Data Retention
Entscheidungskriterien für Systemgestaltung

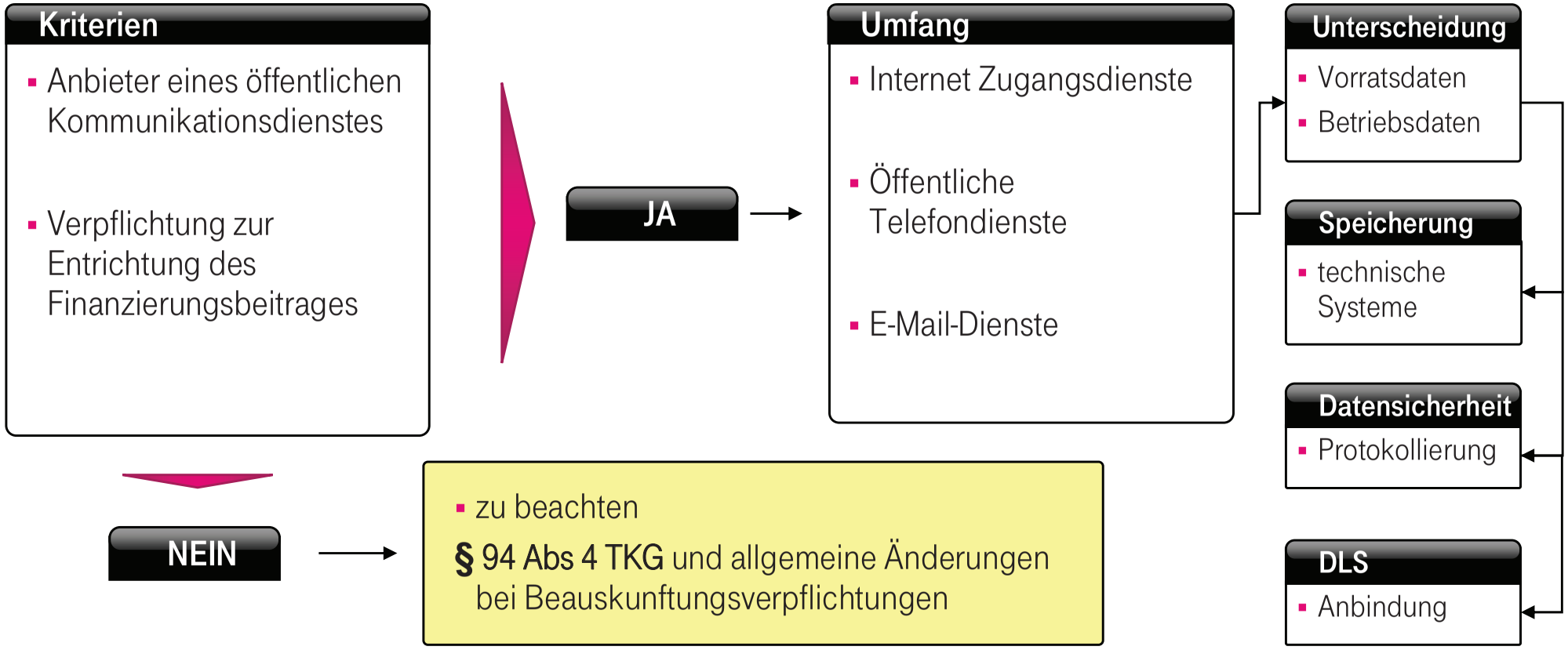
Markus Wolfger

Inhalt.

Frage Nr. 1
„Bin ich zur Vorratsdatenspeicherung verpflichtet?“

Kriterien: § 102a Abs 6 TKG

§ 102a (6) „Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.“



Frage Nr. 2 „Ich bin nicht zur Vorratsdatenspeicherung verpflichtet – wie kann ich meine Betriebsdaten an Behörden übermitteln?“

Kriterien: § 94 Abs 4 TKG

§ 94 (4) „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als “Comma-Separated Value (CSV)“...

Kriterien

- **Identifikation** und **Authentifizierung** von Sender und Empfänger
- Sicherstellung der **Datenintegrität**
- Verwendung einer **technisch anspruchsvollen Verschlüsselungstechnologie**

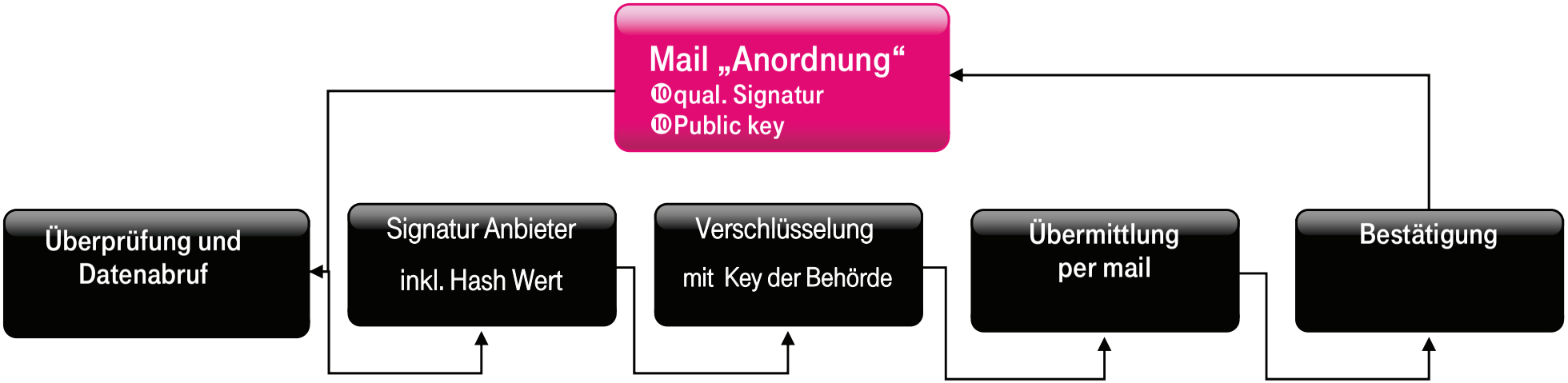
Risiken / Hindernisse

- Anbindung an DLS ist gemäß § 15 DSVO für nicht speicherpflichtige Anbieter faktisch **nicht vorgesehen**
- § 94 Abs.4 trifft aber keine Unterscheidung – Frage: DSVO auch für nicht VDS pflichtige Anbieter relevant?
- Sanktionen bei Verstoß gegen § 94 Abs 4 TKG

Lösungsvorschlag I: Übermittlung von Betriebsdaten an Behörden durch nicht speicherpflichtigen Anbieter

Variante I (Idealfall)

- Anordnung per Mail inklusive qualifizierter Signatur und public Key der Behörde (=Identifikation und Authentifizierung Sender)
- Datenabruf, Signatur des Anbieters (inkl. Hash Wert) , Verschlüsselung mit public Key der Behörde = Identifikation und Authentifizierung Sender, Sicherstellung der Datenintegrität und der Verschlüsselung
- Übermittlung der Daten per Mail
- telefonische Bestätigung bei Übermittlung/Erhalt der Daten

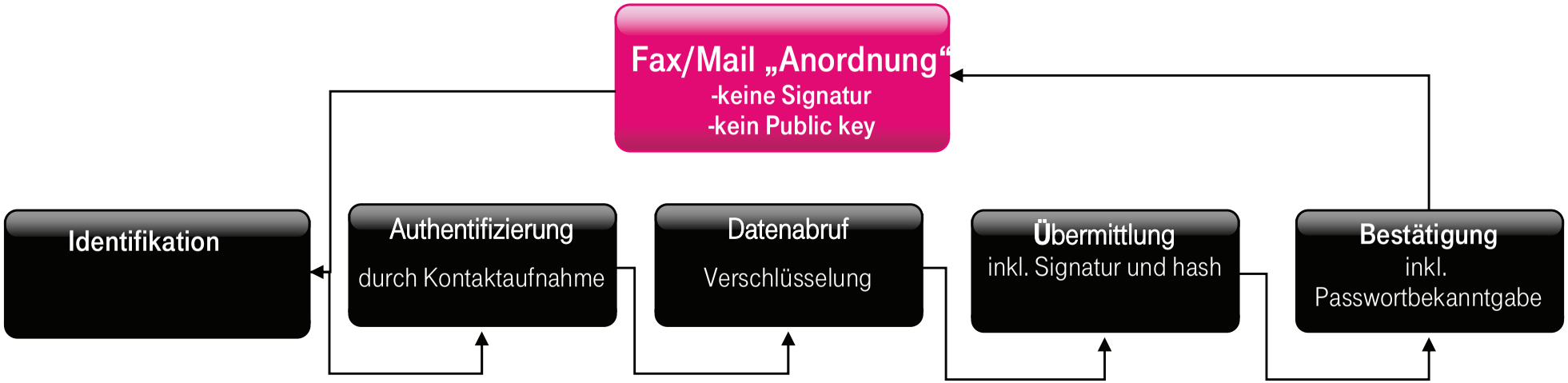


⓾ mandatory

Lösungsvorschlag II: Übermittlung von Betriebsdaten an Behörden durch nicht speicherpflichtigen Anbieter

Variante II (beschränkt tauglich)

- **Anordung per Fax oder Mail** von Dienststelle der Behörde
- Identifikation: Behördenkennung, Name des Beamten und tel. Kontaktinformationen, Mail-Adresse
- Authentifizierung: Anruf Kopfnummer der Dienststelle – über Vermittlung mit anforderndem Beamten Kontakt aufnehmen und Daten bzw. Anforderung bestätigen lassen
- Datenabruf, Signatur des Anbieters (inkl. Hash Wert), symmetrische Verschlüsselung (zB OpenPGP) inkl. Wahl eines sicheren Passwortes = Identifikation und Authentifizierung Sender, Sicherstellung der Datenintegrität und der Verschlüsselung)
- Übermittlung der Daten per Mail (Alternative: Speicherung auf Datenträger sowie Abholung oder Versand)
- telefonische Bestätigung bei Übermittlung/Erhalt der Daten inkl. Bekanntgabe des Passwortes.



Abschnitt II

Wichtige Entscheidungskriterien für Anbieter, die zur Vorratsdatenspeicherung verpflichtet sind

Definition: Betriebsdaten und Vorratsdaten Notwendigkeit einer „Betriebsdatenrichtlinie“

Vorratsdaten: § 92 (3) Z 6b TKG bzw. § 2 (1) Z 2 DSVO

§ 92 (3) Z 6b TKG: *„Vorratsdaten“ Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;“*

§ 2 (1) Z 2 DSVO: *„Vorratsdaten“, soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß § 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).*

Jedwede betriebliche Nutzung von Vorratsdaten ist ausgeschlossen; Es gelten überdies erhöhte Sicherheitsbestimmungen für die Speicherung und den Zugriff auf Vorratsdaten (revisionssichere Protokollierung, 4-Augen Prinzip bei Zugriff, etc.) – siehe auch § 102c TKG bzw. DSVO, 2. Abschnitt

Betriebsdaten: § 2 (1) Z 1 DSVO

§ 2 (1) Z 1 DSVO: „Betriebsdaten“, soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;

Diese Unterscheidung, die jeder Anbieter aufgrund der individuellen Notwendigkeit von Betriebsdaten (Dauer und Umfang) treffen muss, bildet die Basis für die weitere Systemplanung.

- welche Daten sind für welchen Zeitraum betriebsnotwendig
- Begründung für Betriebsnotwendigkeit (Verrechnung, Störungsbehebung, Sicherstellung der Netzqualität, Betrugsbekämpfung, etc.)

Checklist: vorhandene Daten, neue Daten, Datenquellen, Formate, Kosten und Volumen

Für die weitere Systemplanung sind folgende Evaluierungen durchzuführen:

1. welche Daten liegen bereits in Systemen vor, die betrieblich genutzt werden (z.b. Data Warehouse)
2. welche Daten, die der Speicherpflicht gemäß § 102a TKG unterliegen, sind derzeit nicht bzw. nicht für 6 Monate gespeichert (Internet, Telefonie, E-mail) – technische Details zu Datenarten finden sich in Erläuterungen zum TKG (z.B. Erläuterungen zu Portinformationen, internen IP-Adressen, e-Mail i.S.d. RFC 821, etc.)
3. in welchen Netzelementen werden diese (fehlenden) Daten erzeugt und verarbeitet
4. in welchen Formaten bzw. wie können diese an eine (Vorrats)Datenbank übergeben werden
5. welche zusätzlichen Kriterien sind zu beachten (Verfügbarkeit, Sicherheitskriterien, Zugriffe, Protokollierung)
6. welches zusätzliche Volumen ist durch die Speicherung dieser Daten zu erwarten
7. müssen zusätzliche Anforderungen (z.B. Historisierung von Stammdaten, Historisierung von Senderstandorten, etc. noch umgesetzt werden
8. wie wird die Datenbank gestaltet, um geforderte Zusatzinformationen (z.B. Daten wie IMEI/IMSI zu B-Nummer) effektiv abfragbar zu gestalten – diese Daten sind nicht im Datenset des Targets enthalten.
9. bestehen bereits Systeme zur Beauskunftung von Betriebsdaten bzw. in welcher Form sind Anpassungen notwendig
10. welche Anforderungen werden an die Systeme betreffend Speicherung, Beauskunftung (workflow, Prozessdefinitionen, Abfragelogik) und Protokollierung (Sicherstellung 4-Augen-Prinzip, Erfassung aller Daten und Übergabe an die DLS) gestellt.

Auf Basis dieser Evaluierungen kann ein „Lastenheft“ erstellt werden und die Entscheidung zur technischen Ausgestaltung der Speicherung erfolgen (mehrere Optionen sind möglich).

Weiters kann entschieden werden, ob eine innerbetriebliche Umsetzung erfolgt, oder eine „out of the box“ Solution gewählt wird.

Speicher-Option Nr. 1: Speicherung von Vorratsdaten in bestehenden Systemen

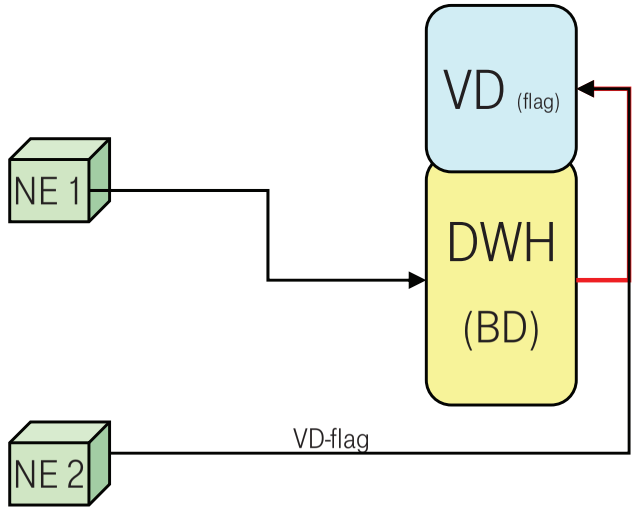
Da keine physische Trennung zwischen Betriebs- und Vorratsdaten erfolgen muss (§ 5 (2) DSVO), können die zusätzlichen Daten auch in bestehenden Systemen gespeichert werden (z.B. DWH)

Zu beachten ist folgendes:

1. „flag“ für Vorratsdaten
2. Sicherstellung Zugriffkonzept (inkl. Protokollierung und 4-Augen-Prinzip) und Schutz der Daten (siehe §§ 5-7 DSVO bzw. 102c TKG)

Nachteile:

- enorm hohe Speicherkosten
- klassische DWH System sind nicht für Einzelabfragen ausgelegt
- Sicherheitsvorgaben sind gegebenenfalls schwieriger umzusetzen



Speicher-Option Nr. 2: „Doppelspeicherung“ von Vorratsdaten

Da gemäß § 6 (3) DSVO der Anbieter Daten auch bereits in der Vorratsdatenbank speichern darf, wenn diese zugleich als Betriebsdaten gespeichert sind, besteht die Möglichkeit der „Doppelspeicherung“

Zu beachten ist folgendes:

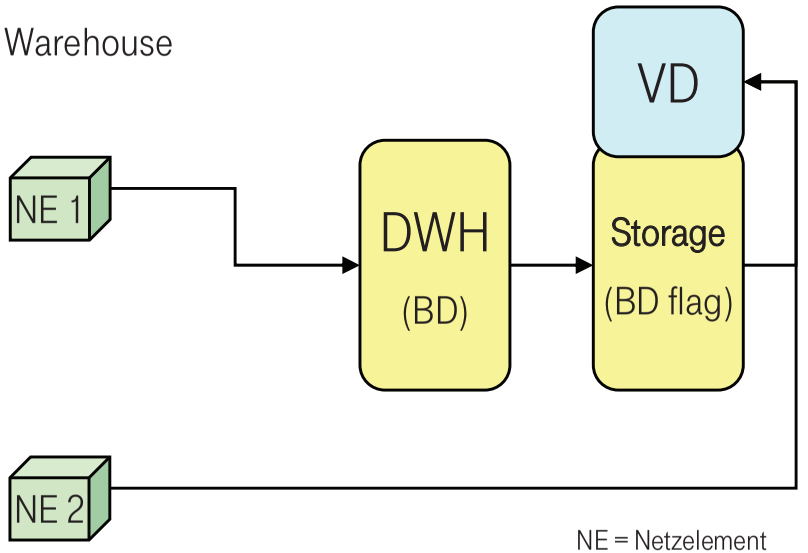
1. Kenntlichmachung, dass diese Daten zugleich als Betriebsdaten gespeichert sind = „flag“ für Betriebsdaten
2. Sicherstellung Zugriffkonzept (inkl. Protokollierung und 4-Augen-Prinzip) und Schutz der Daten (siehe §§ 5-7 DSVO bzw. 102c TKG) für Vorratsdaten

Vorteile:

- System zur Speicherung von Betriebsdaten wird nicht beeinflusst
- Daten, die von Beginn an Vorratsdaten sind können teilweise direkt von den Netzelementen in die Vorratsdatenbank überführt werden
- Speicher (Server/Storage) ist kostengünstiger als Speicherung im Data Warehouse

Nachteile:

- ebenfalls hohe Speicherkosten durch zusätzliches Datenvolumen (Verdopplung im Bereich der Betriebsdaten = xy Terrabyte zusätzlich benötigtes Speichervolumen)
- betriebswirtschaftlich in den meisten Fällen nicht sinnvoll



Speicher-Option Nr. 3: dezidierter Speicher für Vorratsdaten „rollierender Übertrag“

Betriebsnotwendige Daten werden im DWH gespeichert - wenn keine betriebliche Rechtfertigung für Speicherung mehr vorliegt (Betriebsdatenrichtlinie) werden diese im DWH gelöscht und „rollierend“ in eine gesonderte Vorratsdatenbank überführt.

Zu beachten ist folgendes:

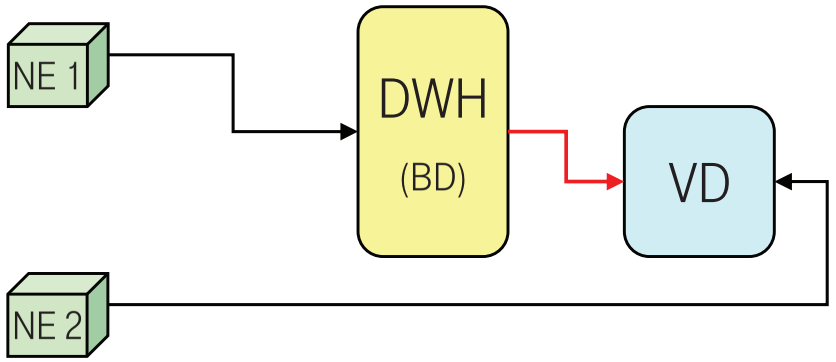
1. Sicherstellung dass Löschung im DWH und Übertragung gemäß Betriebsdatenrichtlinie an Vorratsdatenbank erfolgt
2. Sicherstellung Zugriffkonzept (inkl. Protokollierung und 4-Augen-Prinzip) und Schutz der Daten (siehe §§ 5-7 DSVO bzw. 102c TKG) für Vorratsdaten

Vorteile:

- keine Doppelspeicherung
- Daten, die von Beginn an Vorratsdaten sind können teilweise direkt von den Netzelementen in die Vorratsdatenbank überführt werden
- einfachere Umsetzung von Zugriffskonzepten, Protokollierungen und Datensicherheitsmaßnahmen
- System zur Speicherung von Betriebsdaten wird nicht beeinflusst
- geringere Speicherkosten: Server/Storage ist wesentlich kostengünstiger als Speicherung im Data Warehouse

Nachteile:

- rollierender Übertrag von Daten muss spezifiziert und sichergestellt werden



NE = Netzelement

Innerbetriebliche Umsetzung oder Beauftragung „out of the box System“

Voraussetzungen:

Innerbetriebliche Umsetzung

- IT know-how muss vorhanden sein
- Ressourcen müssen frei sein (Beeinflussung laufender Projekte)
- Datenquellen und Ausgangsformate (Netzelemente)müssen analysiert werden
- Datenbanken müssen erweitert bzw. zusätzlich angeschafft werden
- Datensicherheitsmaßnahmen müssen umgesetzt werden (z.B. Protokollierung)
- Abfragelogik und Ausgabeformat muss definiert und IT-seitig umgesetzt werden

Out of the box Solution

- “Komplettpaket” auf Basis des Spezifikation
- Datenquellen und Ausgangsformate (Netzelemente) müssen analysiert werden.
- Datenbank ist im Regelfall Teil des Angebotes
- Datensicherheitsmaßnahmen müssen spezifiziert werden
- Abfragelogik und Ausgabeformate müssen spezifiziert werden

***Ein Lastenheft, welches die entsprechenden Anforderungen (Requirements) definiert, ist in beiden Fällen erforderlich**

Innerbetriebliche Umsetzung oder Beauftragung „out of the box System“

	Innerbetriebliche Umsetzung	„out of the box Solution“
Vorteile	▪ kostengünstige Umsetzung ▪Anpassungen und Änderungen können schnell und flexibel vorgenommen werden (zB bei Änderung von Ausgangsformaten) ▪Vorteile bei Störungsbehebung und Fehleranalyse ▪Kontrolle über Datenbank und Datensicherheitsmaßnahmen ▪ genaue Kenntnis der Vorsysteme	▪ keine (bzw. geringere) IT Ressourcen werden benötigt ▪ Datenbanksystem wird meist mitgeliefert bzw. angeboten
Nachteile	▪ IT Ressourcen und know-how werden benötigt (Planung, Entwicklung und Umsetzung)	▪ im Regelfall höhere Kosten ▪ Anbindung an bestehende Infrastruktur gestaltet sich oft schwierig da keine Kenntnis der Vorsysteme vorhanden ist ▪ Änderungen/Anpassungen müssen beauftragt werden ▪ Störungsbehebung kann nur durch Lieferanten durchgeführt werden

Abfragelogik und Prozessdefinition

Da lt. Schätzungen des Bundesministeriums für Justiz von einer nicht linearen Steigerung der Anfragen von +30 % ausgegangen wird (Erläuterungen zur TKG Novelle) und überdies die Möglichkeiten in Zusammenhang mit SPG Anfragen erweitert wurden (Zugriffe auf Vorratsdaten gemäß § 99 (5) Z. 3 und Z. 4 TKG), ist eine effektive Gestaltung der Systeme erforderlich.

Zu beachten sind hierbei:

a) Funktionale Anforderungen an die Applikation

- Definition von Berechtigungsgruppen
- Pflichtfelder bei Datenabfragen Betriebsdaten/Vorratsdaten - Einschränkungen der Maximalausprägung gemäß EP020 bei Abruf
- Konvertierung in EP020 Format (csv)

b) Protokollierung

- Sicherstellung Vier-Augen-Prinzip
- korrekte Erfassung der Protokoll- und Statistikinformationen (Inhalt)
- Protokollierungsumfang bei Betriebsdaten
- Protokollierungsumfang bei Vorratsdaten (Statistikinformationen DLS / erweiterte Daten intern)

Protokollierung I

§ 7 Abs 3 DSVO

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage (Zustellung in das Postfach des Anbieters in der Durchlaufstelle gemäß § 17 Abs. 1) sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft (Zustellung der Antwort in das Postfach der Behörde in der Durchlaufstelle gemäß § 17 Abs. 3), wobei diese Daten von der Durchlaufstelle als Zusatzinformation an den Anbieter zu übermitteln sind,
4. die nach dem Datum des Beginns des Kommunikationsvorganges und den Kategorien gemäß § 102a Abs. 2 bis 4 TKG 2003 (Einteilung der Kategorien gemäß der Anlage, Kapitel 1.1.2) aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten ab dem Datum, seit dem die Daten als Betriebsdaten (§ 2 Abs. 1 Z 1) und als Vorratsdaten gemäß § 2 Abs. 1 Z 2 gespeichert wurden, zum Zeitpunkt der Anordnung der Auskunft (Datum der staatsanwaltschaftlichen Anordnung gemäß § 138 Abs. 3 StPO oder Datum der Anfrage nach § 53 Abs. 3a und 3b des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991 in der Fassung BGBl. I Nr. 33/2011),
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt,
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben sowie
8. im Fall von Auskünften über Vorratsdaten (§ 135 Abs. 2a StPO) die der Anordnung zu Grunde liegende strafbare Handlung, ansonsten den Hinweis, dass nur Betriebsdaten verwendet werden.

§ 102c Abs 2 TKG

(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b revisionssicher protokolliert wird. Diese Protokollierung umfasst

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.

Pflichtfelder Abfrage Vorratsdaten

- Target (Indikator)
- Zeitpunkt (Zeitraum)
- Unique-Id
- Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung oder Aktenzahl der Sicherheitsbehörde („Referenz“)
- Datum der Anordnung (StPO) oder Datum der Anfrage (SPG)

Protokollierung II

Grundsätzlich ist zur Protokollierung bei Vorratsdaten festzuhalten, dass die erforderlichen Protokolldaten in § 102c TKG und § 7 Abs 3 DSVO definiert werden:

Datenquellen für Protokolldaten sind:

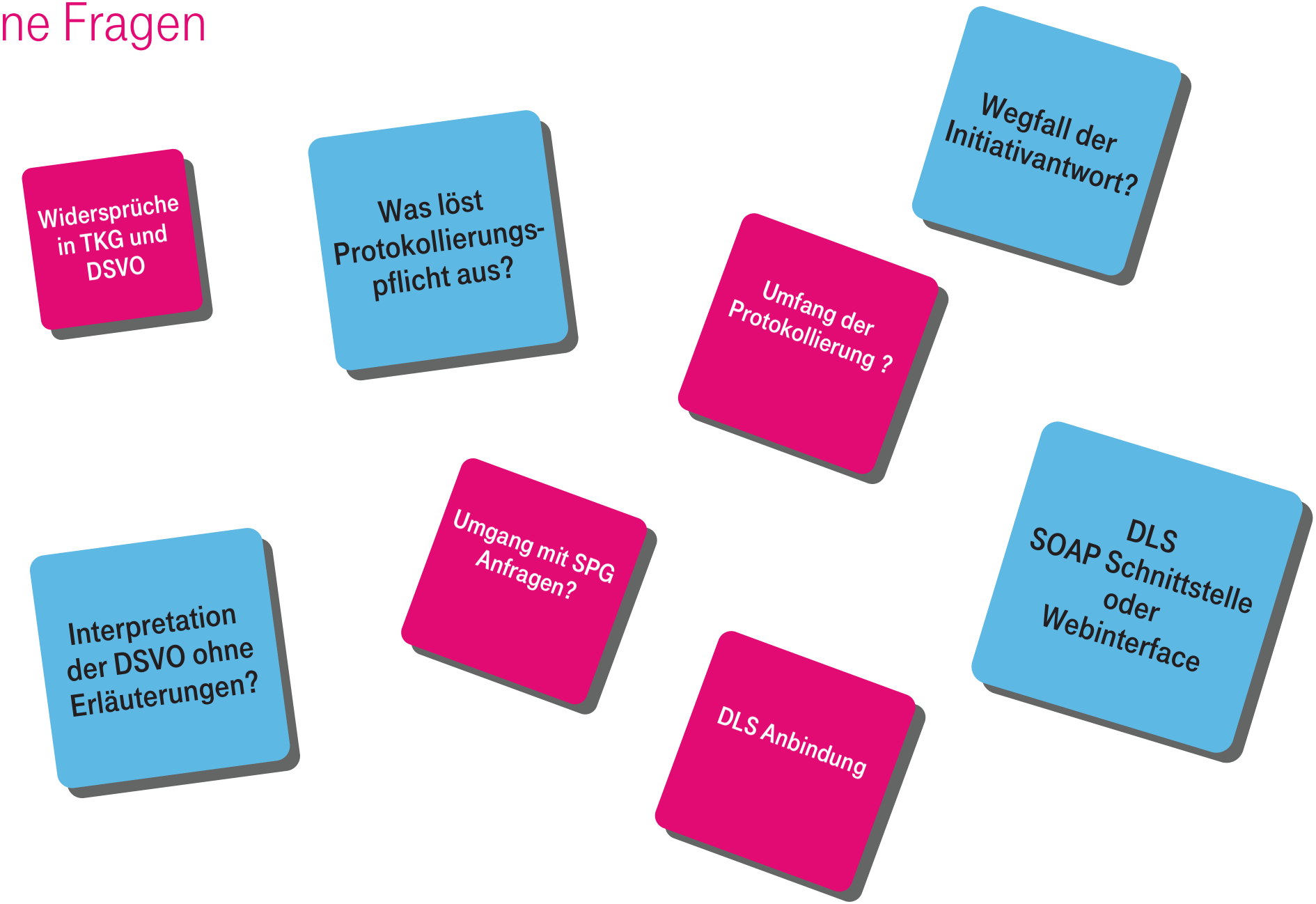
- **Daten der Abfrage und Pflichtfeldern** (inkl. UserId und Authorisierung) = § 7 Abs 3 Z 1,2 und 7 DSVO)
- **Daten aus dem Ergebnis der Abfrage** (Bsp. Anzahl Datensätze?, Berechnung Alter pro Datensatz, betroffene Teilnehmer, etc) = § 7 Abs 3 Z 4?,5 und 6 DSVO)
- **und Daten der DLS** (Bsp. Eingang und Zustellung in Postfach) = § 7 Abs 3 Z 3 bzw. Z 8 DSVO)

Weiters muss eine Teilmenge der Protokolldaten direkt an die DLS übermittelt werden – diese Daten werden in § 22 und § 23 DSVO definiert:

Anmerkung: aufgrund der Änderungen der DSVO im Vergleich zur **„**Begutachtungsversion**“** und der fehlenden Erläuterungen ergeben sich unklare bzw. teilweise widersprüchliche Regelungen (= Rechtsunsicherheit) **–** siehe z.B.

1. Wegfall des § 6 (1) DSVO: brachte in der vorhergehenden Version klar und unverständlich zum Ausdruck dass nur bei einem Zugriff auf Vorratsdaten eine Protokollierung stattfinden muss
2. § 3 DSVO **–** keine Anwendung der Bestimmungen des 3. Abschnittes bei SPG Anfragen
3. § 7 (2) DSVO: Anordnungen der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO (Protokollierung Zugriffe Betriebsdaten)

Offene Fragen



Vielen Dank für Ihre Aufmerksamkeit.