

Löschkonzept & Sicherheitsstandards

DAS DISKETTENWERK · Version 1.0 · Stand: 15.02.2026

Dieses Dokument beschreibt das Datenlöschverfahren des DISKETTENWERK für alle eingesandten Disketten-Datenträger. Es dient als Nachweis gegenüber Datenschutzbeauftragten, Auditoren und Entscheidungsträgern. Das Verfahren orientiert sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und erfüllt die Anforderungen der DSGVO an eine sichere Datenlöschung.

1. Geltungsbereich

Dieses Löschkonzept gilt für alle Disketten-Datenträger, die dem DISKETTENWERK zur Verarbeitung übergeben werden. Es umfasst:

Format	Kapazität	Schnittstelle
3,5-Zoll HD	1,44 MB	Standard-Diskettenlaufwerk
3,5-Zoll DD	720 KB	Standard-Diskettenlaufwerk
5,25-Zoll HD	1,2 MB	Legacy-Diskettenlaufwerk
5,25-Zoll DD	360 KB	Legacy-Diskettenlaufwerk
8-Zoll	bis 1,2 MB	Speziallaufwerk
Iomega ZIP	100/250/750 MB	Parallel/SCSI/USB/IDE

Mit Übergabe der Datenträger geht das Eigentum unwiderruflich auf das DISKETTENWERK über. Die Verantwortung für die Klassifizierung der enthaltenen Daten und die Entscheidung, ob eine zertifizierte Vernichtung erforderlich ist, liegt beim Auftraggeber.

2. Das 13-Stufen-Löschverfahren

Jeder lesbare Datenträger durchläuft ein vollautomatisiertes 13-Stufen-Verfahren. Das Verfahren kombiniert mehrere Überschreibungsstrategien mit Verifikation und Stress-Tests, um eine Datenwiederherstellung zuverlässig auszuschließen.

Nr.	Verfahrensschritt	Beschreibung
01	Low-Level-Format	Physische Neuinitialisierung aller Spuren (Track/Sector Rewrite). Setzt die magnetische Grundstruktur zurück.

02	Überschreibung 0x00	Vollständiges Überschreiben mit Null-Bytes zur Löschung bestehender Magnetmuster.
03	Überschreibung 0xFF	Invertiertes Überschreiben zur Prüfung der Magnetisierungsstärke.
04	Muster 0x55 (0-1-Wechsel)	Schreiben von 01010101 zur Stressprüfung der Flusswechsel.
05	Muster 0xAA (1-0-Wechsel)	Schreiben von 10101010 zur Erkennung von Bit-Shift-Fehlern.
06	Timing-Test 0x33/0xCC	Prüfung auf Timing-Jitter durch Doppel-Bit-Muster.
07	Nibble-Test 0x0F/0xF0	Grenzprüfung der Halbbytes zur Erkennung schwacher Sektoren.
08	Random-Write-Verification	Überschreiben mit Zufallszahlen zur Entropie-Maximierung.
09	Data-Retention-Check	Prüfung, ob die Magnetisierung auch nach Wartezeit stabil bleibt.
10	Lese-Stress-Test	10-faches sequenzielles Lesen zur Simulation von Alterungseffekten.
11	Clean-Format	Setzen eines sauberen Dateisystems (FAT12/FAT16).
12	CHKDSK-Prüfung	Logische Prüfung der Sektorenuordnung und Dateisystemintegrität.
13	Protokollierung	Erstellung des digitalen Prüfprotokolls auf dem Medium.

Datenträger, die in einem der Schritte fehlerhafte Sektoren aufweisen oder nicht zuverlässig beschrieben werden können, werden automatisch aus dem Wiederverwendungsprozess ausgeschlossen und der fachgerechten Materialverwertung zugeführt.

3. Einordnung & Standards

BSI-Orientierung

Das Verfahren orientiert sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur sicheren Datenlöschung durch mehrfaches Überschreiben. Konkret werden die Prinzipien der BSI-Richtlinie zum sicheren Löschen magnetischer Datenträger angewandt: mehrfache Überschreibung mit definierten Bitmustern, anschließende Verifikation jedes Sektors und lückenlose Dokumentation.

DSGVO-Konformität

Die Verarbeitung erfüllt die Anforderungen der Datenschutz-Grundverordnung (DSGVO) an eine sichere Löschung personenbezogener Daten nach Art. 17 DSGVO (Recht auf Löschung). Auf Wunsch wird ein Auftragsverarbeitungsvertrag (AV-Vertrag) nach Art. 28 DSGVO bereitgestellt.

Abgrenzung

Das beschriebene Verfahren ist BSI-orientiert, entspricht jedoch **nicht** einer zertifizierten Vernichtung nach DIN 66399 oder ISO/IEC 27040. Auftraggeber mit gesetzlicher Pflicht zur zertifizierten Datenvernichtung (z.B. Berufsgeheimnisträger nach § 203 StGB) werden gebeten, spezialisierte Entsorger zu beauftragen.

Für Unternehmen, Privatpersonen, Schulen, Universitäten, Vereine, Archive und Behörden ohne spezielle Zertifizierungspflicht ist das Verfahren vollkommen ausreichend und deutlich nachhaltiger als physische Vernichtung.

4. Dokumentation & Nachweis

Jede erfolgreich geprüfte Diskette erhält ein digitales Prüfprotokoll als Textdatei direkt auf dem Medium. Das Protokoll enthält:

Inhalt	Beschreibung
Datum und Uhrzeit	Start- und Endzeitpunkt des Löschvorgangs
Durchgeführte Tests	Alle 13 Stufen mit individuellem Ergebnis
Sektorenprüfung	Anzahl geprüfter und ggf. fehlerhafter Sektoren
Gesamtergebnis	PASS/FAIL-Bewertung des Datenträgers
Systemkennung	Identifikation der verwendeten Prüfsoftware

Auf Wunsch kann eine zusammenfassende Löschbestätigung per E-Mail ausgestellt werden.

5. Physische Sicherheit & Transport

Der Transport der Datenträger erfolgt über das DHL-Paketnetz. Nach Eingang werden alle Sendungen bis zur Verarbeitung verschlossen aufbewahrt. Der Zugang zu den Verarbeitungsräumen ist auf autorisiertes Personal beschränkt.

Datenträger, die den Löschprozess nicht bestehen (defekte Sektoren, mechanische Schäden), werden aus dem Wiederverwendungsprozess ausgeschlossen. Diese Medien werden getrennt gesammelt und über zertifizierte Entsorgungswege der Materialverwertung zugeführt.

6. Auftragsverarbeitung (DSGVO)

Für Unternehmen und Organisationen, die personenbezogene Daten verarbeiten, stellt das DISKETTENWERK auf Wunsch einen Auftragsverarbeitungsvertrag (AV-Vertrag) nach Art. 28 DSGVO bereit. Dieser regelt:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Technische und organisatorische Maßnahmen (TOMs)
- Weisungsgebundenheit des Auftragsverarbeiters
- Pflichten nach Beendigung der Verarbeitung

Der AV-Vertrag ist kostenlos unter www.diskettenwerk.de/av-vertrag/ abrufbar.

7. Kontakt & Rückfragen

Verantwortlich: Daniel Wesseling, Inhaber
Anschrift: DAS DISKETTENWERK · Achtenbuhr 12 · 48599 Gronau
E-Mail: info@diskettenwerk.de
Web: www.diskettenwerk.de/datensicherheit/

Dieses Dokument dient der Information und Dokumentation. Es ersetzt keine individuelle Rechtsberatung. Bei Fragen zur Klassifizierung Ihrer Daten wenden Sie sich an Ihren Datenschutzbeauftragten.