

AKTEN

VERNICHTUNG?



JA! MUSS!

ABER BITTE DATENSCHUTZKONFORM!



THE AGENDA

1) DIN 66399 BÜRO- UND DATENTECHNIK – VERNICHTEN VON DATENTRÄGERN

- Warum?
- DIN 66399-1: Grundlagen und Begriffe
- DIN 66399-2: Anforderungen an Maschinen
- DIN 66399-3: Prozess der Datenträgervernichtung

2) STAND DER TECHNIK – DOOF, ABER SO ISSES!

- Handaktenvernichter, Großaktenvernichter oder Dienstleister

THE AGENDA

3) EXTERNER DIENSTLEISTER – DIE WICHTIGSTEN FRAGEN UND HINWEISE

- Checkliste

4) DATENSCHUTZ UND MEDIZIN – ACHTUNG, LIEBE GEHEIMNISTRÄGER!

- §203 StGB
- §203 StGB und Aktenvernichtung
- Bedeutet...

THE AGENDA

5) MIT DER DATENSCHUTZGRUNDVERORDNUNG KOMMT'S NOCH DICKER...

- Mögliche Strafen
- Rechenbeispiel

DIN 66399

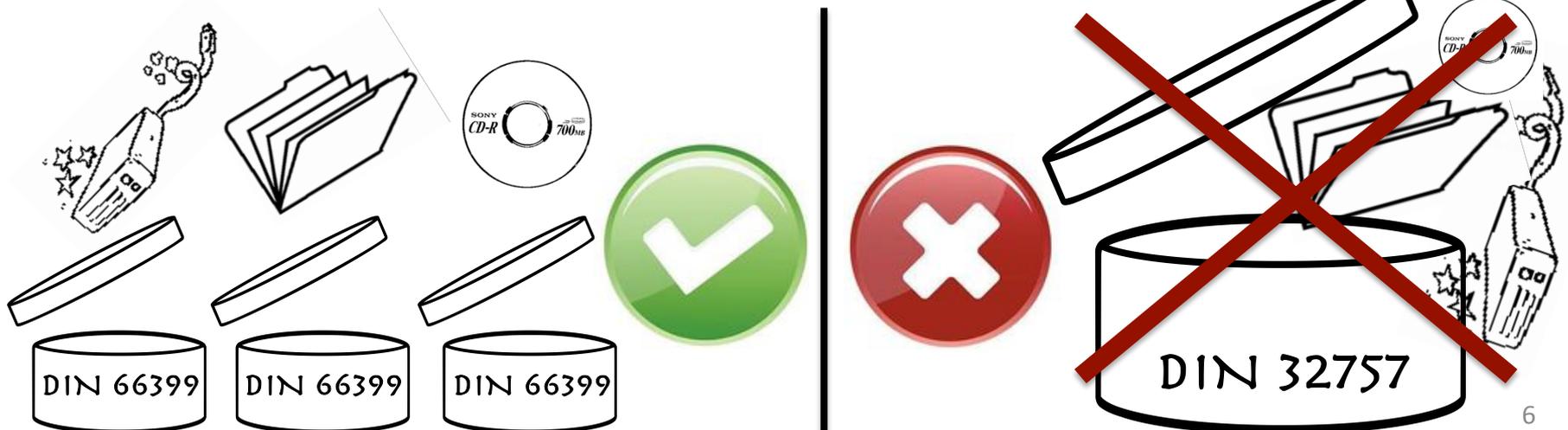


DIN 66399



WARUM?

- Die **DIN 66399** „Büro- und Datentechnik – Vernichtung von Datenträgern“ greift die Besonderheiten der vielseitigen digitalen Datenträger auf und legt somit einen **neuen Standard** fest.
- Die neue **DIN 66399** ersetzt seit 2012 die in die Jahre gekommene DIN 32757



DIN 66399

Teil 1

Grundlagen und Begriffe

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



- Jedes Unternehmen ist Produzent von Daten und muss sich daher zwangsläufig mit deren Vernichtung auseinandersetzen.
- Als Hilfestellung legt die DIN 66399 **drei Schutzklassen** und **sieben Sicherheitsstufen** fest und setzt diese in Beziehung zueinander.

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



Ermittlung des Schutzbedarfs und Zuordnung der Schutzklasse

Um bei der Datenträgervernichtung dem Wirtschaftlichkeits- bzw. Angemessenheitsprinzip Rechnung zu tragen, ist es notwendig, die Daten in Schutzklassen einzuteilen.

Schutzklasse 1	NORMALER SCHUTZBEDARF FÜR INTERNE DATEN: Unberechtigte Offenlegung oder Weitergabe hätte begrenzte negative Auswirkungen auf das Unternehmen.
Schutzklasse 2	HOHER SCHUTZBEDARF FÜR VERTRAULICHE DATEN: Eine unberechtigte Weitergabe hätte erhebliche Auswirkungen auf das Unternehmen und könnte gegen vertragliche Verpflichtungen oder Gesetze verstoßen.
Schutzklasse 3	SEHR HOHER SCHUTZBEDARF FÜR BESONDERS VERTRAULICHE UND GEHEIME DATEN: Zugriffsberechtigten erforderlich. Eine unberechtigte Weitergabe hätte ernsthafte (existenzbedrohende) Auswirkungen auf das Unternehmen und/oder würde gegen Berufsgeheimnisse, Verträge und Gesetze verstoßen.

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



DIE SCHUTZKLASSEN...

- Helfen Ihnen dabei das **angemessene Schutzniveau** Ihrer Daten zu bestimmen.
- Stellen Sie sich bei der Wahl der Schutzklasse bei allen Daten die Frage:

„Wie hoch ist der **persönliche oder unternehmerische Schaden, wenn Dritte diese Information in die Finger bekommen oder verstoße ich sogar gegen Verträge oder mein Berufsgeheimnis, wenn Dritte diese Information einsehen?“**

- Desto höher die gewählte Schutzklasse, desto höher die Schutzmaßnahmen beim Vernichtungsprozess, desto höher die Sicherheit.

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



Der Grad der Schutzbedürftigkeit ist ausschlaggebend für die zu treffende Wahl der Sicherheitsstufe in Bezug auf die Vernichtung der Datenträger.

Sicherheitsstufe	Erläuterung
1	Allgemeines Schriftgut , das unlesbar oder entwertet werden soll.
2	Interne Unterlagen , die unlesbar gemacht oder entwertet werden sollen.
3	Sensible und vertrauliche Daten sowie personenbezogene Daten, die einem höheren Schutzbedarf unterliegen.
4	Besonders sensible und vertrauliche Daten sowie personenbezogenen Daten , die einem erhöhten Schutzbedarf unterliegen.
5	Geheim zu haltende Informationen mit existenzieller Wichtigkeit für eine Person, ein Unternehmen oder eine Einrichtung.
6	Geheim zu haltende Unterlagen, wenn außergewöhnliche Sicherheitsvorkehrungen einzuhalten sind.
7	Strengst geheim zu haltende Daten, bei denen höchste Sicherheitsvorkehrungen einzuhalten sind.

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



DIE SICHERHEITSTUFEN...

- Legen fest, wie groß das einzelne geschredderte Stück Akte/ Papier/ Festplatte etc. nach der Vernichtung sein darf.
- Das bedeutet für Sie:

**Desto höher die gewählte Sicherheitsstufe,
desto kleiner die Partikel,
desto schwieriger die Reproduktion,
desto höher der Schutz Ihrer Daten
bei und nach der Vernichtung.**

DIN 66399-1

GRUNDLAGEN UND BEGRIFFE



Zuordnung von Schutzklassen und Sicherheitsstufen

SCHUTZKLASSE	SICHERHEITSTUFE						
	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

Vermischen und Verpressen (...) erschwert die Reproduktion. Eine Beeinflussung des möglichen Informationsgehaltes einzelner Materialteilchen erfolgt hierdurch nicht.

Zum Beispiel

- Sie sind Geheimnisträger und bestimmen für Ihre zu vernichtenden Akten folglich selbst ein hohes Schutzniveau, da die Dokumente solche Informationen wie Namen, Anschrift, Befund, Medikation etc. enthalten
→ Schutzklasse 3
- Der DIN 66399 entsprechend bedingt die Schutzklasse 3 mindestens die Sicherheitsstufe P-4. Jedoch sind Sie verpflichtet Ihr Berufsgeheimnis zu wahren und entscheiden sich für die **Sicherheitsstufe P-6**.
- Ergo: Während des gesamten Prozesses kann niemand die Akten einsehen, das Höchstmaß an Sicherheitsvorkehrungen wird eingehalten und ein einzelner Schnipsel der vernichteten Akte ist nicht größer als 10 qmm.

DIN 66399

Teil 2

Anforderungen an
Maschinen zur Vernichtung
von Datenträgern

DIN 66399-2

ANFORDERUNGEN AN MASCHINEN



Materialbezug der Sicherheitsstufen – **PFOT(H)E ;-**

	ART DER DARSTELLUNG	BEISPIEL
P	Informationsdarstellung in Originalgröße	Papier, Filme, Druckformen
F	Informationsdarstellung verkleinert	Film, Folie
O	Informationsdarstellung auf optischen Datenträgern	CD, DVD
T	Informationsdarstellung auf magnetischem Datenträger	Disketten, ID-Karten, Magnetbandkassetten
H	Informationsdarstellung auf Festplatten mit magnetischem Datenträger	Festplatten
E	Informationsdarstellung auf elektronischen Datenträgern	Speicherstick, Chipkarte, Halbleiterfestplatten, mobile Kommunikationsmittel

ZUSAMMENFASSUNG 66399-2

Informationsdarstellung in Originalgröße z.B. Papier	Informationsdarstellung verkleinert z.B. Mikrofilm	Optische Datenträger z.B. DVD, CD	Magnetische Datenträger z.B. Disketten, Magnetbandkassetten	Festplatten	Elektronische Datenträger z.B. USB-Sticks, SSD
P-1, bisher S1*	F-1	O-1	T-1	H-1	E-1
Fläche $\leq 2000\text{mm}^2$ oder Streifenbreite $\leq 12\text{mm}$, Streifenlänge nicht begrenzt	Fläche $\leq 160\text{mm}^2$	Fläche $\leq 2000\text{mm}^2$	Mechanisch funktionsunfähig	Festplatte mechanisch / elektronisch funktionsunfähig	Medium mechanisch / elektronisch funktionsunfähig
P-2, bisher S2*	F-2	O-2	T-2	H-2	E-2
Fläche $\leq 800\text{mm}^2$ oder Streifenbreite $\leq 6\text{mm}$, Streifenlänge nicht begrenzt	Fläche $\leq 30\text{mm}^2$	Fläche $\leq 800\text{mm}^2$	Fläche $\leq 2000\text{mm}^2$	Datenträger beschädigt	Medium zerteilt
P-3, bisher S3*	F-3	O-3	T-3	H-3	E-3
Fläche $\leq 320\text{mm}^2$ oder Streifenbreite $\leq 2\text{mm}$, Streifenlänge nicht begrenzt	Fläche $\leq 10\text{mm}^2$	Fläche $\leq 160\text{mm}^2$	Fläche $\leq 320\text{mm}^2$	Datenträger verformt	Medium zerteilt, Fläche $\leq 160\text{mm}^2$
P-4	F-4	O-4	T-4	H-4	E-4
Fläche $\leq 160\text{mm}^2$ und Streifenbreite $\leq 6\text{mm}$	Fläche $\leq 2,5\text{mm}^2$	Fläche $\leq 30\text{mm}^2$	Fläche $\leq 160\text{mm}^2$	Datenträger zerteilt, verformt, Fläche $\leq 2000\text{mm}^2$	Datenträger zerteilt, Fläche $\leq 30\text{mm}^2$
P-5, bisher S4*	F-5	O-5	T-5	H-5	E-5
Fläche $\leq 30\text{mm}^2$ und Streifenbreite $\leq 2\text{mm}$	Fläche $\leq 1\text{mm}^2$	Fläche $\leq 10\text{mm}^2$	Fläche $\leq 30\text{mm}^2$	Datenträger zerteilt, verformt, Fläche $\leq 320\text{mm}^2$	Datenträger mehrfach zerteilt, Fläche $\leq 10\text{mm}^2$
P-6, bisher S5*	F-6	O-6	T-6	H-6	E-6
Fläche $\leq 10\text{mm}^2$ und Streifenbreite $\leq 1\text{mm}$	Fläche $\leq 0,5\text{mm}^2$	Fläche $\leq 5\text{mm}^2$	Fläche $\leq 10\text{mm}^2$	Datenträger zerteilt, verformt, Fläche $\leq 10\text{mm}^2$	Datenträger mehrfach zerteilt, Fläche $\leq 1\text{mm}^2$
P-7	F-7	O-7	T-7	H-7	E-7
Fläche $\leq 5\text{mm}^2$ und Streifenbreite $\leq 1\text{mm}$	Fläche $\leq 0,2\text{mm}^2$	Fläche $\leq 0,2\text{mm}^2$	Fläche $\leq 2,5\text{mm}^2$	Datenträger zerteilt, verformt, Fläche $\leq 5\text{mm}^2$	Datenträger mehrfach zerteilt, Fläche $\leq 0,5\text{mm}^2$

* vergleichbare Sicherheitsstufe nach veralteter DIN 32757

DIN 66399

Teil 3

Prozess der
Datenträgervernichtung

DIN

66399-3

PROZESS DER VERNICHTUNG



Variante 1

Datenträgervernichtung durch die verantwortliche Stelle direkt

Organisation und Personal

Anfallstelle zur Datenträgervernichtung

Sammeln gegebenenfalls Lagern

Datenträgervernichtung direkt

Variante 2

Datenträgervernichtung, vor Ort durch Dienstleister

Organisation und Personal

Anfallstelle zur Datenträgervernichtung

Sammeln gegebenenfalls Lagern

Transport vor Ort

Datenträgervernichtung Dienstleister vor Ort

Variante 3

Datenträgervernichtung, extern durch Dienstleister

Organisation und Personal

Anfallstelle zur Datenträgervernichtung

Sammeln gegebenenfalls Lagern

Transport zum externen Dienstleister

Sammeln gegebenenfalls Lagern

Datenträgervernichtung Dienstleister extern

Stand der Technik – Doof, aber so isses!

- HANDAKTENVERNICHTER sind für alle Sicherheitsstufen (P-1 bis P-7) von verschiedenen Herstellern erhältlich und dienen im Wesentlichen der unmittelbaren Vernichtung von ‚Schreibtischmaterial‘. Einer datenschutzkonformen Entsorgung im großen Stil sind sie jedoch nicht gewachsen.
 - GROSSAKTENVERNICHTER werden meist zentral und für alle zugänglich platziert und haben einen deutlich höheren Durchsatz (meist gemessen in der Quantität von Blättern – z.B. 500 Blatt). Doch Achtung, desto höher die Sicherheitsstufe, desto höher sind Staubentwicklung und Brandgefahr zu bewerten
- Achten Sie daher beim Kauf auf die Qualität und die zu installierende Peripherie (Besonderer Brandschutz, Staubabsaugung etc. nötig?).



Stand der Technik – Doof, aber so isses!

- BEAUFTRAGUNG EINES DIENSTLEISTERS

- Meist erhalten Sie hier die Schutzklasse 2 oder 3 einhergehend mit der Sicherheitsstufe P-3 / P-4.
- Wirklich nur sehr vereinzelt bedienen Entsorger in Deutschland auch die Notwendigkeit einer P-5 im Service.
- Ist das Schutzniveau Ihrer zu vernichtenden Daten hoch und erfordert einen Partikelschnitt von P-5 oder höher, ist ein Großaktenvernichter im eigenen Haus zu installieren.



Externer Dienstleister – die wichtigsten Fragen und Hinweise



- 1) Überprüfen Sie VOR der Vertragsunterzeichnung ob der Dienstleister in der Lage ist, Ihre Daten auf datenschutzkonforme Weise zu vernichten:
 - Wie wird der sichere Transport gewährleistet?
 - Welche Sicherheitsbehältnisse werden genutzt?
 - Sind die verwendeten Geräte am Standort des Entsorgers tatsächlich für die vereinbarte Sicherheitsstufe geeignet und entsprechen der DIN 66399?
 - Hat der Entsorger alle relevanten Maßnahmen für die entsprechenden Schutzklassen installiert?

Externer Dienstleister – die wichtigsten Fragen und Hinweise

A hand is pointing towards a document that has several checkboxes, some of which are marked with an 'X'. The image is in grayscale and serves as a background for the title.

- 2) Geben Sie sich NICHT mit der Zusicherung der Umsetzung der geltenden Datenschutzgesetze zufrieden! Prüfen Sie!
- 3) Prüfen Sie in regelmäßigen Abständen die ordnungsgemäße Durchführung der Aktenvernichtung am Standort des Dienstleisters! Im Vertrag sollte folglich das Recht auf unangemeldete Kontrollen erfasst sein!
- 4) Definieren Sie Vertragsstrafen für den Fall der Nichteinhaltung!
- 5) Unterschreiben Sie nicht blind Standardverträge! Prüfen Sie stets genau, was Sie für Ihr Geld bekommen und ob dies Ihrem Schutzbedarf angemessen ist!
- 6) Jede Vertragsverlängerung muss geprüft werden. Hat der Stand der Technik sich verändert? Ist mein Schutzniveau gestiegen und kann der Entsorger dieses überhaupt noch bedienen?

Datenschutz & Medizin

**ACHTUNG, liebe
Geheimnisträger!**





203 StGB

Verletzung von Privatgeheimnissen

- (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung* erfordert

anvertraut worden oder sonst bekanntgeworden ist, wird mit **Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.**

*Krankenschwestern/-pfleger, Krankenpflegehelfer/ -innen, Kinderkrankenschwestern/- pfleger, Altenpfleger/-innen, Hebammen/Entbindungspfleger, Krankengymnasten/-innen, Masseur/-innen, medizinisch-technische Assistenten/-innen, pharmazeutisch- technische Assistenten/-innen, Arzthelfer/-innen, Diätassistenten/-innen usw.

§203 StGB & Aktenvernichtung

Folgendes sagt das ULD zu diesem Thema...

„Entscheidet man sich für eine Entsorgung durch ein externes Unternehmen, muss unter Berücksichtigung des strafrechtlich geschützten Patientengeheimnisses sichergestellt sein, dass keine unbefugte Offenbarung im Sinne des §203 StGB an die Mitarbeiter des Entsorgungsunternehmens erfolgt.“

§ 203 StGB & Aktenvernichtung

Folgendes sagt das ULD zu diesem Thema...

„Eine datenschutzkonforme Vernichtung durch Dritte ist nur möglich,

1) wenn der Arzt die Verfügungsgewalt über die Datenträger bis zur Vernichtung behält...

2) wenn das Unternehmen ausschließen kann, dass eine Einsichtnahme in die Unterlagen überhaupt möglich ist...“

BEDEUTET:

Eine Verhinderung der unbefugten Offenbarung kann nur durch die

SCHUTZKLASSE 3 und die Vernichtungsstufe mind. P-5 oder höher

gewährleistet werden und ist für Patientendaten unerlässlich!!!



Klartext!
Wenn ich's durch die Blume haben will,
schaue ich Biene Maja!

Mit der **DS-GVO** kommt's noch dicker...

Die am **25.05.2016** in Kraft getreten EU-Datenschutzgrundverordnung wird ab dem **25.05.2018 geltendes Recht sein** und konfrontiert Datenproduzenten mit sehr hohen Sanktionen:

Die Nichteinhaltung wird bestraft mit hohen Bußgeldern:

Datenschutzmanagement €10 Mio. bzw. 2% des weltweiten Jahresumsatzes
(bisher €50.000) > Artikel 83, Absatz 4

Betroffenerecht €20 Mio. bzw. 4% des weltweiten Jahresumsatzes
(bisher €300.000) > Artikel 83, Absatz 5

Ein Rechenbeispiel

Klinikgruppe mit 3 Mrd. € Umsatz pro Jahr

Verstoß Datenschutzmanagement:
60.000.000€ Strafe

Verstoß Betroffenenrecht:
120.000.000€ Strafe

Fazit



RISK = NO FUN

... bis Mai 2018 ist es nicht mehr lang!