Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das

- Verfahren zur Datenvernichtung -

der

Recall Deutschland GmbH Hamburg

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 37 89 05
fax 04822 – 37 89 04
email bethke@datenschutz-guetesiegel.de

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
email sh@hansen-oest.com

Stand:
März 2013

Inhaltsverzeichnis

A. Einleitung 4
B. Zeitpunkt der Prüfung 4
C. Änderugen und Neuerungen des Verfahrens 4
D. Datenschutzrechtliche Bewertung 4
I. Anforderungen an die Prüfung / Prüfumfang 4
II. Vernichtung von Papier 5
III. Vernichtung von harten Daten durch einen separaten Shredder 7
IV. Zertifizierung von Recall gem. Payment Card Industry Data Security Standards (PCI) 9
V. Überarbeitung des QM-Systems 9
VI. Einführung einer Videoüberwachung mit Aufzeichnungsfunktion im Betrieb 9
VII. Erneuerung des Anlieferungsbereichs 10
VIII. Erweiterung des Fuhrparks durch zwei Sicherheitspresswagen 10
IX. Umsetzung der DIN EN 15713 10
X. Bewertung des Vernichtungsprozesses (DIN 66399-3) – Variante 3 10
E. Zusammenfassung 14

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Art der Änderung	Bemerkung
10.09.2012	Erstellung	Version 1.0
20.09.2012	Ergänzung	Version 1.1
04.10.2012	Erweiterung	Version 1.2
08.10.2012	Änderung	Version 1.3
12.10.2012	Überarbeitung	Version 2.0
31.05.2013	Erweiterung	Version 2.1
02.07.2013	Ergänzung	Version 2.2.
30.09.2013	Ergänzungen	Version 2.3
10.12.2013	Überarbeitung	Version 2.4
15.12.2013	Korrekturen	Version 2.5
18.03.2014	Überarbeitung nach GS Bericht	Version 3.0

A. Einleitung

Mit dem vorliegenden Gutachten beabsichtigt die Recall Deutschland GmbH (nachfolgend Recall genannt) ihr Verfahren zur Datenvernichtung für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) erneut rezertifizieren zu lassen.

Die Vorlage des Gutachtens beim ULD erfolgt durch den Auftraggeber.

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zu Grunde gelegt.

Recall möchte mit diesem Gutachten den Nachweis führen, dass das Produkt nach wie vor die datenschutzrechtlichen Anforderungen erfüllt.

B. Zeitpunkt der Prüfung

Die Prüfung des Verfahrens fand im Zeitraum 07.09.2012 – 18.03.2014 statt.

C. Änderugen und Neuerungen des Verfahrens

Die Firma Recall bietet ihren Kunden nach wie vor die Vernichtung von Akten und Datenträger (sog. harte Datenträger, womit herkömmliche Festplatten und CDs gemeint sind) durch ein Shredderverfahren. Das Verfahren ist wie in den Gutachten von 2006, 2008 und 2010 beschrieben. Recall bietet seinen Kunden immer noch folgende Leistungen zur Vernichtung von Daten an:

- Abholung der Daten in Einzelbehältern
- Alternativ persönliche Anlieferung bei Recall
- Automatische Beschickung der Shredderanlage nach Entleerung der Einzelbehälter auf ein Unterflurförderband
- Manuelle Beschickung der Shredderanlage durch Selbstanlieferer
- Vermischung der Daten (unterschiedlicher Kunden) im gesamten Vernichtungsprozess
- Vernichtung der Daten durch ein einstufiges Shreddersystem
- Pressen des zerkleinerten Materials für spätere Recyclingaufgaben

Es gibt derzeit folgende Veränderungen/Neuerungen:

- Für die Vernichtung von harten Daten gibt es einen separaten Shredder
- Der Betrieb hat ein Payment Card Industry Data Security Standard (PCI) Zertifikat
- Überarbeitung des QM-Systems.
- Einführung einer Videoüberwachung mit Aufzeichnungsfunktion im Betrieb.
- Erneuerung des Anlieferungsbereichs
- Erweiterung des Fuhrparks durch 2 Sicherheitspresswagen.
- Umsetzung der DIN 66399.

D. Datenschutzrechtliche Bewertung

I. Anforderungen an die Prüfung / Prüfumfang

Neben dem Prüfkatalog des ULD sind im Bereich der Aktenvernichtung u.a. geltende Normen und Richtlinien für die Prüfung des Verfahrens maßgeblich. Die Vorgaben hierzu bestimmt die Zertifizierungsstelle.

In der Vergangenheit wurden so Aktenvernichtungsverfahren gegen die DIN 32757 geprüft. Im vergangenen Gutachten aus dem Jahr 2010 wurde festgelegt, dass eine technische Leitlinie des BSI bei der Prüfung Berücksichtigung finden muss. Im Laufe der Prüfung, genauer im Oktober 2012 ist die DIN 32757 von der DIN 66399[1] abgelöst worden. Diese DIN besteht aus 3 Teilen (DIN 66399 -1, DIN 66399 – 2 und DIN SPEC 66399 – 3). Die Zertifizierungsstelle hat festgelegt, dass Verfahren zur Aktenvernichtung gegen die komplette DIN 66399 geprüft werden müssen.

Im Gegensatz zur DIN 32757 kategorisiert die DIN 66399 folgende Materialbezüge:

P - Informationsdarstellung in Originalgröße (Papier, Film, 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, …)

Somit sind für das Verfahren die Bezüge P, O und H relevant.

Zudem wird nachfolgend auf ein Dokument des BSI verwiesen, in dem es um die Vernichtung von Verschlusssachen in öffentlichen Stellen geht.

Um den Bezug zu älteren Gutachten und deren Einstufung zu behalten, wird in diesem Gutachten an den entsprechenden Stellen auf alte und andere Normen verwiesen, auch wenn diese nicht prüfungsrelevant sind. Gleiches gilt für die DIN EN 15713, bei der es sich um eine europäische Norm handelt, die Recall von sich aus erfüllen möchte. Demnach ist eine Prüfung ebenfalls in das Gutachten eingeflossen.

II. Vernichtung von Papier

Um eine Bewertung gem. neuer DIN durchführen zu können wurden erneut aktuelle Partikelproben gezogen und untersucht, auch wenn es hier keine Veränderungen im Prozess oder durch neue Shreddersysteme bei Recall gegeben hat.

Die Messungen haben ergeben, dass in einzelnen Fällen eine maximale Partikelfläche von 800 mm² nicht überschritten wurde. Der gesamte Bereich der „großen“ Partikel lag zwischen 320 und 800 mm². Insgesamt blieb die Anzahl jedoch unter der geforderten 10%-Marke. Die Mehrzahl der Partikel hatte eine Größe von unter 320 mm². Dies führt zu einer Bewertung gem. Sicherheitsstufe P-3.

1 Vlg. http://www.nia.din.de/cmd?artid=155420083&bcrumblevel=1&contextid=nia&subcommitteeid=54771182&level=tpl-art-detailansicht&committeeid=54738935&languageid=de
http://www.nia.din.de/cmd?artid=155420668&bcrumblevel=1&contextid=nia&subcommitteeid=54771182&level=tpl-art-detailansicht&committeeid=54738935&languageid=de

Der Bewertung gem. DIN liegen folgende Maßstäbe zu Grunde[2]:

Sicherheitsstufe	Zustand, Form und Größe nach der Vernichtung	Toleranz
P-1	Materialteilchenfläche max. 2000 mm²	10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 3800 mm² groß sein.
P-2	Materialteilchenfläche max. 800 mm²	. 10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 2000 mm².
P-3	Materialteilchenfläche max. 320 mm²	10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 800 mm² groß sein.
P-4	Materialteilchenfläche max. 160 mm²	10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 480 mm² groß sein.
P-5	Materialteilchenfläche max. 30 mm²	10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 90 mm² groß sein.
P-6	Materialteilchenfläche max. 10 mm²	10 % des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch höchstens 30 mm² groß sein.

Hierbei ist folgenden zu beachten: Die Norm 66399-1:2012-10 sieht unter bestimmten Vorraussetzungen die Erhöhung einer Sicherheitsstufe aus den Stufen P1-P3 um eine Stufe auf maximal P4 durch Vermischen und Verpressen vor.

Diese Bedingungen lauten:

- Zustimmung durch die verantwortliche Stelle
- Mindestmenge von 100 kg Datenträger, die in einem Durchgang ununterbrochen vernichtet wird,
- deutliche Anzeige der Sicherheitsstufe der Maschine und Art, wie die Erhöhung erreicht wird.

Da bei Recall der Prozess des Vermischens und Verpressens direkt an den Vernichtungsprozess gekoppelt sind und aus Effizienzgründen keine Mindermengen vernichtet werden, erfüllt Recall zwei der 3 Bedingungen. Es hängt somit von der verantwortlichen Stelle ab, ob diese der Erhöhung auf Stufe P-4 zustimmt.

Für öffentliche Stellen, die Verschlusssachen vernichten möchten, weist das BSI in einem Dokument[3] darauf hin, dass „*kommerzielle Dienstleister, die nur aufgrund der Anwendung von Vermischen/Verpressen die Sicherheitsstufe P-4 / 4 erreichen, für die Vernichtung von VS nicht geeignet“*. Grundlage des Dokumentes sind die §§ 29 und 30 der Verschlusssachenanweisung (VS-Anweisung – VSA).

[2] Zwar klassifiziert die DIN auch noch die Stufe P-7, diese spielte für die Bewertung jedoch keine Rolle.

[3] Überschrift des Dokumentes: „Vernichtung von Verschlusssachen (VS) bei Papier als Datenträger durch einen kommerziellen Dienstleister“. Das Dokument ist zwar nicht öffentlich zugänglich, liegt jedoch bestimmten öffentlichen Stellen vor.

III. Vernichtung von harten Daten durch einen separaten Shredder

In den letzten zwei Jahren hat Recall einige Investitionen getätigt. Dazu gehört ein neuer Shredder mit dem nun ausschließlich harte Datenträger vernichtet werden. Dies bedeutet, dass die anderen beiden Shreddersystem nun ausschließlich Papier vernichten. Das Gros der harten Datenträger besteht bei Recall aus alten herkömmlichen Festplatten. Aus der Stichprobe war ersichtlich, dass die Materialien, die keinen hohen Aluminumanteil hatten (z.B. Platinen) eine gleichmäßige Partikelgröße hatten, während Teile mit hohem Aluminumanteil sehr unterschiedliche Partikelgrößen aufwiesen. Insgesamt lagen die Partikelflächen zwischen 63 und 400 mm². In der Bewertung für den gesamten Bereich der „harten Datenträgern“ (also herkömmliche Festplatten und CDs) muss gem. der DIN-Vorschriften etwas differenziert werden. Die DIN 32757 sah hier keine Klassifizierung für die Vernichtung für Festplatten oder optische Datenträger vor. Aus diesem Grund wurde für dieses Material die DIN 66399, sowie die DIN EN 15713:2009, die Recall selbst als Maßstab zu Grunde legt, zur Bewertung herangezogen. Letztere klassifiziert „ID-Karten, CDs und DVDs“ in der Kategorie E und Computer inkl. Festplatten in der Kategorie D und sieht eine grundsätzliche Bewertung der Vernichtung von Stufe 1 (größtes Restmaterial) bis Stufe 8 (kleinstes Restmaterial) vor. Für die Klasse E lässt die DIN EN 15713:2009 nur eine Bewertung der Stufen 5-8 zu. Hierfür darf das geshredderte Material maximal eine mittlere Oberfläche von 800 mm² (Stufe 5), 320 mm² (Stufe 6), 30 mm² (Stufe 7) und 10 mm² (Stufe 8) besitzen.

Zwar wurden in der Stichprobe keine Anteile von CD-Material oder ID-Karten gefunden, aber laut Recall werden diese auch durch den Shredder vernichtet. Damit kann und muss von der gleichen Partikelgröße ausgegangen werden, wie oben beschrieben. Also liegt die mittlere Oberfläche der zerstörten Teile von optischen Datenträger ebenfalls zwischen 63 und 400 mm², bei einer mittleren Größe von 320 mm². Damit ist eine Vernichtung nach Stufe E-5 der DIN EN 15713:2009 für ID-Karten, CDs und DVDs gegeben.

Beim Blick auf die DIN 66399-2 wird die Sicherheitsstufe[4] O-3 erreicht, wobei auch hier wieder gilt: 10 % des Materials dürfen die geforderte Materialteilchenfläche von 320 mm² überschreiten, jedoch höchstens 800 mm² groß sein. Diese 10% waren in der Stichprobe gegeben.

Da die Informationsdichte auf dieser Art von Datenträgern unter Umständen sehr groß ist (je moderner das Medium, desto höher die Dichte), sollte von der verantwortlichen Stelle im Vorwege untersucht werden, ob die angebotene Vernichtungsstufe nach der DIN 66399-2 genügt, oder ob ggf. eine höhere Stufe erreicht werden muss.

Für die Vernichtung von magnetischen Festplatten[5] wird im Hinblick auf die DIN 66399 die Sicherheitsstufe H-5 eingehalten. Im Hinblick auf die DIN EN 15713:2009 wird die Stufe D-5 erreicht (alle Teile < 800 mm²).

Die letztendliche Entscheidung, ob die erreichte Partikelgröße den Anforderungen des zu vernichtenden Materials, insbesondere hinsichtlich der Informationsdichte auf dem Datenträger, genügt, obliegt der verantwortlichen Stelle. Als Hilfestellung kann hierfür (insbesondere in Behörden und öffentlichen Stellen) zum Beispiel das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen werden.

---

4 Analog zur DIN EN 15713 klassifiziert die DIN 66399 die Sicherheitsstufe von 1 (größte Partikel) bis 7 (kleinste Partikel).

5 Die magnetischen Festplatten werden hier explizit erwähnt, da es auf dem Festplattenmarkt auch Chip-basierte Festplatten (SSD) gibt. Diese gehören in andere Kategorien.

Dort gibt es im Maßnahmenkatalog M 2.167 eine „Empfehlung zum Vernichten von Datenträgern“[6]: *Demnach sollten Papierdokumente mit Aktenvernichtern zerkleinert werden. Bei normalem Schutzbedarf sollten hierfür Aktenvernichter der Sicherheitsstufe 3 nach DIN 32757-1 "Vernichten von Informationsträgern" bzw. der Zerkleinerungsnummer 6 nach DIN EN 15713 "Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln" genutzt werden, bei höherem Schutzbedarf solche der Sicherheitsstufe 4 oder 5 bzw. der Zerkleinerungsnummern 7 oder 8 (siehe auch M 2.435 Auswahl geeigneter Aktenvernichter).*

Zum Thema Festplattenvernichtung heißt es dort: *Festplatten können mechanisch mit einem Shredder zerkleinert werden. Dabei darf bei hohem Schutzbedarf die Größe der entstehenden Partikel 300 Quadrat-Millimeter nicht überschreiten (bzw. die Anforderungen der DIN EN 15713 bei Zerkleinerungsnummer 6 sind zu erfüllen). Bei normalem Schutzbedarf sind Partikelgrößen bis 1000 Quadrat-Millimeter durchaus vertretbar. Sie können auch thermisch vernichtet werden, dafür muss das Festplattenlaufwerk mindestens 15 Minuten lang auf über 1.000°C erhitzt werden. Da die hierfür erforderliche Ausstattung teuer ist, kann auf zuverlässige Dienstleister zurückgegriffen werden (siehe M 2.436 Vernichtung von Datenträgern durch externe Dienstleister).*

Und für optische Datenträger gilt: *Diese Datenträger können mechanisch mit einem Vernichter zerkleinert werden. Bei optischen Datenträgern darf die Größe der Partikel 200 Quadrat-Millimeter nicht überschreiten, bei höherem Schutzbedarf muss sie unter 10 Quadrat-Millimetern liegen. Sie können auch thermisch vernichtet werden, dafür müssen sie mindestens 60 Minuten lang auf über 300°C erhitzt werden.*

Für Halbleiterspeicher gilt: *Diese Datenträger können mit geeignetem Gerät mechanisch zerkleinert werden. Die Geräte sollen der Sicherheitsstufe 5 nach DIN 32757-1 bzw. DIN EN 15713 Zerkleinerungsnummer 8 entsprechen. Sie können auch verbrannt werden. Dafür müssen sie mindestens 15 Minuten lang auf über 800°C erhitzt werden.*

Und letztlich für Chipkarten gilt: *Chipkarten können verbrannt oder mechanisch mit einem Vernichtungsgerät zerkleinert werden. Bei höherem Schutzbedarf sollten hierfür Vernichter der Sicherheitsstufe 5 nach DIN 32757-1 genutzt werden bzw. der Zerkleinerungsnummer 8 nach DIN EN 15713.*

Das BSI sagt aber auch sehr deutlich: *Welche Verfahren geeignet sind, um die in der Institution vorkommenden Daten oder Datenträger zu löschen oder zu vernichten, hängt von der Art der Datenspeicherung, der Datenträger und vom Grad der Schutzbedürftigkeit der Informationen ab.* Eine vorherige eingehende Analyse in Form einer Schutzbedarfsfeststellung ist somit obligatorisch.

Für die elektronische Speicherung auf externen Datenträgern empfiehlt sich zu dem immer der Einsatz von Datenverschlüsselung.

Die Festlegung der für die Datenlöschung erforderlichen technischen und organisatorischen Maßnahmen sowie der Schutzbedürftigkeit obliegt gem. § 5 Abs. 2 i.V.m. § 17 Abs. 1 und 2 LDSG-SH bzw. §§ 9, 11 BDSG der Daten verarbeitenden Stelle.

Die Daten verarbeitende Stelle hat die Schutzbedürftigkeit der zu löschenden Daten/Datenträger in jedem Einzelfall zu definieren und zu deklarieren. Hierbei hat die Da-

6 Vgl. https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

ten verarbeitende Stelle den Schutzbedarf der Daten für die Auswahl der unterschiedlichen Sicherheitsstufen bei der Vernichtung der Datenträger zu berücksichtigen.

Für die Vernichtung von sensiblen Daten im Sinne des § 3 Abs. 9 BDSG (bzw. § 11 Abs. 3 LDSG) und der Vernichtung von Datenträgern von Geheimnisträgern oder von Berufs wegen zur Verschwiegenheit verpflichteten Personen, wird die Selbstanlieferung und Überwachung des Vernichtungsprozesses von den Aufsichtsbehörden des Datenschutzes als erforderlich betrachtet.

Zur Sicherstellung der besonderen Anforderungen von sog. Berufsgeheimnisträgern i. S. d. § 203 StGB gibt es bei Recall nach wie vor die Möglichkeit der persönlichen Anlieferung und Begleitung der Vernichtung außerhalb des Sicherheitsbereichs. Allerdings müssen Berufsgeheimnisträger i. S. d. § 203 StGB prüfen, ob das Verfahren zur Vernichtung ihrer konkreten Daten ausreichend ist. Für besonders sensible Daten (z. B. medizinische Daten) ist in der Regel eine Vernichtung nach Sicherheitsstufe 4 bis 5 im Sinne der DIN 32757 erforderlich.

IV. Zertifizierung von Recall gem. Payment Card Industry Data Security Standards (PCI[7])

Die Payment Card Industry Data Security Standards, kurz PCI genannt, umfassen eine Reihe von verbindlichen Regeln für alle Parteien, die Kartendaten verarbeiten, speichern oder weiterleiten. Händler sind hier genauso mit eingeschlossen wie Acquirer, Payment Service Provider (PSP) oder Drittdienstleister. Zwei dieser Regelungen lauten:

- Regelmäßige Prüfungen aller Sicherheitssysteme und -prozesse
- Einführen und Einhalten von Richtlinien in Bezug auf Informationssicherheit

Diese wurden im Rahmen der Zertifizierung entsprechend erstellt und umgesetzt. Bei Recall als Drittdienstleister umfasst dies nicht nur die IT-Systeme, sondern den gesamten Prozess. Insbesondere kommt dies der Dokumentation und somit der Transparenz zu Gute. Daraus resultiert u.a. auch der nächste Punkt.

V. Überarbeitung des QM-Systems

Im Zuge der Überarbeitung des QM-Systems wurden alle Dokumente inhaltlich erneuert und in einen neuen, einheitlichen Standard überführt. Somit gibt es nun auch ein Notfallkonzept, das sog. Safty Security Health Environment (SSHE). Hier sind alle Notfallmaßnahmen beschrieben, die sich auch auf den Vernichtungsprozess erstrecken.

VI. Einführung einer Videoüberwachung mit Aufzeichnungsfunktion im Betrieb

Als weiteren Nebeneffekt der Zertifizierung durch die PCI ist nun eine Videoüberwachung der Ein- und Ausgänge, sowie des Vernichtungsbereichs eingeführt worden. Diese dient ausschließlich der Sicherheit und nicht der Leistungsüberwachung der Mitarbeiter. So sollen Zutrittskontrollen und Zugriffskontrollen gem. § 9 BDSG gewährleistet und überwacht werden. Die Aufzeichnung der Daten erfolgt auf einem PC und werden automa-

7 Weitere Informationen über PCI finden sich unter https://www.pcisecuritystandards.org/

tisch nach 7 Tagen gelöscht.

VII. Erneuerung des Anlieferungsbereichs

Um die Zutrittskontrolle zu verbessern, wurde der Außenbereich und somit auch der Zugang zum Gelände neu gestaltet. Der Vernichtungshalle vorgelagert ist nun eine gesicherte Fläche mit Pförtnerhaus, bei der sich Anlieferer anmelden. Das Gelände ist durch ein massives automatisches Rolltor gesichert, das nur vom Pförtnerhaus aus geöffnet werden kann. Für einen Zugang von Personen gibt es eine separate Tür, die kameraüberwacht vom Verwaltungsgebäude aus geöffnet werden kann. Alternativ können Mitarbeiter diese über ihren Schlüssel öffnen. Die Vernichtungshalle ist mit weiteren Türen und Toren gesichert.

VIII. Erweiterung des Fuhrparks durch zwei Sicherheitspresswagen

Es fand eine Erweiterung des Fuhrparks um 2 neue Sicherheitspresswagen statt, die sowohl die besonderen Anforderungen an die Sicherheit des Kunden als auch an den Arbeitschutz der Mitarbeiter erfüllen.
Die Sicherheitspresswagen sind mit einer Schleuse ausgestattet, in der Sammelbehälter beim Kunden vor Ort automatisch in das innere des Wagens entleert werden. Die Öffnung der Sammelbehälter geschieht dabei durch den Kunden selbst. Die Kontrolle auf vollständige Entleerung erfolgt durch Recall-Mitarbeiter.
Durch die Aufnahme von Material mehrerer Kunden wird eine Vermischung von Material im Vorwege durchgeführt.

IX. Umsetzung der DIN EN 15713

Für Recall bedeutet die Umsetzung der DIN EN 15713, die im August 2009 veröffentlicht wurde, dass Datenträger aus Papier (entspricht Kategorie A) durch die Zuführung zu den Shredderanlagen vernichtet, verwirbelt, verpresst und zu Transporteinheiten zusammengefasst und bis zur Abholung auf die entsprechende Stellfläche des Zwischenlagers verbracht werden. Ebenso wird mit harten Datenträgern (entspricht Kategorie E) und Festplatten (entspricht Kategorie D), die sich im bereits ausgebauten Zustand befinden, verfahren.
Weiterhin werden die vernichteten Datenträger täglich stichprobenartig auf die ordnungsgemäße Vernichtung überprüft. Werden dabei Abweichungen festgestellt, wird das Material wiederholt dem Vernichtungsprozess zugeführt. Werden technische Mängel festgestellt, die die ordnungsgemäße Vernichtung nicht zulassen, dann wird das Material gesperrt. Nach Beseitigung der technischen Störung wird der Vernichtungsprozess erneut durchgeführt.

X. Bewertung des Vernichtungsprozesses (DIN 66399-3) – Variante 3

Gemäß der Forderung des ULD muss auch der Im dritten Teil der DIN 66399 beschrieben und bewertet werden. In diesem Teil wird der Vernichtungsprozess als solches festgelegt. *„Dabei ist die Vernichtung von Datenträgern als Prozess aufzufassen, der in seinen einzelnen Prozessabschnitten zu untersuchen und sicher zu gestalten ist.“ (Quelle: DIN 66399-3)*

Die Verantwortung für den Prozess liegt bei der verantwortlichen Stelle selbst. Dies gilt

jedoch nur für die Prozessabschnitte, auf die die verantwortliche Stelle die alleinige Kontrolle ausübt. Die Pflichten des Dienstleisters sind hiervon nicht beeinträchtigt.
Im Vorwege ist eine Sicherheitsstufe zu vereinbaren und der Prozess endet mit dem Erreichen dieser.

Die DIN unterscheidet dabei zwischen 3 Varianten, von denen hier nur die dritte Variante maßgeblich ist, da die Vernichtung bei einem externen Dienstleister (hier Recall) stattfindet.

In der DIN werden Kriterien benannt, die für alle Varianten übergreifend gelten und anzuwenden sind. In speziellen Szenarien kann es sinnvoll sein, Kriterien aus mehreren Varianten in Kombination anzuwenden. Darüber hinaus dürfen zwischen verantwortlicher Stelle und Dienstleister zusätzliche Kriterien vereinbart werden.

Zunächst müssen dabei die allgemeinen Prozesskriterien festgelegt werden. Dies bedeutet:

- Festlegung der Sicherheitsstufen in Abhängigkeit des Schutzbedarfs nach DIN 66399-1
- Der Dienstleister / die verantwortliche Stelle muss die ordnungsgemäße Vernichtung durch regelmäßige Probennahme kontrollieren.
  Recall führt eine regelmäßige Probenkontrolle durch und protokolliert dies. Ggf. werden sofort Maßnahmen ergriffen um das Ergebnis wieder zu verbessern.
- Es müssen Maschinen zur Vernichtung von Datenträgern nach DIN 66399-2 eingesetzt werden.
  Recall hält diese Maschinen vor und hat sich die Konformität vom Hersteller der Maschinen bestätigen lassen.

Die weiteren Kriterien für die 3. Variante (Datenträgervernichtung beim Dienstleister) sind der DIN 66399-3 zu entnehmen. Im Folgenden wird beschrieben wie diese analog bei Recall umgesetzt sind. Recall selbst hat die Einhaltung in einem SOP (Standard Operating Procedure) in ihrem Qualitätshandbuch beschrieben.
Die Gutachter gehen davon aus, dass jeweils die höchste Schutzklasse (3) erreicht werden soll. Sollte ein **erforderliches** Kriterium zur Erfüllung dieser Klasse nicht gegeben sein, so wird im Folgenden darauf hingewiesen.

- Alle Mitarbeiter von Recall sind nach den anzuwendenden Vorschriften des BDSG (Bundesdatenschutzgesetz) und des SGB (Sozialgesetzbuch) auf das Datengeheimnis verpflichtet. Gleiches gilt auch für Besucher.
- Besucher oder Anlieferer werden während des Aufenthalts in der Sicherheitszone durch Mitarbeiter begleitet.
- Besucher werden dabei mit einem Besucherausweis ausgestattet.
- Es sind technische und organisatorische Maßnahmen für den Vernichtungsprozess (Anfallstelle, Sammlung, Lagerung, Transport, Vernichtung) definiert. Die verantwortliche Stelle legt fest, welche Prozessabschnitte und Aufgaben der Dienstleister im Vernichtungsprozess übernimmt. Recall legt dies mit jedem Kunden individuell fest.
- Die technischen und organisatorischen Maßnahmen (bezogen auf die Umgebung)

werden durch schriftliche SOPs (Standard Operating Procedures) beschrieben und definiert. Die SOPs bilden das QM-Handbuch.

- Recall führt einen Nachweis, dass sie geeignete Maschinen für die zu vernichtenden Datenträgerkategorien verwendet. Dieser Nachweis stammt vom Hersteller der Maschinen. Weiterhin werden regelmäßig Audits durchgeführt.
- Die Verfügbarkeit der Maschine zur Vernichtung der Datenträger ist sichergestellt. Notfallpläne (Bestandteil des SSHE-Konzeptes) liegen im Recall-Vernichtungszentrum vor. Falls der Betrieb einer Maschine gestört sein sollte, werden umgehend vorher festgelegte Maßnahmen ergriffen um den Betrieb schnellstmöglich wieder aufzunehmen. Jeder Mitarbeiter weiß was im Falle von Störungen oder Maschinenfehlern zu tun ist.
- Recall gestattet der verantwortlichen Stelle die Überwachung der Vernichtung der Datenträger.
- Für die Sammlung, Lagerung und den Transport von Datenträgern werden geschlossene und verschlossene Sicherheitsbehälter eingesetzt. Ausnahmen sind von der verantwortlichen Stelle festzulegen.
- Es finden protokollierte Übergaben in Form eines Dienstleistungsauftrages/Übernahmeprotokolls statt.
- Im Bezug auf den Umgang mit losen Datenträgern (z. B. Umladen, Umleeren) sind Recall-Kuriere angewiesen nur verschlossene Sicherheitsbehälter beim Kunden anzunehmen. Ausnahmen sind von der verantwortlichen Stelle festzulegen. Eine Umleerung der Sicherheitsbehälter erfolgt bei Recall beim Einsatz von Sicherheitspresswagen statt. Hierbei werden die Sicherheitsbehälter bei der verantwortlichen Stelle vor Ort geöffnet, deren Inhalt in einen Fahrzeug-Pressenaufbau verbracht und der entleerte Behälter verbleibt verschlossen beim Kunden.
- Recall wendet bei Umleerverfahren und Vermischung von Datenträgern, die für die Vernichtung in unterschiedlichen Sicherheitsstufen vorgesehen sind, die höchste vereinbarte Sicherheitsstufe für die gesamte Ladung an.
- Die Lagerung (bis zur Vernichtung) und Entleerung der Sicherheitsbehälter findet ausschließlich innerhalb eines geschlossenen und überwachten Bereichs am Recall Standort statt.
- Der Recall Standort ist mit Systemen der Video-, Zutritts-, Einbruchs- und Brandüberwachung ausgestattet und auf zertifizierte Notrufleitstellen zur Überwachung auf Störung und Alarm aufgeschaltet.
- Zum Transport werden ausschließlich Fahrzeuge mit geschlossenem und verschlossenem festem Aufbau verwendet.
- Fahrzeuge verfügen derzeit nicht über ein GPS System. Fahrer sind mit Hilfe von Diensthandys jederzeit in der Lage mit dem Recall Standort zu kommunizieren. Transporte werden derzeit nur mit einer Person durchgeführt. Alternativ sind begleitete Transporte durch die verantwortliche Stelle nach vorheriger Absprache grundsätzlich möglich. Hier ist die Schutzklasse 3 nicht erfüllt, da dies ein erforderliches Kriterium ist.

- Dem Bedienpersonal ist der Zugriff auf zu vernichtenden Datenträger mit Informationsdarstellung in Originalgröße (DIN66399-2 Kategorie P) grundsätzlich untersagt, jedoch ist ein Zugriff möglich. Dem Bedienpersonal ist die Kenntnisnahme der zu vernichtenden Datenträger grundsätzlich untersagt. Jeder Recall Mitarbeiter hat dazu eine schriftliche Unterweisung unterschrieben. Die Datenträger werden direkt dem Vernichtungsvorgang zugeführt. Eine Unterbindung des Zugriffs auf die Datenträger ist nicht möglich, da das Bedienpersonal die Sicherheitsbehälter öffnen, der Vernichtung zuführen und zur Kontrolle auf vollständige Entleerung oder mögliche Anhaftungen untersuchen muss. Alternativ sind begleitete Vernichtungen durch die verantwortliche Stelle nach vorheriger Absprache grundsätzlich möglich. Hier ist die Schutzklasse 3 nicht erfüllt, da dies ein erforderliches Kriterium ist.
- Die Bereiche der Zuführung und der Vernichtung sind videoüberwacht. Die verantwortliche Stelle kann sich eine Probe seiner vernichteten Datenträger nehmen oder aushändigen lassen, wenn die Vernichtung vollkommen separiert durchgeführt wird. Im Normalfall werden auf Grund der anonymisierten Sicherheitsbehälter sämtliche angelieferten Datenträger kundenunabhängig nacheinander vernichtet. Durch diese zusätzliche Vermischung der Datenträger ist eine kundenspezifische Probemitnahme dann nicht mehr möglich.
- Die Vernichtung erfolgt innerhalb eines Werktages nach Übernahme der zu vernichtenden Datenträger da Recall innerhalb der normalen, geplanten Arbeitszeiten die Vernichtung betreibt. Sollte eine Vernichtung am gleichen Tag gewünscht werden, muss dies mit Recall im Vorwege abgesprochen und geplant werden.
- Der geschlossene Vernichtungsbereich von Recall wird ausschließlich zu diesem Zweck genutzt und ist auf einem gesicherten Betriebsgelände. Eine Einsicht von außen ist nicht möglich.
- Das Betriebsgebäude ist in massiver Bauausführung ausgeführt.
- Für Fahrzeuge stehen Andocktore und/ oder Rolltore zur Einfahrt zur Verfügung, die ausschließlich im innen liegenden Bereich der Sicherheitszonen geöffnet werden können. Die Steuerung der Öffnungen obliegt Recall. Die Bereiche der Gebäudezugänge sind videoüberwacht.
- Die Anlieferzone befindet sich innerhalb des umzäunten Geländes. Die LKW fahren rückwärts an eine Rampe, die zu einer Schleuse führt.
- Türen und Tore verschließen nicht automatisch. Der operative Ablauf zum Verschluss und Öffnung von Zugängen ist in den organisatorischen Betriebsabläufen geregelt. Die Steuerung der Öffnungen obliegt Recall. Hier ist die Schutzklasse 3 nicht erfüllt, da dies ein erforderliches Kriterium ist.
- Türen und Tore können durch Recall Mitarbeiter jederzeit eingesehen werden (per Videoüberwachung und visuell). Der operative Ablauf zum Verschluss und Öffnung von Zugängen ist in den organisatorischen Betriebsabläufen geregelt. Die Steuerung der Öffnungen obliegt Recall. Hier ist die Schutzklasse 3 nicht erfüllt, da dies ein erforderliches Kriterium ist.
- Sämtliche Sicherheitszonen werden durch Videokameras überwacht.

- Die Notfallredundanz ist durch das Vorhandenseins eines zweiten Shredders und/ oder andere Recall-Vernichtungszentren gewährleistet. Bei der Nutzung anderer vorhandener Recall-Vernichtungszentren kann aber auf Grund des zeitlichen Zusatzaufwandes für den Umtransport keine taggleiche Vernichtung stattfinden. Hier ist die Schutzklasse 3 nicht erfüllt, da dies ein erforderliches Kriterium ist.

Nach Meinung der Gutachter wird durch die o. g. Art und Weise Erfüllung der Kriterien bis auf die o.g. Ausnahmen die Schutzklasse 3 erreicht. Die einsetzende Stelle muss jedoch für sich prüfen, ob die genannte Umsetzung ausreicht.

E. Zusammenfassung

Nachfolgend sollen die Prüfergebnisse für die beiden DIN noch einmal zusammenfasst werden:

a) Anforderung und Ergebnis nach DIN 66399-2

Reines Shredderergebnis = P3 weil die Materialteilchenfläche von 320 mm² mit einer maximal 10%-igen Abweichung bis zu 800 mm² eingehalten wird.

Gesamtprozessergebnis = P4 weil das reine Shredderergebnis um eine Stufe erhöht werden darf, wenn die Sicherheit durch vor- und nachgelagerte Prozesse der Verwirbelung und Verpressung ergänzt wird. Voraussetzung: Zustimmung durch die Daten verarbeitende Stelle.

b) Anforderung und Ergebnis nach DIN EN 15713

Reines Shredderergebnis = Zerkleinerungsnummer 6 weil die Materialteilchenfläche von 320 mm² mit einer maximal 10%-igen Abweichung bis zu 800 mm² eingehalten wird.

In keinem Fall konnten vom vorliegenden Akten-Shreddermaterial ein personenbezogenes Datum vollständig rekonstruiert werden, wenngleich Teile (wie z.B. der Teil eines Vornamen oder einer Adresse) als solche identifiziert werden konnten.

Die letztendliche Entscheidung, ob die erreichte Partikelgröße den Anforderungen des zu vernichtenden Materials, insbesondere hinsichtlich der Informationsdichte auf dem Datenträger, genügt, obliegt der verantwortlichen Stelle.

In rechtlicher Hinsicht hat es zwischenzeitlich keine Änderung der gesetzlichen Anforderungen gegeben, die für die vorliegende Rezertifizierung von Belang sind.

Um den besonderen Anforderungen von sog. Berufsgeheimnisträgern i.S.d. § 203 StGB Rechnung zu tragen, gibt es bei Recall nach wie vor eine Betriebsanweisung für Mitarbeiter, aus der sich ergibt, wie Kunden zu beraten sind, die zur Gruppe der Berufsgeheimnisträger i.S.d. § 203 StGB zu rechnen sind. Diese müssen jedoch prüfen, ob das Verfahren zur Vernichtung der konkreten Daten ausreichend ist.
In der Betriebsanweisung werden die Mitarbeiter entsprechend angewiesen, Kunden aus diesem Personenkreis auf die Möglichkeit hinzuweisen, dass diese ihre zu vernichtenden Unterlagen eigenhändig in den Shredder werfen können und die Vernichtung vor Ort überwachen können. Das Vernichtungsverfahren von Recall lässt sich nach wie vor als vorbildlich bewerten. Auf dem Transport vom Kunden zum Vernichtungswerk sind die Datenträger in Papierform vor der unbefugten Kenntnisnahme Dritter gesichert.

Die Veränderungen seit der letzten Rezertifizierung sind allesamt positiv zu bewerten. Hervorstechend sind dabei das neue QM mit der einhergenden Dokumentation und den daraus resultierenden transparenten Prozessen, sowie die Verbesserungen der Zutrittskontrolle für das gesamte Betriebsgelände, das nun in vorbildlichem Maße gesichert ist. Das verwendete Shredderverfahren und die Weiterverarbeitung der vernichteten Datenträger sorgen dafür, dass eine wirksame, gesetzeskonforme Vernichtung von Akten, magnetischen Festplatten und optischen Datenträgern wie folgt gewährleistet ist:

Material	**Sicherheits- oder Zerkleinerungsstufe**	**Vorschrift / Maßstab**	**Geeignet für Schutzbedarfstufe nach BSI M 2.167**
Papier	P-3	DIN 66399-2	normal
Magnetische Festplatten	H-5 D-5	DIN 66399-2 DIN EN 15713:2009	normal
Optische Datenträger	O-3 E-5	DIN 66399-2 DIN EN 15713:2009	keine

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den _____

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Flensburg, den

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)