

## § 1 Definitionen

INFORMATIONEN sind alle zwischen den Vertragspartnern bezüglich des in der Präambel genannten Gebiets schriftlich, mündlich oder in sonstiger Weise offenbarte vertrauliche Informationen. Dazu gehören insbesondere Daten, Zeichnungen, Entwürfe, Skizzen, vertrauliche Beschreibungen, Spezifikationen, Messergebnisse, Berechnungen, Erfahrungen, Verfahren, Muster, Kenntnisse und Vorgänge einschließlich geheimen Know-how sowie Werke oder noch nicht veröffentlichte Anmeldungen gewerblicher Schutzrechte.

## § 2 Geheimhaltungsverpflichtung

Die Vertragspartner verpflichten sich, alle INFORMATIONEN geheim zu halten und sie oder Teile davon nicht an Dritte weiterzugeben. Die Vertragspartner verpflichten sich, die notwendigen Vorkehrungen zu treffen, dass Dritte Kenntnis von diesen INFORMATIONEN nehmen können. Insbesondere werden die Vertragspartner zu solchen Mitarbeitern diese INFORMATIONEN zur Kenntnis geben, die zur Geheimhaltung verpflichtet sind.

Die Pflicht zur Geheimhaltung gilt auch gegenüber Konzerngesellschaften, Lizenznehmern oder sonstigen Dritten, wenn die Vertragspartner INFORMATIONEN an ein mit ihm verbundenes Unternehmen gegeben hat. Den anderen Vertragspartner über eine solche Weitergabe von INFORMATIONEN vorab zu unterrichten und sicherzustellen, dass diese Unternehmen die in der vorliegenden Geheimhaltungsvereinbarung getroffenen Regelung ebenfalls anerkennen.

## § 3 Ausnahmen von der Geheimhaltungspflicht

Diese Vertraulichkeitsverpflichtung gilt nicht für INFORMATIONEN, die nachweislich dem empfangenen Vertragspartner vor der Mitteilung bereits bekannt waren, oder welche dem

**itWatch GmbH**

Aschauer Str. 30  
D-81549 München

Tel.: +49 (0) 89 62 03 01 00  
Fax: +49 (0) 89 62 03 01 069

info@itWatch.de  
www.itWatch.de

## – Sicher löschen und formatieren

**dataEx** erlaubt Ihnen, auf Wechseldatenträgern (Flash-Speicher-Technologie) UND Festplatten (magnetische Speicher) beliebige Informationen (Dateien oder ganze Ordner) sicher zu löschen oder das ganze Medium sicher zu formatieren (auch wiederbeschreibbare optische Medien).

### Gefährdungslage:

- ⦿ Betriebssystemeigene Löschfunktionen löschen nicht – sie geben nur den belegten Speicher für die zukünftige Nutzung frei. Ob und wann dieser freigegebene Speicher wirklich genutzt wird, ist Zufall. Die Daten bleiben also auf dem Datenträger für jeden, der Zugriff auf den Datenträger hat, lesbar.
- ⦿ Bei USB-Sticks oder anderen Wechseldatenmedien ist natürlich der Zugriff besonders einfach. Der Anwender glaubt, die Daten augenscheinlich gelöscht zu haben – trotzdem gelangen sie in unbefugte Hände, ohne dass es jemand merkt oder bewusst falsch gehandelt hat.
- ⦿ Ein PC oder Datenträger soll zur Wartung oder „Reparatur“ – d.h. beispielsweise auch Gewährleistungsansprüche oder Klärung von technischen Problemen – an Dritte gegeben werden. Vertrauliche Daten werden gelöscht – aber eben nicht sicher gelöscht.

### Herausforderungen:

- ⦿ Unternehmen sind bei bestimmten Daten gesetzlich dazu verpflichtet, das technisch Mögliche zum Schutz der Daten zu unternehmen – hierzu zählt das sichere Löschen. Die Haftung für die Einhaltung der Gesetze liegt hier immer bei der Geschäftsführung / dem Vorstand und kann NICHT an Dritte delegiert werden.
- ⦿ Aus ureigenem Interesse sollten Sie Ihre Finanz-, Entwicklungs- und andere vertrauliche Daten vor Spionage und dem unerwünschten insbesondere unkontrollierten Zugriff Dritter schützen, auch über die aktive Lebensdauer der Information hinaus.
- ⦿ Empfehlenswert (in manchen Umgebungen zwingend notwendig) ist es, den Anforderungen des BSI an das „sichere Löschen“ von schützenswerten Informationen zu genügen.

## dataEx von itWatch ist die optimale Lösung für KMU und große Unternehmen

Das Modul **dataEx** ermöglicht auf der Basis der vorhandenen Berechtigungen zum Einen das **sichere Löschen** von Dateien bzw. Ordnern und deren Metainformationen, so dass diese auch mit den besten forensischen Werkzeugen nicht mehr rekonstruiert werden können.

Zum Anderen erlaubt es das **sichere Formatieren** vorhandener Datenträger (auch wiederbeschreibbare optische Datenträger), so dass keine alten Daten mehr auf dem Datenträger vorhanden sind.

Die beiden Funktionen lassen sich, je nach Vorliebe, auf zwei Arten einsetzen:

- ⦿ Das Kontextmenü des Datenträgers, der Ordner und der betroffenen Dateien bzw. des zu formatierenden Datenträgers enthält die Einträge „Sicher löschen“ bzw. „Datenträger sicher formatieren“. Sie können die Funktion durch Anklicken auswählen.
- ⦿ Alternativ können Sie auf dem Desktop das Drop-Target-Symbol „itWESS Aktenvernichter“ für ein sicheres Löschen von Dateien und Ordnern nach Art der Drag-&-Drop-Methode nutzen. Wechseldatenträger lassen sich damit ebenfalls sicher formatieren.

Nach jedem dieser Vorgänge erhalten Sie eine Meldung über den Erfolg bzw. das Fehlschlagen der Ausführung. Alle Verfahren folgen den internationalen Standards und den BSI Auflagen.

**Kostensenkung:** Durch dieses Verfahren können Sie kostengünstige Entsorgungsverfahren für Festplatten und mobile Datenträger verwenden – auch wenn diese gesetzlichen Compliance Auflagen unterliegen.