Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das

- Verfahren zur Akteneinlagerung -

der

Recall Information Service 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:
August 2014

Inhaltsverzeichnis

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Art der Änderung	Bemerkung
22.01.2014	Erstellung	Version 1.0
31.01.2014	Ergänzungen	Version 1.1
21.03.2014	Ergänzungen	Version 1.2
25.04.2014	Überarbeitung	Version 1.3
30.08.2014	Ergänzungen	Version 1.4

A. Einleitung

Mit dem vorliegenden Gutachten beabsichtigt die Recall Information Services GmbH (vormals recall Deutschland GmbH und nachfolgend Recall genannt) ihr Verfahren zur Aktenarchivierung 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 01.12.2013 – 26.08.2014 statt.

C. Änderungen und Neuerungen des Verfahrens

2014 wurde der Bereich der Datenträgerarchivierung in die Firma Recall Information Services GmbH verschoben. Dies hat jedoch keinen Einfluss auf den Standort oder sonstige technische oder organisatorische Maßnahmen in diesem Bereich.
Die Firma Recall bietet ihren Kunden nach wie vor ein Verfahren zur Akteneinlagerung an. Das Verfahren ist wie in den Gutachten von 2006 und 2012 beschrieben. Auf der Webseite von Recall werden in der Produktübersicht der Archivierung verschiedene Produkte angeboten. Der Zertifizierungsgegenstand (Target of Evaluation – ToE) umfasst nach wie vor nur die folgenden Einlagerungsarten (Produkte):

- Legacy
- OnCall und
- ReFile.

Alle anderen Arten und Produkte sind nicht Bestandteil des ToE.

Bei dem Produkt „Legacy“ geht es um die Dokumentenaufbewahrung in Kartons, die selten benötigt werden, oder auf die selten zugegriffen werden muss.

Bei Kartons mit höher frequentiertem Zugriff bietet das „OnCall“ Produkt neben der Aufbewahrung auch optional Routine- (in einem bestimmten Zyklus), Priorität- und Expressbereitstellung.

Das Produkt „ReFile“ beinhaltet die Lagerung auf Aktenebene mit den gleichen optionalen Auslieferungsmöglichkeiten wie bei dem Produkt „OnCall“.

Die Anforderung der Auslieferung per Internet gehört nach wie vor nicht zum ToE.

Die Leistungen im Einzelnen stellen sich immer noch wie folgt dar:

- Einlagerung von Behältnissen
- Einlagerung in Behältnissen mit Inhaltsangaben durch den Kunden
- Einlagerung von Akten mit niedrigem Schutzniveau mit Inhaltsangaben durch „recall“
- Einlagerung von Daten mit hohem Schutzniveau
- Einlagerung von Daten von Berufsgeheimnisträger

Der technische Sachverständige Andreas Bethke hat die Räumlichkeiten 2013 vor Ort in Augenschein genommen und einem Ein- und Auslagerungsprozess des modernen automatischen Hochregallagers beigewohnt. Es wurde weiter kontrolliert, dass das Gelände und das Gebäude durch hinreichende Maßnahmen vor dem Zutritt unberechtigter Dritter gesichert sind.

Es gibt derzeit folgende Veränderungen/Neuerungen:

- Erneuerung des Anlieferungsbereichs
- Überarbeitung des QM-Systems.
- Zertifizierung gem. DIN EN ISO 9001 : 2008
- Der Betrieb hat ein Payment Card Industry Data Security Standard (PCI) Zertifikat

D. Datenschutzrechtliche Bewertung

In rechtlicher Hinsicht trat am 01.01.2014 die neue Datenschutzverordnung (DSVO) des Landes Schleswig-Holstein in Kraft. In dieser gibt es im Vergleich zur DSVO 2009 Änderungen bei der Erstellung der Verfahrensdokumentation (§ 3), bei der Dokumentation der Sicherheitsmaßnahmen (§ 3) (hier insbesondere die Erweiterung bei der Dokumentation des Datenschutzmanagements), bei der Dokumentation des Tests und der Freigabe (§ 5).

Planen öffentliche Stellen den Einsatz des Verfahrens von Recall, so obliegt die Dokumentation zwar der einsetzenden Stelle, jedoch ist entscheidend, ob der Anbieter diesen Prozess unterstützt. Recall wird diesem Anspruch voll und ganz gerecht. Ausführungen folgen.

I. Erneuerung des Anlieferungsbereichs

Um die Zutrittskontrolle zu verbessern, wurde der Außenbereich und somit auch der Zugang zum Gelände neu gestaltet. Der Halle zur Akteneinlagerung ist nun eine gesicherte Fläche mit Pförtnerhaus vorgelagert, bei der sich Anlieferer anmelden müssen. 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 Lagerhalle ist ein separates Gebäude, das mit weiteren Türen und Toren gesichert ist, für die wiederum nur ein ausgewählter Mitarbeiterkreis Zutritt hat. Die Halle ist während der normalen Arbeitszeiten ständig besetzt, so dass ein unbefugter Zutritt sofort bemerkt wird.

II. Überarbeitung des QM-Systems

Im Zuge der Überarbeitung des QM-Systems wurden alle Dokumente inhaltlich erneuert und in einen neuen, einheitlichen Standard überführt. Den Gutachtern wurden folgende Dokumente zur Prüfung vorgelegt:

• Rahmenvertrag DMS-P Blanko	*Vertrag zur Auftragsdatenverarbeitung*
• SOP-4.4.1.1 - Securitykonzept DMS	*Beschreibung der Maßnahmen gem. § 9 BDSG (nebst Anlagen)*
• SOP-4.4.1.6 - DMS-Kundenhinweis für Berufsge-	

heimnisträger	
• SOP-4.3.1.2.1-Verhalten bei Security Vorfällen	
• F-4.3.2.1 - SSHE Vorfall - Analysebericht	
• SOP-4.9.1.1-Ablauf Audit	*Beschreibung von Abläufen bei folgenden Audits:* • *Kundenaudits bei recall (externe Prüfung)* • *Zertifizierungsaudits bei recall (externe Prüfung)* • *Behördenaudits bei recall (externe Prüfung)* • *Versicherungsaudits bei recall (externe Prüfung)* • *recall Audits bei recall (interne Prüfung)* • *recall Audits bei Kooperationspartnern (interne Prüfung)*
• SOP-3.2.1-Betriebsordnung recall Hamburg	
• SOP-3.6.1.2-Verpflichtungserklärung Datenschutz	*Für Mitarbeiter von recall*
• SOP-3.6.1.1-Verfahrensverzeichnis gem. § 4 Abs.2 Satz 2 BDSG	
• F-9.2.3.1 - Checkliste Neueinstellung	
• MUSTER Einarbeitungsplan - Führungskraft	
• F-9.2.1.6.3. IC Spezialist_Archivar	*Stellenbeschreibung für Mitarbeiter in der Akteneinlagerung und -archivierung*
• JES_(6) Kartons in Regal einlagern	*Exakte Arbeitsanweisung Stellenbeschreibung für Mitarbeiter in der Akteneinlagerung und -archivierung*
• JES_(1) Umzug Kartons Ziehen und auf Palette Packen	*Exakte Arbeitsanweisung Stellenbeschreibung für Mitarbeiter in der Akteneinlagerung und -archivierung*
• F-6.2.2.1.15 - (blau) Unterweisungen recall Mitarbeiter	
• ISO 9001-recall Deutschland-22525-10-12	*Zertifikat*
• PCI DSS - recall Europa - vom 31.10.13	*Zertifikat*
• ISO 27001 - recall ISO Letter of Intent	

Ein Teil dieser Dokumente helfen der Daten verarbeitenden Stelle bei der Erstellung ihrer eigenen Dokumentation.

III. Zertifizierung von recall gem. DIN EN ISO 9001 : 2008

Als Ergebnis der Dokumentation wurde dem Unternehmen Recall für den Geltungsbereich „Planung und Erbringung von Dienstleistungen im Bereich Dokumentenmanagement (Datenträgerarchivierung und Datenträgervernichtung) im November 2012 bescheinigt, ein Qualitätsmanagementsystem nach DIN EN ISO 9001 : 2008 aufgebaut und in die Praxis umgesetzt zu haben, was durch ein entsprechendes Audit der ESC Cert GmbH überprüft wurde. Das Zertifikat ist bis 12. November 2015 gültig.

Darüber hinaus befindet sich das gesamte recall-Unternehmen (weltweit) derzeit in einem Prozess zur Zertifizierung gem. ISO/IEC 27001:2005, was im Juni 2013 durch das SRI in Pitsburg (USA) bestätigt wurde. Auch wenn hier noch keine abschließende Zertifizierung vorliegt, zeigt es, dass recall dem Bereich Qualitätssicherung (und somit Dokumentation und Transparenz) einen hohen Stellenweg beimisst.

IV. Zertifizierung von recall gem. Payment Card Industry (PCI[1]) Data Security Standards (DSS) – Version 2.0

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. Der Prüfzeitraum war vom 01.08.2013 bis 31.10.2013. Das Zertifikat erstreckt sich auf das gesamte Recall-Unternehmen in Europa.

V. Neuer Auftragsdatenverarbeitungsvertrag

Recall verwendet einen neuen Auftragsdatenverarbeitungsvertrag („Standardvertrag DMS“). Der Auftragsdatenverarbeitungsvertrag enthält alle nach § 11 Abs. 2 BDSG erforderlichen Angaben. Für Zwecke der Übersichtlichkeit sind die jeweiligen Anforderungen aus § 11 Abs. 2 BDSG sowie die jeweils im Vertrag zu findende Umsetzung in der anliegenden „Checkliste“ (**Anlage 1**) beigefügt.

E. Zusammenfassung

Das Akteneinlagerungsverfahren von Recall lässt sich nach wie vor als vorbildlich bewerten. Die schon bei den letzten Zertifizierungen festgestellten Maßnahmen zum Schutz der Dokumente vor der unberechtigten Kenntnisnahme Dritter wurden noch einmal verbessert und nach wie vor eingehalten.

Durch die Verbesserung des QS-Systems und die einhergehende Zertifizierung schafft das

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

Unternehmen eine größtmögliche Transparenz, da alle Prozesse entsprechend dokumentiert und nachvollziehbar sind.

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

Kellinghusen, den 30.08.2014

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

Flensburg, den 30.08.2014

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