht unverändert aufrecht erhalten bleiben. Ferner besteht der Bedarf, die DIN 32757 den neuen gesetzlichen Vorgaben zum Datenschutz anzupassen.“

Da die DIN EN 15713 zu sehr auf dem britischen Standard basiere und zu wenig auf die deutschen Bedürfnisse und Gesetzesvorschriften (z. B. BDSG, SGB) eingehe, sollten bei der neuen DIN auch mehr die deutschen Gegebenheiten und der neueste Stand der Technik berücksichtigt werden.

Daher wurde innerhalb von drei Jahren die neue **DIN-Norm 66399** von dem Normenausschuss erstellt. Der Normenausschuss bediente sich dabei der Hilfe von Mitarbei-

tern von Bundesbehörden, Datenschutzexperten und im Bereich der Aktenvernichtung tätigen Firmen. Diese neue DIN-Norm besteht aus drei Teilen:

- DIN 66399-1 „Büro- und Datentechnik – Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe“ (definiert die Grundlagen und Begriffe, die bei der Datenträgervernichtung beachtet werden sollten)
- DIN 66399-2 „Büro- und Datentechnik -Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern“ (beschreibt die Anforderungen an Maschinen zur Vernichtung von Datenträgern)

DIN SPEC 66399-3 „Büro- und Datentechnik - Vernichten von Datenträgern - Teil 3: Prozess der Datenträgervernichtung“ (bildet den kompletten Prozess der Datenträgervernichtung ab, SPEC = specification und somit Spezifikation)

Während die ersten beiden Teile im Oktober 2012 in Kraft getreten sind, erlangte der dritte Teil erst zum Jahreswechsel 2012/13 seine Gültigkeit. Gleichzeitig traten die DIN 32757-1 und DIN 44300 außer Kraft.

Die Festlegungen zur Informationsdatenträgervernichtung der DIN-Norm 66399 Teil 1 bis Teil 3 können als Anhaltswert für die datenschutzgerechte Entsorgung von Datenträgern herangezogen werden, auch wenn sie keine Rechtsnorm ist. Während die ersten beiden Teile der DIN 33699 offizielle Normen des Deutschen Instituts für Normung sind, handelt es sich bei dem Teil 3 lediglich um eine Spezifikation, die vom Arbeitsausschuss „Informationstechnik und Anwendungen (NIA)“ ausgearbeitet wurde.

Trotzdem berücksichtigen die 3 Teile erstmals alle für die Datenträgervernichtung relevanten Faktoren:

- Schutzklassen und Sicherheitsstufen
- Datenträgerarten
- Einflussgrößen für die Rekonstruktion von Informationen
- technisch-organisatorische Sicherheitsmaßnahmen

a) DIN 66399

Der **Teil 1** der DIN 66399 legt – unter Berücksichtigung des aktuellen Standes der Technik – Grundlagen und Begriffe fest, die bei der Vernichtung der Datenträger beach-

tet werden sollten. So werden Schutzklassen und Sicherheitsstufen definiert, die die zu ergreifenden technisch-organisatorischen Sicherheitsmaßnahmen – abhängig vom jeweiligen Schutzbedarf – enthalten. Grundlage der Einteilung sind die Schutzbedürftigkeit der auf den Datenträgern gespeicherten Daten und das Wirtschaftlichkeits- und Angemessenheitsprinzip bei der Datenträgervernichtung.

aa) Schutzklassen

Schutzklasse 1	**Normaler Schutzbedarf** für interne Daten (z. B. Telefonlisten, Lieferantendateien, Adressdatenbanken, Notizen) – werden diese Daten nicht entsprechend geschützt, besteht die Gefahr, dass ein Betroffener in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird, zudem hätte die unbefugte Kenntnisnahme der Daten negative Auswirkungen für die speichernde Stelle
Schutzklasse 2	**Hoher Schutz** für vertrauliche Daten (z. B. Personal- und Finanzdaten), bei diesen Daten besteht die Gefahr, dass ein Betroffener in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird, außerdem hätte die unbefugte Kenntnisnahme der Daten erhebliche negative Auswirkungen für die speichernde Stelle
Schutzklasse 3	**Sehr hoher Schutzbedarf** für besonders vertrauliche und geheime Daten (Daten, die – wenn sie nicht entsprechend geschützt werden – zu einer Gefahr für Leib oder Leben von Personen oder für die Freiheit eines Betroffenen führen können), außerdem hätte die unbefugte Kenntnisnahme der Daten ernsthafte (existenzbedrohende) Auswirkungen für die speichernde Stelle und würde gegen Berufsgeheimnisse, Verträge oder Gesetze verstoßen (z. B. Forschungs- und Entwicklungsdokumente, Verschlusssachen, Gesundheitsdaten)

bb) Sicherheitsstufen

Die Sicherheitsstufen sind den Schutzklassen zugeordnet und geben den Aufwand wieder, der für eine (unberechtigte) Wiederherstellung der Daten erforderlich ist. So ist beispielsweise bei der Sicherheitsstufe 7 eine Datenherstellung nach dem derzeitigen Stand der Technik nicht möglich. Dagegen erlaubt die Sicherheitsstufe 1 die Wiederherstellung der Daten ohne besondere Hilfsmittel und Fachkenntnisse und erfordert lediglich einen erheblichen Zeitaufwand.

Sicherheitsstufe 1	Allgemeine Daten 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. 2.000 mm², Streifenbreite max. 12 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm² **Optische Datenträger**: Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm² **Magnetische Datenträger**: Medium muss funktionsunfähig sein **Festplatten**: Festplatte muss funktionsunfähig sein **Halbleiterspeicher** (z. B. Speichersticks, Chipkarten, mobile Kommunikationsmittel): Datenträger muss funktionsunfähig sein
Sicherheitsstufe 2	**Interne Daten** (z. B. Behördenrichtlinien, Aushänge und Formulare) 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. 800 mm², Streifenbreite bis max. 6 mm, Streifenlänge unbegrenzt, Tole-

	ranz für 10 % der Fläche des Materials: maximal 2000 mm^2 **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm^2 **Optische Datenträger**: Materialteilchenfläche max. 800 mm², Toleranz für 10 % der Fläche des Materials: maximal 2000 mm^2 **Magnetische Datenträger**: Medium mehrfach zerteilt und Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm^2 **Festplatten**: Datenträger beschädigt **Halbleiterspeicher**: Datenträger muss zerteilt sein
Sicherheitsstufe 3	**Sensible Daten** (Unterlagen mit vertraulichen Daten, wie sie in jeder Behörde anfallen) 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: Materialteilchenfläche max. 320 mm^2, Streifenbreite max. 2 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 480 mm^2 **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2 **Optische Datenträger**: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm^2 **Magnetische Datenträger**: Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm^2 **Festplatten**: Datenträger verformt **Halbleiterspeicher**: Datenträger muss zerteilt sein und Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm^2

Sicherheitsstufe 4	**Besonders sensible Daten** (z. B. Gehaltsabrechnungen, Personaldaten / -akten, Arbeitsverträge, medizinische Berichte, Steuerunterlagen von Personen) 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: Materialteilchenfläche max. 160 mm^2 und für gleichförmige Partikel: Streifenbreite max. 6 mm, Toleranz für 10 % der Fläche des Materials: maximal 800 mm^2 **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 2,5 mm^2, Toleranz für 10 % der Fläche des Materials: maximal 7,5 mm^2 **Optische Datenträger**: Materialteilchenfläche max. 30 mm^2, Toleranz für 10 % der Fläche des Materials: maximal 90 mm^2 **Magnetische Datenträger**: Materialteilchenfläche max. 160 mm^2, Toleranz für 10 % der Fläche des Materials: maximal 480 mm^2 **Festplatten**: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 2000 mm^2, Toleranz für 10 % der Fläche des Materials: maximal 3800 mm^2 **Halbleiterspeicher**: Datenträger muss zerteilt sein und Materialteilchenfläche max. 30 mm^2, Toleranz für 10 % der Fläche des Materials: maximal 90 mm^2
Sicherheitsstufe 5	**Geheim zu haltende Daten** (Datenträger mit geheim zu haltenden Informationen mit existenzieller Wichtigkeit für eine Person, eine Behörde, ein Unternehmen oder eine Einrichtung.) 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: Materialteilchenfläche max. 30 mm^2 und für gleichförmige Partikel: Streifenbreite max. 2 mm, Tole-

	ranz für 10 % der Fläche des Materials: maximal 90 mm^2 **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 3 mm^2 **Optische Datenträger**: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2 **Magnetische Datenträger**: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm^2 **Festplatten**: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm^2 **Halbleiterspeicher**: Datenträger muss zerteilt sein und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2
Sicherheitsstufe 6	**Geheime Hochsicherheitsdaten** (z. B. geheimdienstliche oder militärische Bereiche) Datenträger mit geheim zu haltende Unterlagen, wenn außergewöhnliche Sicherheitsvorkehrungen einzuhalten sind **Papiere und Filme** in Originalgröße: Materialteilchenfläche max. 10 mm^2 und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2 **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 0,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 1,5 mm^2 **Optische Datenträger**: Materialteilchenfläche max. 5 mm², Toleranz für 10 % der Fläche des Materials: maximal 15 mm^2 **Magnetische Datenträger**: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2 **Festplatten**: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2

	Halbleiterspeicher: Datenträger muss mehrfach zerteilt sein und Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm^2
Sicherheitsstufe 7	Top Secret Hochsicherheitsdaten Datenträger mit strengst geheim zu haltende Daten, bei denen höchste Sicherheitsvorkehrungen einzuhalten sind **Papiere und Filme** in Originalgröße: Materialteilchenfläche max. 5 mm^2 und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen **Kunststoff wie Identifikationskarte oder Mikrofilm**: Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen **Optische Datenträger**: Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: maximal 0,6 mm^2 **Magnetische Datenträger**: Materialteilchenfläche max. 2,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 7,5 mm^2 **Festplatten**: Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 5 mm², Toleranz für 10 % der Fläche des Materials: maximal 15 mm^2 **Halbleiterspeicher**: Datenträger muss mehrfach zerteilt sein und Materialteilchenfläche max. 0,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 1,5 mm^2

Eine datenschutzgerechte Vernichtung von Schriftgut mit besonders sensiblen personenbezogenen Daten sollte – um sicherzugehen – eine Vernichtung nach DIN 66399 von **mindestens Sicherheitsstufe 4** voraussetzen. Denn nur bei Vernichtung nach mindestens dieser Stufe sind die Reststücke so klein, dass eine Reproduktion der jeweiligen Informationen nur unter erheblichen Aufwand von Personen, Zeit und Hilfsmittel möglich und die Gefahr dafür gering ist. Die dazu verwendeten Geräte (in der Regel Aktenvernichter) müssen der Norm entsprechend gekennzeichnet werden. Allerdings sind die Anforderungen an die Schriftgutvernichtung der Sicherheitsstufe 4 bereits der-

art hoch, dass sie viele Aktenvernichter nicht mehr erfüllen. Spätestens ab der Sicherheitsstufe 5 ist der Einsatz sogenannter Cross Cutter erforderlich.

Die DIN 66399 lässt die Möglichkeit offen, bei großen Durchsatzmengen und entsprechender Nachbehandlung durch Vermischung oder Verpressung (z. B. durch Einsatz von Ballenpressen und Verwirblern oder einer Nachbehandlung in Form von Verbreiung oder Brikettierung) wegen der dadurch erschwerten Reproduktionsmöglichkeit bis zum Erreichen der Sicherheitsstufe 4 eine niedrigere Sicherheitsstufe zu wählen. Dies ist insbesondere bei der Vernichtung von Papierunterlagen und Mikrofilmen möglich.

Für elektronische oder magnetische Datenträger (z. B. Disketten, ID-Karten, Festplatten, Magnetbandkassetten, Speichersticks, Chipkarten) kann immer dann eine niedrigere als die an sich erforderliche Sicherheitsstufe gewählt werden, wenn zuvor die entsprechenden Datenträger entweder gelöscht oder überschrieben wurden.

Umgekehrt kann bei geringeren Durchsatzmengen, die eine Reproduktion der Daten erleichtern, auch eine höhere Sicherheitsstufe erforderlich werden. Grundsätzlich gilt aber für die Erreichung der gewählten Sicherheitsstufe, dass das Vernichtungsgut vollständig erfasst und der Vernichtung zugeführt wird, und dass die vollständige Vernichtung kontrolliert werden kann. Die Norm verlangt deshalb entsprechende konstruktive Vorkehrungen und geeignete Hilfseinrichtungen.

Fallen zu vernichtende Datenträger an, die **verschiedenen Sicherheitsstufen** zuzuordnen sind, müssen diese entweder getrennt oder gemäß der höheren Sicherheitsstufe entsorgt werden.

cc) Zuordnung der Sicherheitsstufen zu den Schutzklassen

Die Sicherheitsstufen werden den Schutzklassen gemäß folgender Matrix zugewiesen:

Schutzklasse:	Sicherheitsstufen:						
	1	2	3	4	5	6	7
1	x[1)]	x[1)]	x				
2			x	x	x		
3				x	x	x	x

x[1)] = für personenbezogene Daten nicht anwendbar

dd) Kennzeichnung der Datenträgerarten

Zusätzlich wurden im **Teil 2** der DIN 66399 alle Datenträgerarten aufgenommen und mit einem Kürzel gekennzeichnet, das der jeweiligen Sicherheitsstufe vorangestellt ist. Derzeit sind folgende Kürzel in der DIN enthalten:

P	Informationsdarstellung in Originalgröße (Papier, Film, Druckformen etc.)
F	Informationsdarstellung verkleinert (z. B. Film, Mikrofilm, Folie)
O	Informationsdarstellung auf optischen Datenträgern (CD, DVD, Blu Ray usw.)
T	Informationsdarstellung auf magnetischen Datenträgern (Disketten, ID-Karten, Magnetbandkassetten …)
H	Informationsdarstellung auf Festplatten mit magnetischem Datenträger (Festplatten)
E	Informationsdarstellung auf elektronischen Datenträgern (USB-Sticks, Chipkarten, Halbleiterfestplatten, mobile Kommunikationsmittel wie Flash-Speicher aus Smartphones und Tablet-PCs, Speicherkarten aus Digital Kameras usw.)

Beispiel: O-4 bedeutet die Gewährleistung der Sicherheitsstufe 4 bei der Datenspeicherung auf einer CD bzw. DVD.

Die in diesen 6 Kategorien festgeschriebenen Materialbeschaffenheiten spielen natürlich bei der Datenträgervernichtung ebenfalls eine große Rolle. So muss beachtet werden, ob 50.000 Papierseiten entsorgt werden sollen oder ein USB-Stick, der über das gleiche Datenvolumen verfügt.

ee) Varianten der Datenträgervernichtung

Der Teil 3 der neuen DIN-Norm beschreibt erstmalig den kompletten Prozess der Datenträgervernichtung und die dabei erforderlichen technisch-organisatorischen Maßnahmen. Dabei wird zwischen drei Prozessvarianten bei der Datenträgervernichtung unterschieden:

externe Datenträgervernichtung durch einen Dienstleister in Form der Auftragsdatenverarbeitung

Datenträgervernichtung durch einen Dienstleister in Form der Auftragsdatenverarbeitung vor Ort (z. B. im Hof des Auftraggebers)

eigenverantwortliche Datenträgervernichtung durch die betreffende speichernde Stelle selbst vor Ort

ff) Bestandteile der ordnungsgemäßen Datenträgervernichtung

Bestandteile einer ordnungsgemäßen Datenträgervernichtung sind gemäß DIN SPEC 66399-3:

- Festlegung der Zuständigkeiten, der Sicherheitsklasse und der Sicherheitsstufe
- Spezifizierung der gesetzlichen und betrieblichen Rahmenbedingungen (z. B. bezüglich der Anfallstelle, der Sammlung und Lagerung der Datenträger, eventuell des Transports sowie der Vernichtung)
- Beschreibung der Anforderungen an das eingesetzte Personal (z. B. Verpflichtung auf das Datengeheimnis)
- Sicherstellung der Kontrolle und Prüfung des Prozessablaufs (durch Personal der speichernden Stelle)
- Dokumentation des Ablaufs der Datenträgervernichtung

gg) Verantwortlichkeit der speichernden Stelle

Die Sicherheitsstufen der DIN 66399 bieten einer speichernden Stelle eine geeignete Hilfe, um das Schutzbedürfnis ihrer Daten nach ihrer Bedeutung und den jeweiligen Umgebungsbedingungen zu beurteilen und daraus eine geeignete Sicherheitsstufe abzuleiten. Als Mindestanforderung an eine datenschutzgerechte Entsorgung personenbezogener Daten ist – wie bereits erwähnt die Sicherheitsstufe 4 anzusehen.

Die speichernde Stelle hat – auch im Rahmen einer Auftragsdatenverarbeitung – sowohl die Schutzklasse als auch entsprechende Sicherheitsstufe festzulegen.

b) DIN EN 15713

Die DIN EN 15713 fordert öffentliche und nicht-öffentliche Stellen dazu auf, eine Reihe von Qualitätskriterien bei der Vernichtung von vertraulichen, personenbezogenen Daten zu beachten und gibt entsprechende Hinweise sowohl zum Vernichtungsvorgang selbst als auch für dessen Überwachung bei einer Datenträgervernichtung im Auftrag.

Die Norm gibt dazu Hinweise für die Durchführung und Überwachung der Vernichtung von vertraulichen Unterlagen, um Sorge dafür zu tragen, dass diese Unterlagen zuverlässig und sicher entsorgt werden. Die Norm will dabei sicherstellen, dass das beauf-

tragte Unternehmen den anzuwendenden Anforderungen entspricht, der Abfall recycelt wird und dass Firmen- und Kundendaten nicht in die falschen Hände geraten können.

So fordert die DIN-Norm z. B. bezüglich einer Datenträgervernichtung im Auftrag die Einhaltung folgender Kriterien:

- Bis zur Abholung des Entsorgungsgutes müssen die zu vernichtenden Unterlagen sicher aufbewahrt werden.
- So muss beispielsweise eine nach EN 501131-1 zugelassene Einbruchmeldeanlage in diesen Räumlichkeiten installiert und eine Alarmempfangszentrale vorhanden sein.
- Bezüglich der Datenträgervernichtung muss ein schriftlicher Vertrag zwischen Auftragnehmer und Auftraggeber existieren.
- Die zur Abholung der zu vernichtenden Datenträger eingesetzten Fahrzeuge müssen entweder über einen Kofferaufbau oder einen gesicherten Containeraufbau verfügen.
- Die Vernichtung der Datenträger sollte innerhalb eines Werktags nach Eintreffen beim Auftragnehmer erfolgen.

Die DIN EN 15713 sieht eine Bewertung der Vernichtung von Stufe 1 (größtes Restmaterial) bis Stufe 8 (kleinstes Restmaterial) vor:

Zerkleinerungsstufe:	Mittlere Oberfläche in mm^2	Maximale Schnittbreite in mm
1	5.000	25
2	3.600	60
3	2.800	16
4	2.000	12
5	800	6
6	320	4
7	30	2
8	10	0,8

Die Zerkleinerungsstufen sind auf verschiedenen Materialen anzuwenden. Diese Materialkategorien von vertraulichen Unterlagen in der Kategorisierung der EN 15713 sind:

- **A**: Papier, Pläne, Dokumente und Zeichnungen
- **B**: SIM-Karten und Negative
- **C**: Video-/Tonbänder, Disketten, Kassetten und Filme
- **D**: Computer einschließlich Festplatte, eingebetteter Software, Chipkartenleser, Komponenten und anderer Hardware
- **E**: ID-Karten, CDs und DVDs
- **F**: Gefälschte Waren, Druckplatten, Mikrofiche, Kredit- und Kundenkarten und andere Produkte
- **G**: Firmen- oder Markenkleidung und Uniformen
- **H**: Medizinische Röntgen- und Overheadprojektor-Platten

Nochmals der Hinweis: Die gegenwärtig parallel zur DIN 66399 gültige DIN EN 15713 wird häufig mit Ihrem teilweise wenig verbindlichen („sollte“) Charakter den deutschen Anforderungen an die verbindliche Gewährleistung von Datenschutz und Informationssicherheit nicht gerecht. Ein „Stand der Technik“, wie bei der DIN 66399, kann aus dieser daher nicht verbindlich abgeleitet werden. Somit ist der DIN 66399 der Vorzug zu geben.

Außerdem ist zu bedenken, dass zwar ein alter – nach der DIN 32757 abgeschlossener – Vertrag weiter bestehen kann, besser ist es aber – zumindest beim Abschluss eines neues Vertrages – diesen an die Gegebenheiten der DIN 66399 anzupassen.

Die DIN-Normen können vom Beuth Verlag GmbH, Burggrafenstr. 4-10, 10787 Berlin, bezogen werden.

4 Entsorgungskonzept

Die Notwendigkeit der Vernichtung nicht mehr benötigter personenbezogener Unterlagen wird zwar in der Regel erkannt, allerdings besteht häufig Unklarheit darüber, welche Maßnahmen dazu zu ergreifen sind. Deshalb kommt es immer wieder zu Pannen bei der Entsorgung von Datenträgern, hauptsächlich durch Leichtsinn und Unwissenheit (z. B. bezüglich der gesetzlichen Forderungen) der Mitarbeiter. So hat beispielsweise ein Industriespion leichtes Spiel, wenn wichtige Unterlagen im Müllcontainer landen. Häufig werden auch magnetische Datenträger (z. B. Festplatten) weitergegeben ohne zuvor die darauf gespeicherten Daten datenschutzgerecht gelöscht zu haben, so dass sie nicht wieder hergestellt werden können.

Auch wird häufig übersehen, dass neben PCs und Laptops auch andere IT-Geräte (z. B. Smartphones, Handys, Kopier- und Navigationsgeräte) über einen Datenspeicher verfügen, auf dem sensible personenbezogene Daten gespeichert sein können.

Auch eine (scheinbare) physikalische Vernichtung eines Datenträgers (z. B. Deformierung durch Hammerschläge) bietet keinen absoluten Schutz, da Daten grundsätzlich rekonstruierbar sind, solange sie physikalisch auf einem Datenträger vorhanden sind. So haben Datenrettungsunternehmen bereits verkohlte, durchbohrte oder plattgewalzte Festplatten teilweise oder vollständig wiederhergestellt.

a) Erstellung eines Entsorgungskonzeptes

Damit keine derartigen Pannen geschehen, sollten die wesentlichsten Anforderungen an die datenschutzgerechte Entsorgung von Datenträgern mit schutzwürdigen Daten und die dabei zu ergreifenden Sicherheitsmaßnahmen innerhalb eines Entsorgungskonzeptes festgehalten werden. Voraussetzung für die Erstellung eines derartigen Konzeptes ist es, das Klarheit über die Menge und Art der regelmäßig zu entsorgenden Datenträger und die Schutzbedürftigkeit der darauf aufbewahrten Daten besteht. Liegt die Sicherheitsstufe fest, so können ein geeignetes Vernichtungsverfahren und entsprechende Sicherheitsmaßnahmen in allen Phasen festgelegt werden.

b) Bestandteile des Entsorgungskonzeptes

In dem Entsorgungskonzept sind technische und/oder organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten bei Verkauf oder Vermietung, Aus-

sonderung, Rückgabe, Reparatur, Wartung und letztendlicher Vernichtung von Datenträgern gewährleisten.

Ein Entsorgungskonzept darf sich dabei nicht nur auf Maßnahmen zur Vernichtung der Datenträger beschränken, sondern muss auch die Sammlung und Lagerung (einschließlich einer etwaigen Zwischenlagerung), den Transport des Vernichtungsgutes, die Organisation sowie bei externer Entsorgung die Vertragsgestaltung einbeziehen und damit den gesamten Entsorgungsvorgang und seine Vorphasen entsprechend berücksichtigen. Maßnahmen für den Fall menschlichen Versagens sind ebenso zu berücksichtigen wie solche für den Fall von Funktionsstörungen technischer Systeme. Das Ziel muss dabei sein, von der Sammlung des Vernichtungsgutes bis zur endgültigen Entsorgung ein gleichmäßig hohes Sicherheitsniveau zu erreichen, das der festgelegten Sicherheitsstufe entspricht.

In einem Entsorgungskonzept sind insbesondere folgende Fragen zu beantworten:

- Welche Arten von Datenträgern mit personenbezogenen Daten müssen entsorgt werden?
- Welche Sicherheitsstufen sind dabei zu beachten?
- Welche Möglichkeiten zur datenschutzgerechten Entsorgung der Datenträger sind bereits vorhanden und wo muss nachgebessert werden?
- Anhand welcher Kriterien muss die Auswahl der Geräte und Verfahren erfolgen?
- Können alle Datenträger in Eigenregie vernichtet werden oder müssen Fremdfirmen beauftragt werden?
- Welche Kriterien sind bei einer externen Entsorgung bezüglich der Auswahl des Auftragnehmers zu beachten?
- Natürlich müssen bei der Erstellung eines Entsorgungskonzeptes auch etwaige **gesetzliche Regelungen** (z. B. Aufbewahrungspflichten oder Löschungsfristen) beachtet werden.

c) Feststellung der anfallenden Datenträger und der darauf gespeicherten Daten

Bei allen Unternehmen und Behörden ist eine Vielzahl von Daten auf ganz unterschiedlichen Datenträgern (z. B. Papier, Festplatten, CD, DVD, USB-Sticks, Speicherkarten, ZIP-, Audio-, Videokassetten, Mikrofilme) gespeichert. 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. Bevor die dadurch entbehrlichen Datenträger entsorgt werden können, muss zunächst die Sensibilität der auf ihnen gespeicherten (personenbezogenen) Daten festgestellt werden. Daraus ergeben sich in der Regel unterschiedliche Sicherheitsanforderungen an die Entsorgungsart und den Entsorgungsvorgang.

Auf einem Datenträger können unterschiedlich schutzbedürftige Daten gespeichert sein. In diesen Fällen müssen sich die erforderlichen Sicherheitsmaßnahmen nach den sensibelsten dieser Daten richten.

d) Festlegung der Entsorgungsart

Sollen Datenträger mit personenbezogenen Daten entsorgt werden, so ist die entsprechende Entsorgungsart festzulegen, da häufig verschiedene Entsorgungsarten für einen Datenträger in Frage kommen. Ausschlaggebend für die Auswahl der am ehesten geeigneten Entsorgungsart sind:

- die Schutzbedürftigkeit der auf dem Datenträger gespeicherten Daten,
- die Masse der anfallenden Daten,
- die örtlichen Gegebenheiten und
- ob die Datenträgerentsorgung in Eigenregie oder in Form einer Auftragsdatenverarbeitung stattfinden soll.

Dabei sollte es sich von selbst verstehen, dass die zu entsorgenden Datenträger nicht einfach dem normalen Hausmüll zugeführt werden.

e) Regelung der Zuständig- und Verantwortlichkeiten

Für die Datenträgerentsorgung sind die personellen Zuständig- und Verantwortlichkeiten für folgende Bereiche zu regeln:

- Einsammlung, Transport und Aufbewahrung der Datenträger
- Art der Vernichtung
- Kontrolle und Protokollierung des gesamten Ablaufs

f) (Zwischen)Lagerung des Entsorgungsguts

Eine Schwachstelle stellt häufig die ungesicherte Lagerung des Entsorgungsgutes bis zu seiner Vernichtung dar. Deshalb muss mit Hilfe der Maßnahmen der Zugriffskontrolle verhindert werden, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Datenträger mit personenbezogenen Daten sind bis zu ihrer endgültigen Vernichtung unter Verschluss in abschließbaren Räumen oder verschließbaren Containern aufzubewahren. Dafür muss eine Zugangsregelung bestehen. Der Schlüsselverwaltung kommt deshalb besondere Bedeutung zu. Bei der Auswahl von Container ist außerdem darauf zu achten, dass die Deckel ausreichend verstärkt sind, so dass das Vernichtungsgut nicht durch leichtes Anheben oder Verbiegen des Deckels entnommen werden kann. Die Befülleinrichtungen (Klappe, Schlitz) müssen außerdem so gestaltet sein, dass auch auf diesem Wege kein Material entnommen werden kann. Diese Vorgehensweise gilt sowohl für die Vernichtung in Eigenregie als auch für die Datenträgerentsorgung im Auftrag.

g) Transport der Datenträger

Eine datenschutzgerechte Datenträgerentsorgung muss auch den sicheren Transport des Vernichtungsgutes zur eigenen Vernichtungsanlage bzw. zum Entsorger einschließen, d. h. es muss ausgeschlossen sein, dass während des Transports Datenträger verloren gehen oder dass dabei Unbefugte auf schutzbedürftige Daten zugreifen können (Weitergabekontrolle).

Es ist deshalb notwendig, den Transport des Vernichtungsgutes in abgeschlossenen Containern durchzuführen, wie sie beispielsweise auch für die Sammlung verwendet werden. Dabei muss darauf geachtet werden, dass sich die Schlüssel für die Container nicht im Besitz des Transporteurs befinden.

Transportfahrzeuge müssen zudem mit einem passiven GPS-Ortungssystem ausgestattet sein, oder der Transport ist durch mindestens zwei Personen zu begleiten.

In besonders gelagerten Fällen, z. B. bei der Entsorgung geheimer, vor unbefugtem Zugriff besonders zu schützender Unterlagen, kann es zusätzlich notwendig sein, auch den Transportweg zu sichern.

h) Geeignetheit des Entsorgungskonzepts

Soweit ein derartiges Entsorgungskonzept überhaupt erstellt wird, ist es häufig auf den Standardfall ausgerichtet. Bei Archivaussonderungen und größeren Mengen zu entsorgenden Gutes erweist sich dieses Konzept häufig als nicht geeignet. Vielfach geraten dann beispielsweise Papierunterlagen in den Hausmüll und werden auf Deponien wieder gefunden.

i) Sensibilisierung und Unterrichtung der Mitarbeiter

Selbstverständlich müssen auch die verantwortlichen Entscheidungsträger, Administratoren und alle Mitarbeiter durch geeignete Information und Schulung zum Thema Datenträgerentsorgung sensibilisiert werden. Das Datenträgerentsorgungskonzept sollte daher auch den Mitarbeitern bekannt gegeben werden.

j) Dokumentation des Entsorgungsablaufs

Der gesamte organisatorische Ablauf ist schriftlich festzuhalten. Dabei ist auch zu berücksichtigen, dass es trotz aller Vorkehrungen zu Pannen kommen kann, die vielfach qualitative Beeinträchtigungen (z. B. Imageverlust), im Einzelfall auch quantitativ messbare Schäden nach sich ziehen. Die Organisation der Entsorgung von Datenträgern muss deshalb auch Maßnahmen zur Schadensbegrenzung vorsehen. Materielle Schäden können häufig durch eine entsprechende Versicherung abgedeckt werden. Soweit eigene Mitarbeiter an der Entsorgung beteiligt sind, müssen diese in den Ablauf und mögliche Fehlerquellen eingewiesen, über die gesetzlichen Bestimmungen belehrt und auf das Datengeheimnis verpflichtet werden.

5 Datenträgervernichtung in Eigenregie

Als sicherste – wenn auch nicht immer wirtschaftlichste – Lösung der Datenträgervernichtung wird weiterhin die unmittelbar nach Anfall ohne Zwischenlagerung erfolgende sofortige Entsorgung vor Ort angesehen, weil dadurch das Entsorgungsgut nicht in die Hände Dritter kommt und Risikostrecken weitgehend vermieden werden.

Die Entsorgung in Eigenregie findet in der Regel im eigenen Haus statt. Dabei bietet sich beim Anfall kleiner Mengen zu vernichtender Papierunterlagen der Einsatz kleinerer Aktenvernichter in den einzelnen Abteilungen an.

In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiter die Vernichtung ihrer Unterlagen durchzuführen haben. Sie sind dafür entsprechend zu schulen und zu einer sicheren Verwahrung der Unterlagen bis zu deren Vernichtung zu verpflichten.

a) Regelungsbedarf

Werden die Datenträger selbst vernichtet, empfiehlt es sich, insbesondere Folgendes zu regeln:

- Einsammlung, Transport und Aufbewahrung der Datenträger und personelle Zuständigkeiten
- Art der Vernichtung und personelle Zuständigkeiten
- Kontrolle und Protokollierung des gesamten Ablaufs

b) Festlegungen

Im Hinblick auf die Vernichtung von Datenträgern mit personenbezogenem Inhalt in Eigenregie 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.

Eine weitere Frage, die zu klären ist wäre, 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 Festlegung der abteilungsinternen Ver-

nichtung könnten 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 muss aber auch hier das Schutz- und Vertraulichkeitsbedürfnis der auf dem jeweiligen Datenträger 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. Daher sollten z. B. für die Sammlung keine unverschlossenen Behältnisse auf allgemein zugänglichen Fluren aufgestellt werden.

Somit ist darauf zu achten, dass nur wenige, berechtige Mitarbeiter Zugang zu diesen abgesicherten Räumlichkeiten erhalten.

Zu treffen sind angemessene technische und organisatorische Sicherungsmaßnahmen (z. B. gemäß Art. 7 Abs. 2 BayDSG), 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.

c) Geeignetheit der eingesetzten Geräte

Die für die Vernichtung eingesetzten Geräte wie z. B. Schredder sollten für die Mitarbeiter handhabbar und praktisch sein. Wer eine längere Zeit für die Entsorgung von Einzelblättern benötigt, weil der Schredder nur einen geringen Durchsatz hat, ist geneigt, unkontrollierte Wege der Entsorgung einzuschlagen.

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 66399 drei Sicherheitsklassen und sieben Sicherheitsstufen definiert. Nähere Informationen dazu können unter „3. Beachtung von Normen“ weiter oben nachgelesen werden.

d) Vernichtung von Papierunterlagen

Durch die Verbreitung der IuK-Technik ist bei vielen öffentlichen und nicht-öffentlichen Stellen das Erfordernis nach datenschutzgerechtem Umgang mit Papier im allgemeinen Bewusstsein in den Hintergrund gerückt. Dies ist jedoch nicht nachvollziehbar, denn gerade mit dem Einsatz der IuK-Technik hat die Produktion von schriftlichen Unterlagen auch mit personenbezogenen Daten enorm zugenommen.

Dabei wird häufig übersehen, dass nicht nur die elektronisch gespeicherten Daten vor unbefugter Kenntnisnahme u.a. zu schützen sind, sondern auch und nach wie vor gedruckte oder geschriebene personenbezogene Daten. Die besten und aufwändigsten Schutzmechanismen im Bereich der IuK-Technik relativieren sich hinsichtlich ihrer Wirksamkeit sofort, wenn andererseits personenbezogene Unterlagen/Akten in frei zugänglichen Räumen oder Gebäudeteilen offen gelagert werden oder wenn Fehlablichtungen, Fehldrucke, Zwischenmaterial oder korrigierte Schreiben u. ä. lediglich über normalen Hausmüll oder das allgemeine Altpapier entsorgt werden.

Gerade zur Entsorgung geringer Mengen von Papierabfällen bietet sich der Einsatz kleinerer **Aktenvernichter** in den einzelnen Abteilungen an. In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiter die Vernichtung ihrer Unterlagen durchzuführen haben. Sie sind dabei zu einer sicheren Verwahrung der Unterlagen bis zu deren Vernichtung zu verpflichten.

Im Wesentlichen unterscheidet man bei Aktenvernichtern heutzutage zwischen Streifenschnitt und Kreuzschnitt/Partikelschnitt. Während Streifenschnitt-Aktenvernichter das Papier lediglich in schmale Streifen (wie es der Name schon sagt) schneidet, schneiden sogenannte Cross-Cutter zusätzlich horizontale Schnitte. Damit liefern Cross-Cutter kleineres Schnittgut und entsprechen somit den höheren Sicherheitsanforderungen der DIN 66399.

e) Physikalische Löschung von magnetischen Datenträgern

Für die physikalische Löschung von magnetischen Datenträgern (z. B. Streamer Tapes) sind spezielle Löschgeräte erhältlich. Festplatten, die sich nicht mehr mittels Software-Tools komplett und mehrfach überschreiben lassen, müssen ebenfalls physikalisch zerstört bzw. mit Hilfe eines starken Magnetfeldes irreversibel gelöscht werden. Dabei ist aber zu bedenken, dass ein Durchbohren oder Häckseln von Festplatten nicht immer

zum gewünschten Erfolg führt, da hierbei zwar der Datenträger zerstört wird, die Daten dabei aber unter Umständen erhalten bleiben und wieder rekonstruiert werden können.

Aus diesen Gründen liegt gemäß den Empfehlungen des Centers for Magnetic Recording Research (CMRR) der USA und der Empfehlung 800-88 des US-Amerikanischen National Institute for Science and Technology (NIST) die komplette Zerstörung einer Festplattenoberfläche erst dann vor, wenn die resultierenden Partikel nicht mehr groß genug sind, um einen einzigen Speicherblock von 512 KB zu enthalten. Nur dann ist – zumindest nach derzeitigem Kenntnisstand – keine Datenwiederherstellung möglich.

f) Logisches Löschen

Häufig wird einem Anwender eine Datenlöschung suggeriert, die in Wirklichkeit überhaupt nicht stattfindet. So wird von System- und Anwendungsprogrammen beispielsweise dem Nutzer von IT-Geräten vor dem Löschen die Frage gestellt: „Wollen sie wirklich diese Daten endgültig löschen“. Dabei findet ein derartiger Löschvorgang gar nicht statt. So ist ein einfaches Löschen der Daten (so genanntes „Logisches Löschen“ – z. B. durch das Verschieben einer Datei in den Windows-Papierkorb oder durch Lösch- und Formatbefehle) in keinem Fall ausreichend, da beispielsweise bei der Benutzung von Löschbefehlen nicht tatsächlich die Daten gelöscht werden, sondern lediglich der Verweis auf diese Informationen im „Inhaltsverzeichnis“ (File Allocation Table = FAT) des Datenträgers entfernt wird. Die Datei selbst ist jedoch weiterhin vorhanden.

Es gibt eine Vielzahl von Programmen, die z. B. kostenlos über das Internet bezogen werden können, mit denen die scheinbar gelöschten Daten restauriert werden können. Beim High-Level-Formatieren wird zwar die gesamte FAT gelöscht, die eigentlichen Daten sind jedoch auch hier weiterhin vorhanden. Selbst nach einer Formatierung von Partitionen oder einer Low-Level-Formatierung (physikalisches Neuanlegen von Spuren und Sektoren eines Datenträgers) ist es – zwar aufwendig – möglich, die ursprünglichen Daten anhand von Restmagnetspuren wieder herzustellen.

g) Überschreiben von Dateien

Gelöschte Dateien verschwinden erst, wenn der von der gelöschten Datei belegte Bereich komplett überschrieben ist. Das kann sehr lange dauern, denn wenn die neuen Daten ein Cluster nicht vollständig belegen, bleibt die Information der gelöschten Datei

im restlichen Clusterbereich erhalten. Allerdings sind verschiedene (kostenpflichtige und kostenlose) Löschprogramme erhältlich, die entweder die gesamte Festplatte oder ausgewählte Teile davon komplett überschreiben. Beim Erwerb dieser Programme ist darauf zu achten, dass sie ein Mehrfachüberschreiben mit unterschiedlichen Bitmustern gewährleisten. Nur dann ist eine Wiederherstellung der Dateien nicht mehr möglich.

Um internationalen Standards gerecht zu werden, ist ein mehrmaliges Überschreiben erforderlich. So schreibt der U.S. Standard, DoD 5220.22-M (E) des amerikanischen Verteidigungsministeriums drei Schreibdurchläufe vor:

- Der 1. Durchlauf dient dem Überschreiben der Daten mit fest vorgegebenem Wert
- Der 2. Durchlauf überschreibt der Daten mit dem Komplementwert des ersten Durchlaufs
- Der 3. Durchlauf überschreibt die Daten mit Pseudo-Zufallswerten.

Eine erweiterte Variante des DoD 5220.22-M – der DoD 5220.22-M (ECE) verlangt sogar sieben Überschreibungsdurchläufe.

Auch das **BSI-Geheimschutzverfahren** verlangt, dass ein magnetischer Datenträger in sieben Durchgängen überschrieben werden muss, wobei bei den ersten sechs Durchgängen das Bitmuster des vorherigen Durchgangs umgekehrt wird.

Eine von Peter Gutmann entwickelte Methode nimmt insgesamt sogar 35 Überschreibungsdurchgänge der verschiedensten Art vor und gilt damit als derzeit zwar zeitaufwändigste, aber auch sicherste Methode.

Die Vorteile einer Datenlöschung mittels Überschreibung der Datenträger liegen insbesondere darin, dass die Tools sehr preisgünstig (z. T. auch kostenlos) sind und sie gezielt und flexibel einsetzbar sind. Ihr Hauptnachteil liegt darin, dass Daten auf defekten Datenträger mit Hilfe einer Softwarelösung im Regelfall nicht gelöscht werden können. Außerdem kann der Zeitaufwand für den Überschreibvorgang in Abhängigkeit von der Größe des Datenträgers und der Anzahl der Überschreibvorgänge mehrere Stunden betragen.

Außerdem hängt die Vertrauenswürdigkeit und Sicherheit dieses Löschverfahrens (siehe Maßnahmenkatalog M 2.433 „Überblick über Methoden zur Löschung und Vernichtung von Daten“ der BSI-IT-Grundschutzkataloge) von folgenden Faktoren ab:

- Die Software muss durch die Benutzer richtig eingesetzt werden. Eine fehlerhafte Anwendung kann dazu führen, dass der Datenträger nicht oder nur teilweise überschrieben wird.
- Die Konfiguration der Löschtools hat wesentliche Auswirkungen darauf, dass die Datenträger vollständig und zuverlässig gelöscht werden. Daher muss sichergestellt sein, dass die Tools optimal konfiguriert sind und die Einstellungen nicht durch Unbefugte verändert werden können.
- Die Löschsoftware muss gewährleisten, dass alle Bereiche des Datenträgers, auch die geschützten oder schadhaften Sektoren, in der gewünschten Weise überschrieben werden.

Bei einer lediglichen Überschreibung einzelner Dateien ist zu bedenken, dass durch Betriebssystem oder Anwendungen Kopien der Daten an ganz unterschiedlichen Orten abgelegt wurden, die die Benutzer häufig weder kennen oder kontrollieren können. So befinden sich gelöscht geglaubte Daten unter Umständen (z. B. als Zwischendateien oder temporäre Dateien, Sicherungskopien, Auslagerungsdateien) weiterhin auf dem Datenträger und lassen sich mit entsprechenden Verfahren auslesen. Daher sollte möglichst der komplette Datenträger gelöscht werden, um sicherzustellen, dass sich keine weiteren Kopien der Informationen auf dem Datenträger befinden.

h) Entmagnetisieren von magnetischen Datenträgern

Eine weitere Entsorgungsmöglichkeit von magnetischen Datenträgern besteht in deren Entmagnetisierung. Dabei kommen entsprechende Löschgeräte (so genannte Degausser) zum Einsatz, die eine weitgehende Entmagnetisierung der ursprünglich vorhandenen magnetischen Aufzeichnungen durch die Einwirkung eines externen Magnetfeldes vornehmen.

Durch das Magnetfeld des Löschgerätes werden die aufgezeichneten magnetischen Domänen auf den Datenträgern zerstört. Bei Verwendung eines geeigneten Löschgerätes sind deshalb nach dem Löschen auf dem Datenträger keine Informationen mehr vorhanden.

Der Vorteil beim Löschen mit einem Löschgerät besteht darin, dass mit geringem Zeitaufwand der gesamte Datenträger sicher gelöscht werden kann. Allerdings ist zu beachten, dass Festplatten und verschiedene Arten von Magnetbändern nach dem Lö-

schen nicht mehr verwendet werden können, weil mit den aufgezeichneten Daten auch die Servospur, mit der der Schreib-/ Lesekopf gesteuert wird, gelöscht wird. Eine Wiederverwendung der Datenträger ist somit lediglich bei Disketten und Magnetbändern ohne Servospuren möglich.

Außerdem stellen Degausser eine vergleichsweise teure Lösung dar, da brauchbare Geräte zwischen 20.000 und 60.000 Euro kosten. Desweiteren können diese Löschgeräte nur bei magnetischen Datenträgern eingesetzt werden, für DVD, CD und Flashspeicher sind sie nicht geeignet.

i) Vernichtung optischer Datenträger

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.

j) Rückgabe von geleasten Festplatten

Bei der Rückgabe von geleasten (defekten) Festplatten sollte dem Dienstleister mittels Vertrag verboten werden, die auf dem Datenträger gespeicherten personenbezogenen Daten zu kopieren, sie weiterzugeben oder selbst zu verwenden. Stattdessen sollte er dazu verpflichtet werden, die Daten unwiederbringlich zu löschen bzw. die Festplatte zu vernichten.

k) Vernichtung von Mikrofilmen und -fiches

Bei Mikrofilmen und -fiches reicht zu Sicherstellung der Unlesbarkeit ein Zerschneiden in den Papieraktenvernichtern nicht aus. Auch für diese Datenträger sind spezielle Geräte auf dem Markt, die das zu entsorgende Datengut in kleinste Partikel schneiden, pulverisieren oder einschmelzen.

I) Checkliste zur Datenträgerentsorgung in Eigenregie

Die folgende Checkliste soll zur Gewährleistung des Datenschutzes und der Datensicherheit bei der Datenträgerentsorgung in Eigenregie beitragen, kann aber natürlich nicht alle denkbaren Aspekte (insbesondere hinsichtlich aller Datenträgerarten) abdecken.

Frage	Ja	Nein	Anmerkungen
Sind die gesetzlichen Verpflichtungen zur Datenlöschung bekannt?	□	□	
Wurde ein Entsorgungskonzept entwickelt?	□	□	
Wurde eine Verfahrensanweisung bezüglich der Datenträgerentsorgung erlassen?	□	□	
Werden die Regelungen zur Datenträgerentsorgung in Eigenregie ständig aktualisiert?	□	□	
Werden die Maßnahmen regelmäßig auf ihre Wirksamkeit hin untersucht?	□	□	
Ist die Verfahrensanweisung jeden Beschäftigten bekannt?	□	□	
Wird die Einhaltung der Anweisung überwacht?	□	□	
Wurden die Verantwortlichkeiten für die Regelung und Überwachung der Datenträgerentsorgung festgelegt?	□	□	
Sind die mit der Datenträgerentsorgung beauftragten Mitarbeiter bezüglich der datenschutzgerechten Entsorgung geschult und un-	□	□	

Frage	Ja	Nein	Anmerkungen
terwiesen?			
Wurde festgelegt, welche Datenträger zu entsorgen sind?	□	□	
Werden die zu vernichtenden Datenträger zentral gesammelt?	□	□	
Stehen für die Aufbewahrung der zu entsorgenden Datenträger geeignete Sammelbehälter und/oder Lagerräumlichkeiten zur Verfügung, die stets unter Verschluss gehalten werden?	□	□	
Wird auch beim Transport des Vernichtungsgutes zur eigenen Vernichtungsanlage bzw. zur Sammelstelle der Datenschutz eingehalten?	□	□	
Erfolgt die Entsorgung der Datenträger hinsichtlich ihrer Art und der Sensibilität der Daten gemäß den Forderungen der DIN 66399?	□	□	
Entsprechen die für die Entsorgung eingesetzten Maschinen den gewünschten Anforderungen der DIN 66399?	□	□	
Findet zumindest bei der Vernichtung sensibler Daten eine Protokollierung der Tätigkeiten statt?	□	□	
Finden zumindest stichprobenartige Überprüfungen der Datenträgerentsorgung statt?	□	□	

6 Vernichtung von Datenträgern in Form einer Auftragsdatenverarbeitung

Auf die Vernichtung von Datenträgern im Auftrag wird zwar bereits in der Orientierungshilfe „Auftragsdatenverarbeitung“ (ebenfalls abrufbar auf unserer Homepage im Bereich „Veröffentlichungen/Orientierungshilfen“ eingegangen. Trotzdem soll an dieser Stelle noch einmal auf die wichtigsten Punkte eingegangen werden.

a) Arten der Datenträgerentsorgung im Auftrag

Bei der Datenträgerentsorgung im Auftrag muss zwischen stationärer und mobiler Entsorgung unterscheiden werden. Die Mehrzahl der beauftragten Entsorgungsunternehmen führt die Vernichtung von Datenträgern mit fest installierten Geräten durch, die in ein geschlossenes Entsorgungskonzept integriert sind. Gelegentlich wird jedoch auch die mobile Vernichtung angeboten. Das Entsorgungsunternehmen fährt dabei beispielsweise bei einer Papierentsorgung mit einem geschlossenen Lastkraftwagen beim Kunden vor, auf dem ein mit einer Ballenpresse kombinierter Reißwolf montiert ist, und vernichtet die Datenträger vor Ort. Diese Art der Auftragsdatenverarbeitung kann natürlich besser überwacht werden, da sie ja auf dem Gelände des Auftraggebers geschieht. Allerdings scheidet dieses Verfahren aus Gründen des Lärmschutzes oder wegen bestehender Verkehrsbeschränkungen in dicht besiedelten Gebieten häufig aus.

b) Gefahren

So manche Behörde erlebte bei der Datenträgervernichtung im Auftrag bereits einige unangenehme Überraschungen, beispielsweise in der Form, dass sie einer Zeitung entnehmen musste, dass ihre Akten von spielenden Kindern ungeschützt in dem Hof eines Altpapierhändlers gefunden wurden.

Vertragsstrafen können zwar dabei helfen, einen etwaig entstehenden materiellen Schaden ersetzen zu können, aber in einem Schadensfall bleibt zumindest die Rufschädigung. Besonders groß kann das Risiko bei einem Auftragnehmer sein, der weniger an einer datenschutzgerechten Entsorgung von Datenträgern interessiert ist, sondern dessen Geschäftsziel in erster Linie die Wiederverwendung von Rohstoffen ist.

c) Verantwortung für die Einhaltung des Datenschutzes

Deshalb ist es für alle Stellen wichtig, die eine Datenträgerentsorgung im Auftrag vornehmen lassen, sich nicht nur die datenschutzgerechte Entsorgung der Datenträger vom Auftragnehmer schriftlich bescheinigen zu lassen, sondern auch Kontrollen bei den mit der Entsorgung beauftragten Vertragsfirmen vorzunehmen, um mögliche Schwachstellen leichter erkennen zu können. Der Auftraggeber trägt schließlich auch dann die Verantwortung für die Einhaltung der Datenschutzvorschriften, wenn er einen Auftragnehmer mit der Vernichtung der Datenträger mit personenbezogenen Daten beauftragt (Art. 6 Abs. 1 Satz 1 BayDSG).

d) Sorgfältige Auswahl des Auftragnehmers

Der Auftraggeber muss einen Auftragnehmer unter Berücksichtigung seiner Eignung und der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen (Art. 6 Abs. 2 Satz 1 BayDSG). Zu einer sorgfältigen Auswahl eines Auftragnehmers gehört es auch, dass vor Vertragsabschluss geprüft wird, ob der Auftragnehmer die geforderte Sicherheit in allen seiner Zuständigkeit unterliegenden Phasen gewährleisten kann, ob er einen fachkundigen Datenschutzbeauftragten gemäß § 4f Abs. 2 BDSG bestellt und seine Mitarbeiter über die Bestimmungen des BDSG unterrichtet und auf die Wahrung des Datengeheimnisses nach § 5 BDSG verpflichtet hat. Auch sollten entsprechende Referenzen über den Auftragnehmer eingeholt werden.

e) Vertragsgestaltung

Gemäß Art. 6 Abs. 2 Satz 2 BayDSG muss ein Auftrag schriftlich erteilt werden. Im Vertrag muss insbesondere klar geregelt sein,

- für welche Phasen der Auftragnehmer zuständig sein soll,
- wie die Übergabe der Datenträger erfolgt,
- dass die Vernichtung außer in genau festgelegten Ausnahmefällen unverzüglich entsprechend den Weisungen des Auftraggebers zu erfolgen hat,
- welche technisch-organisatorischen Maßnahmen bestehen oder noch zu treffen sind,

- ob der Auftragnehmer Subunternehmer einschalten darf und unter welchen Bedingungen.

Weiterhin sollte festgelegt werden, dass der Auftragnehmer den Auftraggeber über alle Vorfälle (z. B. Betriebsstörungen oder Fehler) zu informieren hat, die zu einem Schaden für den Auftraggeber führen können. Mindestens für derartige Fälle müssen Haftung und Schadensersatz geregelt und die Möglichkeit der außer-ordentlichen Kündigung vorgesehen werden.

Bei der Vernichtung von personenbezogenen Daten im Auftrag ist insbesondere Folgendes vertraglich zu regeln:

- Festlegung der Art und Menge der zu entsorgenden Datenträger und der dabei zu berücksichtigenden Schutzstufe
- Auswahl eines geeigneten Vernichtungsverfahrens
- Schriftliche Vertragsgestaltung
- Bestimmung des Ortes und des Zeitpunktes der Vernichtung (z. B. unverzüglich vor Ort beim Auftraggeber oder in der Betriebsstätte des Auftragnehmers) und der dabei zu ergreifenden Maßnahmen der Zutrittskontrolle (z. B. Maßnahmen zur Gebäudesicherung)
- Festlegung der Verantwortlichkeiten für die Aufbewahrung (in mit Sicherheitsschlössern ausgestatteten Containern oder verschlossen Lagerräumen) und den Transport der Datenträger (evtl. durch Subunternehmer) und der dabei zu ergreifenden Maßnahmen der Transportkontrolle (z. B. Beschreibung der Transportwege und von Transportbehältnissen)
- Verpflichtung des Personals des Auftragnehmers auf das Datengeheimnis
- Gewährleistung durch den Auftraggeber, dass Unbefugte keine Kenntnis der auf den Datenträgern gespeicherten Daten erhalten können
- Verpflichtung des Auftraggebers zur lückenlosen Protokollierung des gesamten Entsorgungsvorgangs
- Informationspflicht des Auftraggebers in bestimmten Ausnahmefällen (beispielsweise bei Betriebsstörungen, im Fehlerfalle, bei Verstößen)
- Möglichkeiten der außerordentlichen Kündigung bei Vertragswidrigkeiten
- Haftungsregelung

- Regelung von Unterauftragsverhältnissen
- Berechtigung des Auftraggebers zur Durchführung von Kontrollen bei der Aufbewahrung, dem Transport und bei der Vernichtung der Datenträger
- Festlegung von Art und Form der zu übergebenden Bescheinigungen bei Abholung bzw. nach der ordnungsgemäßen Vernichtung durch den Auftragnehmer bei jedem Entsorgungsvorgang

f) Überprüfung der Einhaltung der technisch-organisatorischen Sicherheitsmaßnahmen

Ein Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (Art. 6 Abs. 2 Satz 3 BayDSG). Bereits vor Vertragsunterzeichnung sollte der Auftraggeber deshalb vor Ort überprüfen, ob der Auftragnehmer auch tatsächlich dazu in der Lage ist, die datenschutzgerechte Entsorgung sicherzustellen (z. B. ob die eingesetzten Gerätschaften den Anforderungen der DIN 66399 entsprechen). Der Auftraggeber darf sich nicht mit der Erklärung eines Auftragnehmers zufrieden geben, dass dieser die Vorschriften der Datenschutzgesetze beachten werde. Auch die ordnungsgemäße Durchführung der Vernichtung der Datenträger ist sporadisch zu überprüfen. Dazu sollten bei der Vertragsgestaltung mit den beauftragten Entsorgungsunternehmen das Recht auf unangemeldete Kontrollen bei der Entsorgung und angemessene Vertragsstrafen für den Fall der Verletzung von Datenschutzvorschriften durch das beauftragte Unternehmen vereinbart werden.

g) Mustervertrag über die Vernichtung von Datenträgern

Einen Mustervertrag über die Vernichtung von Datenträgern als Form der Auftragsdatenverarbeitung finden Sie auf unserer Homepage im Bereich „Veröffentlichungen/Mustervordrucke“.

h) Checkliste zur Vernichtung von Datenträgern in Form einer Auftragsdatenverarbeitung

Die folgende Checkliste soll zur Gewährleistung des Datenschutzes und der Datensicherheit bei der Datenträgerentsorgung in Form einer Auftragsdatenverarbeitung beitragen, kann aber natürlich nicht alle denkbaren Aspekte (insbesondere hinsichtlich aller Datenträgerarten) abdecken.

Frage	Ja	Nein	Anmerkungen
Sind die gesetzlichen Verpflichtungen zur Datenlöschung bekannt?	□	□	
Wurde ein Entsorgungskonzept entwickelt?	□	□	
Wird oder wurde der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt?	□	□	
Wurde der Auftragnehmer bereits von der zuständigen Aufsichtsbehörde überprüft?	□	□	
Liegt ein schriftlicher Vertrag vor?	□	□	
Ist im Vertrag detailliert geregelt, für welche Phasen der Datenträgervernichtung der Auftragnehmer zuständig ist und was er dabei zu beachten hat?	□	□	
Wurde eindeutig festgelegt, welche Sicherheitsmaßnahmen zu ergreifen sind?	□	□	
Wurden die Arbeitnehmer des Auftragnehmers auf das Datenschutz-	□	□	

Frage	Ja	Nein	Anmerkungen
geheimnis verpflichtet?			
Sind die mit der Datenträgerentsorgung beauftragten Mitarbeiter des Auftragnehmers bezüglich der datenschutzgerechten Entsorgung geschult und unterwiesen?	□	□	
Wurde festgelegt, welche Datenträger auf welche Art und Weise zu entsorgen sind?	□	□	
Wurde der Auftraggeber dazu verpflichtet, zu gewährleisten, dass Unbefugte keine Kenntnis der auf den Datenträgern gespeicherten Daten erhalten können?	□	□	
Beinhaltet der Vertrag Aussagen zu eventuellen Haftungs- und Schadensersatzfragen?	□	□	
Wurde das Kontrollrecht des Auftraggebers und die Art und Weise der Kontrollgestaltung in den Vertrag aufgenommen?	□	□	
Wurde geregelt, ob und unter welchen Bedingungen der Auftragnehmer Subunternehmer einschalten darf?	□	□	
Stehen für die Zwischenaufbewahrung der zu entsorgenden Datenträger geeignete Sammelbehälter und/oder Lagerräumlichkeiten zur Verfügung, die stets unter Verschluss gehalten werden?	□	□	

Frage	Ja	Nein	Anmerkungen
Wird beim Transport des Vernichtungsgutes zur Vernichtungsstelle der Datenschutz eingehalten?	□	□	
Erfolgt die Entsorgung der Datenträger hinsichtlich ihrer Art und der Sensibilität der Daten gemäß den Forderungen der DIN 66399?	□	□	
Entsprechen die für die Entsorgung eingesetzten Maschinen den gewünschten Anforderungen der DIN 66399?	□	□	
Findet eine Protokollierung der Datenträgervernichtung statt?	□	□	
Finden zumindest stichprobenartige, unangemeldete Überprüfungen der Datenträgerentsorgung vor Ort statt?	□	□	

Autor: Udo Höhn