Kurzgutachten zur Zertifizierung des Verfahrens „Datenträgervernichtung der Firma Rhenus Data Office GmbH“

nach DSGSVO Schleswig-Holstein

(Datenschutz-Prüfsiegel)

Version: 10.2

Stand: 02.11.2016

Status: Freigegeben

Verantwortlich: Mission 100 e.V.

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck der Begutachtung

Die Begutachtung von Produkten im Datenschutzumfeld ist in einigen Datenschutzgesetzen (u.a. Bundesdatenschutzgesetz / BDSG, Landesdatenschutzgesetz Bremen) zwar aufgenommen worden, eine komplette Konkretisierung in Gestalt von Verordnungen oder Durchführungsgesetzen ist bislang aber erst in Schleswig-Holstein und Bremen erfolgt.

Rechtsgrundlage der Gütesiegelvergabe in Schleswig-Holstein ist § 4 Absatz 2 des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG-SH), der von öffentlichen Stellen des Landes Schleswig-Holstein fordert, dass vorrangig solche Produkte zum Einsatz kommen sollen, die mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar sind.

Mit Satz 2 des § 4 Abs. 2 ist die Voraussetzung zum Erlass einer Landesverordnung geschaffen worden. Mit der Landesverordnung über ein Datenschutzgütesiegel (DSGSVO) wurde hiervon Gebrauch gemacht. Die DSGSVO regelt die Einzelheiten und Anforderungen an die Vergabe von Datenschutz-Gütesiegeln. Diese Regelungen sind die Grundlage dieses Gutachtens.

Aufgrund der Vergleichbarkeit der landes- und bundesgesetzlichen Regelungen lassen sich die zur Erlangung des Datenschutz-Gütesiegels erforderlichen Eckwerte auch auf andere Bereiche übertragen, so auch auf den im BDSG geregelten nicht-öffentlichen Bereich.

Gleichwohl muss das zu zertifizierende Produkt auch und gerade wegen der landesgesetzlichen Regelung insbesondere im öffentlichen Bereich, potentiell zur Nutzung durch öffentliche Stelle geeignet sein. In diesem Sinne reicht für eine Produkteignung aus, dass eine öffentliche Stelle das auditierte Verfahren selbst nutzen könnte.

Entsprechend § 1 Abs. 2 der DSGSVO sind IT-Produkte im Sinne der Verordnung Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind.

Mit dem zur Begutachtung vorliegenden Produkt „Datenträgervernichtung (DV)“ können Kunden der Rhenus Data Office GmbH Datenträger mit personenbezogenem Inhalt vernichten lassen.

Im vorliegenden Gutachten wird geprüft, inwieweit das Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit gerecht wird.

1.2 Gegenstand der Begutachtung

Gegenstand der Begutachtung ist das Produkt „Datenträgervernichtung (DV)“ der Rhenus Data Office GmbH. Die Datenträgervernichtung umfasst

- Sammeln der Datenträger in verschlossenen Containern beim Kunden
- Mobile Datenträgervernichtung:
  - Vernichtung der Datenträger an Standorten des Kunden
- Stationäre Datenträgervernichtung
  - Transport in verschlossenen Containern zur Vernichtungsanlage o d e r
  - Transport in geschlossenen Shuttle-Fahrzeugen o d e r
  - Selbstanlieferung der Datenträger durch Kunden
  - Vernichtung der Datenträger
- Entsorgung des Restmaterials

Siehe hierzu auch Kapitel **Error! Reference source not found.** „**Error! Reference source not found.**“.

„Datenträger“ heißt in diesem Fall in der Notation der Norm DIN 66399 „Materialtyp P - Informationsdarstellung in Originalgröße (Papier, Film, Druckformen, …)“, kurz „Akten“.

1.3 Art der Begutachtung

Es handelt sich um eine Prüfung im Rahmen einer Rezertifizierung.

Das Verfahren ist vom ULD unter der Nummer 04-08/2009 zertifiziert worden, erstmals am 21.8.2009 und zuletzt am 11.9.2014.

2 Teil I: Allgemeiner Teil

entsprechend Vorgabe „Prüfschema des Gutachtens für die Produktzertifizierung“ / V 2.0 vom 17.06.2015; siehe **Error! Reference source not found.**.

2.1 Zeitpunkt der Prüfung

August 2016	Erstmalige Begutachtung der „Mobilen Aktenvernichtung“ nach den Vorschriften des Datenschutz Gütesiegels
Ratingen, 1.6.2016	Vor-Ort-Begutachtung Entsorgungsstandort Ratingen
Hamburg, 10.6.2016	Vor-Ort-Begutachtung Entsorgungsstandort Hamburg
Wunstorf, 9.8.2016	Vor-Ort-Begutachtung Entsorgungsstandort Wunstorf
Leipzig, 11.8.2016	Vor-Ort-Begutachtung Entsorgungsstandort Leipzig
Nottuln, 12.8.2016	Begutachtung der zentralen Verfahren Begutachtung der Verfahrensdokumentation
München, 19.8.2016	Vor-Ort-Begutachtung Entsorgungsstandort München Begutachtung der „Mobilen Aktenvernichtung“

2.2 Adressen der Antragsteller

Firma:	Rhenus Data Office GmbH
Ansprechpartner:	Gerhard Friederici
Adresse:	Industriestr. 5 48301 Nottuln
Telefon:	+49 2509 89 63
E-Mail:	gerhard.friederici@de.rhenus.com

Rhenus bietet seine Dienste auch unter dem Namen seiner 100%-Tochter Datenmühle GmbH an. Datenmühle nutzt den Rhenus-Standorte in München und die gleichen Systeme und Verfahren, u.a. einen baugleichen Mobilen Aktenvernichter (MAV). Rhenus und Datenmühle haben die gleiche Geschäftsführung und stehen am Markt nicht im Wettbewerb miteinander. Sie können als zwei Marken eines Unternehmens verstanden werden.

Firma:	Datenmühle GmbH
Ansprechpartner:	wie vor
Adresse:	Rupert-Bodner-Str. 5 81245 München

2.3 Adressen der Sachverständigen

Prüfstelle:

Firma:	Mission 100 e.V.
Ansprechpartner:	Michael J. Erner
Adresse:	Gartenäckerstr. 13 86825 Bad Wörishofen
Telefon:	+49 8247 99 88 780
E-Mail:	info@mission100.org

131

Rechtliches Gutachtern:	**Gutachter**	**Leiter der Prüfstelle**
Firma:	Mission 100 e.V.	dto.
Name:	Michael J. Erner	
Adresse:	Gartenäckerstr. 13 86825 Bad Wörishofen	
Telefon:	+49 (0) 172 451 05 04	
E-Mail:	me@mission100.org	

132

Technisches Gutachten:	**Gutachterin**	**Leiter der Prüfstelle**
Firma:	Mission 100 e.V.	dto.
Name:	Friedrich Abraham	
Adresse:	Auf den Dreien 52 50354 Hürth	
Telefon:	+49 (0) 172 98 24 009	
E-Mail:	fa@mission100.org	

133

134 2.4 Kurzbezeichnung des IT-Produktes

135 Das Produkt „Datenträgervernichtung (DV)“ der Firma Rhenus Data Office GmbH, nachfolgend kurz
136 „Rhenus“, dient der Datenträgervernichtung durch Löschung im Sinne des § 2 Abs. 2 Ziffer 5 des
137 Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG) und
138 § 3 Abs. 4 Ziffer 5 des Bundesdatenschutzgesetzes (BDSG). Das Verfahren erfüllt die Anforderungen
139 an einen sicheren Löschungsprozess von Datenträgern. Das Gutachten beschreibt den Stand August
140 2016.

2.5 Detaillierte Bezeichnung des IT-Produktes

2.5.1 Produktbezeichnung

Die Rhenus Data Office GmbH inkl. ihrer Tochter Datenmühle GmbH bietet verschiedene Verfahren zur Vernichtung von Datenträgern an. Zu unterscheiden sind die Verfahren nach Art der behandelten Datenträger (Akten bzw. elektronische Datenträger) sowie hinsichtlich der Frage, ob die Vernichtung am Standort des Kunden (mobil) oder an einem Standort von Rhenus (stationär) erfolgt.

Gegenstand der Begutachtung sind die Verfahren der mobilen und stationären Datenträgervernichtung von Papierdokumenten (dies entspricht **Materialtyp P** gemäß DIN 66399) an Standorten des Kunden und Standorten von Rhenus. Zur genauen Abgrenzung siehe Verfahrensbeschreibung im Anhang (Kapitel **Error! Reference source not found.**).

Geprüfte Version: Stand des Verfahrens im August 2016.

2.5.2 Produktbeschreibung

Eine grobe Produktbeschreibung kann dem aktuellen Produktblatt **Error! Reference source not found.** entnommen werden.

Das Produkt wird in verschiedenen Verfahren angeboten. Eine Beschreibung findet sich im Anhang in Kapitel **Error! Reference source not found.**.

2.5.3 Abgrenzung

Folgende technische Komponenten sind Teil des geprüften Produkts

- Die bereitgestellten Aktencontainer; vgl. **Error! Reference source not found.**
- Shredder-LKW (vgl. Shredder-LKW – Fotos **Error! Reference source not found.**)
- Transportfahrzeuge (Koffer- und Shuttle-Fahrzeuge)
- Betriebsgelände und – gebäude (Vernichtungsstandorte der Rhenus Data Office GmbH; Die Datenmühle GmbH nutzt nur den Standort München, und auch nur für die Verwaltung, da sie nur mobile Aktenvernichtung betreibt)
  - Nottuln / Hauptsitz
  - Berlin
  - Braunschweig
  - Cadolzburg (Nürnberg)
  - Denkendorf (Stuttgart)
  - Freiburg im Breisgau
  - Hamburg
  - Kavelstorf (Rostock)
  - Leipzig
  - München
  - Nidderau (Frankfurt/Main)
  - Ratingen (Düsseldorf)
  - Wilhelmshaven
  - Wunstorf (Hannover)

  Auf gegebenenfalls weitere Standorte bezieht sich diese Prüfung nicht, insbesondere nicht auf Sembach (Kaiserlautern).
- Technische Einrichtung zur Datenträgervernichtung an diesen Standorten

Folgende technische Komponenten und Verfahren sind ausdrücklich nicht Teil des geprüften Produkts:

- IT-Verfahren „RUMS“ zur Tourenplanung
- Überwachung des Shredder-LKWs (GPS) und des Bedienpersonals im Rahmen der Einsatz- bzw. Tourenplanung inkl. der diesbezüglichen Datenschutzaspekte
- Andere gegebenenfalls eingesetzte Transportbehältnisse, zum Beispiel Kunststoffbehälter, insbesondere bei Eigenanlieferung von Kunden

Diese internen, den Endkundenservice „DV“ unterstützende Verfahren verwenden keine Dokumente der Kunden.

Einzelne der vorgenannten Standorte bieten über den Standardumfang hinausgehenden Formen der Datenträgervernichtung an. Das Gutachten betrachtet jedoch nur Leistungen, die flächendeckend angeboten werden. Solche Erweiterungen werden teilweise in Kapitel **Error! Reference source not found.** mit beschrieben, jedoch jeweils entsprechend gekennzeichnet.

Anmerkung: Die genannten Systeme und Verfahren werden sowohl unter dem Namen Rhenus als auch unter dem Namen Datenmühle benutzt. Sie sind technisch identisch, aber unterschiedlich lackiert.

2.6 Tools, die zur Herstellung des IT-Produktes verwendet wurden

nicht anwendbar

2.7 Zweck und Einsatzbereich

Der Zweck und Einsatzbereich des Produkts „Datenträgervernichtung“ der Rhenus Data Office GmbH ist das Löschen von Daten im Sinne des §2 Abs. 2 Ziffer 5 des LDSG und § 3 Abs. 4 Ziffer 5 des BDSG. Dies beinhaltet die Vernichtung von Akten in Papierform. Die Klassifizierung nach DIN 66399 ist:

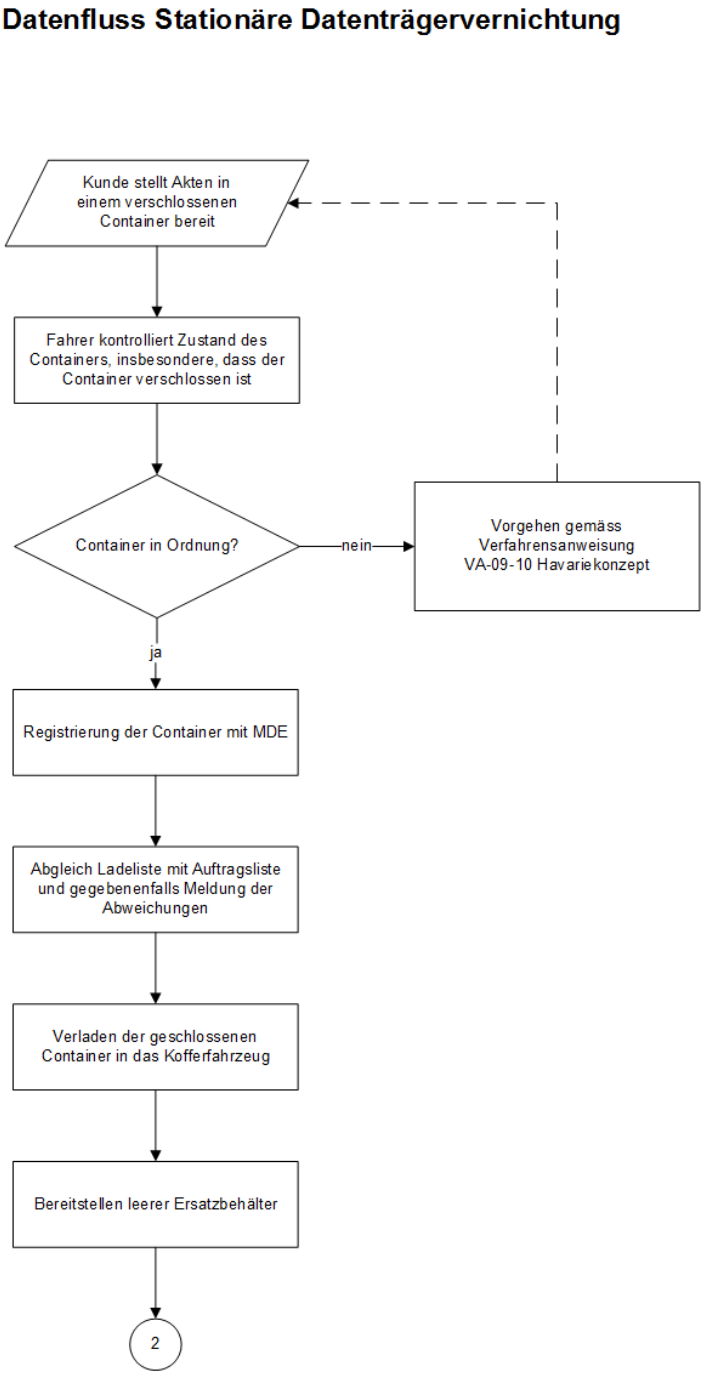
- Materialtyp P
- Variante 3: Datenträgervernichtung extern durch einen Dienstleister
  (betrachtet wird dabei nur die externe Dienstleistung, bei welcher der Datenträgervernichter auf Weisung der verantwortlichen Stelle handelt)

Das Verfahren ist sowohl im öffentlichen als auch im nichtöffentlichen Bereich einsetzbar und sowohl bei stationärer Vernichtung (unter Berücksichtigung einer Anlieferung des zu vernichtenden Materials durch den Auftraggeber) als auch bei mobiler Vernichtung für Akten von Berufsgeheimnisträgern gem. § 203 StGB geeignet.

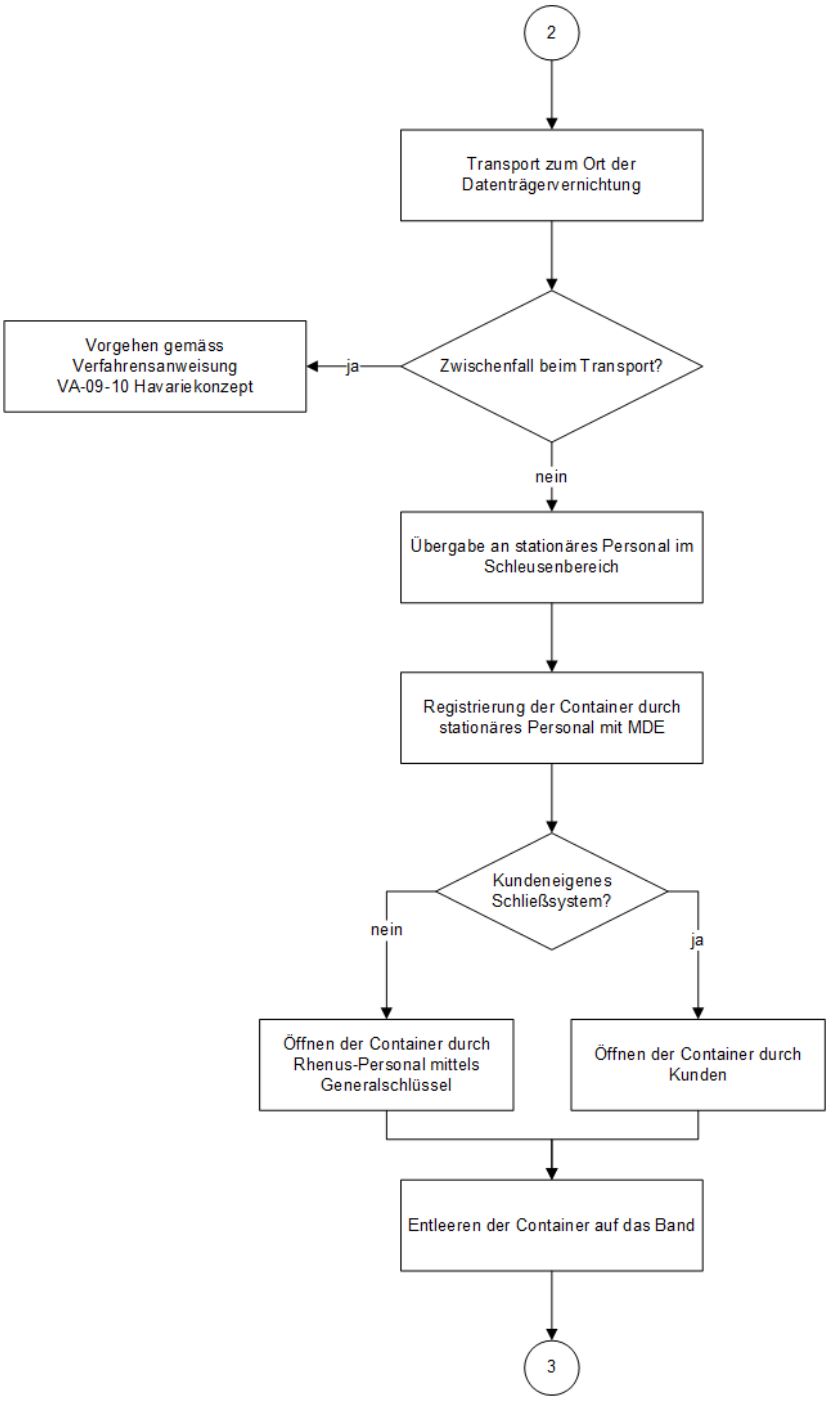
2.8 Modellierung des Datenflusses

2.8.1 Stationäre Datenträgervernichtung

Abbildung 1: Datenfluss Stationäre Datenträgervernichtung

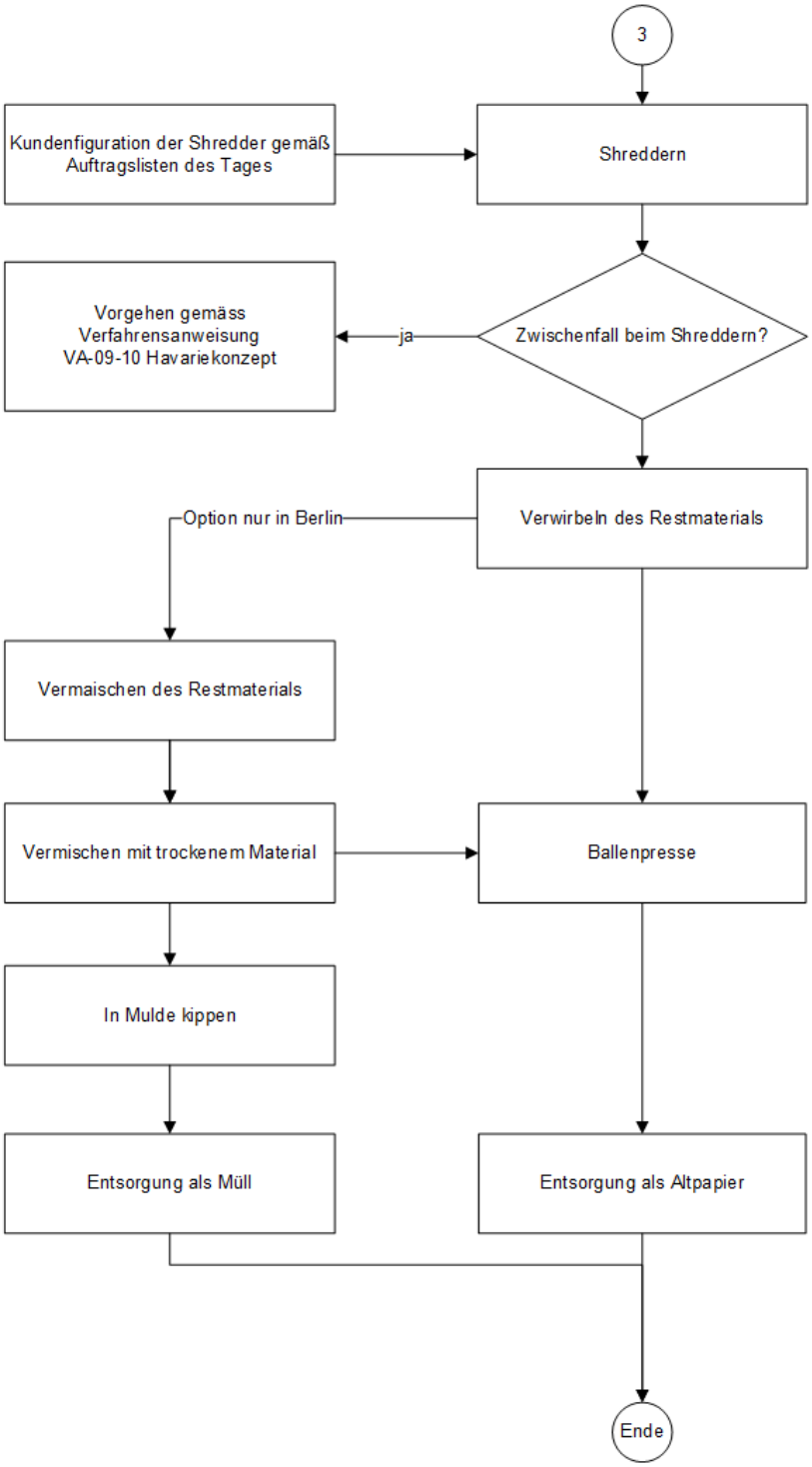


Datenfluss Stationäre Datenträgervernichtung (Fortsetzung)



218
219

Datenfluss Stationäre Datenträgervernichtung (Fortsetzung)

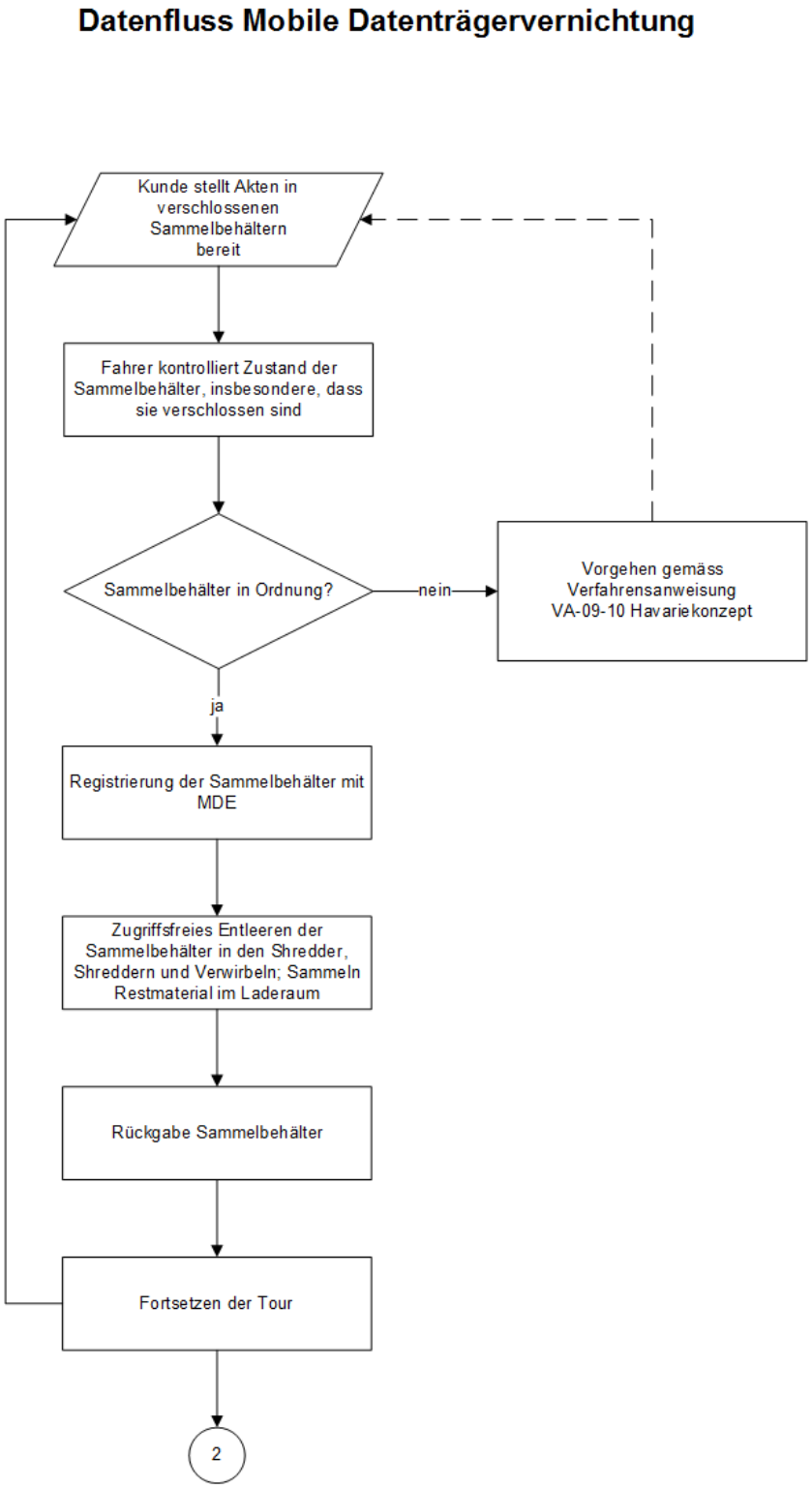


220
221

222 ### 2.8.2 Stationäre Datenträgervernichtung

223 Abbildung 2: Datenfluss Mobile Datenträgervernichtung

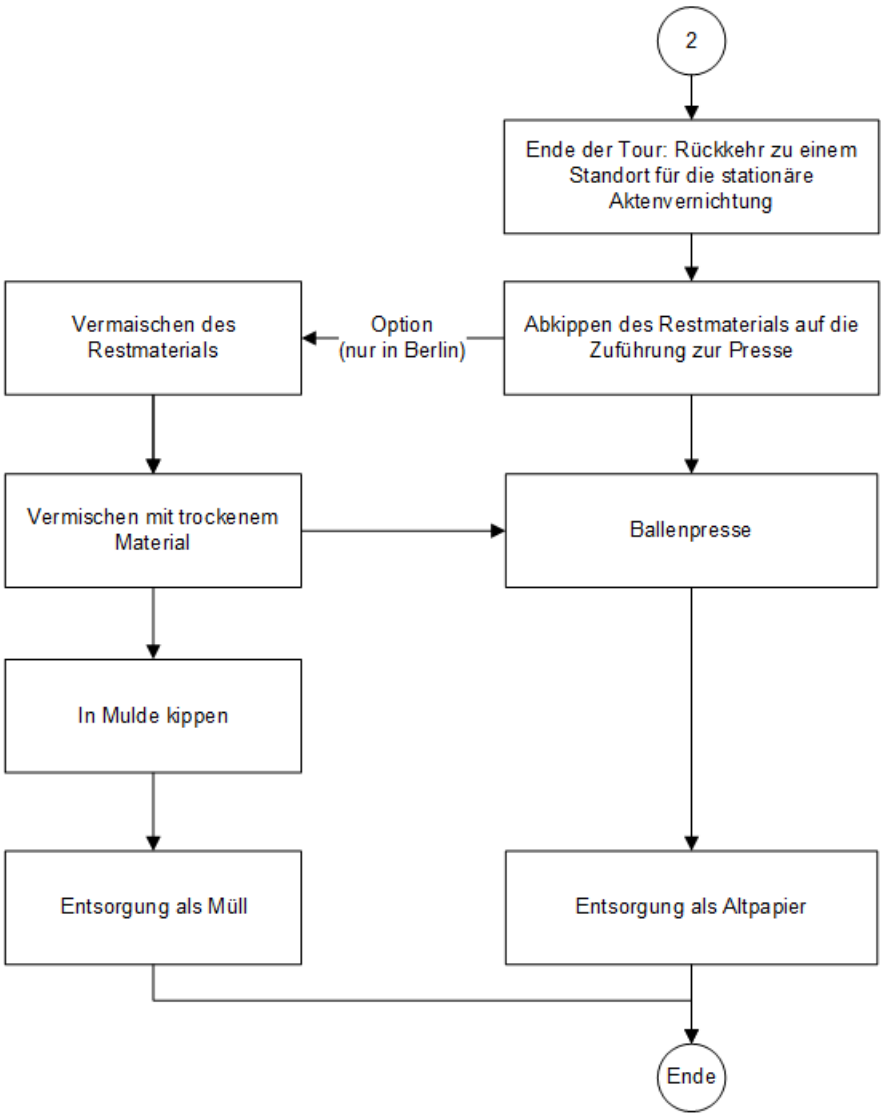
224



225

226

Datenfluss Mobile Datenträgervernichtung (Fortsetzung)



227

228

2.9 Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog V 2.0 vom 28.11.2014

2.10 Angewandte Evaluationsmethoden

2.10.1 Modus der Prüfung

Die Begutachtung dient der Rezertifizierung.

2.10.2 Vorgehensweise

Die **zentralen Verfahren**, z.B. das Sicherheitsmanagement und die zentralen IT-Verfahren, wurden vor Ort am Hauptsitz des Unternehmens in Nottuln geprüft.

Die **stationäre Aktenvernichtung** wurde durch Ortbesichtigungen in Ratingen (Düsseldorf), Hamburg, Wunstorf (Hannover), Leipzig und München geprüft. Die übrigen Standorte wurden bereits in den letzten Jahren auditiert bzw. sind für eine Auditierung in 2016 und 2017 vorgesehen. Solche zyklischen Audits finden unabhängig von einer Begutachtung für das Datenschutzgütesiegel statt. Dieses Gutachten beschreibt nur den Sicherheitsstandard, der von allen Standorten erreicht wird. Eventuell vorhandene erhöhte Sicherheitsmaßnahmen an einzelnen Standorten und darauf fußende Produkte wurden nicht berücksichtigt.

Das System für die **mobile Aktenvernichtung** wurde am Standort München geprüft. Der **Transportprozess** von der verantwortlichen Stelle zur Stelle der Datenträgervernichtung (mit Ausnahme der LKW-Fahrt selbst) wurde ebenfalls begutachtet.

Der Datenträgervernichtungsprozess wurde gemäß den Kriterien der hierfür maßgeblichen Norm **DIN 66399** bewertet. Die **Restmaterialprüfung** erfolgte durch optische und Siebanalyse.

Die im Gutachten berücksichtigten **Dokumente** sind vollständig in Kapitel **Error! Reference source not found.** aufgeführt. Stand der Dokumentation ist der 12.8.2016. Alle in diesem Gutachten getroffenen Aussagen basieren auf der Grundlage dieser Prüfungen.

Prüfung nach DIN 66399

Gemäß den Vorgaben der Norm wurden eine formale Prüfung für die mobile und stationäre Danteträgervernichtung durchgeführt sowie Prüfberichte in der von der Norm vorgeschriebenen Form angefertigt (siehe [69]).

Im Einzelnen fanden unter anderem folgende Prüfungen statt:

- Prüfung der Standorte der stationären Vernichtung (Liste der Standorte siehe Kapitel 2.5.3; Umfang der Prüfung siehe [69]; u.a.
  - Gelände und Abgrenzung des Grundstück bzw.Gebäudes
  - Bauliche Beschaffung
  - Zutrittskontrolle und ~überwachung inkl. Schließsysteme, Videoüberwachung, Wachdienst
- Prüfung der stationären Vernichtungsanlagen (siehe auch [69])
  - Anlieferung Material
  - Vernichtung
  - Verarbeitung des Restmaterials
  - Zugriffskontrolle, z.B. Kapselung der Anlagen (für Schutzklasse 3)
- Prüfungen der mobilen Aktenvernichtung
  - dto.; zusätzlich:
  - Fahrzeug (MAV)
  - Sicherheit der Sammelbehälter (siehe [63]) (*)
  - Schließsystem der Sammelbehälter (siehe [62]) (*)
- Prüfung am Kundenstandort (Details siehe [76])
  - Einsammeln Datenträger
  - Mobile Vernichtung vor Ort
- Verfahren der Aktenvernichtung
  - Prozesse
  - Dokumentation
- Allgemeine Sicherheitsfragen, u.a.
  - Umsetzung der Sicherheitsmaßnahmen nach Grundschutz & ISO 27001
  - Interne und externe Audits
- Prüfung des Restmaterials:
  - Probenentnahme
  - Optische Analyse
  - Siebanalyse durch ein technisches Prüflabor (siehe [76]) (*)
  - Siebanalyse bei Eigenzertifizierung des Herstellers der Maschinen (siehe **Error! Reference source not found.**) (*1)

Die mit (*) markierten Prüfungen wurden im Auftrag durch Dritte durchgeführt, wobei die Prüfergebnisse durch die Auditoren kontrolliert wurden. Die übrigen Prüfungen führten die Auditoren selbst durch.

2.10.3 Veränderungen im Produkt

Gegenüber der Begutachtung von 2014 gibt es folgende Veränderungen am Produkt:

- Die Firma Datenmühle GmbH ist eine 100%-Tochter der Rhenus Data Office GmbH und verwendet die gleichen Systeme, Verfahren und Standorte, u.a. den gleichen, jedoch andersfarbig lackierten, mobilen Aktenvernichter. Datenmühle wird erstmals in die Begutachtung einbezogen. Datenmühle findet hier nur eine formelle Erwähnung, da es sich um dasselbe Verfahren handelt und die Zertifizierung nach der DSGVO für ein Verfahren und nicht für den Betreiber des Verfahrens erfolgt.
- Im Vergleich zur letzten Begutachtung hat es mehrere Standortumzüge gegeben (Düsseldorf, Hamburg, Leipzig). Es handelt sich um Zusammenlegungen örtlicher Standorte nach Akquisition von Mitbewerbern. Deswegen wurden alle drei Standorte auditiert. Technik und Verfahren entsprechen inzwischen den Vorgaben und Regeln von Rhenus.

2.11 Zusammenfassung der Prüfergebnisse

Nach Ansicht der Auditoren werden folgende Prüfergebnisse erzielt.

2.11.1 Prüfkatalog des ULD

Die Anforderungen werden erfüllt.

2.11.2 DIN 66399 (2012-10)

Die Anforderungen werden wie folgt erfüllt:

Erreichte Schutzklasse

Verfahren	Erreichte Schutzklasse
Mobile Vernichtung	3
Stationäre Vernichtung	2

Erreichte Sicherheitsstufe

Technik	Erreichte Sicherheitsstufe
Mindestens Sieb mit 20er-Lochmaske	4

Bei Benutzung angemessener Siebe wird Sicherheitsstufe 4 erreicht, womit die Reproduktion der auf den Datenträgern wiedergegebenen Daten nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich ist

Anmerkungen zum Prüfumfang

Die Prüfung bezog sich nur auf:

- Variante 3: Datenträgervernichtung extern durch Dienstleister, hier wurde nur der Teil des Verfahrens geprüft, der durch den externen Dienstleister erbracht wird. Die Erfüllung der Aufgaben der verantwortliche Stelle wurde nicht bewertet.
- Datenträgertyp P - Informationsdarstellung in Originalgröße (Papier, Film, Druckformen, …)

2.12 Ausgleichende Maßnahmen

Abweichungen wurden nur hinsichtlich einzelner Anforderungen der DIN festgestellt, und auch nur dann bezüglich der Schutzklasse 3. Hinsichtlich des Prüfkatalogs des ULD gab es keine Abweichungen.

2.12.1 Zugriff auf das zu vernichtende Material

Forderung der Norm:

Das Bedienpersonal darf grundsätzlich keinen Zugriff auf zu vernichtende Datenträger mit Informationsdarstellung in Originalgröße (DIN 66399-2 Kategorie P) haben. Der Maschine zur Vernichtung der Datenträger wird der Inhalt der eingesetzten Sicherheitsbehälter entweder direkt oder über eine entsprechend gesicherte Zuführeinrichtung zugeführt.

Anmerkung: Gemäß den Forderungen der DIN ist dies nur für Schutzklasse 3 zwingend vorgeschrieben. Aus Gründen des Datenschutzes ist die Forderung aber immer sinnvoll.

Situation:

Aus technisch-physikalischen Gründen ist die Möglichkeit eines Zugriffs auf die zu vernichtenden Datenträger nicht in jedem Fall auszuschließen. Einzelne Seiten können sich in Transporteinrichtung verklemmen, um bewegliche Teile wickeln oder unter Transportbänder gleiten. Spätestens im Fall von Systemwartungen erhält das Personal damit Zugang zum Material.

Als nicht relevant im Sinn der Forderung der Norm werden Vorgänge betrachtet, bei denen Personen unter erheblicher Gefährdung der eigenen Gesundheit in die Verarbeitung der Maschinen eingreifen, zum Beispiel in Transporteinheiten.

Ausgleichende Maßnahmen hierzu sind:

- Durchführung der Aktenvernichtung in geschlossenen Bereichen
- Zugang nur eingeschränkten Personenkreis
    - für Standortpersonal, das entsprechend den Regeln des Datenschutzes geprüft und auf den Datenschutz verpflichtet wurde; Auditoren sind logisch diesem Personenkreis gleichgestellt.
    - für sonstige Personen nur, wenn ausschließlich eigene Akten vernichtet werden, aus Gründen der Überwachung des Vorgangs
- Tägliche Reinigung der Betriebsstätte ist schon aus Gründen des Brandschutzes vorgeschrieben
- Videoüberwachung: Unrechtmäßige Zugriffe würden auffallen. Sicherung der Betriebsstätten

2.12.2 Sicherung der Zugänge zum Vernichtungsbereich

Forderung der Norm:

Alle Türen oder Tore, die direkt in den Sicherheitsbereich führen, schließen automatisch oder offene Türen/Tore werden durch optische oder akustische Meldeeinrichtungen angezeigt.

Die Sicherheitszone des Betriebsgebäudes wird durch Videokameras überwacht.

Situation:

Die entsprechenden technischen Maßnahmen werden von den Standortverantwortlichen eigenverantwortlich ausgewählt. Hierbei kommt es zu Abweichungen der Standorte untereinander.

Ausgleichende Maßnahmen hierzu:

- Mit der Richtlinie für die physikalische Sicherheit definiert das Unternehmen den Mindeststandard für die physikalische Sicherheit
- Die Umsetzung wird zentral nachverfolgt.

2.13 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das BDSG definiert in § 3 Abs. 4 den Vorgang des Löschens ausdrücklich als Teil der Verarbeitung personenbezogenen Daten und unterwirft diesen Vorgang damit eigenen Sicherheitsanforderungen. Mit dem geprüften Produkt sind verantwortliche Stellen in der Lage, diesen Forderungen nachzukommen.

Rhenus selbst verarbeitet diese Daten nur insoweit, als dass sie unter den in 2.12.1 beschriebenen Möglichkeiten einer Kenntnisnahme vernichtet werden. Das Verfahren verarbeitet darüber hinaus keine anderen bzw. eigenen datenschutzrelevanten Daten.

Für die Vernichtung von Datenträgern werden den verantwortlichen Stellen (Kunden) mehrere Verfahren des Sammelns und der Vernichtung angeboten, die in geeigneter Kombination den Anforderungen der Sicherheitskonzepte der Kunden entsprechen. Der Sicherheitsstandard der gewählten Verfahrensvarianten ist gemäß den Regeln der maßgeblichen Norm (DIN 66399) beschrieben und durch Begutachtung nachgewiesen.

Für das Einsammeln der zu vernichtenden Datenträger stehen insbesondere verschiedene Sammelbehälter bereit, deren Widerstandskraft gegen Versuch der unbefugten Einsichtnahme in das gesammelte Material ebenfalls durch Gutachten belegt wurde.

2.13.1 Mobile Datenträgervernichtung:

Nach der Abholung und direkt im Anschluss an den abgeschlossenen Shreddervorgang erhält der Auftraggeber ein vom Rhenus-Mitarbeiter ausgefertigtes Protokoll über die Vernichtung (Anlage). Die Vernichtung von Akten erfolgt somit in nachvollziehbarer und durch den Auftraggeber in leicht kontrollierbarer Weise.

2.13.2 Stationäre Datenträgerentsorgung:

Der Transport zum Ort der Vernichtung erfolgt in verschlossenen Fahrzeugen. Der Transportvorgang wird selbst überwacht, u.a. mittels GPS-Ortung.

Die eigentliche Vernichtung erfolgt unmittelbar nach Anlieferung am Rhenus-Standort innerhalb geschlossener Sicherheitszonen.

Der Kunde hat die Möglichkeit, alle Vorgänge zu begleiten und zu überwachen. Alternativ kann er Teilvorgänge selbst übernehmen, z.B. Sammlung und Transport durch Rhenus durch Eigenanlieferung ersetzen.

In der technischen Umsetzung erfüllt das Verfahren alle Anforderungen der gegenwärtig gültigen Normen. Siehe dazu Absatz „Technische Umsetzung“ in Kapitel **Error! Reference source not found.** sowie das Gutachten zur Erfüllung von DIN 66399.

3 Teil II: Erfüllung der Rechtsvorschriften

3.1 § 11 BDSG

Eine Auftragsdatenverarbeitung gem. § 11 BDSG liegt vor, wenn die Vorgaben zur Ausgestaltung der Auftragsdatenverarbeitung in § 11 BDSG erfüllt sind.

Aus dem Wortlaut des in § 11 Abs. 1 Satz 1 BDSG festgeschriebenen Grundsatzes, der Auftraggeber sei für die Einhaltung der Vorschriften des BDSG verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, ergibt sich, dass der Auftraggeber für die Rechtmäßigkeit der Datenverarbeitung verantwortlich bleibt und sich von dieser Verpflichtung nicht durch die Einschaltung anderer Stellen befreien kann. Die Verantwortung des Auftraggebers wird durch die mit dem BDSG 2001 erfolgte Neufassung der Definition des § 3 Abs. 7 BDSG noch dadurch unterstrichen, dass dort statt von der „speichernden Stelle“ von der „verantwortlichen Stelle“ gesprochen wird. Auch die Definition des Begriffs der verantwortlichen Stelle in § 3 Abs. 7 BDSG, wonach verantwortliche Stelle jede Person oder Stelle sei, die personenbezogene Daten für sich selbst erhebe, verarbeite oder nutze oder dies durch andere im Auftrag vornehmen lasse, verweist darauf, dass der Auftraggeber auch bei einer Erhebung, Datenverarbeitung oder Nutzung durch eine andere Stelle verantwortlich bleibt. Nach § 11 Abs. 1 Satz 1 BDSG ist der Auftraggeber dafür verantwortlich, dass die datenschutzrechtlichen Zulässigkeitsvoraussetzungen unmittelbar auch vom Auftragnehmer eingehalten werden.

Als erstes ist hierzu die fehlende Entscheidungsbefugnis des Auftragnehmers über die Daten zu nennen, insbesondere die Auswahl der Daten sowie Art und Weise der Verarbeitung. Weiter muss sich die Datenverarbeitung ausschließlich auf Daten beschränken, die der Auftraggeber zur Verfügung stellt. Schließlich muss der Auftragsschwerpunkt auf die praktisch-technische Durchführung einer Verarbeitung gerichtet sein, die der Auftraggeber nach außen in eigener Verantwortung vertritt. Auch bleibt festzuhalten, dass eine Auftragsdatenverarbeitung vorliegt, wenn der Auftraggeber Weisungs- und Kontrollrechte hat, also „Herr der Daten“ bleibt. Mithin hat ein Auftragnehmer als beauftragte Stelle nur eine Hilfs- und Unterstützungsfunktion und agiert in diesem Rahmen in völliger Abhängigkeit von den Vorgaben der verantwortlichen Stelle wie eine ausgelagerte Abteilung. Es bleibt damit für die Abgrenzung entscheidend, inwieweit der Auftragnehmer faktisch eigene Entscheidungsbefugnisse über die Daten bzw. deren Verarbeitung besitzt, und ob die Durchführung in praktisch-technischer Hinsicht eine weisungsgebundene Tätigkeit darstellt.

Der gesamte Verarbeitungsprozess der Datenträgervernichtung durch Rhenus ist darauf ausgerichtet, Kundendaten im Auftrag zu vernichten und dies möglichst sicher, effizient und ohne eine Möglichkeit der Einsichtnahme der Daten. Um diesen Ansprüchen gerecht zu werden, hat Rhenus Prozesse und Technologien entwickelt, die in einer Kombination aus Organisation und Technik den Anforderungen an eine Auftragsdatenverarbeitung entsprechen.

Zunächst wird mit der Vertragsgestaltung zwischen Kunden und Rhenus deutlich darauf abgestellt, dass der Kunde eigenverantwortlich bleibt, so lange, bis das zu vernichtende Material keinen Personenbezug mehr herstellen lässt. Wie aus der Verfahrensbeschreibung (siehe Kapitel **Error! Reference source not found.**) ersichtlich, stellt Rhenus dem Kunden Optionen als Gestaltungsspielraum zur Verfügung. Die Verantwortung des Kunden ist hier vertraglich deutlich hervorgehoben.

Die Begutachtung der vertraglichen und organisatorischen Positionen als auch der Prozess- und Technikbeschreibung macht es notwendig, dass der Kunde selbst zunächst die Schutzklasse zu definieren hat (siehe **Error! Reference source not found.**).

Für Schutzklasse 2 ist die stationäre Vernichtung aus juristischer Perspektive geeignet, ohne dass der Auftraggeber selbst eine Anlieferung vornimmt, Liefert der Auftraggeber Daten nicht selbst an, ist vom Auftraggeber für Daten der Schutzklasse 3 das mobile Verfahren vorzugeben, das - wie schon im Erstgutachten zum MAV beschrieben - für diese hohe Schutzklasse geeignet ist.

Auch wenn die mobile Datenträgervernichtung eine sichere Lösung für eine datenschutzgerechte Aktenvernichtung ist, obliegt die Ausgestaltung der Prozesse immer noch dem Auftraggeber (siehe

Kapitel **Error! Reference source not found.**), Beispielhaft sei hier die Schlüsselverwaltung benannt. Es obliegt dem Kunden, zu entscheiden, ob der Schlüssel für die jeweiligen Container innenseitig der Container verwahrt werden soll, oder ob der Kunde den Schlüssel selbst in seine Obhut nimmt. Gleichfalls obliegt es dem Kunden zu entscheiden, ob der Vernichtungsvorgang von einem Berechtigten des Kunden beobachtet wird, oder ob Rhenus den Vorgang unbeaufsichtigt durchführt. Die Verantwortung des Kunden ist hier vertraglich deutlich hervorgehoben.

Die Begutachtung der vertraglichen und organisatorischen Positionen als auch der Prozess- und Technikbeschreibung lässt wie schon im Erstgutachten nur die Frage aufkommen, wie mit einem nach der Befüllung der Anlage im Container verbleibendem Rest an zu vernichtendem Material umgegangen werden könnte. Es lässt sich technisch nicht verhindern, dass gelegentlich einzelne Papiere (bspw. durch Feuchtigkeit) im Container verbleiben und an den Kunden zurückgegeben werden. Praktisch hat dies nur insofern Bedeutung, wenn der Kunde den Schlüssel für den Container selbst verwaltet und der Schlüssel für die einzelnen Container nicht, wie oben beschrieben, innenseitig im Container verwahrt wird. Da die Container durch einen Schließmechanismus am LKW nach der Entleerung geschlossen werden, bevor der Fahrer des LKW eine Möglichkeit der Einsichtnahme hat, sind im Container verbleibende Papiere nur dann als problematisch anzusehen, wenn die Container nicht in die Abteilung zurück verbracht werden, aus der das zu vernichtende Material stammte. Letztlich ist dies aber eine Frage der Schlüsselverwaltung und liegt im Verantwortungsbereich des Aufraggebers. Wenn der Schlüssel, wie von Rhenus vorgesehen, im Container verwahrt wird, besteht zu keinem Zeitpunkt ein Risiko einer unberechtigten Einsichtnahme, Rhenus unterstützt den Auftraggeber in seiner Verantwortung dahingehend, dass die Schlüsselverwaltung in der Vertragsgestaltung als Option und nicht als Standard des Verfahrens zu verstehen ist. Dies ist auch Teil der Dokumentation.

Zusammenfassend betrachtet hat der Fahrer zu keinem Zeitpunkt des MAV die Möglichkeit einer Einsichtnahme des zu schreddernden Materials, womit die Datenträgervernichtung der Fa. Rhenus aus datenschutzrechtlicher Sicht als vorbildlich betrachtet werden kann.

3.2 § 17 LDSG SH

Der insbesondere für die öffentliche Verwaltung einschlägige § 17 LDSG SH stellt inhaltlich auf die gleichen Parameter wie der § 11 des BDSG ab. Verantwortlichkeit des Auftraggebers, Wahrung von Betroffenenrechten, Weisungsbindung des Auftragnehmer und insbesondere die Anforderungen an allgemeine Maßnahmen zur Datensicherheit gem. § 5 LDSG SH sind deckungsgleich mit den Ausführungen zu § 11 BDSG, als auch den Beschreibungen zu technischen und organisatorischen Maßnahmen zur Datensicherheit im technischen Teil des Gutachtens.

3.3 Berufsgeheimnisträger gem. § 203 StGB, § 80 Abs. 5 SGB X

Entsprechend dem Ergebnis des technischen Gutachtens kann die mobilen Datenträgervernichtung der Firma Rhenus auch im Kreis der Berufsgeheimnisträger (gem. § 203 StGB; § 80 Abs. 5 SGB X) als zulässige Auftragsdatenverarbeitung bejaht werden, da aufgrund der Natur des Verfahrens der Auftragnehmer keine Möglichkeit der Kenntnisnahme von Daten des Auftraggebers erlangt.

Das mobile Verfahren entspricht den Anforderungen der Schutzklasse 3 gem. DIN 66399-1.

Die stationäre Datenträgervernichtung, könnte entsprechend dem Ergebnis des technischen Gutachtens, im Kreis der Berufsgeheimnisträger (gem. § 203 StGB; § 80 Abs. 5 SGB X) als zulässige Auftragsdatenverarbeitung bejaht werden, sofern Berufsgeheimnisträger, deren Daten der Schutzklasse 3 entsprechen, die Anlieferung selbst vornehmen und die Anlage auch selbst beschicken. Dieses ist vornehmlich dadurch bedingt, dass die Container zur Beschickung der Anlage im SDV durch einen Rhenus–Mitarbeiter geöffnet werden und hierbei eine Kenntnisnahme der Datenbestände erfolgen könnte, auch wenn die Mitarbeiter dazu verpflichtet sind, dies nicht zu tun. Unter diesen Bedingungen bestünde aber keine Möglichkeit der Kenntnisnahme von Daten des Auftraggebers, womit das Verfahren die Anforderungen der Schutzklasse 3 der DIN 66399 erfüllt. Allerdings kann die Möglichkeit einer stationären Vernichtung nach SK 3 dadurch gehemmt werden, dass ein Zutritt in eine nach SK 2 zertifizierte Umgebung für eigene Anlieferungen sich dann ausschließt, wenn dem SK 3 – Verpflichteten durch die eigene Anlieferung die Möglichkeit einer Einsichtnahme in SK 2 Daten anderer Kunden im laufenden Vernichtungsprozess ermöglicht werden könnte. Dies liegt darin begründet, dass im laufenden Vernichtungsprozess von SK 2 Daten ein SK 3 – Verpflichteter so nah an den Schredderprozess herangeführt werden müsste, um seiner Verschwiegenheitsverpflichtung gerecht zu werden, dass eine Einsichtnahme in andere Daten, die nicht seinem Verantwortungsbereich zugerechnet werden können, möglich werden kann. Bedingt ist dies auch durch den Umstand, dass die SK 3 Daten nicht an Mitarbeiter von Rhenus übergeben werden können.

Dieser Umstand lässt sich nur dadurch ausschließen, dass durch organisatorische und technische Maßnahmen die Möglichkeit einer unberechtigten Einsichtnahme in andere vertrauliche Daten nach SK 2 vermieden wird, z.B. durch zeitliche und/oder räumliche Trennung der Vernichtung unterschiedlich klassifizierter Daten. Dies ist abhängig von den Standorten, die vereinzeln den SK 3 – Markt bedienen können. Der Regelfall in einer SK 2- Umgebung sieht als Mindeststandard vor, dass niemand unberechtigt Zutritt zur Vernichtungsanlage erlangen kann. Und dazu gehören eben auch SK 3 – Verpflichtete. Hier ist es Sache des Sonderrechtsverpflichteten für den Vernichtungsprozess das MAV zu wählen, sollte eine stationäre Vernichtung am Standort nicht SK 3 – fähig sein.

3.4 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten gem. § 42a BDSG

Das gesamte Verfahren der datenschutzgerechten Datenträgervernichtung dient der Verhinderung einer unrechtmäßigen Kenntniserlangung von Daten und ist durch die in diesem Gutachten beschriebenen rechtlichen, technischen sowie organisatorischen Maßnahmen darauf ausgerichtet, dass selbst durch den Auftragnehmer keine solchen Kenntniserlangungen erfolgen können. Nicht zuletzt wird dies dadurch sichergestellt, dass der Auftraggeber

- beim mobilen Vernichtungsprozess das Vernichtungsgutes überprüft und damit das Ergebnis abnimmt,
- beim stationären Verfahren die Anlage selbst beschickt (s. 3.4.3)

3.5 Bestätigung

Hiermit bestätigen wir, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und der Datensicherheit entspricht.

Wir versichern, an der Entwicklung und Betreuung des Verfahrens nicht beteiligt gewesen zu sein und mit Ausnahme des Prüfauftrages für das Datenschutz-Gütesiegel über keine geschäftliche oder private Beziehung zu der Auftraggeberin zu verfügen.

(Michael J. Erner)

Bad Wörishofen, den 03. November 2016

(Friedrich Abraham)

Hürth, den 04. November 2016