Gesellschaft für Datenschutz und Datensicherung e.V.

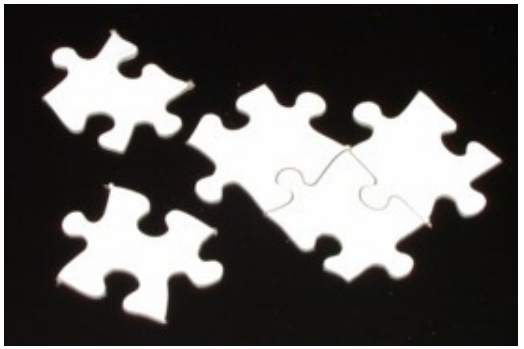
REMONDIS®

Sichere Datenschutzentsorgung
- Stand der Technik -

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

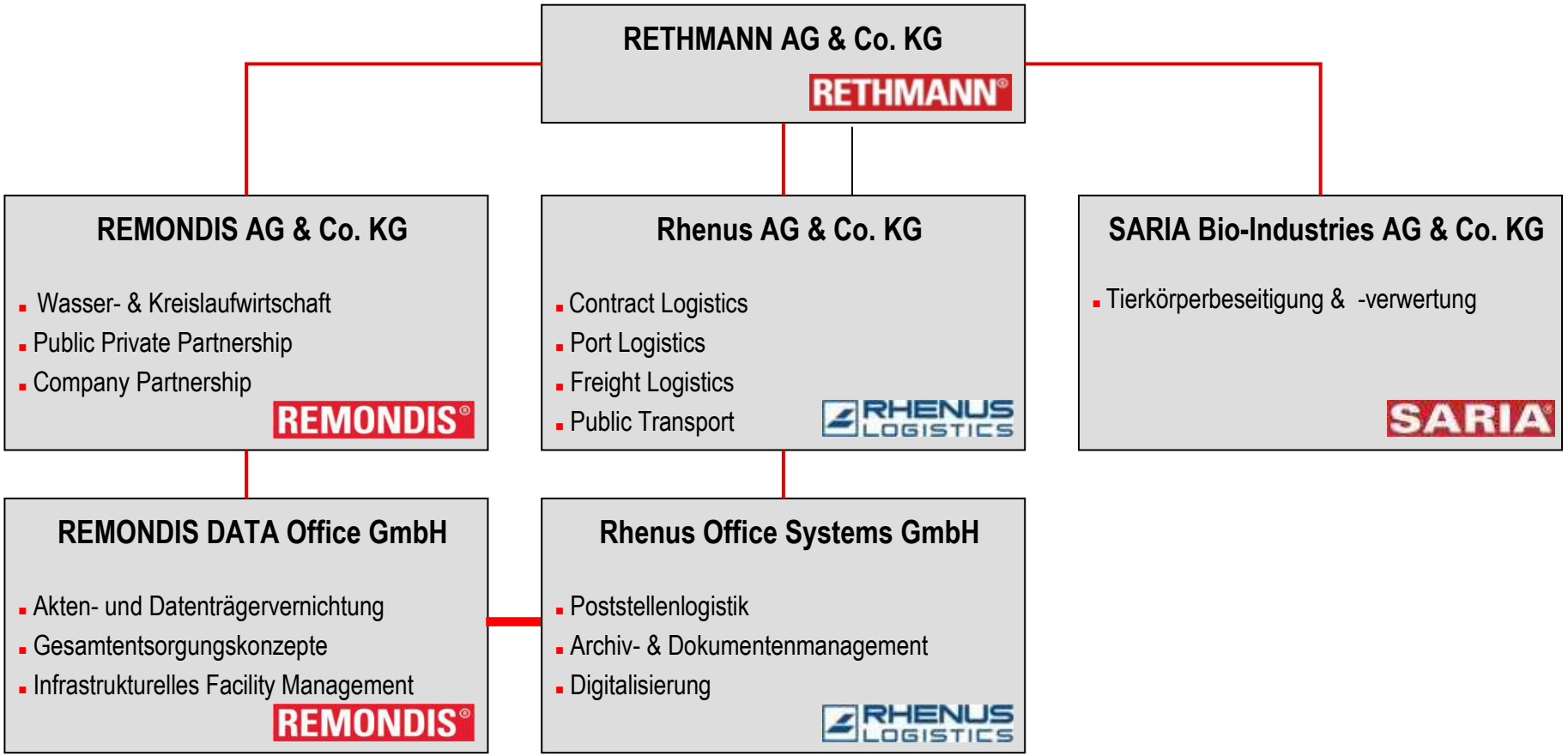
Agenda



- **Vorstellung REMONDIS DATA Office GmbH**
- **Problemstellung:**
  - **Anforderungen des Gesetzgebers und derzeitige Praxis**
- **Ziele:**
  - **Entwicklung eines einheitlichen und verbindlichen Standards**
- **Ergebnis:**
  - **Stand der Technik in der Datenträgervernichtung**
- **weitergehende Überlegungen**
  - **Ausblick auf besondere Lösungen**

Die RETHMANN AG - Systempartner

Sichere Datenschutzentsorgung – Stand der Technik



REMONDIS DATA Office GmbH

Sichere Datenschutzentsorgung – Stand der Technik

- **Die REMONDIS DATA Office GmbH ist eine Tochtergesellschaft der REMONDIS-Gruppe**

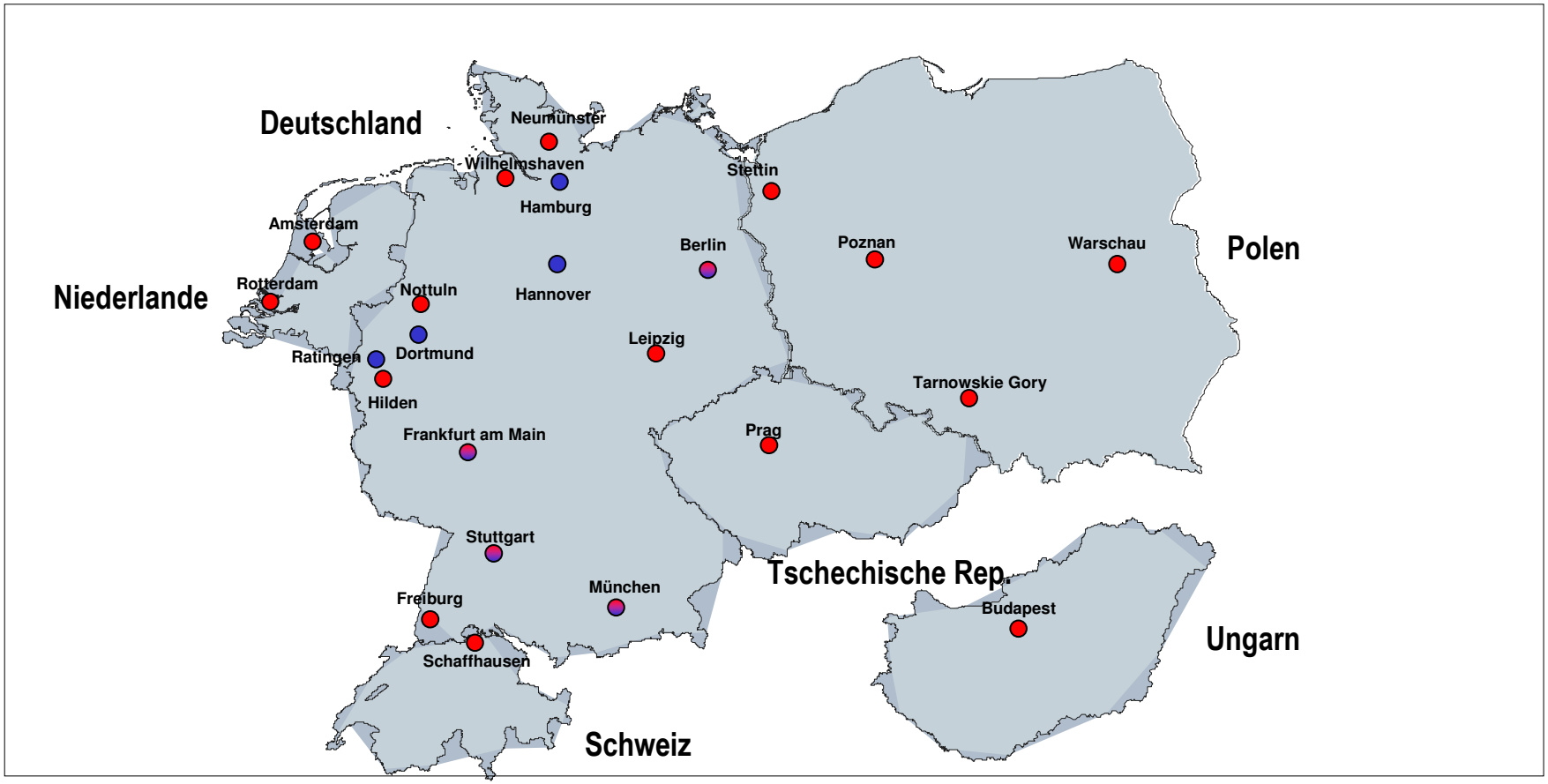
- **Die REMONDIS-Gruppe ist eines der größten Unternehmen der Wasser- und Kreislaufwirtschaft**

- **Der Gesamtkonzern erwirtschaftete mit ca. 35.000 Mitarbeiter einen Umsatz von über 8 Mrd. Euro im Jahr 2007**

- **Die REMONDIS DATA Office GmbH ist ein europaweiter Dienstleister mit Kernkompetenz in den Bereichen der Akten- und Datenträgervernichtung**

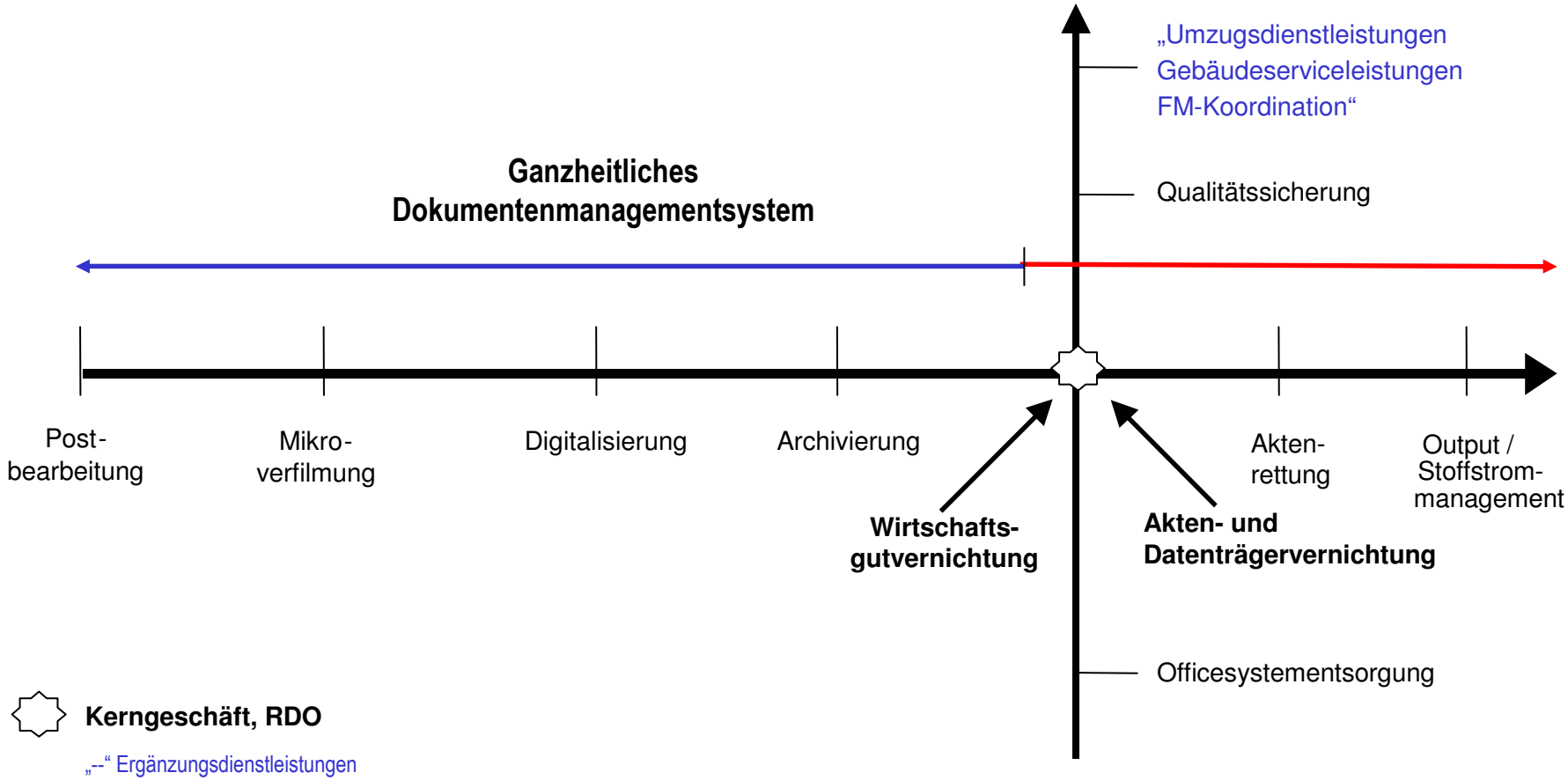
Office Systemdienstleistungen - Standorte

Sichere Datenschutzentsorgung – Stand der Technik



Dienstleistungsspektrum

Sichere Datenschutzentsorgung – Stand der Technik



Beispiel Dresdner Bank

Sichere Datenschutzentsorgung – Stand der Technik

- Postlogistik
  - täglich bis zu 75.000 Sendungen
- Archivierung
  - 100.000 laufende Meter Altarchive
  - 12.000 Vorgänge werden werktäglich aus dem allgemeinen Schriftverkehr der Kontoführung bearbeitet
- Vernichtung und Entsorgung
  - Betreuung von über 200 Standorten der Dresdner Bank
  - Gesamtentsorgungskonzeption und Abwicklung
  - Abfallbilanzierung
- Aktenrettung
  - Wiederherstellung der Akten nach Oderhochwasser
- BNP
  - Teilnutzung der Business Networking Plattform

Dresdner Bank
Die Beraterbank

REMONDIS®

Aktenrettung – Prozessablauf für Ihren Notfallplan

Sichere Datenschutzentsorgung – Stand der Technik

www.aktenrettung.de

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Problem in der Praxis

- ...“ich bekomme eine Vernichtungsbestätigung, und das langt uns“...
- ...“das brauch ich nicht. Mir ist nur der Preis wichtig“...
- ...“ich würde keinem Entsorger meine Ordner geben, die verbrenne ich lieber selber im Heizungskeller“
- Aktueller Ausschreibungstext vom Amt für Vermögen und Bau mit dem einzigen Bezug zu Anforderungen an die Aktenvernichtung:

...„die Anforderungen des BDSG sind einzuhalten“... ?

Was meinen die damit konkret?

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Problemstellung

Welche Anforderungen stellt der Gesetzgeber ?

- **EU-Rahmenrichtlinie 95/46 EG fordert die Einhaltung des aktuellen „Standes der Technik“**
- **Das Bundesdatenschutzgesetz schreibt die Eignung der technischen und organisatorischen Maßnahmen vor**
- **Beide Formulierungen lassen bewusst einen großen Spielraum für Interpretationen und Auslegung**

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS

Problemstellung

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stellt fest:

- **„Der Gesetzgeber hat darauf verzichtet, bestimmte einzelne Maßnahmen vorzuschreiben, sondern verlangt nur, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Gesetzes zu gewährleisten.“**

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Referat I Grundsatzangelegenheiten, nicht-öffentlicher Bereich, Öffentlichkeitsarbeit Aktenzeichen: I - 103 II #1741

- **Ist-Situation im Markt stellt sich als wahrer „Flickenteppich“ von Einzellösungen dar**

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Anforderungen

1. **Schutzzweck (Brisanz der Daten)**
2. **Verhältnismäßigkeit (Kosten)**
3. **Vorschriften des Gesetzes (z.B. Anlage §9, EG-Richtlinie)**

BDSG §9:

- **...„**haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

BDSG § 11:

- ...“der Auftraggeber ist für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich“...

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Ziele

- **Der GDD-Arbeitskreis „Stand der Technik“ nimmt diese Situation auf, und macht sich zur Aufgabe einen einheitlichen Standard für die Datenträgervernichtung zu formulieren**

- **Dieser Standard soll sich an den gesetzlichen Regelungen orientieren, und Interpretationsspielräume mit konkreten, praxisorientierten Umsetzungen und Vorschlägen ausfüllen**

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Der GDD-Arbeitskreis

- **Der GDD-Arbeitskreis besteht aus Vertretern namhafter Unternehmen der Industrie, Finanzwirtschaft und dem Bundesamt für Informationstechnik**

- **Das ersten Zusammentreffen des Arbeitskreises fand am 30.11. 2006 in Main-Metropole Frankfurt statt. Seit dem ist eine regelmäßige Zusammenarbeit organisiert**

- **Anspruch des Workshops ist die fortlaufende Ausarbeitung eines europaweit-einheitlichen Datenschutzstandards**

- **Die Checkliste, als Ergebnis, soll Datenschutzverantwortlichen helfen, an den gesetzlichen Vorschriften orientiert, prozessorientierte Datenschutzkonzepte zu erstellen**

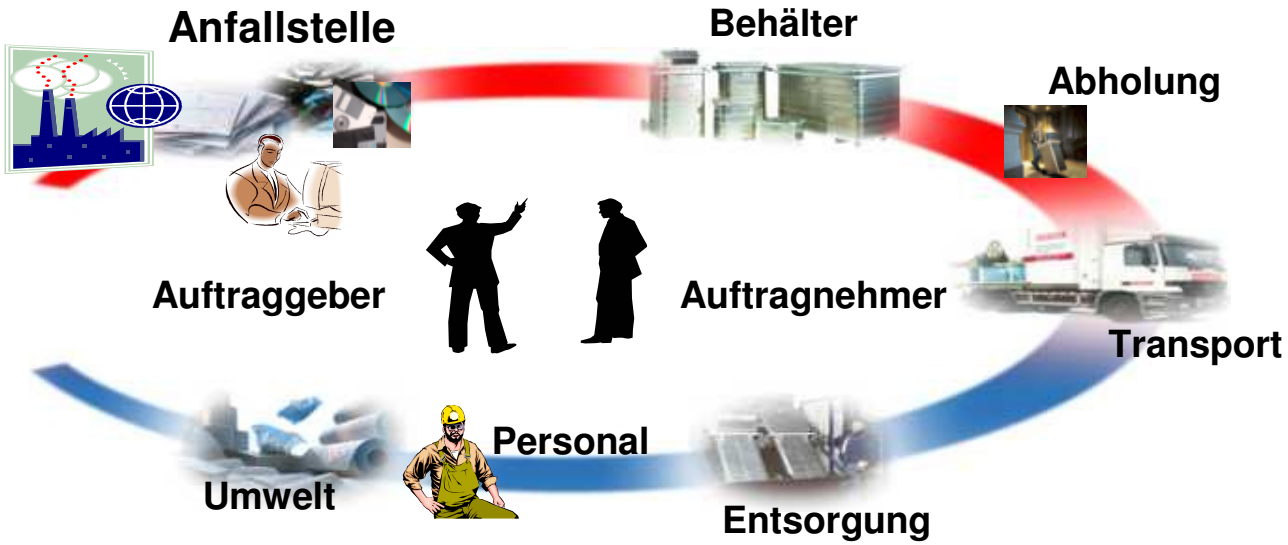
Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Datenschutz als Prozesskette

Sichere Datenschutzentsorgung – Stand der Technik

Datenschutz ist als ganzheitlicher Prozess zu verstehen und im Rahmen der sicheren Datenträgervernichtung auf folgende Punkte hin zu untersuchen:



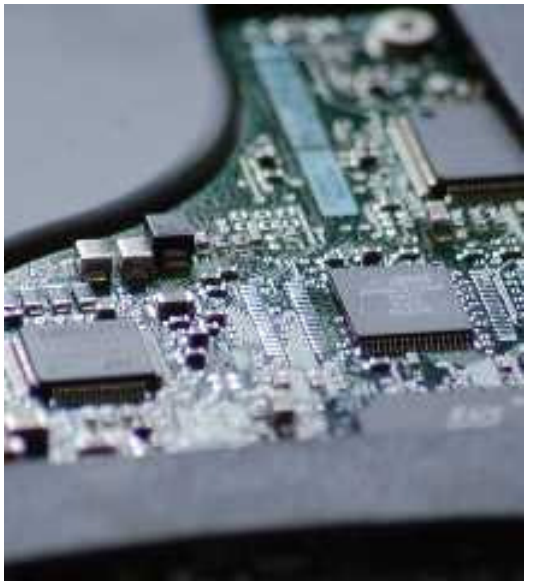
Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Datenschutz als Prozess

Sichere Datenschutzentsorgung – Stand der Technik

- **Prozessausrichtung ist auch ein besonderer Schwerpunkt der Checkliste „Stand der Technik“. Als Beispielfragen sind hier zu nennen:**
- Sind unternehmensinterne Zuständigkeiten/Verantwortlichkeiten für einzelne Prozessstufen (interne Sammlung, Lagerung, Transport, etc.) geregelt?
- Während des Transports ist technisch sichergestellt, dass die Fahrer oder Dritte keinen Zugriff auf die in den Behältern enthaltenen Daten haben können (Schließsystem und Schlüsselverteilung)
- Ist eine Videoüberwachung mit Aufzeichnung oder ein Behälterverfolgungssystem im Sicherheitsbereich vorhanden?



- Beispielhaft Überlegungen zur Frage
  - Was ist ein Sicherheitsbehälter?

Schließart, Sturzprüfung, Bauart, Brandschutz, Säcke möglich?, RAL-Prüfung, Schlüsselverteilung, geschützte Schließung/ Mister Minit-Prüfung...

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Schutzniveau

Sichere Datenschutzentsorgung – Stand der Technik

- **Zuordnung der Sicherheitsstufen DIN 32757-1 zu den Schutzklassen:**

Zuordnung DIN zu Schutzklasssen	DIN 32757-1 Sicherheitsstufe 1	DIN 32757-1 Sicherheitsstufe 2	DIN 32757-1 Sicherheitsstufe 3	DIN 32757-1 Sicherheitsstufe 4	DIN 32757-1 Sicherheitsstufe 5
Schutzklasse 1 Geringes Risiko	X	X			
Schutzklasse 2 Mittleres Risiko		X	X		
Schutzklasse 3 Hohes Risiko			X	X	X

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Schutzniveau

Sichere Datenschutzentsorgung – Stand der Technik

Klassifizierung von digitalen Datenträgern gemäß BSI

	niedrige Sicherheit	mittlere Sicherheit	hohe Sicherheit
Vernichten und Löschen von Festplatten	Durchbohren der Festplatten	Verformen der Festplatten	Shreddern der Festplatten Partikel max. 1000 mm² Löschen der Festplatten mit geeignetem Löschgeräten
Vernichten von optischen Datenträgern (CD, DVD)	Durchtrennen der Datenträger	Shreddern der Datenträger Partikel max. 200 mm²	Shreddern der Datenträger Partikel max. 10 mm² (Diagonale max. 5 mm)

In ihrer Wertigkeit sind die Klassen niedrig, mittel und hoch etwa mit den Definitionen der Sicherheitsstufen 3, 4 und 5 der DIN 32757 vergleichbar. Dabei ist zu beachten, dass bei den digitalen Datenträgern – im Unterschied zu Papierdokumenten – eine Rekonstruktion von Daten auch bei niedriger Sicherheit schon ein hohes Maß an Kenntnissen und Ausstattung verlangt.

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Ergebnis

Sichere Datenschutzentsorgung – Stand der Technik

- **Die ausführliche Checkliste gibt der Verantwortlichen Stelle einen Handlungsleitfaden bei der Umsetzung einer sicheren Datenentsorgung nach dem Stand der Technik.**

- **Der GDD-Arbeitskreis stellt die Checkliste „Stand der Technik“ allen Interessierten als Printmedium zur Verfügung.**

  https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenschutzgerechte-datentragerentsorgung-nach-dem-stand-der-technik

- **Darüber hinaus steht auch eine praxisorientierte Softwarelösung zur einfachen Umsetzung als Demo-Version bereit. (Fa. 2B Advice)**

Gesellschaft für Datenschutz und Datensicherung e.V.

REMONDIS®

Reichweite der Checkliste

Die Checkliste wurde so konzipiert, dass aktuelle und zukünftige Normierungen inhaltlich berücksichtigt wurden und werden.

Gegenwärtig gültig:

- **BDSG, LDSG´s, öffentliches Recht (z.B. StGB) usw.**

In Voraussicht:

- **Die europäische Norm prEN 15713**
- **Die Neuregelung der einschlägigen DIN-Norm**

Technikentwicklung und spezielle Themen der Vernichtung

1. **Mobile Hochsicherheitslösungen für z.B. Patientendaten (§203 StGB, LKHG Ba-Wü)**

2. **Festplattenvernichtung aber auch Speicherkarten, Handys**

Problemstellung 1: Patientendaten

- Patientengeheimnis § 203 Strafgesetzbuch
- **Pflicht des Arztes** zur datenschutzgerechten Vernichtung
- gemäß § 35 des Bundesdatenschutzgesetzes bzw. z.B. § 28 des Landesdatenschutzgesetzes Schleswig-Holstein und anderer LDSG
- Sicherstellung dass keine unbefugte Offenbarung im Sinne des § 203 Strafgesetzbuch an die Mitarbeiter des Entsorgungsunternehmens erfolgt

➢ Offenbarungs**möglichkeit** besteht beim Abkippen, beim offenen Förderband, auf der Sortierstrecke → Ausschluss stationärer Anlagen

- Durch Dritte nur möglich wenn das Unternehmen ausschließen kann, dass eine Einsichtnahme in die Unterlagen **überhaupt möglich ist**, weil die im Beisein des Arztes in Behältnissen verschlossenen Datenträger ohne weitere **Kenntnisnahmemöglichkeit** unmittelbar der Vernichtung zugeführt werden.

Rechtsprechung - Einwilligung

- Erforderlich ist bei Outsourcingmaßnahmen stets eine **ausdrückliche Einwilligung** (§4a BDSG, §12 LDSG SH, § 50 LKHG Ba-Wü).
- Zu beachten ist jedoch eine restriktive Rechtsprechung in Bezug auf die Einwilligung in die Offenbarung von medizinische Daten.
- **Mutmaßliche oder konkludente** (stillschweigend erteilte) Einwilligungen scheiden bei systematischen Beauftragungen schon deshalb aus, weil die Patienten ausdrücklich gefragt werden könnten.
- So meinte z. B. das Oberlandesgericht Düsseldorf: "Von einer - mutmaßlichen oder sogar konkludenten - rechtfertigenden Einwilligung der Geheimnisgeschützten, also der betroffenen Patienten, kann nicht ausgegangen werden. **Patienten erwarten nicht, dass ihre oft hoch sensiblen Daten [...] ‚umherkutschiert und von - aus der Sicht der Patienten - beliebigen Dritten eingelesen, verfilmt, kopiert usw. werden. „**

Durchführung und Kontrolle bei der Auftragsvernichtung

- unter dem "berufsmäßig tätigen Gehilfen„(des Arztes) des § 203 Abs. 3 StGB ist nur derjenige zu verstehen, der innerhalb des beruflichen Wirkungskreises eines Schweigepflichtigen eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit ausübt, welche die Kenntnis fremder Geheimnisse mit sich bringt.
- Z.B. Arzt selbst, Mitarbeiter, angestellter Hausmeister in der Klinik → KEIN Externer !
- Vgl: Landeskrankenhausgesetz Baden –Württemberg LKHG:

§ 48
Verarbeitung im Auftrag

(1) Patientendaten sind in dem Krankenhaus selbst oder im Auftrag des Krankenhauses durch ein anderes Krankenhaus zu verarbeiten.

- Trotzdem Umgehungsversuche: Keine Dienstleistung sondern Anmietung von Personal

Problemstellung 2: Festplatten

Digitale Datenlöschung

Formatieren

Überschreiben

Einsatz von Spezialsoftware

Magnetische Datenlöschung

Einwirkung eines Magneten

Sicherheit ?

Sind die Daten wirklich gelöscht?

Wie kann der Kunde die Datenlöschung kontrollieren bzw. nachvollziehen?

Ist das Risiko der Datenrekonstruktion wirklich ausgeschlossen?

Steht der Aufwand im Verhältnis zur Sicherheit?

Festplattenvernichtung durch (Mobiles-) Schreddern

Shreddern - die einzig sichere Methode!

- **Keine Datenrekonstruierung möglich!**
- **Nachweisliche und nachvollziehbare Vernichtung**
- **Vernichtung nach Sicherheitsstufe 5, gemäß Einordnung BSI!**

Lösungsansatz

Sichere Datenschutzentsorgung – Stand der Technik

- Schreddern vor Ort beim Kunden mit Aufzeichnung und persönlicher Kontrollmöglichkeit
- Berührungsloses Schreddern ohne Zugriffsmöglichkeit

- Austauschsystem: Es wird garantiert, dass kein Dritter Zugriffsmöglichkeit hat
- **Mobilschreddersystem:**
  Wir garantieren, daß der Zweite (der Dienstleister) keine Zugriffsmöglichkeit hat (z.B. Patientendaten, Forschungsdaten, Pharmaunterlagen, Personalakten, ...)
- **→ Sie müssen uns nicht vertrauen – Misstrauen Sie bitte!**
- Momentan: laufende Einführung der Technik,
  Zertifizierung, dass damit die Anforderungen für Patientendaten umgesetzt werden

Danke für Ihre Aufmerksamkeit

Ihr Ansprechpartner

Stefan Burkart

Mitglied des Arbeitskreises der GDD

„Datenschutzgerechte Datenträgerentsorgung“

REMONDIS DATA Office GmbH

Telefon: 0711/ 351 305-50

Fax: 0711/ 351 305-29

stefan.burkart@remondis.de