Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen durch das Verfahren zur Datenvernichtung

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.sh

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@premium-datenschutz.de

Stand:
September 2010

Inhaltsverzeichnis

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Beschreibung	Kommentar
20.02.2010	Erstellung	Version 1.0
01.04.2010	Erweiterung	Version 1.1
15.05.2010	Änderungen	Version 1.2
13.06.2010	Erweiterungen	Version 1.3
20.07.2010	Änderungen	Version 1.4
20.09.2010	Ergänzungen	Version 1.5

A. Einleitung

1 Mit dem vorliegenden Gutachten beabsichtigt die recall Deutschland GmbH (nachfolgend recall genannt) (ehemals recall Deutschland GmbH & Co. KG) ihr Verfahren zur Datenvernichtung für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) 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

2 Die Prüfung des Produktes fand vom 14. Januar 2010 bis 20. September 2010 statt.

C. Änderungen und Neuerungen des Produktes

3 Das Verfahren ist wie im Gutachten von 2006 beschrieben. Es gibt keine Veränderungen und keine Neuerungen. Der Kunde bietet immer noch folgende Leistungen 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

Gegenüber dem Gutachten von 2006 ist **die Vernichtung von Microfichen nicht mehr Bestandteil der Zertifizierung**.

Die von recall verwendeten Einzelbehälter (aus Metall oder Kuststoff) können - nach Kundenwunsch - mit individuellen Schlössern (integriert oder Vorhängeschloss) versehen werden. Auch Mehrfachschließsysteme kommen zum Einsatz, worauf der Kunde im Gespräch hingewiesen wird. Die Aufteilung ist liegt hier bei 30% (individuell) und 70% (mehrfach)

Bei der individuellen Schlossvariante besteht die Möglichkeit, dass recall einen Schlüssel hat, aber es ist auch möglich, dass nur der Kunde über einen Schlüssel verfügt. Dann kommt eine sog. „begleitete Vernichtung“ zum tragen, bei der der Kunde den Behälter erst in der Entsorgungshalle aufschließt. Auch dies gehört zum Angebot von recall, auf das der Kunde hingewiesen wird.

Technisch erreichen die eingesetzten Shredder die Sicherheitsstufe 3 gem. DIN 32 757, die durch mehrfache Vermischung (vor und während der Vernichtung)

und nachgelagerte Verwirbelung und (bei der Vernichtung von Papier) sofortige Verpressung des geshredderten Materials um eine Stufe auf Sicherheitsstufe 4 erhöht wird.

Die Fahrzeuge sind nun alle mit zwei unabhängigen Alarmanlagen versehen. Eine für den Fahrerraum und eine für den Transportraum.

D. Datenschutzrechtliche Bewertung

6 Gemäß der Änderungen an die Prüfung für Aktenvernichtungsverfahren, muss überprüft werden, ob die Anforderungen der BSI-TL 03420 erfüllt sind.

Diese Richtlinien gelten für das Löschen oder Vernichten von schutzbedürftigen Informationen, die auf Papier (Dokumente) oder anderen analogen Datenträgern (z.B. Mikrofilm) und auf digitalen Datenträgern (elektronisch, magnetisch, optisch) gespeichert sind.

Die Richtlinien gelten für Verschlusssachen (VS), die gemäß § 28 der Verschlusssachen-Anweisung (VSA) gelöscht oder vernichtet werden müssen.

Daten werden demnach in zwei Sicherheitsstufen klassifiziert:

- *mittlere Sicherheit - Sicherheitsanforderungen für Informationen bis einschließlich VS-NfD (und vergleichbaren Geheimhaltungsgraden anderer Staaten/Organisationen) sowie personenbezogene Daten (vgl. § 3 Abs. 1 BDSG), sowie*
- *hohe Sicherheit - Sicherheitsanforderungen für Informationen VS-Vertraulich und höher (und vergleichbaren Geheimhaltungsgraden anderer Staaten/Organisationen) sowie besondere personenbezogene Daten (§ 3 Abs. 1 und 9 BDSG).*

Für die Vernichtung von Dokumenten mit einem hohen Grad der Schutzbedürftigkeit (z.B. Verschlusssachen aller Geheimhaltungsgrade) sind Aktenvernichter der Sicherheitsstufe 4 oder 5 gemäß DIN 32757 zu verwenden. Bei sonstigen Informationsträgern, die z.B. dem Datenschutz unterliegen, ist in vielen Fällen die Sicherheitsstufe 3 ausreichend.[1]

7 Die Shredderverfahren für Datenträger in Papierform erfüllt nach Angaben des Herstellers die Sicherheitsstufe 3 gemäß DIN 32757-1. Hiermit wird erreicht, dass das Shreddergut nicht größer als 320 mm² ist. In der Arbeitsanweisung AA6 von „recall“ ist geregelt, dass bei der Aktenvernichtung mindestens Sicherstufe 3 der DIN 32757-1 einzuhalten ist. Jegliche Größenabweichungen um mehr als 10% einer Probe werden gemeldet. Unzureichend geshreddertes Material wird erneut geshreddert.

Da andere Datenträger, sog. „harte Datenträger“ (Festplatten, CDs, Chipkarten etc.), ebenfalls durch dieselbe Shredderanlage vernichtet werden, ist auch hier gewährleistet, dass das Shreddergut bzw. die „Schnipselgröße“ nicht größer als 320 mm² beträgt. Auch hier greift eine entsprechende Verfahrensanweisung (14), in der geregelt ist, dass bei Datenträgervernichtung die Sicherheitsstufe 3 der DIN 32757-1 einzuhalten ist.

1 Quelle: BSI-Technische Leitlinie mit dem Kürzel: BSI – TL 03420 und der Bezeichnung: „Richtlinien für das Löschen und Vernichten von schutzbedürftigen Informationen auf analogen und digitalen Datenträgern

Die BSI Richtlinie schreibt jedoch vor, dass im Bereich der „harten Datenträger“ eine Partikelgröße von unter 10 mm² erreicht werden um Datenmaterial mit hoher Schutzbedürftigkeit zu vernichten. Dies ist durch die eingesetzten Maschinen nicht gegeben, so dass hier auch nur Daten mit mittlerer Schutzbedürftigkeit vernichtet werden können. Es besteht die Möglichkeit einer gesonderten Überprüfung des Shreddermaterials beim BSI und die Ausstellung eines Zertifikates durch das BSI. Ein solches Zertifikat vom BSI über die Vernichtung von harten Datenträgern liegt nicht vor.

Folgende Tabelle fasst die Ergebnisse in der Übersicht zusammen:

Datenträgerart	***erreichte Partikelgröße [mm²]***	***erreichte Sicherheitsstufe (DIN 32757)***	***erreichte Sicherheit (BSI - TL 03420) – worst case***
Papier, Pappe, Karton, Dokumente	31 - 320	3 (mit Verwirbelung 4)	mittlerer Grad der Schutzbedürftigkeit
Festplatten	< 320	k.A.	mittlerer Grad der Schutzbedürftigkeit
Optische Datenträger (CD, DVD)	< 200	k.A.	mittlerer Grad der Schutzbedürftigkeit
USB-Sticks	< 200	k.A.	mittlerer Grad der Schutzbedürftigkeit

Ergänzend sei darauf hingewiesen, dass die für die Daten verantwortliche Stelle (z.B. ein Arzt) das Datenmaterial selbst auf das Förderband kippen kann, so dass gewährleistet ist, dass keine unbefugte Kenntnisnahme stattfindet.

8 In rechtlicher Hinsicht hat es zwischenzeitlich eine teilweise Änderung der gesetzlichen Anforderungen gegeben, die für die vorliegende Rezertifizierung von Belang sind. Konkret betroffen ist das Verfahren durch die Änderungen des § 11 BDSG, die mit Wirkung zum 01.09.2009 in Kraft getreten sind. Der geänderte § 11 Abs. 2 BDSG sieht nun konkrete Inhalte für den schriftlichen Auftrag vor. Im Einzelnen muss der Auftrag nachfolgende Inhalte regeln:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder

gegen die im Auftrag getroffenen Festlegungen,

- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Antragsteller hat diesen Änderungen dahingehend Rechnung getragen, dass er - wie bereits bei der Erstzertifizierung - ein Muster für eine Auftragsdatenverarbeitungsvereinbarung für den Nutzer des Verfahrens vorhält, das verwendet werden kann. Die Verwendung anderer Formen und Inhalte des „Auftrags“ bleibt möglich. Der Antragsteller trägt jedoch Sorge dafür, dass die gesetzlichen Vorgaben des § 11 BDSG auch im Falle einer individuellen Vereinbarung bzw. Weisung berücksichtigt werden.

Ein Muster der Auftragsdatenverarbeitungsvereinbarung zur Akten-/Datenvernichtung wird dem ULD zur Verfügung gestellt.

Im Übrigen sind die Änderungen des BDSG, die zwischenzeitlich in Kraft getreten sind, für das vorliegende Verfahren nicht maßgeblich.

9 Weiterhin wurde die DIN EN 15713:2009 geprüft. Hinsichtlich der Vorgabe einer Videoüberwachung kann festgehalten werden, dass recall eine Überwachung mittels Videokameras einsetzt, derzeit jedoch keine Aufzeichnung stattfindet. Aus Datenschutzrechtlicher Sicht – im Sinne der Datenvermeidung und Datensparsamkeit und im Sinne der Mitarbeiterkontrolle – ist dies positiv zu vermerken.

10 Das Vernichtungsverfahren von recall lässt sich nach wie vor als vorbildlich bewerten. Auf dem Transport vom Kunden zum Vernichtungswerk sind die Akten und Datenträger vor der unbefugten Kenntnisnahme Dritter gesichert.

E. Zusammenfassung

11 Das Betriebsgelände ist in vorbildlichem Maße mittels Schließsystemen und Zutrittsregelungen gesichert. Das verwendete Shredderverfahren und die Weiterverarbeitung der vernichteten Datenträger (aller Art) sorgen dafür, dass eine wirksame, gesetzeskonforme Vernichtung von Daten mit mittlerer Schutzbedürftigkeit nach BSI-TL 03420 erfolgt. Für Daten von Berufsgeheimnisträgern (z.B. Ärzte, Rechtsanwälte, Steuerberater) ist die Vernichtung nur geeignet, wenn diese das Datenmaterial persönlich anliefern und die Vernichtung überwachen.

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

Kellinghusen, den 20.09.2010

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

Flensburg, den 20.09.2010

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