Informationen zur neuen DIN 66399

Vorbemerkung:

Die DIN 32757 war eigentlich nie als Norm gedacht, an der sich die Dienstleister bei der Datenträger- und Aktenvernichtung orientieren sollten sondern sie war vielmehr für die Hersteller von Kleingeräten zur Daten- und Papiervernichtung gedacht. Gleichwohl haben sich in der Vergangenheit in Ermangelung anderer Vorgaben, auch Dienstleister an dieser Norm orientiert.

Allerdings war die DIN 32757 zwischenzeitlich in die Jahre gekommen und musste dringend den heutigen technischen Möglichkeiten und Gegebenheiten angepasst werden.

Das Ergebnis ist eine wirklich praktikable Norm, die den heutigen Stand der Technik widerspiegelt, die DIN 66399

Diese Norm bildet mit ihrem 3. Teil – der DIN SPEC -erstmals sogar den Prozess der Datenträgervernichtung ab.

Als „Datenträger" im Sinne der DIN 66399 wird jeder Informationsträger definiert, auf oder in dem Daten (Informationen) vorübergehend oder auch dauerhaft gespeichert werden können.(siehe auch unten DIN 66399-2)

Struktur der DIN 66399:

Die DIN 66399 besteht aus drei Teilen:

DIN 66399-1	Grundlagen und Begriffe
DIN 66399-2	Anforderungen an Maschinen zur Vernichtung von Datenträgern
DIN SPEC 66399-3	Prozess der Datenträgervernichtung

DIN 66399-1 Grundlagen und Begriffe

Damit bei der Datenträgervernichtung nicht mit „Kanonen auf Spatzen" geschossen wird, muss der Datenverantwortliche zunächst die zu vernichtenden Daten in Schutzklassen einteilen. Dadurch nimmt er auch direkt Einfluss auf die Vernichtungskosten, denn je höher die Schutzklasse ist, desto aufwendiger, und damit teurer ist der Vernichtungsprozess. Der Datenverantwortliche hat die Wahl zwischen drei Schutzklassen:

Schutzklasse 1: normaler Schutzbedarf für interne Daten, z.B.

- Telefonlisten
- Preislisten
- Produktlisten
- Lieferantendate
- Adressdaten

Schutzklasse 2: Hoher Schutzbedarf für vertrauliche Daten, z.B.

- Betriebswirtschaftliche Auswertungen
- Interne Reports
- FiBu_Unterlagen
- Jahresabschlüsse/Bilanzen

Schutzklasse 3: sehr hoher Schutzbedarf für besonders geheime Daten, z.B.

- Unterlagen der Staatsanwaltschaft, z.B. über Zeugenschutzprogramme
- Geheime Unterlagen staatlicher Organe
- Geheime Forschungs- und Entwicklungsunterlagen, usw.

Nachdem der Datenverantwortliche die zu vernichtenden Daten einer Schutzklasse zugeordnet hat, muss er sich noch Gedanken darüber machen, mit welcher der sieben Sicherheitsstufen die Datenträger vernichtet werden sollen:

Sicherheitsstufe 1: **Allgemeine Daten**
Reproduktion mit einfachem Aufwand

Sicherheitsstufe 2: **Interne Daten**
Reproduktion mit besonderem Aufwand

Sicherheitsstufe 3: **Sensible Daten**
Reproduktion mit erheblichem Aufwand

Sicherheitsstufe 4: **Besonders sensible Daten**
Reproduktion mit außergewöhnlichem Aufwand

Sicherheitsstufe 5: **Geheim zu haltende Daten**
Reproduktion mit zweifelhaften Methoden

Sicherheitsstufe 6: **Geheime Hochsicherheitsdaten**
Reproduktion technisch nicht möglich

Sicherheitsstufe 7: **Top Secret Hochsicherheitsdaten**
Reproduktion ausgeschlossen.

Schutzklassen-/Sicherheitsstufen-Zuordnung

Schutzklasse	**Sicherheitsstufen**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	**X***	**X***	**X**				
2			**X**	**X**	**X**		
3				**X**	**X**	**X**	**X**

* für personenbezogene Daten ist diese Kombination nicht anwendbar

In der Praxis hätte die oben gezeigte Zuordnung von Schutzklassen und Sicherheitsstufen zur Folge, dass die Datenträger entsprechend ihrer Klassifizierung natürlich auch getrennt

gesammelt und zur Vernichtung gegeben werden müssen. Es ist zu befürchten, dass der eine oder andere Datenverantwortliche dann entscheidet, dass die gesammelten Datenträger eben nicht entsprechend ihrer eigentlichen Klassifizierung vernichtet werden, sondern unter Kostenaspekten in der „günstigeren" Klasse. Sollten anschließend rekonstruierte Daten aus dieser Vernichtungsaktion wieder an unerwünschter Stelle auftauchen, hat er ein Haftungsproblem, da er die Vernichtung nicht nach den aktuellen Regeln der Technik vorgenommen hat.

DIN 66399 – 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern

Dieser Teil der DIN regelt abhängig von der Datenträgerart und der jeweiligen Sicherheitsstufe die Partikelgröße nach erfolgter Datenträgervernichtung.

Jeder Datenträgerart ist mit einem Leitbuchstaben gekennzeichnet, der der jeweiligen Sicherheitsstufe vorangestellt wird. Alle Leitbuchstaben zusammen bilden das Wort [**PFOTHE]:**

P Informationsdarstellung in Originalgröße: **[P]**apier, Film, Druckformen
Bezeichnung: P1 – P7

F Informationsdarstellung verkleinert: **[F]**ilm, Microfilm, Folie
Bezeichnung: F1 – F7

O Informationsdarstellung auf **[o]**ptischen Datenträgern: CD, DVD
Bezeichnung: O1 – O7

T Informationsdarstellung auf magnetischem Datenträger: Disketten, ID-Karten, Magnetbandkassetten (**[T]**apes)
Bezeichnung: T1 – T7

H Informationsdarstellung auf Festplatten mit magnetischem Datenträger: Festplatten **[H]**DD
Bezeichnung: H1 – H7

E Informationsdarstellung auf **[e]**lektronischen Datenträgern: Speicherstick, Chipkarte, Halbleiterfestplatten, mobile Kommunikationsmittel
Bezeichnung: E1 – E7

Beispiel: Schutzklassen-/Sicherheitsstufen-Zuordnung für papierene Datenträger

Schutzklasse	**Sicherheitsstufen z.B. für Papier-Datenträger**						
	P1 Partikelgröße max 3.800 mm^2	**P2** Partikelgröße max 2.000 mm^2	**P3** Partikelgröße max 800 mm^2	**P4** Partikelgröße max 480 mm^2	**P5** Partikelgröße max 90 mm^2	**P6** Partikelgröße max 30 mm^2	**P7** Partikelgröße max 5 mm^2
1	**X***	**X***	**X**				
2			**X**	**X**	**X**		
3				**X**	**X**	**X**	**X**

Zum Vergleich: In der gebräuchlichsten Sicherheitsstufe 3 der „alten" DIN 32757-1 dürfen die Partikel eine Teilchenfläche von maximal 320 mm^2 haben.

DIN-SPEC-66399-3: Prozesse der Datenträgervernichtung

Dieser Teil der DIN ist kein offizieller Teil der Norm, sondern wurde vom Arbeitsausschuss „Vernichtung von Datenträgern" im Normenausschuss Informationstechnik und Anwendungen (NIA) ausgearbeitet. Dieser Teil der dient der Regelung der praktischen Umsetzung des Vernichtungsprozesses, d.h. er befasst sich mit den technischen und organisatorischen Anforderungen des Vernichtungsprozesses. Dieser Prozess beginnt an der Stelle, an der die zu vernichtenden Datenträger anfallen („Anfallstelle") und endet an der Stelle, an der sie verwertet werden. D.h. es werden hier die einzelnen Prozessabläufe im Ganzen betrachtet und bewertet.

Im Einzelnen wird dabei zwischen den folgenden Prozessabläufen unterschieden:

Variante 1. Datenträgervernichtung durch den Kunden selbst

Bei dieser Variante sollten die an der Vernichtung beteiligten Mitarbeiter zum einen auf den Schutzbedarf der zu vernichtenden Datenträger explizit hingewiesen werden und sollten auch schriftlich auf die Einhaltung des das Datengeheimnisses gemäß ³ 5 BDSG hingewiesen werden. Darüber hinaus muss schriftlich definiert werden, welche technischen und organisatorischen Maßnahmen zur Sicherheit der zu vernichtenden Datenträger getroffen wurden, und es muss nachgewiesen werden, dass entsprechend der Kategorisierung der Datenträger geeignete Maschinen zur Vernichtung verwendet wurden.

Variante 2. Datenträgervernichtung beim Kunden durch externen Dienstleister

Alle am Vernichtungsprozess beteiligten Mitarbeiter müssen schriftlich auf das Datengeheimnis verpflichtet werden.

Die verantwortliche Stelle legt fest in welchem Umfang der Dienstleister am Vernichtungsprozess beteiligt wird: z.B. kann der Dienstleister Aluboxen zum Sammeln der Datenträger aufstellen, wobei geregelt werden muss, wer auf die eigentlich verschlossenen Boxen Zugriff hat, wer für die Verständigung des Dienstleisters zuständig ist usw. Es muss auch wieder sichergestellt sein, dass die entsprechend des Schutzziels der Datenträger geeigneten Maschinen zur Vernichtung eingesetzt werden. Die Mitarbeiter des Dienstleisters dürfen keinen Zugriff auf Datenträger erlangen können und die Einfüllöffnung der Vernichtungsmaschine muss per Video überwacht werden. Der Dienstleister muss sicherstellen, dass bei einem Defekt der Vernichtungseinrichtung geeignete Redundanzen zur Verfügung stehen.

Das Fahrzeug muss über einen festen, verschließbaren Aufbau für die Vernichtungseinrichtung und das Schreddergut verfügen.

DIN-SPEC-66399-33. Datenträgervernichtung beim externen Dienstleister

Dieser Teil der DIN ist keine offizielle Norm des Deutschen Instituts für Normung, sondern wurde im Normenausschuss Informationstechnik und Anwendung (NIA) vom Arbeitsausschuss „Vernichtung von Datenträgern" ausgearbeitet und beschreibt die technischen und organisatorischen Anforderungen an den Prozess der Datenträgervernichtung, abhängig von der jeweiligen Schutzklasse. Außerdem gibt dieser inoffizielle Teil der DIN administrative Empfehlungen zum Inhalt von Übernahme- und Vernichtungsprotokoll.

Im **Übernahmeprotokoll** wird – die Bezeichnung lässt es vermuten – die Übernahme der Datenträger mit dem Namen des übernehmenden Transportmitarbeiters aufgeführt, die Datenträgerkategorie(en),

die nach Vorgaben des Kunden übernommen wurden, in welche Art, Anzahl und/oder Gewicht der Behälter die Datenträger übernommen wurden, Datum und Uhrzeit der Übernahme, Kfz-Kennzeichen des Transportfahrzeugs sowie Unterschrift vom Mitarbeiter sowohl des Dienstleisters als auch des übergebenden Kunden.

Im **Vernichtungsprotokoll** soll angegeben werden auf welcher vertraglichen Basis (Angebot vom…, Vernichtungsrahmenvertrag vom….) die Vernichtung durchgeführt wird, an welchem Tag, zu welcher Uhrzeit und von welcher Person (Name) sie durchgeführt wurde. Außerdem ist anzugeben die Datenträgerart, Menge, verwendete Vernichtungstechnik (z.B. Schredder oder Degausser) und in welcher Sicherheitsstufe vernichtet wurde.