Kurzgutachten zur Zertifizierung des Aktenvernichtungsverfahren der Fa. Shred-it GmbH nach DSAVO S/H

1 Einleitung

Mit dem der Begutachtung vorliegenden Produkt „Akten und Datenträgervernichtung im Vor-Ort-Verfahren“ können Kunden der Shred-it GmbH Akten und Datenträger mit personenbezogenem Inhalt vernichten lassen.
Im vorliegenden Gutachten wird geprüft, inwieweit das Shred-it-Verfahren den Rechtsvorschriften über den Datenschutz und die Datensicherheit gerecht wird.

2 Zeitpunkt der Prüfung

15. Februar 2005 – 15. Januar 2007

3 Adresse des Antragstellers

Shred-it GmbH
Kastenbauerstraße 2
81677 München
www.Shred-it.com / www.securit.com

4 Adressen der Sachverständigen:

Rechtlicher Gutachter:
Michael J. Erner
Wrangelstraße 118
20253 Hamburg

Technischer Gutachter:
Diplom Informatiker Werner Hülsmann
Obere Laube 48
D-78462 Konstanz

5 Kurzbezeichnung des IT-Produktes

Das Verfahren der Firma Shred-it dient der Akten- und Datenträgervernichtung durch Löschung im Sinne des § 2 Abs. 2 Ziffer 5 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG) und § 3 Abs. 4 Ziffer 5 des Bundesdatenschutzgesetzes (BDSG). Das Verfahren erfüllt die Anforderungen an einen sicheren Löschungsprozess von Akten und Datenträgern. Das Gutachten beschreibt den Stand Januar 2007.

6 Detaillierte Bezeichnung des IT-Produktes

Das Verfahren basiert ausschließlich auf physikalischen Akten- und Datenträgervernichtungsfunktionalitäten. Shred-it bietet im Rahmen einer Auftragsdatenverarbeitung folgende Verfahren an:

- Verfahren A: Sammlung von Akten und Datenträgern (CD, DVD, Disketten) in Säcken, die sich in verschlossenen Konsolen beim Auftraggeber befinden, Leerung der Konsolen und Schreddern der Akten und/oder Datenträger beim Kunden vor Ort durch einen Shred-it-Mitarbeiter mit einem hydraulisch betriebenen Schredder, der auf einem geschlossenen LKW montiert ist.

- Alternative: Das zu schreddernde Material kann auch durch den Kunden in eigenen Behältern gesammelt und am LKW angeliefert werden.

- Verfahren B: Persönliche Anlieferung der Akten und Datenträger durch den Kunden in der Niederlassung von Shred-it und Schreddern der Akten und Datenträger auf dem Gelände der Niederlassung in einem mit einem Schredder ausgestatteten LKW.

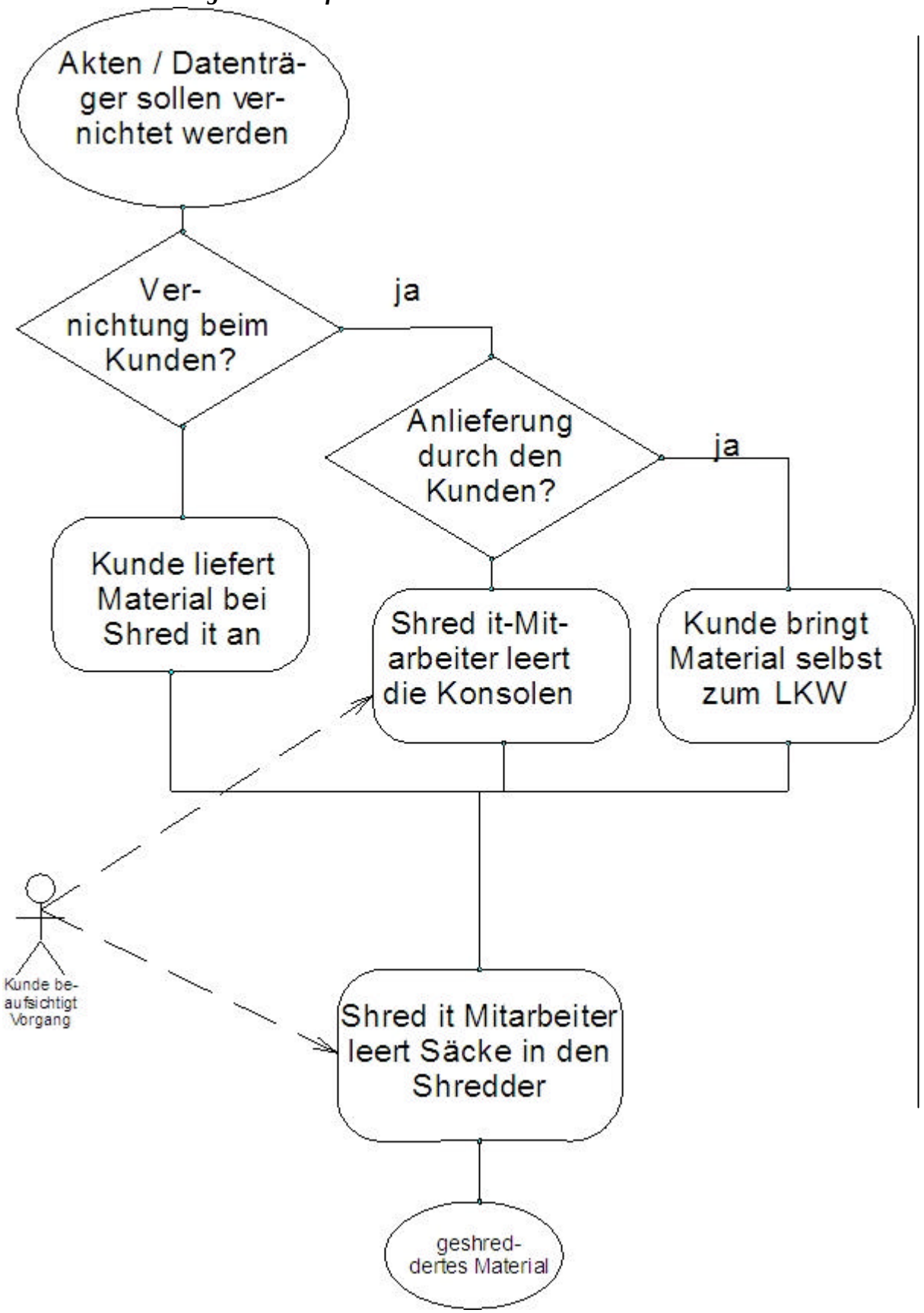
Ergänzend kann der Shred-it Mitarbeiter von einem autorisierten Mitarbeiter des Auftraggebers beim Verfahren A bei der Einsammlung und Anlieferung bis zum LKW begleitet und bei beiden Verfahren der Vernichtungsprozess selbst von außerhalb der Shredderanlage, jedoch in Sichtweite beobachtet werden. Für die Sammlung der Akten und Datenträger werden dem Kunden so genannte Konsolen - in vom Kunden gewünschter Anzahl - zur Verfügung gestellt. Diese Konsolen sind stabile verschlossene Container, zu denen jeweils zwei Schlüssel existieren. Einen Schlüssel hat der Fahrer des Shred-it LKW, ein weiterer kann einem explizit zu benennenden Mitarbeiter im Haus des Auftraggebers zur Verfügung gestellt werden, um im Bedarfsfall (der die Ausnahme bleiben sollte, wenn z. B. unbeabsichtigt Material in den Container entsorgt wurde) auf das zu vernichtende Material zugreifen zu können. Die Größe der Container entspricht der eines gewöhnlichen Büro-Rollcontainers, so dass es möglich ist, die Konsolen direkt am Arbeitsplatz zu positionieren. Die Konsolen haben in der oberen Abdeckplatte einen Einwurfschlitz, der groß genug ist, um auch Disketten, CDs oder gebundene Akten aufzunehmen. Durch einen Durchgreifschutz unterhalb der Öffnung wird sichergestellt, dass einmal hineingeworfene Akten und Datenträger nicht mehr – ohne Aufschließen der Konsole – herauszunehmen sind. In die Konsole ist jeweils ein reißfester Sack zur Aufnahme des zu schreddernden Materials eingehängt.

Auf Anforderung, oder in vereinbarten regelmäßigen Abständen, fährt der LKW am Standort des Auftraggebers vor, um mittels des im LKW eingebauten Schredders die Akten- und/oder Datenträgervernichtung vor Ort durchzuführen. Der Shred-it-Mitarbeiter tauscht hierzu die gefüllten Säcke in den Konsolen gegen leere Säcke aus und bringt die gefüllten Säcke in den Schredderbereich des LWK. Dort leert er die Säcke vollständig in den Schredder. Dieses Vorgehensmodell entspricht der Alternative des Verfahrens A. Verfahren B weicht hiervon nur insofern ab, als dass der Transport des zu vernichtenden Materials durch den Shred-it Mitarbeiter entfällt, da der Kunde selbst das Material am jeweiligen Standort von Shred-it bis zum LWK anliefert.

7 Zweck und Einsatzbereich

Der Zweck und Einsatzbereich des Verfahrens ist das Löschen von Daten im Sinne des § 2 Abs. 2 Ziffer 5 des LDSG und § 3 Abs. 4 Ziffer 5 des BDSG. Dies beinhaltet die Vernichtung von Akten und von elektronischen Datenträgern (z.B. Disketten, CD, DVD). Das Verfahren ist sowohl im öffentlichen als auch im nichtöffentlichen Bereich einsetzbar.

8 Modellierung des Datenflusses



9 Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog v 1.2

10 Zusammenfassung der Prüfungsergebnisse

Zusammenfassend lässt sich das Verfahren von Shred-it als vorbildlich und transparent bewerten. Die zu vernichtenden Unterlagen werden entweder im Verfahren A direkt beim Auftraggeber geschreddert oder im Verfahren B von diesem selbst bei Shred-it angeliefert. In beiden Fällen kann der Schreddervorgang durch den Auftraggeber beobachtet und überwacht werden, um eine unbefugte Kenntnisnahme der zu vernichtenden Akten und Datenträger auszuschließen. Entsprechende Arbeitsanweisungen von Shred-it unterstützen die sichere Vernichtung unter Einsatz des Doppelschredders.

Im Standardverfahren, d.h. dem Einsatz des Vorzerkleinerers mit Minimaleinstellung auf Sicherheitsstufe 1 der DIN 32757-1 (Streifenschnitt 12 mm und schmaler) bestehen dahingehend Risiken im Verfahren der Firma Shred-it, dass das geschredderte Material nicht direkt von Shred-it – entweder bereits auf dem LKW oder auf dem Firmengelände – verwirbelt oder zu Ballen verpresst wird. Dies hat zur Folge, dass zu vernichtendes Material einer höheren Schutzstufe nicht den Erfordernissen der DIN 32575-1 entsprechend vernichtet wird. Dies ist zwar Teil des Verfahrens im Hause Shred-it. Der Kunde selbst hat aber den Schutzbedarf zu definieren. Schutzstufe 3 erfordert den Einsatz des Doppelschredders, d. h. die mechanische Zuschaltung der Partikelschnittwalzen. Eine Optimierung des Systems könnte dahingehend erzielt werden, dass ein Verpressen bzw. Verwirbeln im LKW vor Ort erfolgt, oder zumindest die Firma Shred-it die Erreichung der höheren Sicherheitsstufen bei den Recycling-Unternehmen selbst überwachen könnte. Derzeit wird die direkte Weiterverarbeitung in der Recyclingfabrik normalerweise aber weder vom Auftraggeber noch von Shred-it überwacht. Eine alleinige Überwachung durch den Auftragnehmer Shred-it würde zudem den Anforderungen des §§ 11 BDSG und 17 LDSG nicht gerecht werden.

Allerdings entspricht bereits das jetzige Verfahren beim Einsatz des Doppelschredders den Anforderungen an eine datenschutzkonforme Vernichtung der Sicherheitsstufe 3 der DIN 32757-1.

Hier ist insofern seitens des Auftraggebers darauf zu achten, dass die Sicherheitsstufen vorgegeben werden.

Die Schredder-LKW sind mit sicheren Verriegelungen und Schlössern ausgestattet, so dass ein Diebstahl des geschredderten Materials nur mit erheblichem Aufwand möglich ist. Nachts sind die LKW auf verschlossenem Firmengelände abgestellt.

10.1 Besonderheiten

Die Container der Firma Shred-it werden mit einem Zentralschlüssel geöffnet. Es ist zwar organisatorisch vorgesehen, dass jeder Kunde einen eigenen Schlüssel erhält, der nicht bei den Konsolen anderer Kunden passt. Jedoch kann aufgrund der Vielzahl von Kunden weltweit nicht ausgeschlossen werden, dass Dubletten existieren. Somit bestünde die theoretische Möglichkeit, dass z. B. Kunde A den einzelnen, ihm für den Notfall zur Verfügung stehenden, Schlüssel dazu benutzt, Container von Kunde B zu öffnen. Deswegen genügen die Container nicht den Anforderungen des LDSG SH.

Hier sind zusätzliche Sicherungsmaßnahmen durch den Kunden zu treffen, etwa durch Sicherstellung, dass die Container nicht in Bereichen aufgestellt werden, die unbeobachtet sind, oder im Rahmen eines unternehmensweiten Zutrittsberechtigungskonzeptes von Unberechtigten eingesehen werden können. Es ist hier in diesem Sinne auftraggeberseitig sicherzustellen, dass keine Container in Bereichen aufgestellt werden, in denen andere Kunden der Fa. Shred-it Zutrittsrechte haben könnten. Somit obliegt die Aufstellung der Container den organisatorischen Anforderungen an ein Sicherheitskonzept der Auftraggeber. Diese Notwendigkeit ist in einem Merkblatt (Anlage) aufgeführt, dass als Anlage zum Vertrag jedem Kunden von Shred-it bei Auftragserteilung ausgehändigt wird.

10.2 Datenschutz in der Shred-it GmbH

Die Gewährleistung des internen Datenschutzes in der Fa. Shred-it basiert auf einer externen Schulung mehrerer Mitarbeiter die in den einzelnen Niederlassungen als Datenschutzkoordinatoren aufgestellt sind und einer ext. betrieblichen Datenschutzbeauftragten zuarbeiten.

11 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Die Vernichtung erfolgt unter Berücksichtigung der Weisungsberechtigungen der Auftraggeber auf wirksame Art und Weise, so dass die Anforderungen an die Löschung personenbezogener Daten erfüllt werden.

Da einem Auftraggeber eine beliebige Anzahl Konsolen zur Verfügung gestellt wird, ist es der verantwortlichen Stelle leicht möglich, die eigene Organisation der Entsorgung sensibler Akten und Datenträger so zu gestalten, dass an allen Arbeitsplätzen ohne lange Wege Möglichkeiten zur sicheren Entsorgung von zu vernichtenden Akten und Datenträgern vorhanden sind. Eine unsichere „Zwischenlagerung" von zu entsorgendem Material aus Gründen der Bequemlichkeit auf bzw. unter dem Schreibtisch, oder in einem Karton im Schrank am jeweiligen Arbeitsplatz durch den Mitarbeiter ist somit vermeidbar.

Weiterhin ist die Präsenz der Konsolen selbst ein den Datenschutz förderndes Mittel. Als tragende Säule zur Förderung von Datenschutz und Datensicherheit ist die Sensibilisierung von Personen zu benennen, die aufgrund der Anwesenheit eines Containers zur Aktenvernichtung an die Sinnhaftigkeit dieser Funktion erinnert werden. Überdies erleichtert ein „erweiterter Papierkorb" die Entscheidung, ob ein Dokument, oder ein Datenträger in den gewöhnlichen Müll gehört, oder aufgrund datenschutzrechtlicher Erwägungen fachmännisch zu entsorgen ist. Es ist einfacher, sich des Aktenvernichters zu bedienen, als den Zweifel, „..gehört das jetzt in den Papierkorb oder nicht?" zu Ungunsten einer Sammelstelle (sofern vorhanden) zu entscheiden. Zumal es nicht der Notwendigkeit bedarf, datenschutzrechtlich relevante Unterlagen oder Dateien zu horten und am Ende des Tages zu einer Sammelstelle zu verbringen oder im Schrank zu lagern, bis sich die Gelegenheit findet, die Sammelstelle aufzusuchen.

Daneben ist das Risiko eliminiert, dass ungewollt oder aus fehlender Sensibilität im gewöhnlichen Papierkorb gelandete Datenbestände in falsche Hände gelangen. Ein Shred-it-Container ist verschlossen und bis zur Abholung durch den Shred-it-Mitarbeiter bedarf es keines weiteren Gedankens an die bei Verbleib im Papierkorb ungesichert zugänglichen Bestände des zur Entsorgung bestimmten Materials. Nach der Abholung und direkt im Anschluss an den abgeschlossenen Schreddervorgang erhält der Auftraggeber ein vom Shred-it-Mitarbeiter ausgefertigtes Protokoll über die Vernichtung. Die Vernichtung von Akten und Datenträgern erfolgt somit in nachvollziehbarer und durch den Auftraggeber in leicht kontrollierbarer Weise.

12 Standortbezug

Die Organisationsstruktur der Fa. Shred-it obliegt einem hierarchischen Aufbau. Die Shred-it GmbH in Deutschland ist eine 100 % Tochter einer kanadischen Muttergesellschaft, Teil eines weltweit agierenden Unternehmens sowie Dachorganisation der Niederlassungen in Deutschland. Innerhalb dieser Hierarchie entspricht das Akten- und Datenträgervernichtungsverfahren der Fa. Shred-it weltweit dem gleichen Maßstab. Die Systeme, mit denen Shred-it mobil Aktenvernichtung betreibt, werden durch die kanadische Muttergesellschaft vorgegeben und entsprechen einem durch das Management definierten einheitlichem Muster, das durch ein Qualitätssicherungssystem kontrolliert wird. Ein in der Muttergesellschaft beschäftigter, in seiner Stellung gegenüber den Niederlassungen autonomer Manager, ist unter Bezugnahme eines von der Geschäftsführung der Muttergesellschaft erstellten Qualitätshandbuchs damit beauftragt, die einzelnen Niederlassungen aufzusuchen und Abweichungen von den vorgegebenen Standards sowohl in technischer wie auch organisatorischer Hinsicht zu beseitigen. Die inhaltlichen Vorgaben an die Niederlassungen erstrecken sich hierbei sowohl auf Kundenorientierung, Sicherheitsstandards, Umgang mit dem LKW und dem

Schredder als auch auf Verhaltensregeln der Mitarbeiter gegenüber den Kunden während der eigentlichen Dienstleistung, dem Aktenvernichtungsvorgang. Diese Standardisierung, die auf Basis der Erkenntnisse interner Audits ständig kontrolliert wird, unterstützt in weiten Bereichen die in diesem Gutachten hinterfragten Eckwerte zum Verfahren „mobile Aktenvernichtung".
Im Januar 2007 existierten im Rahmen der Shred-it Expansionspolitik 8 Niederlassungen in der BRD. Die Sachverständigen haben die Verfahren sowie die technischen und organisatorischen Begebenheiten in den Standorten Hamburg, Stuttgart und München begutachtet und ein den internen Vorgaben entsprechendes, einheitliches Bild vorgefunden. Vor diesem Hintergrund und durch den Umstand bedingt, dass es in den einzelnen Niederlassungen durch die betriebsinternen Restriktionen keine Zulässigkeiten gibt, am Verfahren, an der Technik oder an den Qualitätsstandards Veränderungen vorzunehmen, kann das Verfahren der Fa. Shred-it standortunabhängig zertifiziert werden.

Hiermit bestätigen wir, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und der Datensicherheit entspricht.

Michael J. Erner	Werner Hülsmann
Hamburg, 15.01.2007	Konstanz, 15.01.2007

Anlage: Merkblatt zum Kundenvertrag

Merkblatt

1. Auftragsdatenverarbeitung

Unsere Dienstleistung entspricht den Erfordernissen des Datenschutzes. Die Akten- und Datenträgervernichtung durch Shred-it ist eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz. Nicht nur, weil wir es müssen, weisen wir Sie darauf hin, dass Sie gesetzlich verpflichtet sind, unsere Dienstleistung zu überprüfen, uns ggfls. auf Missstände aufmerksam zu machen und diese auszuräumen. Ihre Weisungs- und Kontrollpflicht uns gegenüber, wie die Akten- und Datenträgervernichtung zu erfolgen hat, ist für uns eine weitere Möglichkeit unsere Dienstleistung noch besser an Ihren Bedürfnissen zu orientieren.

2. Schlüssel

Wie Sie auch schon aus unserem Beratungsgespräch wissen, haben die Konsolen, die wir Ihnen zur Verfügung stellen einen eigenen Schlüssel, mit dem ausgeschlossen werden soll, dass ein anderer Kunde mit seinem Schlüssel auf Ihre Konsolen zugreifen kann. Aufgrund der Vielzahl von Shred-it-Kunden weltweit kann dennoch nicht ausgeschlossen werden, dass Dubletten existieren. Deshalb empfehlen wir Ihnen, die Sicherheitskonsolen auf keinen Fall in unbeobachteten oder öffentlichen Bereichen aufzustellen, da dort ein Zugriff durch Dritte nicht auszuschließen ist.

3. DIN 32757-1

Das Verfahren der Fa. Shred-it eignet sich für eine Vielzahl von Materialien und entspricht den Anforderungen der DIN 32757-1. Mikrofilme und Chipkarten sind durch diese Norm aber nicht abgedeckt. Selbst die Partikelschnittgröße von 4 x 80 mm entsprechend der Stufe 3 nach DIN 32757-1 reicht aufgrund der hohen Datendichte nicht aus, diese Art von Datenträger datenschutzkonform zu vernichten.

Sprechen Sie uns bitte an, um auch diese Materialien fachgerecht zu entsorgen.

Eine Aktenvernichtung nach Stufe 3 ist wiederum nur erreichbar, wenn der Doppelschredder - d.h. zusätzlich zum Vorzerkleinerer die Partikelschnittwalzen - eingesetzt wird. Wenn dies von Ihnen gewünscht wird, vermerken Sie dies bitte auf dem Auftragsformular (Anlage 3) unter sonstige Vereinbarungen.
Die Einschränkung der Aktenvernichtung durch unser Verfahren auf die Stufe 3 der DIN 32757-1 beinhaltet, dass ein Einsatz im Umfeld von Berufsgeheimnisträgern nicht abgedeckt ist, da für diese Gruppe die Stufe 4 (Partikelschnittgröße 1,9 X 15 mm) erforderlich ist.