Rechtliches und Technisches Gutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das IT-Produkt

- RWAS R3 -

der
REISSWOLF Deutschland GmbH
Normannenweg 28
20537 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
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

Olaf Lange
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Rahlstedter Bahnhofstr. 12
22143 Hamburg
tel 040 – 25 06 842
email info@anwalt-lange.de

Stand:
November 2015

Inhaltsverzeichnis

Änderungs- und Versionsverwaltung des Gutachtens

13.11.2013	O. Lange	Version 1.0 -Erstellung
25.11.2013	A. Bethke	Version 1.7 - Ergänzungen
01.12.2013	A. Bethke	Version 2.0 - Überarbeitung
02.12.2013	O. Lange	Version 2.1 - Kommentierung
03.12.2013	A. Bethke	Version 2.2 – Korrekturen
23.12.2013	A. Bethke	Version 2.3 – Ergänzungen
12.03.2014	O. Lange	Version 2.4 – Überarbeitung nach GS-Bericht
17.03.2014	A. Bethke	Version 2.5 – Ergänzungen
30.08.2014	A. Bethke	Version 2.6 – Ergänzungen
01.05.2015	A. Bethke	Version 2.7 – Überarbeitung nach neuer Dokumentation
31.05.2015	A. Bethke	Version 2.8 – Ergänzungen
10.06.2015	O. Lange	Version 2.9 – Korrekturen
12.08.2015	O. Lange	Version 2.10 – Überarbeitung
09.11.2015	A. Bethke	Version 2.11 - Ergänzungen

A. Einleitung

Mit dem vorliegenden Gutachten beabsichtigt die Firma REISSWOLF Deutschland GmbH, Normannenweg 28, 20537 Hamburg (nachfolgend REISSWOLF bezeichnet) ihr IT-Produkt „RWAS R2“ rezertifizieren zu lassen.

„RWAS R2“ ist eine Software zur Unterstützung der Prozesse in Aktenarchiven. Die Software dient der Lagerverwaltung, die speziell auf die Bedürfnisse der Akteneinlagerung in einem strukturierten Lagerbetrieb abgestimmt ist. Die Archivierungssoftware „RWAS R2“ wird sowohl von der verantwortlichen Stelle als auch der Firma REISSWOLF Deutschland GmbH genutzt.

Die Software besteht im Kern aus den beiden Modulen „RWASintern“ und „RWASonline“, wobei beide Module auf die gleiche Datenbank zugreifen. Weiterhin gehören die Funktionen von „RWASoffice“, einer optionalen Erweiterung von „RWASonline“, zur Begutachtung.
„RWASintern“ ist ein Programm für Mitarbeiter der Daten verarbeitenden Stelle zur Steuerung, Ausführung und Administration des Archivgeschäfts.

„RWASonline“ ist eine Webapp für Kunden (der Daten verarbeitenden Stelle) zum Zugriff auf Ihre ausgelagerten Dokumente. Beauftragung, Suche, Selbstverwaltung,

„RWASoffice“ ist ein Zusatzmodul von „RWASonline“, welches den Kunden befähigt, neue Dokumente schon vor der Archivierung anzulegen und zu verwalten, inkl. Etikettendruck für Order und Kartons

„RWASoffice“ ist kein eigenständiges Produkt. Es erweitert lediglich die Funktion von „RWASonline“. „RWASonline“ kann nicht ohne „RWASintern“ betrieben werden, da die Einrichtung von Archiven und Beständen nur über das „RWASintern“ geschehen kann. Die Gesamtlösung wird nachfolgend nur „RWAS“ genannt.

Von den Gutachtern wurden neben der Software auch die vorhandenen Dokumentationen geprüft und im Gutachten bewertet.

Die Software wurde in der Praxis im Einsatzumfeld in den Archivbetrieben von REISSWOLF untersucht. Das Einsatzumfeld ist nicht Gegenstand der Begutachtung.

Vom Zertifizierungsgegenstand ausgenommen sind somit die Implementierung und sämtliche technische und organisatorische Maßnahmen im Wirkbetrieb der Software, weil die Software verschiedene Lösungen anbietet. Aus diesem Grunde wurde auch die Hostinglösung im Produktivbetrieb in diesem Rezertifizierungsgutachten, wie auch im Erstgutachten, nicht evaluiert.

Die Firma REISSWOLF möchte mit diesem Rezertifizierungsgutachten den Nachweis führen, dass das Produkt mit den Änderungen und Neuerungen, die seit der Erteilung des Gütesiegels vom 01.11.2011 gemacht worden sind, nach wie vor die datenschutzrechtlichen Anforderungen erfüllt

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 31.10.2013 – 09.11.2015 statt.

C. Änderungen und Neuerungen des Produktes

Seit der Rezertifizierung wurden folgende Änderungen an der Software vorgenommen, die den Datenschutz und damit das Gütesiegel betreffen.

1. Scanfunktion

Die Prüfungen haben ergeben, dass die Scanfunktion die einzige technische Neuerung bzw. Veränderung seit der Erteilung des IT-Gütesiegels ist. Im Rahmen der Scanfunktion werden die Akteninhalte dem Nutzer digital übermittelt.

Aufgrund des RWAS Scan-On-Demand können im Gegensatz zu der klassischen Zustellung die Zugriffszeit und die Kosten gesenkt werden, da kein physischer Transport geplant und durchgeführt werden muss, sondern die Akten oder Teile davon direkt im Archiv eingescannt und elektronisch übermittelt werden können. Dieses Verfahren eignet sich nur, wenn die Vorlage des Originaldokuments nicht erforderlich ist und die zu scannenden Dokumente in Umfang und Beschaffenheit für eine Digitalisierung geeignet sind.

Mit der Scanfunktion können Dokumente als PDF 1.3 mit binarisierten Bildern (TIFF CCITT.6) von 200dpi pro Seite erstellt werden. Eine übliche Seite ist somit durchschnittlich 60 KByte groß. Ein Dokument von 100 DinA4-Seiten wird im Standardformat durchschnittlich 5,86 MByte aufweisen. Mit einem Upstream von 1 MBit/s ergibt sich eine Uploadzeit von 50 Sekunden.

Für die Digitalisierung wird als Mindestvoraussetzung ein PC mit der aktuellsten Version von RWASintern und ein TWAIN-kompatibler Dokumentenscanner benötigt.

Die Scans können elektronisch vom Archiv an den Nutzer übermittelt und lokal auf der Festplatte des Nutzers gespeichert werden.

RWAS ermöglicht die Umsetzung eines Zugriffs- und Rollenkonzeptes, so dass nur die Nutzer Zugang zu den digitalisierten Inhalten erlangen, die auch dazu berechtigt sind. Darüber hinaus wird jeder Download unter Angabe des Benutzernamens und des Zugriffsdatums protokolliert.

Im Praxiseinsatz wird der Nutzer nach einer erfolgten Digitalisierung per E-Mail benachrichtigt. Aus Klarstellungsgründen sei erwähnt, dass die gescannten Dokumente nicht per Email sondern mittels verschlüsselter Datenleitung übermittelt werden. Die digitalisierten Inhalte verbleiben im aktuellen Betrieb der Software für eine Frist von sieben Tagen auf den entsprechenden Servern, bevor sie automatisch gelöscht werden. Der Nutzer kann ausschließlich innerhalb dieser Frist die digitalisierten Dokumente als PDF herunterladen und dann beliebig lange verwenden, da die PDF anschließend gelöscht werden und kein Zugriff mehr möglich ist Vor dem Hintergrund, dass nicht der Produktivbetrieb zum Zertifizierungsgegenstand gehört, wird lediglich darauf hingewiesen, dass die Bereitstellung der PDF skalierbar ist.

Im Hinblick auf eine datenschutzfreundliche Verarbeitung der Scans wurde vom Hersteller die vorgenannte Löschfunktion implementiert. Zur Datenvermeidung und Datensparsamkeit ist die Vorhaltezeit der Dokumente auf den RWASServern zeitlich begrenzt, denn nach einer Vorhaltezeit von 7 Tagen wird das gescannte Dokument gelöscht. Es obliegt dem Nutzer, rechtzeitig die Daten herunterzuladen. Versäumt er dies, muss der Scan-On-Demand-Auftrag komplett wiederholt werden. Die Daten werden 7 Tage lang in der Datenbank vorgehalten und dann unwiederbringlich per DELETE-Befehl aus der Datenbank direkt gelöscht. Als Lösch-Kriterium ist das Ablaufdatum ausschlaggebend. Die Protokoll-

daten werden mit den Scandaten zusammen nach 7 Tagen gelöscht.

„Scan-on-Demand“-Daten werden aus Datenschutzgründen nicht per Backup gesichert um das Ablaufdatum gewährleisten zu können.

Im Sinne der Revisionssicherheit werden die Scan-Verarbeitungen mit dem Nutzernamen und dem Datum protokolliert. Das Protokoll wird ebenfalls nach 7 Tagen gelöscht.

2. Passwörter

Die Mindestpasswortlänge für das RWAS ist mittlerweile auf 10 Zeichen angehoben worden. Weiterhin wurden folgende Anpassungen vorgenommen:

Für eine Zugriffsberechtigung muss im Administrationsteil der Software ein Benutzer angelegt werden. Hierzu wird der Benutzername und eine Benutzerkennung erfasst. Die Kennung kann man sich vom System vorschlagen lassen. Als Algorithmus wird "Anfangsbuchstabe des Vornamen und Nachname" benutzt. Bei der ersten Anmeldung muss der Benutzer immer manuell ein eigenes Passwort vergeben. Für diese erste Anmeldung wird ein temporäres Passwort automatisch erzeugt.
Gleiches gilt für Passwörter, die durch einen Administrator für bestehende Benutzer definiert werden. Dies gilt ebenfalls nur für die nächste Anmeldung und ist nicht darüber hinaus nutzbar.

Im Falle eines vergessenen Passwortes, hat der Benutzer die Möglichkeit auf der Anmeldemaske von RWASonline „Passwort vergessen“ zu wählen und mittels seiner E-Mail-Adresse ein neues Passwort anzufordern. Dann erhält er eine automatisch generierte E-Mail an die im System hinterlegte Adresse mit einem Link, der 24 Stunden gültig ist. Nachdem der Benutzer auf den Link geklickt hat (dahinter verbirgt sich eine SSL-verschlüsselte rwas.de-Website), hat er nun die einmalige Möglichkeit ein neues Passwort festzulegen. Bricht der Benutzer den Vorgang ab oder versäumt es, den Vorgang innerhalb von 24h zu ende zu führen, so muss er erneut beginnen. Der Link wird auch ungültig, wenn sich der Nutzer innerhalb der Frist von 24 Stunden mit dem alten Passwort anmeldet, etwa weil das Passwort dem Nutzer wieder eingefallen ist. Zur Sicherheit kann der Link immer nur an die im System hinterlegte Email-Adresse geschickt werden. Die Änderung der Emailadresse im Zusammenhang mit der Passwortgenerierung ist nicht möglich. Während der Nutzer alleine über sein Passwort bestimmen kann und die alleinige Kenntnis hat, werden die Passwörter entsprechend des Rollenkonzeptes von einer anderen Person der IT-Abteilung vergeben, so dass Doppel- und Fremd-Domainvergaben ausscheiden. Die Passwort-Vergessen-Funktion kann beliebig oft wiederholt werden.

3. Dokumentation

Während des Zeitraums der Begutachtung wurde die Dokumentation für das Produkt komplett überarbeitet und neu erstellt. So gibt es nunmehr nur noch 2 Dokumente:

1. „RWASonline Benutzerhandbuch“, Version 86 vom 09.11.2015,
2. „RWASintern 3“, Revision 154 vom 23.07.2015

In diesen Dokumenten sind alle bisher existierten zusammengefasst worden.

Die bestehende Dokumentation wurde durch ausführliche Datenschutzhinweise zur Förderung eines vorbildlichen datenschutzgerechten Einsatzes ergänzt. In beiden Dokumenten findet sicht dies gleich am Anfang im jeweiligen Kapitel 1. Im Folgenden

tauchen immer wieder Datenschutzhinweise auf. Im Handbuch „RWASintern 3“ finden sich weiterhin ergänzende Hinweise im Kapitel 30.6.1 „Risikomanangement und Datenschutz“ auf Seite 156. Zudem werden auf Seite 8 im Handbuch „RWASintern 3“ auch spezielle Datenschutzhinweise für Berufsgruppen, die einer gesetzlichen Schweigepflicht unterliegen (Kapitel 1.2 Schweigepflicht) erteilt. Generell wird bereits bei der Datenerfassung auf die Datenvermeidung und Datensparsamkeit geachtet und die Vermeidung von personenbezogenen Daten im Rahmen der Aktenverwaltung empfohlen („RWASintern 3“, Kapitel 6.1.3 Erfassungsmaske, Seite 42). Gleiches gilt für die Einrichtung der Benutzerkennung („RWASintern 3“, Kapitel 14 Benutzer, Seite 101). Auch im Rahmen der Implementierung der kundenspezifischen Felder („RWASintern 3“, Kapitel 19.4 Kundenspezifische Felder, Seite 132) wird die Vermeidung von personenbezogenen Daten empfohlen. Ferner werden im Kapitel 22 „Sachbearbeiter“ (Seite 129 und 130) Hinweise für eine datenschutzfreundliche Einrichtung der Onlinezugänge für Mitarbeiter gegeben. An verschiedenen Stellen im Handbuch werden weitere Hinweise zum datenschutzfreundlichen Einsatz der Software bereit gestellt.

In dem Handbuch „RWASonline 3“ werden ebenfalls zahlreiche Hinweise zum datenschutzfreundlichen Einsatz des Zertifizierungsgegenstandes gegeben. Im Kapitel 1.2 Datenschutzhinweis werden ausführliche Anleitungen zum Einsatz des Tools aufgezeigt. Wie schon im anderen Handbuch werden im Kapitel 1.3 Hinweise zur gesetzlichen Schweigepflicht erteilt. Zur Förderung des Datenschutzes durch die Benutzerverwaltung, insbesondere bezüglich des „need to know Principle“, werde dort im Kapitel 4.15 Benutzerverwaltung (Seite 69) Hinweise gegeben. Auch zur Passwortsicherheit werden im Kapitel 4.15.2 entsprechende Hinweise unter Bezugnahme auf die Empfehlungen des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein abgedruckt. Im Kapitel 4.16 „RWASoffice“ auf Seite 82 finden sich weitere Datenschutzhinweise, etwa zur Verwendung von anonymen IDs. Somit werden den verantwortlichen Stellen vielfältige Datenschutzhinweise in den Dokumentationen gegeben, um den Zertifizierungsgegenstand datenschutzfreundlich einzusetzen.

Weitergehend wird auch auf das Thema „Löschfristen“ beim „Scan-on-demand“ eingegangen. Um Kapazitäten zu schonen und datenschutzrechtliche Angriffsfläche zu minimieren, ist die Vorhaltezeit der Dokumente auf den RWAS-Servern zeitlich eng begrenzt. Nach einer Vorhaltezeit von 7 Tagen wird das Dokument gelöscht. Es obliegt dem Benutzer die Daten rechtzeitig herunterzuladen. Versäumt er dies, muss der Scan-On-Demand-Auftrag komplett wiederholt werden. Hierauf wird der Benutzer eindringlich hingewiesen.

An anderer Stelle wird dies mit dem Begriff „Vorhaltefrist“ der Daten noch einmal aufgegriffen. Weiterhin wird der Arbeitsablauf beschrieben, in dem das digitalisierte Dokument aus der Datenbank automatisch entfernt und gelöscht wird. Gleichzeitig wird ein Historieneintrag zur Löschung erstellt.

Für die Scan-On-Demand – Administration wurde die Dokumentation ebenfalls angepasst. So werden dort Benutzerinstruktionen und datenschutzrechtliche Hinweise für den Administrator gegeben, um die organisatorischen Maßnahmen für einen datenschutzfreundlichen Einsatz zu fördern. So wird der Anwender/Administrator für das Speichern von Dokumenteninhalten sensibilisiert.

Gleiches gilt für die Weiterleitung/Übertragung von Inhalten, die nicht außerhalb von RWAS verschickt werden sollten.
Weiterhin wird die Daten verarbeitende Stelle angehalten ihre Mitarbeiter im sicheren Umgang mit Daten im Sinne des Datenschutzgesetzes zu schulen.
Darüber hinaus wird der Daten verarbeitenden Stelle die verdeutlicht, dass sie die Verantwortung für eine sichere Betriebsumgebung der Scan-Arbeitsplätze trägt. Da auf den Festplatten der Arbeitsplätze die gescannten Unterlagen vorgehalten werden, müssen die Maschinen vor unbefugten Dateisystemzugriffen geschützt werden. Im Weiteren werden der Daten verarbeitenden Stelle technische Maßnahmen an die Hand gegeben um diese Forderung durchsetzen zu können.

Durch die Aktualisierung der vorhandenen Dokumentation wird von REISSWOLF der Nachweis erbracht, dass der Datenschutz nachhaltig durch den Einsatz von RWAS gefördert werden soll.

D. Datenschutzrechtliche Bewertung

1. Scanfunktion

a) Nach §5 LDSG (78a SGB-X oder §9 BDSG) wird vom Gesetzgeber gefordert, dass Maßnahmen von der verantwortlichen Stelle ergriffen werden, um Unbefugten den Zugang zu Datenträgern zu verwehren (§ 5 Abs. 1 Nr. 1 LDSG). Zu evaluieren ist deshalb, ob die erforderlichen technischen und organisatorischen Maßnahmen getroffen wurden, um eine Verwaltung von Akten und Funktionsträgerdaten im Auftrag sicher zu stellen. Hierzu bietet die Firma REISSWOLF Deutschland GmbH gem. § 5 Abs. 1 LDSG ein technisches und organisatorisches Verfahren an, das die Sorgfaltsanforderungen erfüllt. Da REISSWOLF nur das Produkt, nicht jedoch die Einsatzumgebung zur Verfügung stellt, obliegt die Verantwortung für die Einsatzumgebung und insbesondere der technischen und organisatorischen Maßnahmen der einsetzenden Stelle. Die Integrität wird durch die Software gewährleistet. Die Vertraulichkeit wird durch ein Zugriffskonzept gewährleistet. Die Transparenz wird durch die umfangreiche Dokumentation gewährleistet. Die Nicht-Verkettbarkeit ist durch den beschränkten Einsatz der Software gegeben: Personenbezogene Daten (Nutzerdaten) werden auf ein Minimum reduziert. Eine Intervenierbarkeit ist somit ebenfalls gegeben.

RWAS R3 ermöglicht auch für den Einsatz der Scanfunktion die Umsetzung eines Zugriffs- und Rollenkonzeptes, so dass nur die Nutzer Zugang zu den digitalisierten Inhalten erlangen, die auch dazu berechtigt sind. Ausgenommen hiervon sind jedoch die Mitarbeiter des Archivbetreibers, die im Praxisbetrieb die Papierdokumente scannen und ein PDF erzeugen müssen. Es obliegt der Daten verarbeitenden Stelle auf die Einhaltung der datenschutzrechtlichen Zulässigkeit zu achten.

Sofern es sich um besondere personenbezogene Daten handelt, die einer gesetzlichen Schweigepflicht unterfallen, ist nur der physikalische Aktenversand und nicht die Nutzung der Scanfunktion gestattet, sofern das Archiv nicht von der Daten verarbeitenden Stelle selbst mit eigenen Mitarbeitern betrieben wird oder Einwilligungserklärungen der Betroffenen vorliegen (vgl. Kapitel 1.2 Schweigepflicht, Seite 8 im Handbuch „RWASintern 3“ bzgl. spezieller Datenschutzhinweise für Berufsgruppen, die einer gesetzlichen Schweigepflicht unterliegen).

b) Protokollierung von Datenverarbeitungsvorgängen (§§ 5 Abs. 1 Nr. 3,6 Abs. 4, 8 Abs. 3, 5 LDSG, § 10 Abs. 4 BDSG, § 79 Abs. 4 SGB-X)

Im Sinne der Revisionssicherheit werden die Scan-Verarbeitungen mit dem Nutzernamen und dem Datum protokolliert. Protokolldaten werden gemeinsam mit dem Datensatz auf den sie sich beziehen gelöscht. Somit ist die Protokollierung der Datenverarbeitungsvorgänge gesetzeskonform.

c) Weitere technische und organisatorische Maßnahmen (§5 Abs. 1 Satz 1 LDSG)

In der Dokumentation „RWASintern 3“ werden im Kapitel 30.6.1 „Risikomanagement und Datenschutz“ zahlreiche Hinweise für technische und organisatorische Maßnahmen gegeben, um den Betrieb des IT-Produktes datenschutzfreundlicher auszugestalten. Vor dem Hintergrund, dass nur das IT-Produkt selber der Zertifizierungsgegenstand ist, ist festzustellen, dass der datenschutzgerechte Einsatz von RWAS auch nach der Implementierung von der Scanfunktion möglich ist.

d) Erleichterung der Vorabkontrolle (§9 LDSG)

Aufgrund der umfassenden und transparenten Dokumentationslage ist eine datenschutzrechtliche Vorabkontrolle möglich. Die einzelnen Funktionen des Tools und die damit verbundene Datenverarbeitung sind somit leichter zu beschreiben und zu bewerten.

e) Erleichterung der Erstellung eines Verfahrensverzeichnisses (§7 LDSG)

Aufgrund der umfassenden und transparenten Dokumentation ist auch ein Verfahrensverzeichnis relativ einfach zu erstellen.

f) Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens (§ 2 abs. 2 Nr. 7 LDSG)

Aufgrund der Möglichkeit sowohl die Nutzername als auch die Aktenbezeichnungen zu pseudonymisieren, ist das IT-Produkt besonders datenschutzfreundlich.

g) Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz

Die Nutzer des IT-Produktes sind „Herr des Verfahrens“, da die Sachbearbeiter selbst die Datenverarbeitung beauftragen und steuern. Für die Scanfunktion wird von den Betroffenen des Akteninhaltes nach den empfohlenen Vorgaben von RWAS eine Einwilligung eingeholt. Die verantwortliche Stelle behält auch in diesem Fall die Umsetzungs- und Steuerungsfunktion. Aufgrund der von RWAS empfohlenen Einwilligung des Betroffenen ist eine Beteiligung gegeben.

h) Aufklärung und Benachrichtigung (§ 26 LDSG, vgl. § 33 BDSG)

In der Dokumentation zu RWAS wird die Einholung der Einwilligung beim Betroffenen bezüglich der Datenverarbeitung im Auftrag mittels Scanfunktion empfohlen. Im Übrigen werden die Akten ausschließlich von der verantwortlichen Stelle bearbeitet, , so dass eine Datenverarbeitung der Akteninhalte und der darin enthaltenen personenbezogenen Daten mittels RWAS nicht durchgeführt wird. Ausgenommen hiervon ist der Einsatz der Scanfunktion, wenn die Akteninhalte im Wege der Auftragsdatenverarbeitung gescannt werden. Der Zertifizierungsgegenstand kann jedoch auch für eigene Archive der verantwortlichen Stelle eingesetzt werden, so dass eine Auftragsdatenverarbeitung nicht die

Voraussetzung für den Einsatz des Zertifizierungsgegenstandes ist.

i) Auskunft (§ 27 LDSG, §§ 25, 83 SGB X, § 34 BDSG, Art. 12 EU-DSRL) Untersuchungsgegenstand:

Auskunft an Betroffene kann mittels der Scanfunktion schneller gewährleistet werden als per physischen Transport. Im Übrigen ist der RWASKunde für Auskünfte zuständig.

j) Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung (§§ 28, 29 LDSG, § 84 SGB X, § 35 BDSG)

Im Handbuch „RWASintern 3“ Kapitel 30.6.2 Ablauffristen ist beschrieben, dass die Ablauffrist für Dokumenteninhalte einen Standardwert von 7 Kalendertagen hat. Die Scans werden, wie in Kapitel 30.6.3 „Datensicherung“ aufgeführt nicht gesichert. Falls die Daten z.B. durch einen nicht fristgemäßen Abruf oder Serverabstürze verloren gehen, so müssen die Daten manuell wiederhergestellt werden. In Kapitel 30.6.5 „Technische Hinweise zur Ablauffrist der Dateien“ ist ferner zum Praxiseinsatz erläutert, dass um Kapazitäten zu schonen und datenschutzrechtliche Angriffsfläche zu minimieren, die Vorhaltezeit der Dokumente auf den RWASServern zeitlich eng begrenzt wird. Nach einer Vorhaltezeit von 7 Tagen wird das PDF-Dokument gelöscht. Es obliegt dem Kunden, rechtzeitig die Daten herunterzuladen. Versäumt er dies, muss der Scan-On-Demand-Auftrag komplett wiederholt werden. Die Daten werden 7 Tage lang in der Datenbank vorgehalten und dann unwiederbringlich per DELETE-Befehl aus der Datenbank direkt gelöscht. Als Lösch-Kriterium ist das Ablaufdatum ausschlaggebend. Nach alledem ist im Zertifizierungsgegenstand eine Löschfunktion im Sinne der vorstehenden Vorschriften implementiert. Die Funktionen zur Berichtigung, Sperrung, Einwand bzw. Widerspruch und Gegendarstellung sind nicht einschlägig, da durch die Scanfunktion des IT-Produktes keine inhaltliche Veränderung des Akteninhaltes vorgenommen werden soll. Die Bearbeitung der Akte ist bewusst der verantwortlichen Stelle, wie z.B. einer Behörde des Landes Schleswig-Holstein vorbehalten. Durch die implementierte Löschroutine ist das IT-Produkt datenschutzfreundlich.

2. Dokumentation

Die Einführung der neuen Scanfunktion wird durch die Erweiterung der Dokumentation ausführlich berücksichtigt. In der neuen Dokumentation sind verschiedene Datenschutzhinweise enthalten. Die Datenschutzhinweise betreffen sowohl die technischen als auch die organisatorischen Maßnahmen.

Die Dokumentation unterstützt den datenschutzfreundlichen Einsatz des IT-Produktes.

3. Allgemeine Bewertung

Es handelt sich um eine Software zur Archivierung und Verwaltung von Akten im Sinne des § 1 Abs. 2 DSAVO, die Archivierung von Datenträger ist der Zweck der Archivierungssoftware. Im Rahmen der Archivierung und der Verwaltung von Akten werden nur personenbezogene Daten im Sinne des § 2 Abs. 2 LDSG verarbeitet Es wird an verschiedenen Stellen in den Dokumentationen empfohlen, die Verwendung von personenbezogenen Daten zu vermeiden und sparsam mit diesen umzugehen. Der Zertifizierungsgegenstand bietet hierzu auch Möglichkeiten, wie die Verwendung von Pseudonymen im Rahmen

von Nutzeraccounts. Auch können die Akten mit anonymen Barcodes gekennzeichnet und verwaltet werden. Klarnamen als personenbezogene Daten werden grundsätzlich nur verarbeitet, wenn etwa der Benutzername des Sachbearbeiters, die Firmen-E-Mailadresse und sonstige berufliche personenbezogene Daten der Sachbearbeiter (Funktionsträgerdaten) für die Nutzung des Archivierungsprogrammes von der verantwortlichen Stelle entgegen der Empfehlung des Herstellers verwendet werden, denn die Angabe der Emailadresse, Telefon- und Faxnummer von Sachbearbeitern ist optional. Somit ermöglicht das IT-Produkt bis auf die Verwendung von Funktionsträgerdaten oder Pseudonymen eine vollständige Datenvermeidung bzw. Datensparsamkeit im Sinne des Schleswig-Holsteinischen Datenschutzgesetzes.

Ausgenommen von dem vorstehenden sehr datenschutzfreundlichen Einsatz ist die Scanfunktion, da in diesem Fall die Mitarbeiter des Archivbetriebs mit dem Akteninhalt in Berührung kommen. In den Fällen, in denen die verantwortliche Stelle im Eigenbetrieb der Archivbetreiber und Softwarenutzer ist, ist mangels einer Auftragsdatenverarbeitung ein rechtskonformer Einsatz ohne zusätzliche Einwilligung des Betroffenen möglich In anderen Fällen obliegt die Entscheidung über die Nutzung der Scanfunktion jedoch der verantwortlichen Stelle, da die Kenntnisnahmemöglichkeit der personenbezogenen Daten des Akteninhalts von den datenschutzrechtlichen Vorschriften und ggf. der Einwilligung der Betroffenen abhängt. Aus diesem Grunde werden in der Dokumentation an verschiedenen Stellen Hinweise zur Einholung von Einwilligungen gegeben.

Die Verwaltung des Aktenbestandes Dritter ist ohne eine Rechtezuweisung der aktenverwaltenden Stelle, einschließlich der Passwörter, nicht möglich.

Das Produkt stellt vier grundsätzliche Berechtigungen (Zugriffsrechte) zur Verfügung: Akten einsehen, Akten anlegen, Akten bestellen, Akten zur Vernichtung freigeben. Dabei beinhalten die höheren Rechte jeweils die darunter eingestuften Rechte.
Diese Berechtigungen können auf einen Bestand angewendet werden. Eine oder mehrere Zuweisungen von Berechtigungen zu einem Bestand können wiederum ein einer Benutzergruppe zusammengefasst werden. Ein oder mehrere Benutzer können dann einer Gruppe zugeordnet werden.
Das Passwort eines Benutzers muss mindestens zehnstellig sein.

Die Regelungen für die Passwortvergabe sind vorbildlich umgesetzt.

Folglich ist es für die verantwortliche Stelle möglich, die datenschutzrechtlichen Bestimmungen in vorbildlicher Weise zu erfüllen.

E. Zusammenfassung

Zusammenfassend kann das IT-Produkt als vorbildlich umgesetzt bewertet werden. Im Sinne der Anwenderfreundlichkeit hat die Firma REISSWOLF eine positive Änderung an dem Verfahren vorgenommen. Durch die Einführung der Scanfunktion können physikalische Aktentransporte entfallen, so dass das IT-Produkt eine schnellere und umweltfreundliche Nutzung der archivierten Akten ermöglicht. Im Rahmen der Evaluierung wurde das Archivierungsprogramm „RWAS R3“ zur Akteneinlagerung mittels der maßgeblichen Rechtsvorschriften, wie unter anderem §§ 3, 5, 6b, 9, 11, 33 BDSG, §§ 183 ff. und 196 ff. LVwG, §§ 84 ff. SGB-X und §§ 4, 17, 20 LDSG überprüft, ohne dass es zu einer Beanstandung gekommen ist.

Falls das Produkt (wie im Prüfumfeld) in den Archiven von REISSWOLF eingesetzt werden sollte, so ist im Hinblick auf die Kenntnisnahmemöglichkeit eines Mitarbeiters von REISSWOLF vom Akteninhalt und damit auch von personenbezogenen Daten im Rahmen des Aktenscans jedoch zu beachten, dass die verantwortlichen Stellen hierüber zu informieren und auf gesetzliche Verbote hinzuweisen sind.

Dem entsprechend ist die neue Scanfunktion von der verantwortlichen Stelle zu beurteilen. Vor dem Hintergrund, dass diese Funktion optional ist, ist ggf. auf diese Funktion zu verzichten.

Es bestehen somit keine Bedenken gegen den Einsatz des IT-Produktes in den die Behörden des Landes Schleswig-Holstein oder eine Rezertifizierung des Verfahrens.

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

Kellinghusen, den 09.11.2015

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

Hamburg, den 09.11.2015

Olaf Lange
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)