TRADEFINITY
trade and finance of it-equipment GmbH

Shred IT

DATENLÖSCHUNG (DIN 66399) DATENTRÄGERVERNICHTUNG

DEKRA Prozesszertifizierte Datenträgervernichtung (DIN 66399)

Jeder, der vertrauliche, personenbezogene oder sensible Daten verarbeitet, muss nach dem Bundesdatenschutzgesetz eine datenschutzgerechte und sichere Vernichtung dieser Daten sowie deren Entsorgung sicherstellen. D.h., Datenträger müssen so vernichtet werden, dass die Reproduktion der Daten, je nach Inhalt, unmöglich oder weitestgehend erschwert wird.

Die TRADEFINITY GmbH bietet Ihnen die Möglichkeit, ihren Datenträger mit einem DEKRA Datenschutz- und Datensicherheits-zertifizierten Datenträgervernichtungsverfahren sicher zu entsorgen. Die Datenträgervernichtungszertifikate sowie die Recycling-Prozesse entsprechen den aktuellen Forderungen des Bundesdatenschutzgesetz (BDSG) und DIN 66399 zur Datenträgervernichtung.

Datenschutz und Datensicherheit gemäß dem Anforderungsprofil für Datenlöschprozess V 1.2

- Regelmäßige freiwillige Überwachung

DEKRA Certification

DEKRA zertifiziert

DIN 66399 - DIN-Norm zur Datenträgervernichtung

Eine zuverlässige Methode zur endgültigen Datenlöschung ist die physikalische Zerstörung von Datenträgern (Datenträgervernichtung). Eine gängige Methode ist das sogenannte Schreddern. Ein Schredder ist ein mechanisches Gerät zum Zerkleinern von unterschiedlichsten Materialien. Das bedeutet, der Datenträger wird zerstört, indem er in kleine Teile zerlegt wird. Die neue DIN 66399 beschreibt die Anforderungen an Maschinen und Prozesse zur Vernichtung von Datenträgern. Die Norm wurde vom Normenausschuss für Informationstechnik und Anwendungen (niA) erarbeitet. Die neue DIN 66399 ersetzt die bisherige DIN 32757.

Zertifikat Nr. 990817035 „Prozesszertifiziert zur Abholung und Rücknahme (gesicherter Transport) von IT-Produkten und der Löschung (durch Software, Degaussierung und Vernichtung) mitgelieferter Datenträger“ gemäß dem DEKRA Assurance Services GmbH Anforderungskatalog V1.2. Der Nachweis wurde mit **Auditbericht-Nr. A15111036** vom **14.08.2017** erbracht.

TRADE & BROKERAGE
FINANCE & LEASE
REMARKETING
TECHNISCHER SERVICE
DATENLÖSCHUNG
DATENRETTUNG
TRANSPORT & LOGISTIK
ENTSORGUNG

TRADEFINITY
trade and finance of it-equipment GmbH
Shred IT

DATENLÖSCHUNG (DIN 66399) DATENTRÄGERVERNICHTUNG

DIN 66399 - SICHERHEITSSTUFEN-, SCHUTZKLASSEN UND ZUORDNUNG

Um bei der Datenträgervernichtung dem Wirtschaftlichkeitsprinzip bzw. Angemessenheitsprinzip Rechnung zu tragen, ist es notwendig, die Daten in Schutzklassen einzuteilen. Dabei ist der Grad der Schutzbedürftigkeit ausschlaggebend für die Wahl der Sicherheitsstufe in Bezug auf die Vernichtung der Datenträger.

Der Schutzbedarf ihrer Daten wird in drei Schutzklassen eingeordnet. Zur Ermittlung des Schutzbedarfes wird in Unternehmen geprüft, welche Art von Daten verwaltet werden. Daraus ergibt sich der Schutzbedarf und damit die Schutzklasse. Die DIN 66399 unterteilt jede Datenträgerkategorie in 7 Sicherheitsstufen. Je höher die Sicherheitsstufe, desto kleiner die Partikel. Die DIN 66399 gruppiert unterschiedliche Datenträger in 6 Kategorien. in der jeweiligen Kategorie wird erläutert, in welchen Formaten die Daten vorliegen.

DATENLÖSCHUNG (DIN 66399)				DATENTRÄGERART			
				OPTISCHE-DATENTRÄGER: CD-ROM, CD-RAM, DVD-ROM, DVD-RAM, Blu-Ray, Telefonkarten, Scheckkarten, MO-Discs	MAGNETISCHE-DATENTRÄGER (BÄNDER): Compact Cassette, DAT, DDS, Disketten, DLT, IBM 3480/3490 Magstar, Jaguar, ZIP, LTO, Mammoth, Ultrium, VXA	MAGNETISCHE-DATENTRÄGER (FESTPLATTEN): Magnetische Festplatten, ATA, IDE, Fibre Channel, FireWire, RAID, iSCSI, SATA, SAS, SCSI, SSA, USB	ELEKTRONISCHE-DATENTRÄGER: USB Sticks, SD-Speicherkarten, CompactFlash-Karten, Microdrives, Flash-Speicher, Speichersticks, SSD
SCHUTZKLASSEN	**1 2 3**	**SICHERHEITSSTUFEN**		**O**	**T**	**H**	**E**
Schutzklasse 1 **Normaler Schutzbedarf für interne Daten** Diese Informationen sind für größere Gruppen bestimmt und zugänglich. Unberechtigte Offenlegung hätte begrenzte negative Auswirkungen auf das Unternehmen. Der Schutz personenbezogener Daten muss gewährleistet sein.		**Sicherheitsstufe 1** **Allgemeine Daten** Reproduktion mit einfachem Aufwand Toleranz für 10% des Materials		O-1 Partikelgröße max. **2.000 mm²** (3.800 mm²)	T-1 Medium funktions-unfähig	H-1 Datenträger funktions-unfähig	E-1 Medium funktions-unfähig
		Sicherheitsstufe 2 **Interne Daten** Reproduktion mit besonderem Aufwand Toleranz für 10% des Materials		O-2 Partikelgröße max. **800 mm²** (2.000 mm²)	T-2 Partikelgröße max. **≤ 2.000 mm²** (3.800 mm²)	H-2 Datenträger-Beschädigt	E-2 Medium zerteilt
Schutzklasse 2 **Hoher Schutzbedarf für vertrauliche Daten** die auf einen kleinen Personenkreis beschränkt sind. Die ungerechtfertigte Weitergabe hätte erhebliche Auswirkungen auf Unternehmen und könnte gegen vertragliche Verpflichtungen oder Gesetze verstoßen. Der Schutz personenbezogener Daten muss hohen Anforderungen genügen.		**Sicherheitsstufe 3** **Sensible Daten** Reproduktion mit erheblichem Aufwand Toleranz für 10% des Materials		O-3 Partikelgröße max. **160 mm²** (480 mm²)	T-3 Partikelgröße max. **≤ 320 mm²** (800 mm²)	H-3 Datenträger-verformt	E-3 Partikelgröße max. **≤ 160 mm²** (480 mm²)
		Sicherheitsstufe 4 **Besonders sensible Daten** Reproduktion mit außergewöhnlichem Aufwand Toleranz für 10% des Materials		O-4 Partikelgröße max. **30 mm²** (90 mm²)	T-4 Partikelgröße max. **≤ 160 mm²** (480 mm²)	H-4 Partikelgröße max. **≤ 2.000 mm²** (3.800 mm²)	E-4 Partikelgröße max. **≤ 30 mm²** (90 mm²)
Schutzklasse 3 **Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten** mit Beschränkung auf einen kleinen, namentlich bekannten Kreis von Zugriffsberechtigten. Eine unberechtigte Weitergabe hätte ernsthafte, existenzbedrohende Auswirkungen für Unternehmen und würde gegen Berufsgeheimnisse, Verträge und Gesetze verstoßen. Der Schutz personenbezogener Daten muss uneingeschränkt gewährleistet sein.		**Sicherheitsstufe 5** **Geheim zu haltende Daten** Reproduktion mit zweifelhaften Methoden Toleranz für 10% des Materials		O-5 Partikelgröße max. **10 mm²** (30 mm²)	T-5 Partikelgröße max. **≤ 30 mm²** (90 mm²)	H-5 Partikelgröße max. **≤ 320 mm²** (800 mm²)	E-5 Partikelgröße max. **≤ 10 mm²** (30 mm²)
		Sicherheitsstufe 6 **Geheime Hochsicherheits-Daten** Reproduktion technisch nicht möglich Toleranz für 10% des Materials		O-6 Partikelgröße max. **2 mm²** (15 mm²)	T-6 Partikelgröße max. **≤ 10 mm²** (30 mm²)	H-6 Partikelgröße max. **≤ 10 mm²** (30 mm²)	E-6 Partikelgröße max. **≤ 1 mm²** (3 mm²)
		Sicherheitsstufe 7 **Top Secret Hochsicherheits-Daten** Reproduktion ausgeschlossen Toleranz für 10% des Materials		O-7 Partikelgröße max. **0,2 mm²** (0,6 mm²)	T-7 Partikelgröße max. **≤ 2,5 mm²** (7,5 mm²)	H-7 Partikelgröße max. **≤ 5 mm²** (15 mm²)	E-7 Partikelgröße max. **≤ 0,5 mm²** (1,5 mm²)

PROZESSDEFINITION

DIN 66399 Teil 3 ist keine offizielle Norm des Deutschen Instituts für Normung, sondern eine Spezifikation, die vom Arbeitsausschuss „Vernichtung von Datenträgern“ im Normenausschuss Informationstechnik und Anwendungen (NIA) ausgearbeitet wurde. Hier werden die technischen und organisatorischen Anforderungen an den Prozess der Datenträgervernichtung beschrieben. Von der Anfallstelle bis zur umweltfreundlichen Verwertung unter Beachtung der gesetzlichen Regelungen steht Ihnen nicht nur eine datenschutzkonforme, sichere Vernichtung zur Verfügung, sondern stets der gesamte Prozess.

Datenschutz und Datensicherheit gemäß dem Anforderungsprofil für Datenlöschprozess V 1.2
▸ Regelmäßige freiwillige Überwachung
DEKRA Certification
DEKRA zertifiziert

TRADE & BROKERAGE
FINANCE & LEASE
REMARKETING
TECHNISCHER SERVICE
DATENLÖSCHUNG
DATENRETTUNG
TRANSPORT & LOGISTIK
ENTSORGUNG

TRADEFINITY
trade and finance of it-equipment GmbH
Shred IT

DATENLÖSCHUNG (DIN 66399) DATENTRÄGERVERNICHTUNG

PROZESSDEFINITION

Fallen Datenträger unterschiedlicher Sicherheitsstufen an der Anfallstelle an, so ist aus ökologischen und ökonomischen Gründen die Trennung in verschiedene Sicherheitsstufen an der Anfallstelle empfohlen. Um eine Basissicherheit vor dem Vernichten elektronischer und magnetischer Datenträger zu erreichen, wird das Löschen oder Überschreiben empfohlen. Nach Abwägung des Schutzbedarfs kann dann bei der Vernichtung eine geringere Sicherheitsstufe gewählt werden. Wenn eine Beeinträchtigung der unmittelbaren Funktionsfähigkeit oder Löschen/Überschreiben nicht möglich ist, muss die notwendige Sicherheitsstufe in der gewählten Schutzklasse angewendet werden.

ÜBERNAHME- UND VERNICHTUNGSPROTOKOLL

Im Übernahmeprotokoll werden die Transfer-Informationen festgehalten: Name des Boten, Datenträgerkategorie, Datenträger-, Behältermenge oder Gewicht, wie, wann und wo zusammengestellt wurde.

Ein Datenträgervernichtungungszertifikat (Destruction Certificate) wird erstellt, wenn bei einem Datenträger oder Gerät keine erfolgreiche Software-Datenlöschung oder Degaussierung möglich waren. Das Datenträgervernichtungsverfahren kann nur nach Rücksprache und Freigabe durch den Eigentümer erfolgen, da die Speichermedien dabei wertlos werden. Die Datenträger sind nach dem Datenträgervernichtungssvorgang zerstört und nicht wiederverwendbar.

Im Vernichtungsprotokoll sind die Informationen zur Person, zum Gegenstand, zur Menge, zur Uhrzeit, zum Ort und zur Sicherheitsstufe nach DIN 66399-2 gelistet.

Datenschutz und Datensicherheit gemäß dem Anforderungsprofil für Datenlöschprozess V 1.2
▸ Regelmäßige freiwillige Überwachung
DEKRA Certification
DEKRA zertifiziert

TRADEFINITY GmbH
Service Center Nord
Waldhofstrasse 1-5
25474 Ellerbek
Deutschland

+49 (0)4101-78081 0
info@tradefinity.de

TRADEFINITY GmbH
Technologiezentrum
Heinrich-Hertz Str. 6
64560 Riedstadt
Deutschland

+49 (0)6158-74097 0
info@tradefinity.de

Möchten Sie mehr über unsere Lösungen und Produkte erfahren? Schicken Sie uns eine eMail oder rufen Sie uns an, wir stehen Ihnen jederzeit gerne zur Verfügung. Persönliche Ansprechpartner in allen Bereichen helfen Ihnen gern weiter - Kontaktieren Sie uns noch heute!

TRADE & BROKERAGE
FINANCE & LEASE
REMARKETING
TECHNISCHER SERVICE
DATENLÖSCHUNG
DATENRETTUNG
TRANSPORT & LOGISTIK
ENTSORGUNG