



33. Neue Technologien und Datenschutz – Konferenz für Mitarbeitervertretungen

9. bis 11. November 2021 in München

Löschen und Sperren von Daten im Betriebs- und Personalratsbüro

Lösch- und Sperrkonzept

1 Einleitung / Gliederung



- 1 Einleitung
- 2 Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch den Betriebsrat
- 3 Begriffsklärungen: Löschen und Sperren
- 4 Technische Umsetzung
- 5 Pflichten zum Löschen und Sperren
- 6 Entwicklung eines Lösch- und Sperrkonzepts
- 7 Zusammenfassung und Fazit



Art. 88 Abs. 1 DSGVO

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke (...) der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von (...) durch Kollektivvereinbarungen festgelegten Pflichten, (...) der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, (...) sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte (...) vorsehen.



§ 26 Abs. 1 BDSG

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies (...) zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.



Erlaubnistatsbestände für die Verarbeitung personenbezogener Daten durch Betriebs- und Personalräte

- Gesetze
- Tarifverträge
- Betriebs-/Dienstvereinbarungen



Unrealistische Grundannahme

Es werden

- von *einem* Verantwortlichen
- die Daten *einer* betroffenen Person
- auf *einem* Datenträger

verarbeitet.

⇒ Was bedeuten die Begriffe *Löschen* und *Sperren* in einem realistischen Kontext?



Löschen - Wortgeschichte

1) „erlöschen“ 2) „löschen“ (8. Jh.)

mittelhochdeutsch *(er)leschen*, althochdeutsch *(ir)lescan*,
lesken, altsächsisch *leskan*, altfriesisch *bileska*

Herkunft unbekannt

Gleichlautend: lösen

„Frachtgüter ausladen“ *fachsprachlich* (18. Jh.)

niederdeutsch, neuniederländisch *lossen* „lösen“, regional
lessen

3 Begriffsklärungen - Sprachlich



Wiedergabe mit freundlicher Genehmigung von André Poloczek



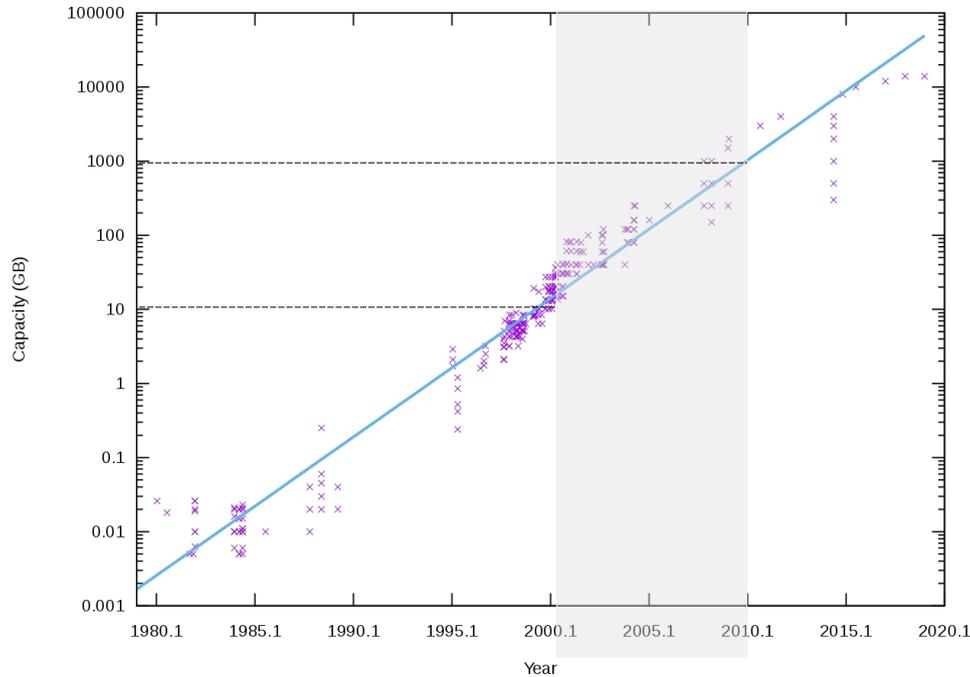
löschen

neuere Bedeutungen:
beseitigen, tilgen

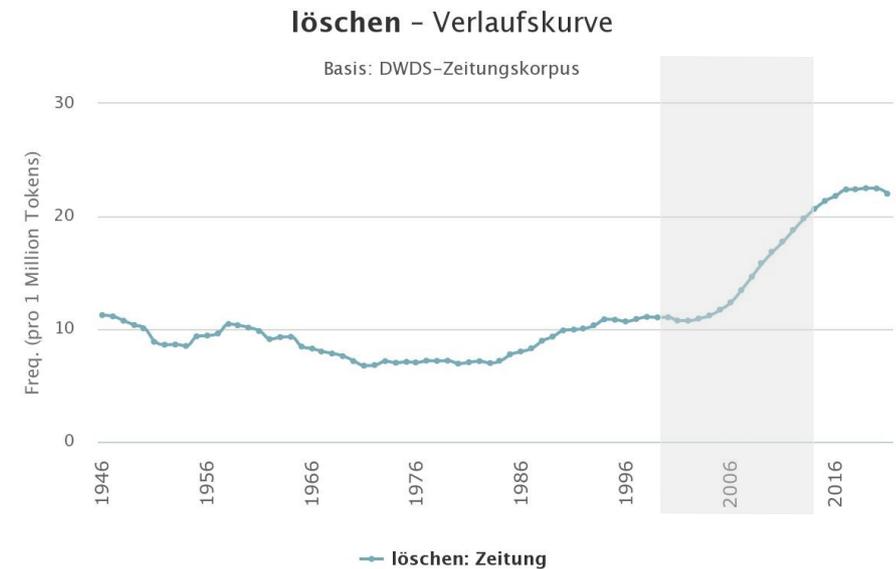
beispielsweise

- Text von einer Tafel
- eine Eintragung
- eine Firma aus dem Handelsregister
- Daten, Dateien

3 Begriffsklärungen - Sprachlich



Entwicklung der Speicherkapazität von Festplatten
Quelle: wikipedia.de, public domain



Wortvorkommen in deutschsprachigen Zeitungen
Quelle: Digitales Wörterbuch der deutschen Sprache, dwds.de, 16.10.2021



löschen

Typische Verbindungen

Quelle:  DWDS-Wortprofil

Brand Datei Durst
Feuer Feuerwehr
Feuerwehrleute
Feuerwehrmann
Flamme ablöschen
auslöschen

Quelle: Digitales Wörterbuch der deutschen Sprache, dwds.de, 16.10.2021



Sperren - Wortgeschichte

(11. Jh.)

mittelhochdeutsch *sperren*, althochdeutsch *sperren*,
altenglisch *gesparrian* „schließen“, altnordisch *sperra*

„Balken aufrichten (wie die Sparren auf dem Dach)“

Bedeutungen

- mit einem Balken, Querriegel usw. sperren
- Sparren, Balken aufrichten



sperren

Bedeutungen nach Online-Duden

1)den Zugang, Durchgang, die Zufahrt, Durchfahrt verbieten, verwehren, [mittels einer Barriere o. Ä.] unmöglich machen; aufgrund seiner Lage bewirken, dass der Zugang, die Zufahrt zu etwas nicht möglich ist; versperren

2)unterbinden

3)die normale Abwicklung, die Benutzung von etwas durch bestimmte Maßnahmen zu verhindern suchen, unmöglich machen

Quelle: <https://www.duden.de/rechtschreibung/sperren>, 17.10.2021



Folgerungen

Zugriff auf gesperrte Daten bleibt möglich.

Zugriff auf gelöschte Daten ist unmöglich.



Art. 4 Nr. 2 DSGVO

„Verarbeitung“ [bezeichnet] (...) die Einschränkung, das Löschen oder die Vernichtung

Interpretation 1

Löschen ist weniger als Vernichten.

Vgl. § 3 Abs. 4 Nr. 5 BDSG alte Fassung: „unkenntlich machen“

Interpretation 2

Vernichten bezieht sich nur auf Gegenstände.

⇒ *Löschen ist mehr als Einschränken.*



Verhältnismäßigkeits-Theorie

- Löschen errichtet sehr hohe Hürden für den Zugriff auf Daten.
- Zugriff auf gelöschte Daten ist nur noch mit unverhältnismäßig hohem technischem Aufwand möglich.
- Daten können prinzipiell wiederhergestellt werden.

Irreversibilitätstheorie

- Löschen sorgt dafür, dass Daten unter keinen Umständen wiederherstellbar sind.
- Der Löschvorgang ist für jedermann unumkehrbar (= irreversibel).
- Diese Theorie wird in der Literatur bevorzugt vertreten.



Baustein CON.6 Löschen und Vernichten

IT-Grundschutz-Kompendium des
Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Gewöhnliche Löschvorgänge über die Funktionen des Betriebssystems bewirken in der Regel kein sicheres Löschen der Informationen, das verhindert, dass die Daten wieder rekonstruiert werden können. Um Informationen sicher zu löschen, bedarf es daher spezieller Verfahren.

⇒ Aus technischer Sicht wird die Irreversibilitätstheorie vertreten.



Definitionen

Löschen ist das Beseitigen von Daten in einer Art und Weise, dass ein Zugriff auf die Daten sowohl für Personen als auch für Maschinen dauerhaft und unwiederbringlich unmöglich gemacht wird.

Sperren ist das Erschweren des Zugriffs auf Daten in einer Art und Weise, dass der Zugriff auf die Daten auf üblichem Wege unmöglich gemacht wird und nur Personen oder Maschinen mit besonderen Berechtigungen und gegebenenfalls unter Verwendung besonderer technischer Verfahren auf die Daten zugreifen können.



Klassische Festplatte

| Sektor 1 | | Sektor 2 | | Sektor 3 | | Sektor 4 | | ... | |
|----------|-------|----------|-------|----------|-------|----------|-------|-----|-----|
| ID | Daten | ID | Daten | ID | Daten | ID | Daten | ... | ... |

„Inhaltsverzeichnis“ des jeweiligen Sektors

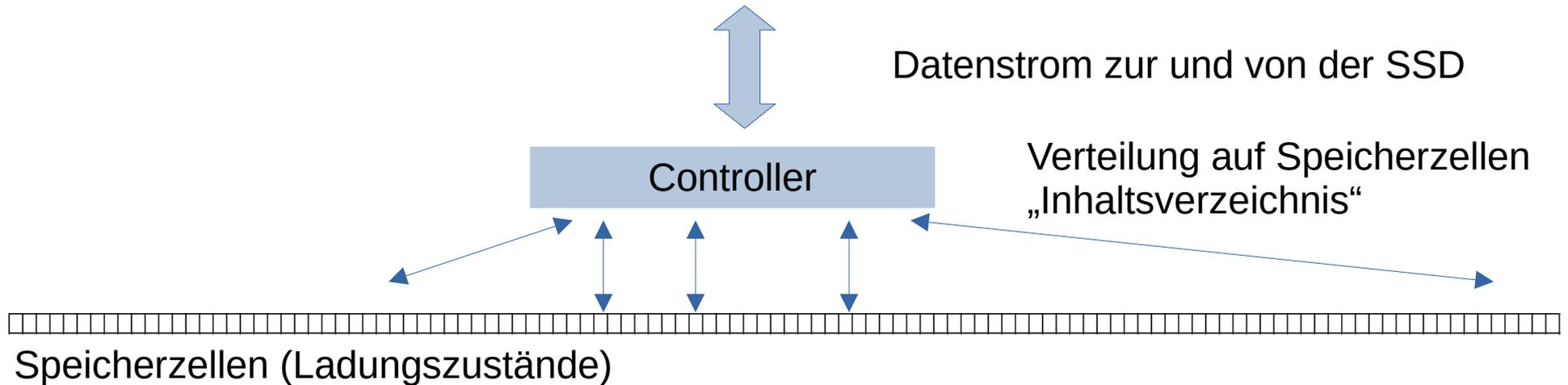
Binärdaten (Magnetisierung)

Übliches Löschen entfernt nur die Einträge aus den Inhaltsverzeichnissen. Die Binärdaten bleiben erhalten.

Abhilfe: Überschreiben der Datenbereiche mit Hilfe spezieller Programme.



Solid State Drive (SSD)



Der Controller verteilt die Daten selbständig auf die Speicherzellen.

Übliches Löschen entfernt nur die Einträge aus dem Controller. Die Binärdaten der Speicherzellen bleiben erhalten.



Solid State Drive (SSD)

Abhilfe: Nutzen von Dienstprogrammen der SSDs.

Wenn diese Programme nicht fehlerfrei arbeiten, bleibt eine Rekonstruktion von vermeintlich gelöschten Daten mit sehr großem Aufwand eventuell möglich.

4 Technische Umsetzung



https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitser 170% ☆ Suchen

Das BSI

Themen

IT-Sicherheitsvorfall

Karriere

Physikalische Vernichtung

Wenn Sie eine Festplatte nicht überschreiben wollen oder wegen eines Defekts nicht können, so sollten Sie die Festplatte physisch beschädigen oder zerstören. Das gilt auch für Speichermedien wie CD/DVDs oder USB-Sticks.

Wenn Sie schon immer mal eine Festplatte von innen sehen wollten, wäre dies genau der richtige Zeitpunkt. Richten Sie am Objekt möglichst maximalen Schaden an. Seien Sie dabei jedoch vorsichtig und ziehen Sie sich entsprechende Schutzkleidung an.

Schon das Verbiegen der Scheiben führt dazu, dass die gängigen Methoden der Datenrettung nicht mehr anwendbar sind.

Bitte beachten Sie, dass einige Festplattenhersteller Glasscheiben verwendet haben und CDs bzw. DVDs sehr heftig zersplittern können. Bei SSD-Festplatten oder USB-Sticks müssen Sie die einzelnen Speicherchips beschädigen.

abgerufen am 17.10.2021



Datenbanken

| gesperrt | gelöscht | Name | Vorname | Tarif-Gruppe | Tarif-Stufe | Wochenstunden | Schwerbehinderung | usw. |
|----------|----------|---------|---------|--------------|-------------|---------------|-------------------|------|
| x | | Adam | Heinz | 3 | 5 | 38,5 | nein | |
| | x | Breiter | Emma | 4 | 2 | 40 | nein | |
| | | ... | | | | | | |

↑ Lösch-Flag ersetzt eventuell das tatsächliche Tilgen der Daten aus der Datenbank

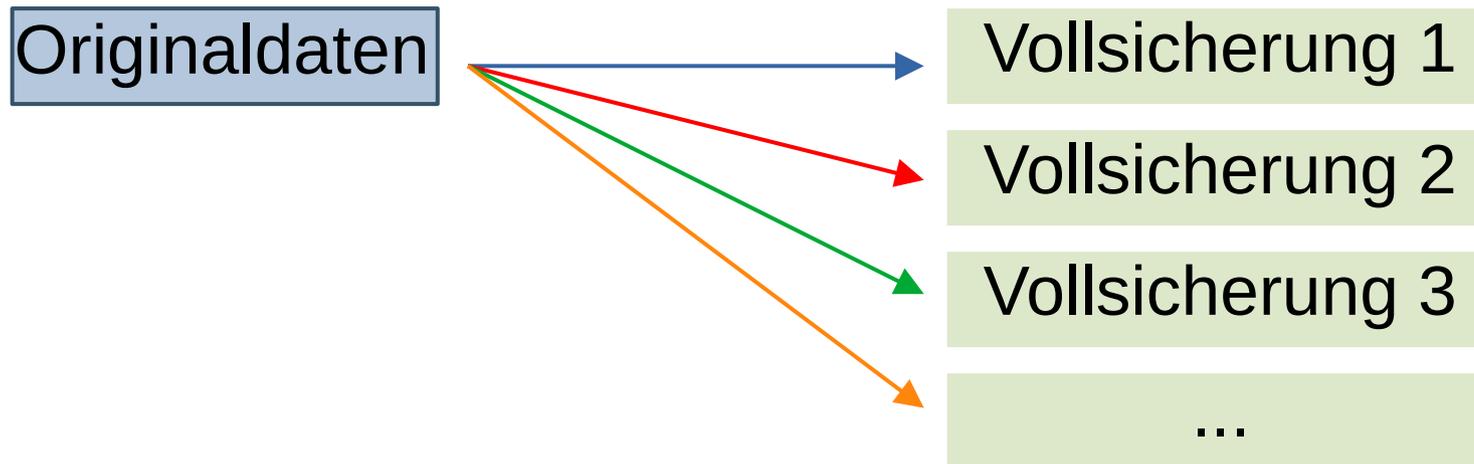
Problem:

Eine programmatische Zugriffssperre lässt sich programmatisch umgehen, Daten bleiben wiederherstellbar.

Selbst bei Löschung der Tabelleneinträge können Daten – an unbekannter Stelle – auf dem Speichermedium verbleiben.



Datensicherung

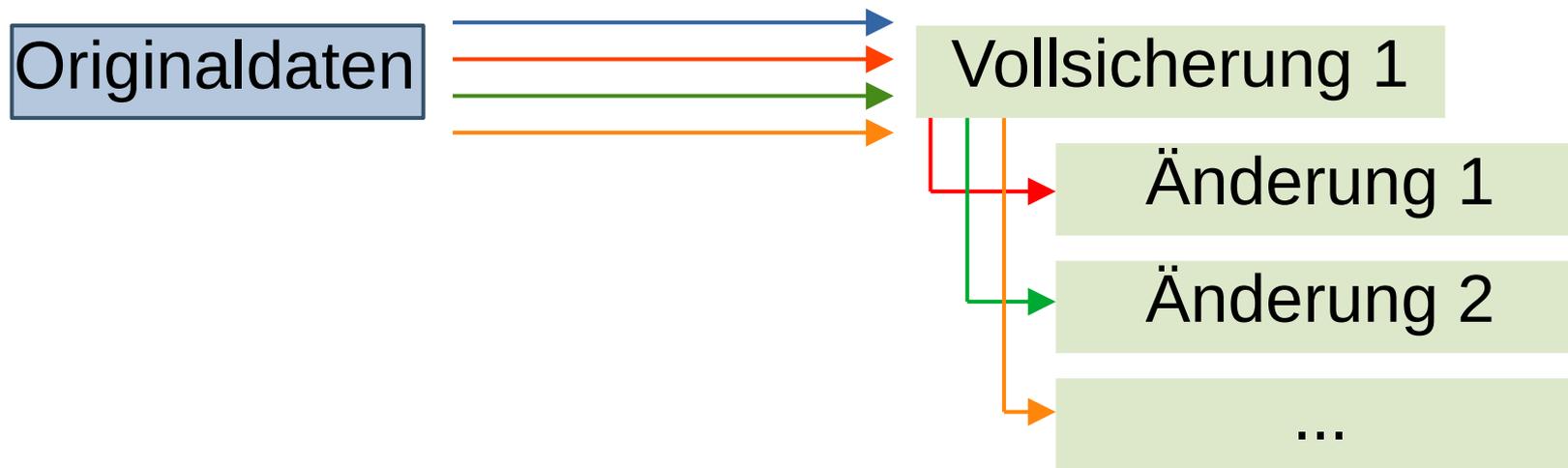


Prinzip der Vollsicherung:

In regelmäßigen zeitlichen Abständen wird der gesamte Datenbestand gesichert.



Datensicherung

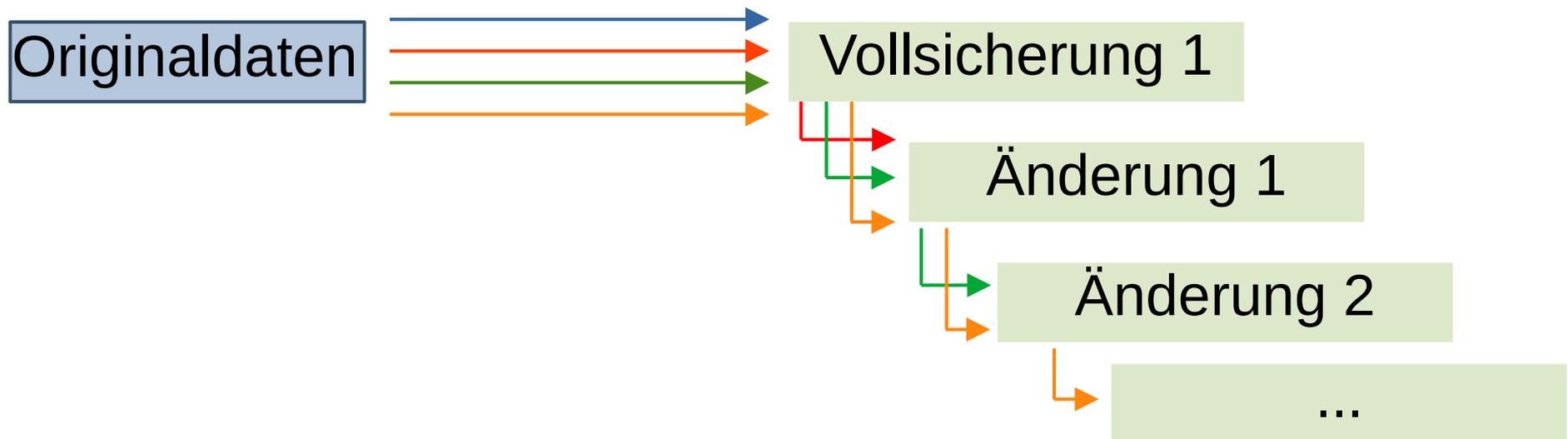


Prinzip der differentiellen Sicherung:

In regelmäßigen zeitlichen Abständen wird der gesamte Datenbestand gesichert, darüber hinaus in kürzeren Abständen die Änderungen gegenüber der letzten *Vollsicherung*.



Datensicherung



Prinzip der inkrementellen Sicherung:

In regelmäßigen zeitlichen Abständen wird der gesamte Datenbestand gesichert, darüber hinaus in kürzeren Abständen die Änderungen gegenüber der letzten *Teilsicherung*.

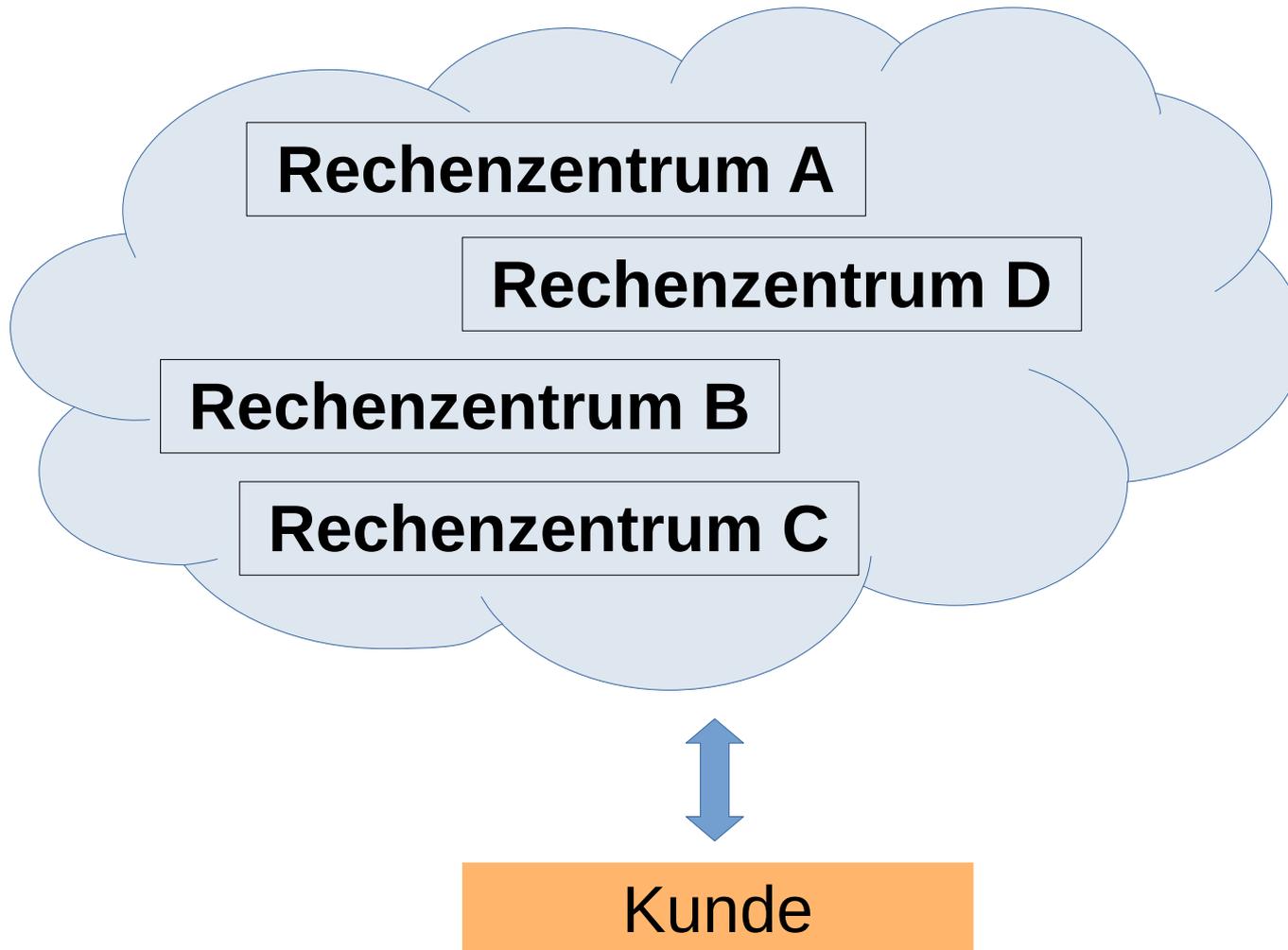


Datensicherung

- Wie vermeidet man unbeabsichtigtes Einspielen von Sicherungen?
- Wie stellt man sicher, dass eigentlich gelöschte Daten durch Einspielen einer Sicherung nicht unbeabsichtigt wiederhergestellt werden?
- Wann sind gelöschte Daten auch aus der ältesten vorhandenen Sicherung getilgt?



Cloud-Systeme



Fragen

Verteilung der Daten?

Welche Speichermedien?

Sicherungsstrategie?

Wann sind „gelöschte“ Daten nicht mehr wiederherstellbar?



Fazit

- Unumkehrbares Tilgen von Daten ist abhängig von
 - Speichermedien
 - Dateisystemen
 - Sicherungskonzepten
 - Verwendung von Cloud-Anwendungen.
- Irreversibles Löschen ist faktisch ein rein theoretisches Konstrukt.
- Löschen ist oft ein mehr oder weniger gut umgesetztes Sperren, weil eine Wiederherstellung nicht restlos ausgeschlossen werden kann.



Löschpflicht

Art. 17 Abs. 1 DSGVO

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern (...)

Die Löschpflicht wird ausgelöst

- von der betroffenen Person und
- unabhängig davon vom Vorliegen der in der Verordnung angegebenen Voraussetzungen.



Löschpflicht

Art. 17 Abs. 1 DSGVO – Voraussetzungen

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig.
- b) Die betroffene Person widerruft ihre Einwilligung.
- c) Die betroffene Person legt Widerspruch ein.
- d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- e) Europäisches oder nationales Recht schreibt die Löschung vor.
- f) Die personenbezogenen Daten wurden in Bezug auf Dienste der Informationsgesellschaft erhoben.



Löschpflicht

Art. 17 Abs. 3 DSGVO – Ausnahmen

Wenn die Verarbeitung erforderlich ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, entfällt die Löschpflicht.

Es ist vorstellbar, dass der Betriebs-/Personalrat die Daten zur Verfolgung eigener Rechtsansprüche benötigt, während die betroffene Person die Löschung verlangt.



Sperrpflicht

Art. 18 Abs. 1 DSGVO –

Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen (...)

Die Sperrpflicht wird allein von der betroffenen Person ausgelöst.

Einschränkung der Verarbeitung = Sperren

§ 3 Abs. 4 Nr. 4 BDSG alte Fassung: „Sperren [ist] das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken“.



Sperrpflicht

Art. 18 Abs. 1 DSGVO – Voraussetzungen

- a) Die betroffene Person bestreitet die Richtigkeit der Daten.
- b) Die Verarbeitung ist unrechtmäßig, aber die betroffene Person verlangt statt der Löschung, dass die Nutzung der Daten eingeschränkt wird.
- c) Die betroffene Person hingegen benötigt die Daten noch, um Rechtsansprüche zu verteidigen, obwohl der Zweck des Verantwortlichen erfüllt/weggefallen ist.
- d) Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt, und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen überwiegen.



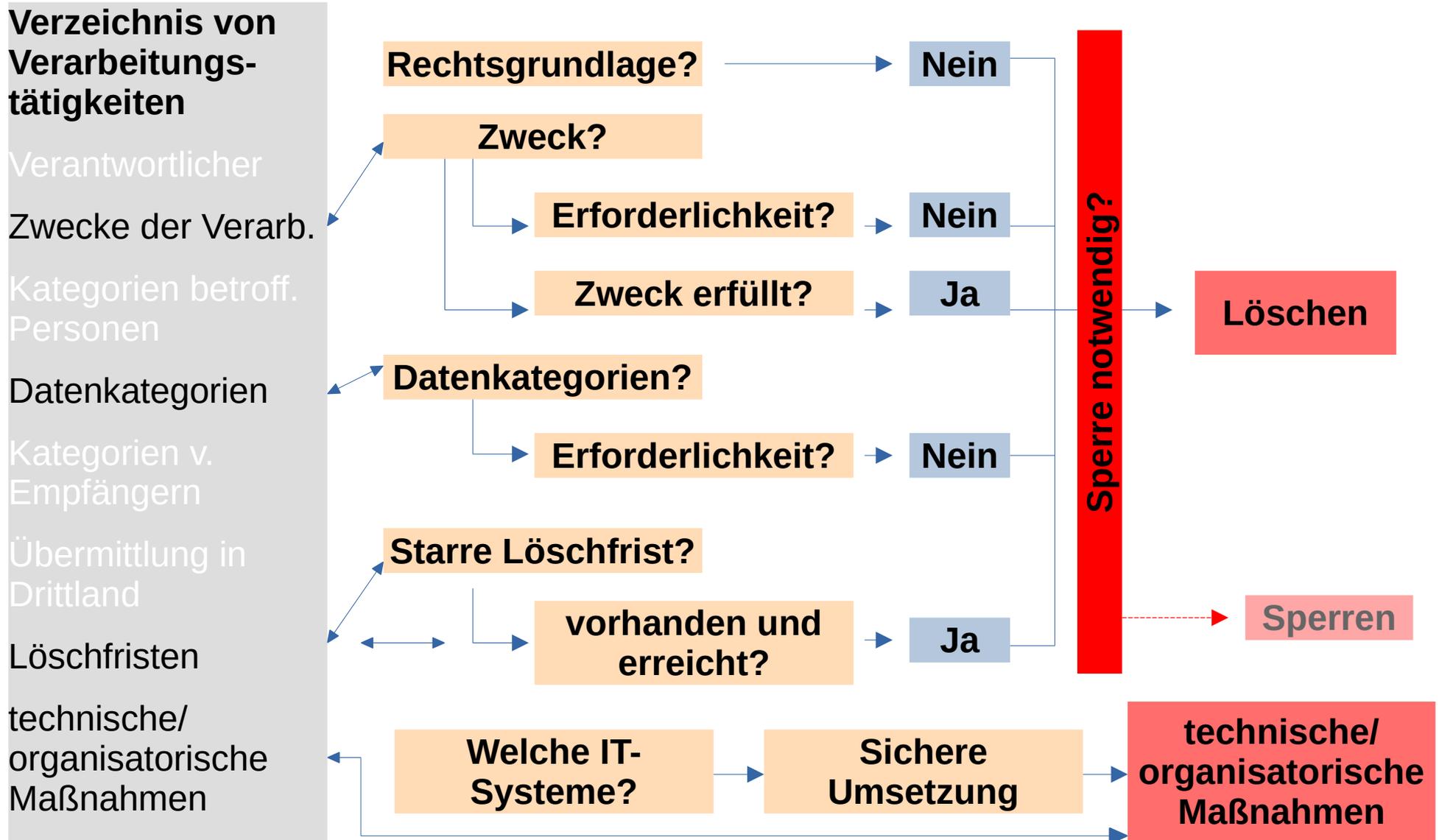
Art. 18 Abs. 2 DSGVO – Folgen der Sperrung

Verarbeitung der Daten ist nur noch zulässig unter vier Voraussetzungen:

1. Einwilligung der betroffenen Person,
2. Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
3. Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
4. wichtiges öffentliches, europäisches oder nationales Interesse.

Folge für Betriebsräte: Sperre ist quasi Verarbeitungsverbot.

6 Lösch- und Sperrkonzept





- Die Begriffe „Löschen“ und „Sperrern“ sind unbestimmt und bedürfen der Auslegung.
- Löschen sollte das unwiederbringliche Tilgen von Daten beschreiben.
- Sperrern sollte beschreiben, dass der Zugriff auf Daten auf üblichem Wege unterbunden wird. Die Daten bleiben aber vorhanden.
- Die Umsetzung des oben genannten Löschbegriffs ist technisch nur unter großen Schwierigkeiten zu leisten. So müssen beispielsweise Speicherbereiche und Sicherungskopien überschrieben werden.



- Löschen ist eine Verarbeitung personenbezogener Daten und muss daher rechtmäßig sein. Gesperrte Daten dürfen nicht gelöscht werden.
- Viele verschiedene Faktoren fließen in ein Lösch- und Sperrkonzept ein, zum Beispiel Verwendungszwecke, Datenkategorien, genutzte Hard- und Software.
- Zwischen dem Verzeichnis der Verarbeitungstätigkeiten und dem Lösch- und Sperrkonzept bestehen gegenseitige Abhängigkeiten.



- Die Entwicklung eines tragfähigen Lösch- und Sperrkonzepts erfordert viel Zeit und Arbeit.
- Offene Fragen:
 - Wie kann die Verarbeitung von personenbezogenen Daten beim Gremium minimiert werden?
 - Ist überwiegend ein Zugriff auf die Systeme des Arbeitgebers möglich, geregelt durch Betriebs-/Dienstvereinbarung?
- Vorteil: Gremium bestimmt bei der Etablierung eines Konzepts mit, ist aber von dessen Durchführung befreit.



Vielen Dank für die Aufmerksamkeit!

Kontakt:

Dr.-Ing. Jan Wiznerowicz

Am Kirchdeich 4

28259 Bremen

Tel.: 04 21 – 98 88 53 38

E-Mail: jan.wiznerowicz@directbox.com