Kurzgutachten

zum Verfahren

„Datenträgervernichtung der Firma Rhenus Data Office GmbH“

nach DSGSVO Schleswig-Holstein

(Datenschutz-Prüfsiegel)

Stand: 29.08.2014

1. Zeitpunkt der Prüfung

Januar 2012 – August 2014

2. Adresse des Antragstellers

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

3. Adresse 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

Gutachter:	**Rechtlicher Gutachter**	**Technischer Gutachter**
Firma:	Mission 100 e.V.	Mission 100 e.V.
Name:	Michael J. Erner	Friedrich Abraham
Adresse:	Gartenäckerstr. 13 86825 Bad Wörishofen	Auf den Dreien 52 50354 Hürth
Telefon:	+49 (0) 172 451 05 04	+49 (0) 172 98 24 009
E-Mail:	me@mission100.org	fa@mission100.org

4. Kurzbezeichnung des IT-Produktes

Das Produkt „Datenträgervernichtung (DV)“ der Firma Rhenus Data Office GmbH, nachfolgend kurz „Rhenus“, dient der Datenträgervernichtung durch Löschung im Sinne des § 2 Abs. 2 Ziffer 5 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG) und § 3 Abs. 4 Ziffer 5 des Bundesdatenschutzgesetzes (BDSG). Das Verfahren erfüllt die Anforderungen an einen sicheren Löschungsprozess von Datenträgern. Das Gutachten beschreibt den Stand August 2014.

5. Detaillierte Bezeichnung des IT-Produkt

Die Rhenus Data Office 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.

Geprüfte Version: Stand des Verfahrens im August 2014.

5.1 Abgrenzung

Folgende technische Komponenten sind Teil des geprüften Produkts

- Die von Rhenus bereitgestellten Aktencontainer.
- Shredder-LKW (vgl. Shredder-LKW – Fotos
- Transportfahrzeuge (Koffer- und Shuttle-Fahrzeuge)
- Betriebsgelände und – gebäude (Vernichtungsstandorte der Rhenus Data Office GmbH)
  - München
  - Berlin
  - Leipzig
  - Freiburg
  - Stuttgart (Denkendorf)
  - Frankfurt/Main (Nidderau)
  - Neumünster
  - Nottuln
  - Hilden
  - Wilhelmshaven
- Technische Einrichtung zur Datenträgervernichtung an diesen Standorten

5.2. Ausnahmen

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.

6. Tools, die zur Herstellung des IT-Produktes verwendet wurden

nicht anwendbar

7. Zweck und Einsatzbereich

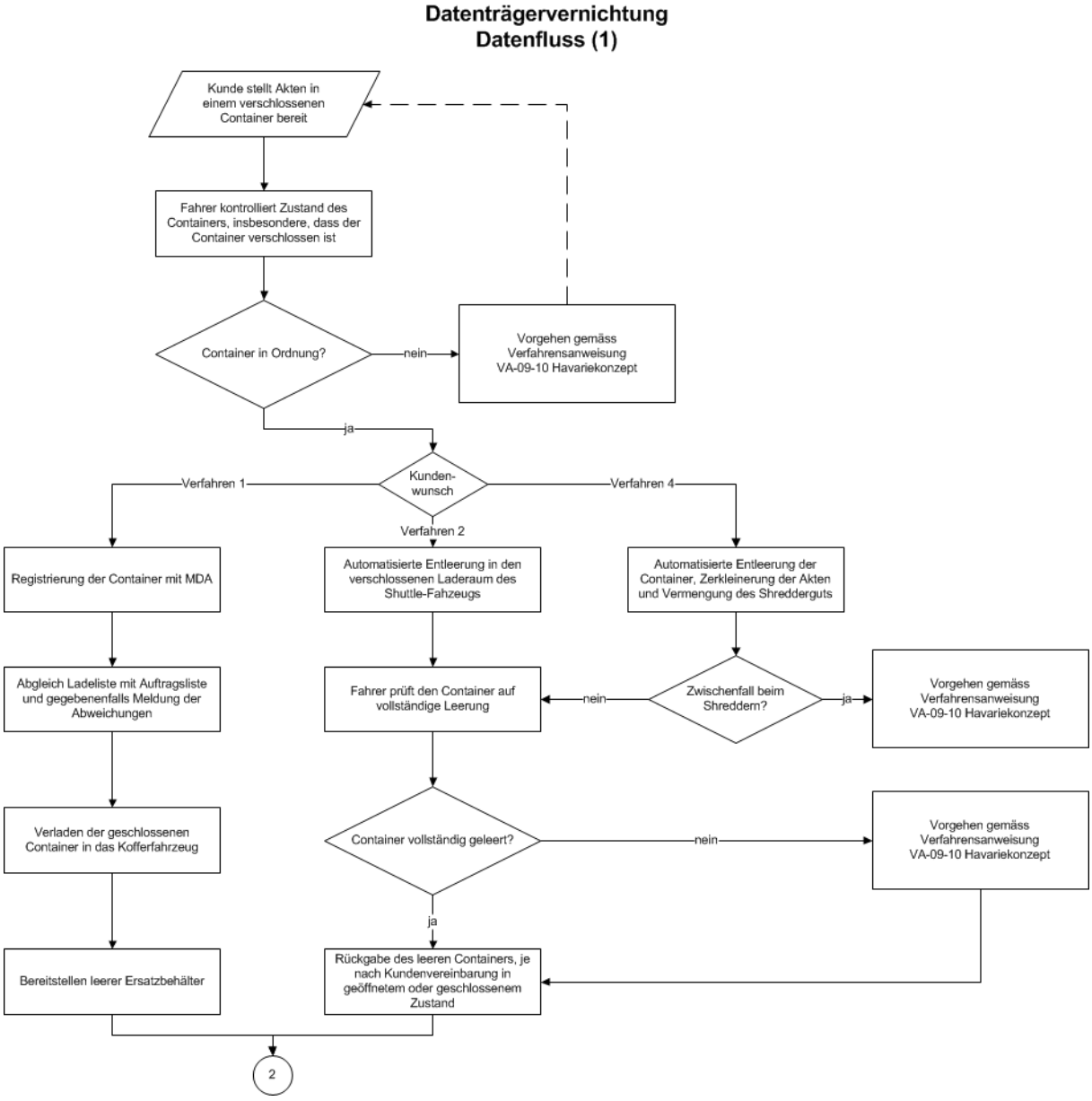
Der Zweck und Einsatzbereich des Produkts „Datenträgervernichtung“ der Rhenus Data Office GmbH ist das Löschen von Daten im Sinne des §2 Abs. 2 Ziffer 5 des LDSG und § 3 Abs. 4 Ziffer 5 des BDSG. Dies beinhaltet die Vernichtung von Akten in Papierform. Die Klassifizierung nach DIN 66399 ist:

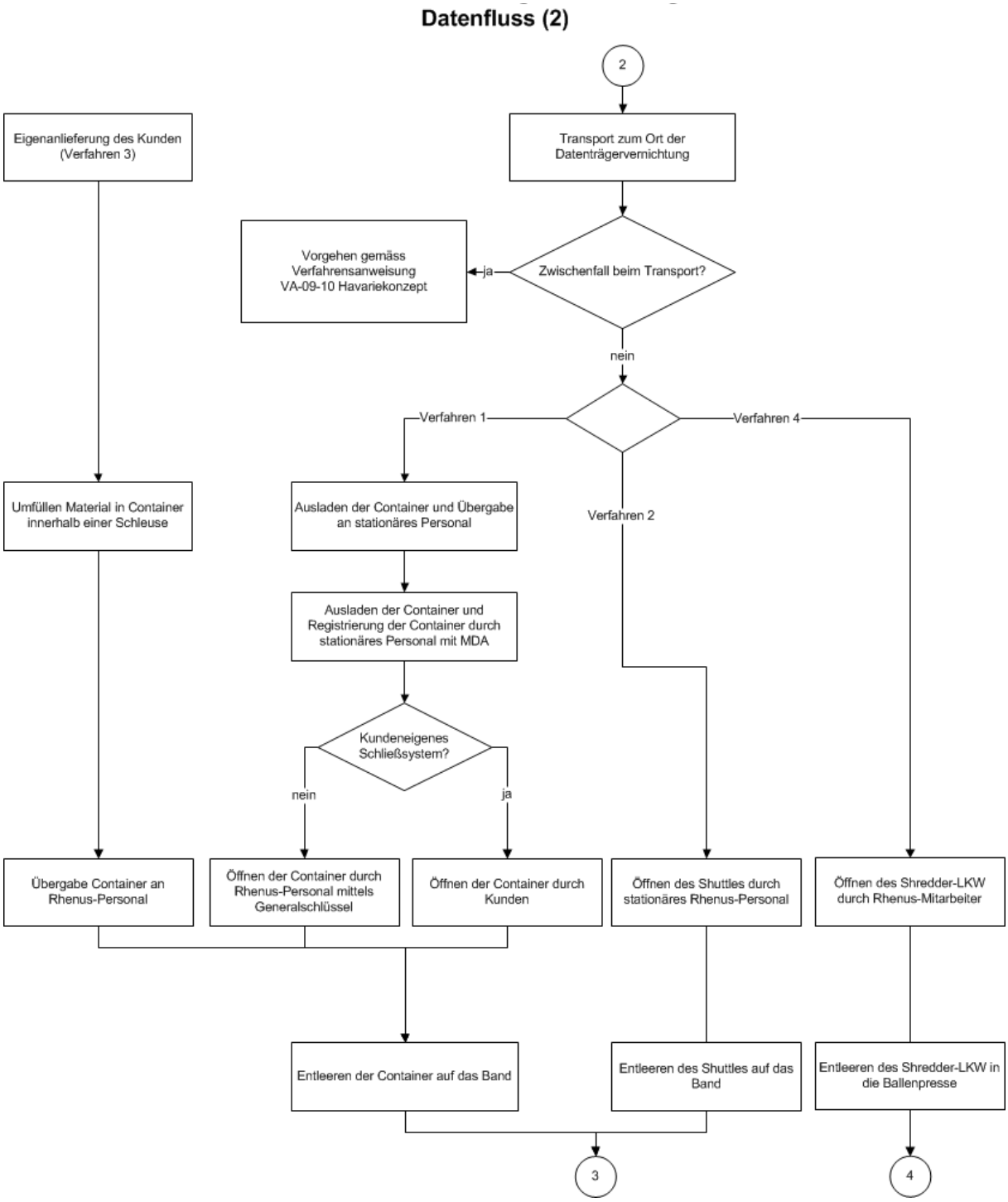
- Materialtyp P
- Variante 3: Datenträgervernichtung extern durch einen Dienstleister
  (betrachtet wird dabei nur die externe Dienstleistung, bei welcher der Datenträgervernichter auf Weisung der verantwortlichen Stelle handelt)

Das Verfahren ist sowohl im öffentlichen als auch im nichtöffentlichen Bereich einsetzbar und 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. In beiden Verfahren haben Berufsgeheimnisträger die Möglichkeit das Verfahren zu begleiten, resp. zu beaufsichtigen.

8. Modellierung des Datenflusses

Nachfolgende Bilder zeigen den Datenfluss.




Datenfluss (2)
2
Eigenanlieferung des Kunden (Verfahren 3)
Transport zum Ort der Datenträgervernichtung
Vorgehen gemäss Verfahrensanweisung VA-09-10 Havariekonzept
ja
Zwischenfall beim Transport?
nein
Verfahren 1
Verfahren 4
Umfüllen Material in Container innerhalb einer Schleuse
Ausladen der Container und Übergabe an stationäres Personal
Verfahren 2
Ausladen der Container und Registrierung der Container durch stationäres Personal mit MDA
Kundeneigenes Schließsystem?
nein
ja
Übergabe Container an Rhenus-Personal
Öffnen der Container durch Rhenus-Personal mittels Generalschlüssel
Öffnen der Container durch Kunden
Öffnen des Shuttles durch stationäres Rhenus-Personal
Öffnen des Shredder-LKW durch Rhenus-Mitarbeiter
Entleeren der Container auf das Band
Entleeren des Shuttles auf das Band
Entleeren des Shredder-LKW in die Ballenpresse
3
4

110
111

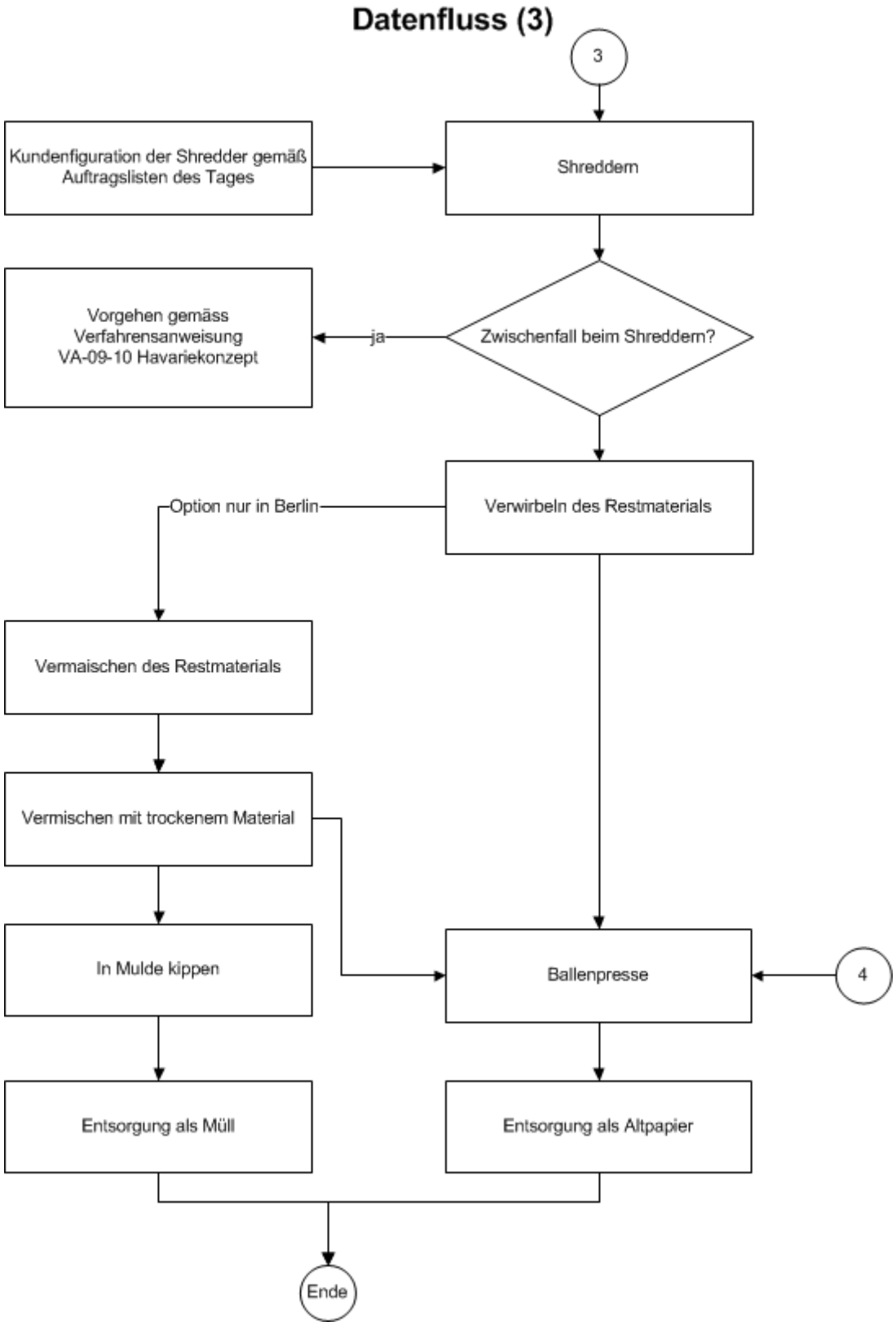


Abbildung 1: Datenfluss

9. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog v 1.2 vom 29.8.2005

10. Zusammenfassung der Prüfergebnisse

Nach Ansicht der Auditoren werden folgende Prüfergebnisse erzielt.

10.1. Prüfkatalog des ULD

Die Anforderungen werden erfüllt.

10.2. DIN 66399 (2012-10)

Die Anforderungen werden wie folgt erfüllt:

Schutzklasse 3

Die Anforderungen der Schutzklasse 3 werden erfüllt

- bei Nutzung der mobilen Vernichtung uneingeschränkt
- bei Nutzung der stationären Vernichtung, sofern von der Möglichkeit der Begleitung des Auftraggebers bis zur endgültigen Entsorgung der Materialien Gebrauch gemacht wird. Andernfalls wird Schutzklasse 2 der DIN 66399 erreicht.

Sicherheitsstufe 4:

Erreicht wird Sicherheitsstufe 4: Datenträgervernichtung derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich ist

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 wurden nicht bewertet.
- Datenträgertyp P - Informationsdarstellung in Originalgröße (Papier, Film, Druckformen, …)

10.3. 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

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.
- Ergänzend kann/muss der Kunde, je nach eigenem Schutzbedarf, ein Verfahren mit höherer Schutzklasse nutzen (Verfahren 3 oder 4).

11. 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 ohne 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.

11.1 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.

11.2 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.

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-Gütesiegels über keine geschäftliche oder private Beziehung zu der Auftraggeberin zu verfügen.

(Michael J. Erner)

Bad Wörishofen, den 29. Aug. 2014

(Friedrich Abraham)

Hürth, den 30. Aug. 2014