Technisches und rechtliches
Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen durch das Verfahren zur Akteneinlagerung

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 ab@datenschutzkontor.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:
22.01.2012

Inhaltsverzeichnis

Einleitung....2
Zeitpunkt der Prüfung....2
Änderungen und Neuerungen des Produktes....2
Datenschutzrechtliche Bewertung....2
Zusammenfassung....2

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Beschreibung	Kommentar
20.08.2010	Erstellung	Version 1.0
04.05.2011	Finalisierung	
02.08.2011	Ergänzungen	Version 1.2
11.10.2011	Ergänzungen	Version 2.2
15.10.2011	Ergänzungen	Version 2.3
22.01.2011	Ergänzungen	Version 2.4

A. Einleitung

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

Die Erstzertifizierung ist am 03.08.2006 erfolgt. Ablauf der Zertifizierung war der 03.08.2008. Nach Auffassung der Sachverständigen scheint eine Rezertifizierung möglich, da sich die tatsächlichen Gegebenheiten des Verfahrens nicht verändert bzw. Verbesserungen erfolgt sind.

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 Produktes fand vom 14. März 2010 bis 10. Oktober 2011 statt.

C. Änderungen und Neuerungen des Produktes

Das Verfahren ist - wie im Gutachten von 2006 beschrieben – im Wesentlichen unverändert geblieben. Auf der Webseite von recall werden in der Produktübersicht der Archivierung verschiedene Produkte angeboten. Der Zertifizierungsgegenstand (Target of Evaluation – ToE) umfasst 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

In tatsächlicher Hinsicht hat sich seit der Erstzertifizierung jedoch eine Änderung ergeben. Die Akten werden in einem anderen Gebäude eingelagert, das auf dem Betriebsgelände von recall in Hamburg neu gebaut wurde. Es handelt sich um ein professionelles Regallager, wie sich aus dem nachfolgenden Foto ersehen lässt.

Der technische Sachverständige Andreas Bethke hat die Räumlichkeiten vor Ort in Augenschein genommen und fotografisch dokumentiert. Er hat insbesondere auch kontrolliert, dass das Gebäude durch hinreichende Maßnahmen vor dem Zutritt unberechtigter Dritter gesichert ist.

Andere Änderungen an dem Verfahren hat es nach Herstellerangabe nicht gegeben.

D. Datenschutzrechtliche Bewertung

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:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
6. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
7. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
8. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
9. 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.

Die einzelnen Anforderungen aus § 11 Abs. 2 BDSG sind im recall-Mustervertrag wie folgt umgesetzt:

1. *der Gegenstand und die Dauer des Auftrags,*

Der Gegenstand des Auftrags ist als Vertragsgegenstand in Verbindung mit einer Vertragsanlage, in der die einzelnen Leistungen von den Parteien festgelegt werden können, in § 1 des Vertrages von recall hinreichend geregelt.

Die Dauer des Auftrages ist in § 9 des Vertrages („Laufzeit“) kodifiziert.

2. *der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,*

Umfang, Art und Zweck der Datenverwendung lassen sich aus dem Gesamtkontext und einzelnen vertraglichen Regelungen gut erkennen. Dem Wesen der Akteneinlagerung entsprechend kann eine Eingrenzung der Datenarten nicht abschließend vorgenommen werden. Auch der Kreis der Betroffenen ist entsprechend nicht konkret eingrenzbar.

3. *die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,*

Die nach § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG zu treffenden Regelungen sind im Vertrag in § 6 des Vertrages allgemein für Akteneinlagerung (und Vernichtung) geregelt. § 6 des Vertrages bezieht jedoch ein Datensicherheitskonzept in den Vertrag mit ein. In diesem Datensicherheitskonzept sind die technischen und organisatorischen Maßnahmen konkreter dargelegt. Die Ausführungen sind hinreichend, um den Anforderungen des § 9 BDSG zu entsprechen. Das Datensicherheitskonzept wird als Anlage zu diesem Gutachten übermittelt.

4. *die Berichtigung, Löschung und Sperrung von Daten,*

Die Berichtigung, Löschung und Sperrung von Daten ist im Vertrag nicht ausdrücklich geregelt.

Nach § 3 verarbeitet recall die Daten jedoch ausschließlich im Rahmen der getroffenen Vereinbarung und nach *Weisungen des Auftraggebers.* Im Falle der Wahrung von Betroffenenrechten, die grundsätzlich gegenüber dem Auftraggeber geltend gemacht werden müssten, müsste der Auftraggeber Sorge dafür tragen, dass entsprechende Weisungen zur Berichtigung, Löschung oder Sperrung von Daten an den Auftragnehmer (recall) erteilt werden.

Dies kann als noch adäquat bewertet werden.

5. *die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,*

Eine entsprechende Regelung zur Zulässigkeit ist in § 3 Abs. 7 im Vertrag enthalten. Danach ist die Beauftragung von Subunternehmern zulässig. Recall wird den Unterauftragnehmer entsprechend auf die Weisungen des Auftraggebers verpflichten und den Auftraggeber vor der Beauftragung informieren. Die Anforderung ist damit in adäquater W*eise* umgesetzt.

6. *die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,*

Die Kontrollrechte sind in § 3 Abs. 5 des Vertrages von recall in hinreichender Weise geregelt. Die Anforderung ist in adäquater Weise umgesetzt.

7. *mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,*

Auch die Mitteilungspflichten sind im Mustervertrag von recall geregelt. Die Regelung ist in § 3 Abs. 4 zu finden.

8. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber

dem Auftragnehmer vorbehält,

Nach § 2 Abs. 3 des Vertrages kann der Auftraggeber Weisungen bzgl. der Datenverarbeitung an den Auftragnehmer erteilen. Damit wird klargestellt, dass auch ergänzende Weisungen des Auftraggebers außerhalb der vertraglichen Vereinbarungen möglich sind.

9. *die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.*

Eine Rückgabe überlassener Datenträger ist in § 3 Abs. 9 explizit geregelt. Die Anforderung ist im erforderlichen Umfang umgesetzt.

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

Einhalten der Anforderungen aus § 17 LDSG-SH

Neben den Anforderungen des § 11 BDSG muss bei dem Verfahren im Rahmen der Prüfung zur Rezertifizierung auch die Einhaltung der Vorgaben des § 17 LDSG-SH geprüft werden. Schließlich muss das Verfahren zum Einsatz beim öffentlichen Stellen des Landes Schleswig-Holstein geeignet sein, und maßgebliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten im Auftrag ist - für die öffentliche Stelle als Auftraggeber - § 17 LDSG-SH.

Nach § 17 LDSG-SH muss die verantwortliche datenverarbeitende Stelle Sorge dafür tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Um dies zu bewerkstelligen muss die öffentliche Stelle sicherstellen, dass die technischen und organisatorischen Maßnahmen von ihr getroffen werden und entsprechende Weisungen und Aufräge an den Auftragnehmer schriftlich erteilt werden. Dies geschieht auch im öffentlichen Bereich mittlerweile üblicherweise durch einen Auftragsdatenverarbeitungsvertrag. recall bietet seinen Kunden an, einen eigenen Auftragsdatenverarbeitungsvertrag zu verwenden, der dann von recall geprüft und entsprechend abgeschlossen werden kann. Dabei kann der Auftraggeber dann

auch entsprechende Regelungen zur Zulässigkeit von Unterauftragsverhältnissen (vgl. § 17 Abs. 2 Satz 4 LDSG-SH) treffen.

Vor der Auftragserteilung hat die öffentliche Stelle ("Auftraggeber") den Auftragnehmer unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. §§ 5, 6 LDSG-SH auszuwählen bzw. seine Eignung zu prüfen. Diese Prüfung ist nicht anders zu bewerten als die sorgfältige Auswahl i.S.d. § 11 BDSG.

Es bestehen insbesondere keine Bedenken bzgl. der Eignung von recall als Auftragnehmer einer Auftragsdatenverarbeitung nach § 17 LDSG-SH. Soweit die verantwortliche Stelle ergänzende Maßnahmen zur Einhaltung der Vorgaben der DSVO-SH an den Auftragnehmer zu erteilen hat, kann dies durch entsprechende Weisungen erfolgen.

Insgesamt ist festzustellen, dass die Vorgaben des § 17 LDSG-SH nicht wesentlich anders zu beurteilen sind als die Vorgaben des § 11 BDSG. Vielmehr sind die Anforderungen des § 11 Abs. 2 BDSG, insbesondere in der Detailtiefe, höher als die des § 17 LDSG-SH.

Es bestehen daher keine Bedenken gegen die Einhaltung der Vorgaben des § 17 LDSG bei einer Beauftragung von recall als Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung.

E. Zusammenfassung

Das Akteneinlagerungsverfahren von recall lässt sich nach wie vor als vorbildlich bewerten. Die schon bei der Erstzertifizierung festgestellten Maßnahmen zum Schutz der Dokumente vor der unberechtigten Kenntnisnahme Dritter werden nach wie vor eingehalten. Die zwischenzeitlich erfolgten gesetzlichen Änderungen sind von recall durch Anpassungen der Vertragsunterlagen berücksichtigt worden.

In tatsächlicher Hinsicht ist durch die Schaffung eines neuen Regallagers zusätzliche Sicherheit geschaffen worden.

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

Kellinghusen, den 22.01.2012

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

Flensburg, den 22.01.2012

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