Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen durch das Verfahren zur Datenvernichtung

Lutz von Wildenradt GmbH

Aukrug

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
fax 0461 – 90 91 357
email sh@hansen-oest.com

Stand:
Mai 2012

Inhaltsverzeichnis

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Beschreibung	Kommentar
10.02.2012	Erstellung	
08.03.2012	Ergänzung	
20.03.2012	Änderung	
26.03.2012	Korrekturen	
03.04.2012	Änderung	
04.04.2012	Ergänzung	
10.04.2012	Ergänzung	
17.04.2012	Korrekturen	
12.05.2012	Korrektur	Nach Veröffentlichung wurde in RN 9 das Wort „obsolet“ gegen das Wort „obligatorisch“ ausgetauscht.
31.05.2012	Ergänzung	Rn. 6, 11, 13

A. Einleitung

1 Mit dem vorliegenden Gutachten beabsichtigt die Lutz von Wildenradt GmbH (nachfolgend LvW 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.

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

B. Zeitpunkt der Prüfung

2 Die Prüfung des Verfahrens fand im Zeitraum 01.01.2012 - 03.04.2012 statt.

C. Änderungen und Neuerungen des Produktes

3 Die Firma LvW bietet seinen 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 2005 und 2010 beschrieben. Es gibt keine Veränderungen und keine Neuerungen. LvW bietet seinen Kunden immer noch folgende Leistungen zur Vernichtung von Daten an:

- Vernichtung der Daten direkt bei der datenverarbeitenden Stelle unter Aufsicht (mobiler Shredder)
- Abholung der Daten in Einzelbehältern
- Alternativ persönliche Anlieferung bei LvW
- Automatische Beschickung der Shredderanlage nach Entleerung der Einzelbehälter auf ein Fließband
- 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

Die von LvW verwendeten Einzelbehälter können - nach Kundenwunsch - mit individuellen Schlössern versehen werden. Auch Mehrfachschließsysteme kommen zum Einsatz. Unabhängig vom verwendeten Verfahren hat LvW grundsätzlich für jedes verwendete Schloss mindestens noch einen Schlüssel, damit die Einzelbehälter im Werk geöffnet werden können.

D. Datenschutzrechtliche Bewertung

6 Die Anforderungen, die im Gutachten aus 2010 geprüft wurden (BSI-TL 03420), wurden nicht mehr überprüft, so dass die Vernichtung von Akten und Papier gegen die aktuell geltende DIN 32757, sowie die sich im Entwurf befindlichen DIN 66399-2[1] und die Vernichtung von herkömmlichen Festplatten und CDs im Hinblick auf die Partikelgröße gegen die DIN 66399, sowie die DIN EN 15713:2009 geprüft wird.

7 Wie im Gutachten von 2005 beschrieben erfüllt die Partikelgröße von geshredderten Akten die Anforderungen an die DIN 32757 Sicherheitsstufe 3. Dies wurde durch Stichprobenmessungen des technischen Gutachters belegt. Bei diesen Messungen wurden insbesondere die „Ausreißer", also die großen Partikel einer exakten Analyse unterzogen. Die Messungen haben ergeben, dass in einzelnen Fällen eine maximale Patikelfläche von 640 mm² nicht überschritten wurde. Der gesamte Bereich der „großen" Partikel lag zwischen 320 und 640 mm². Diese Werte liegen deutlich unterhalb der Grenze für die in der DIN 32757 festgelegten Sicherheitsstufe 2 (800 mm²). Durch Vermischung mit anderen Daten und anschließender Verpressung gemäß DIN wird die Sicherheitsstufe 3 erreicht. Für die DIN 66399 gilt analog die Sicherheitsstufe P-3.

Wie beschrieben handelt es sich um eine Randbetrachtung. Damit ist gemeint, dass die meisten Partikelteilchen bereits eine kleinere Fläche als 320 mm² haben und somit schon ohne Verwirbelung und Verpressung in die Sicherheitsstufe 3 gemäß DIN 32757 fallen. Für das Datenschutzgütesiegel wird jedoch vom so genannten „Worst-Case" ausgegangen, da sich personenbezogene Daten auf den größten Partikeln befinden können und somit eine Rekonstruierbarkeit am wahrscheinlichsten ist. Die DIN 66399 lässt bei der Betrachtung der Sicherheitsstufe P-3 sogar zu, dass 10 % des Materials die geforderte Materialteilchenfläche (320 mm²) überschreiten dürfen, jedoch den Grenzwert von 800 mm² nicht überschreiten. Das Verfahren von LvW bleibt im Ergebnis in diesen Grenzen.

8 Im Bereich der „harten Datenträgern" (herkömmliche Festplatten und CDs) muss gem. der DIN etwas differenziert werden. Die DIN 32757 sieht keine Klassifizierung

1 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.

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 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 muss das geshredderte Material eine maximale mittlere Oberfläche von 800 mm² (Stufe 5), 320 mm² (Stufe 6), 30 mm² (Stufe 7) und 10 mm² (Stufe 8) besitzen.

Im vorliegenden Fall lag die mittlere Oberfläche der zerstörten Teile der optischen Datenträger zwischen 320 und 800 mm². Damit ist eine Vernichtung nach Stufe E-5 der DIN EN 15713:2009 für ID-Karten, CDs und DVDs gegeben. Da die Informationsdichte auf diesen 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 EN 15713:2009 genügt, oder ob ggf. eine höhere Stufe erreicht werden muss.
Gleiches gilt auch für die zweite Vorschrift. Beim Blick auf die DIN 66399 wird die Sicherheitsstufe[2] 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.

Für die Vernichtung von magnetischen Festplatten[3] wird im Hinblick auf die DIN 66399 die Sicherheitsstufe H-5 eingehalten (gleiche Teilchengröße wie in der Papierform, mit dem Unterschied, dass die Teile ggf. auch noch stark verbogen waren, wenn es sich um massiveres Metall handelte). Im Hinblick auf die DIN EN 15713:2009 wird die Stufe D-5 erreicht (alle Teile < 800 mm²).

9 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.

Als Hilfestellung kann hierfür (insbesondere in Behörden und öffentlichen Stellen) zum Beispiel das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen werden. Dort gibt es im Maßnahmenkatalog M 2.167 eine „Empfehlung zum Vernichten von Datenträgern“[4]: *Demnach sollten Pa-*

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

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

4 Vgl. https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02167.html

pierdokumente mit Aktenvernichtern zerkleinert werden. Bei normalem Schutzbedarf sollten hierfür Aktenvernichter der Sicherheitsstufe 3 nach DIN 32757-1 genutzt werden, bei höherem Schutzbedarf solche der Sicherheitsstufe 4 oder 5.

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, bei normalem Schutzbedarf sind Partikelgrößen bis 1000 Quadrat-Millimeter durchaus vertretbar.*

Und für optische Datenträger gilt: *Diese Datenträger können mechanisch mit einem Aktenvernichter 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.*

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.

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

11 Um den besonderen Anforderungen von sog. Berufsgeheimnisträgern i.S.d. § 203 StGB Rechnung zu tragen, gibt es bei LvW 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. 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.
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.

12 Das Vernichtungsverfahren von LvW 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.

E. Zusammenfassung

13 Das Betriebsgelände ist in adäquat bis vorbildlichem Maße mittels Schließsystemen und Zutrittsregelungen gesichert. 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	3 P-3	DIN 32757 DIN 66399[5]	normal
Magnetische Festplatten	H-5 D-5	DIN 66399 DIN EN 15713:2009	normal
Optische Datenträger	O-3 E-5	DIN 66399 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 _____ Flensburg, den _____

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

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

5 Die DIN 66399 wurde nur für die Klassifizierung der Papiergröße herangezogen und nicht auf das Vernichtungsverfahren per se.