PwC & Datenschutz: Umsetzung der gesetzlichen Löschungsverpflichtung in SAP

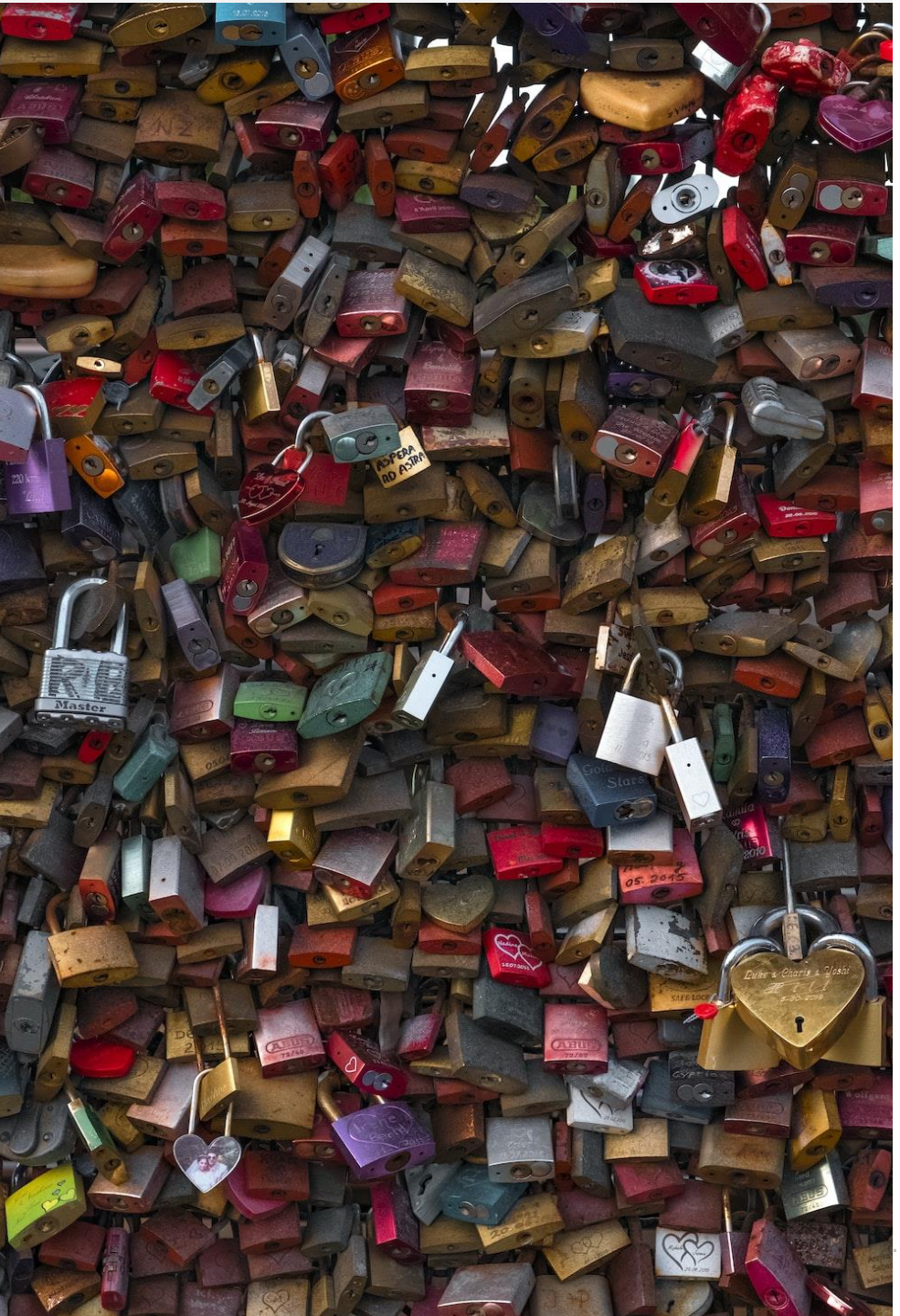
Pascal Kaldenbach

Dr. Jan-Peter Ohrtmann – PwC Legal

AGENDA

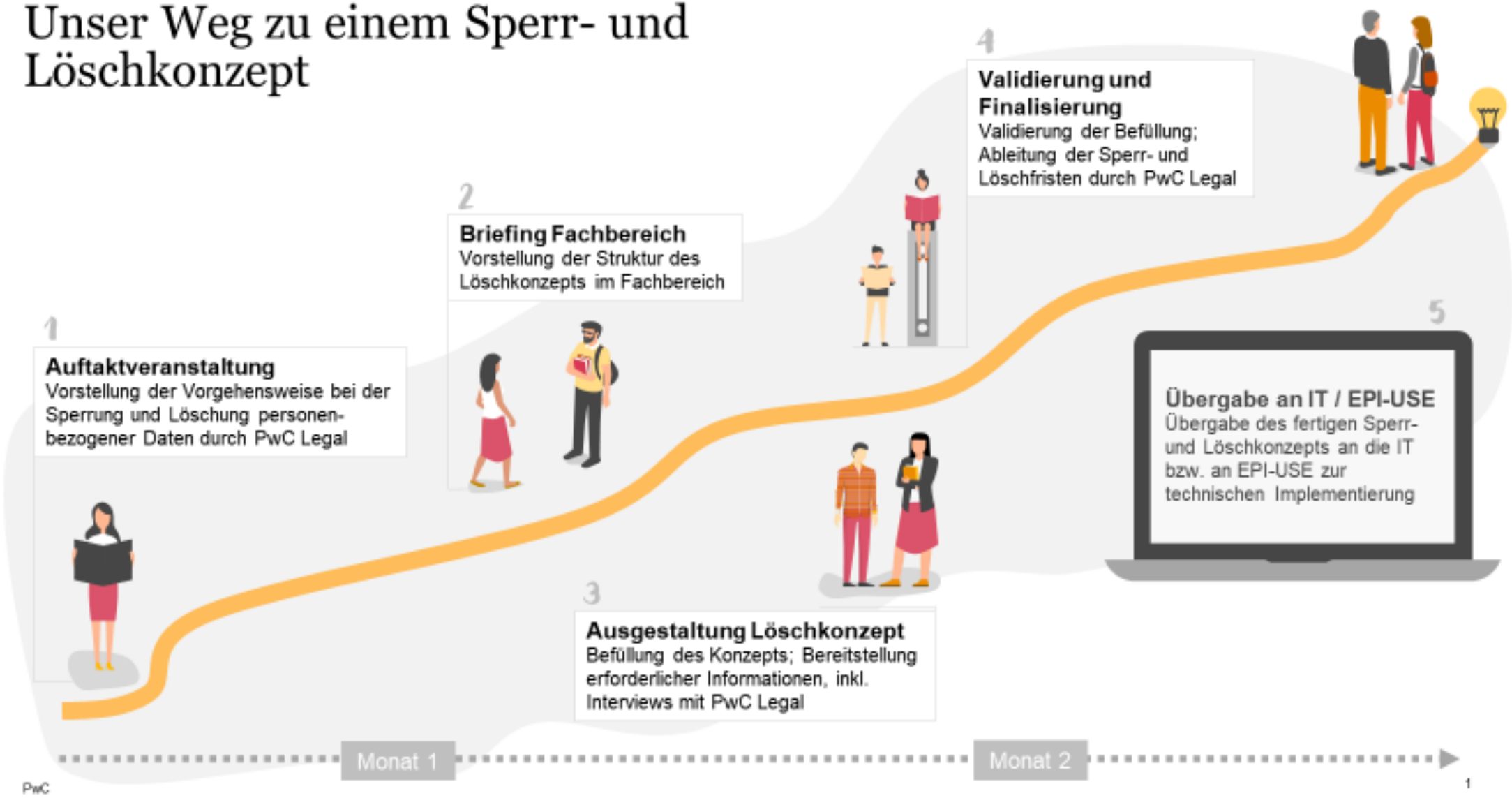
1. Einführung: PwC, EPI-USE
2. Wo kommt die gesetzliche Löschungsverpflichtung her?
3. Grenzen der Löschungsverpflichtung: Aufbewahrungspflichten und -rechte
4. Praxis: Umsetzung der Löschpflicht in SAP


„Hast du den Müll raus gebracht?“



PwC & EPI-USE

Unser Weg zu einem Sperr- und Löschkonzept



Beauskunftung

- Erzeugt PDF zur Beauskunftung anfragender Personen
- Schnelle Erstellung von vollständigen Daten-Footprints
- Durchsucht alle ABAP Stack Systeme & beliebig viele non-SAP-Systeme

Redigieren

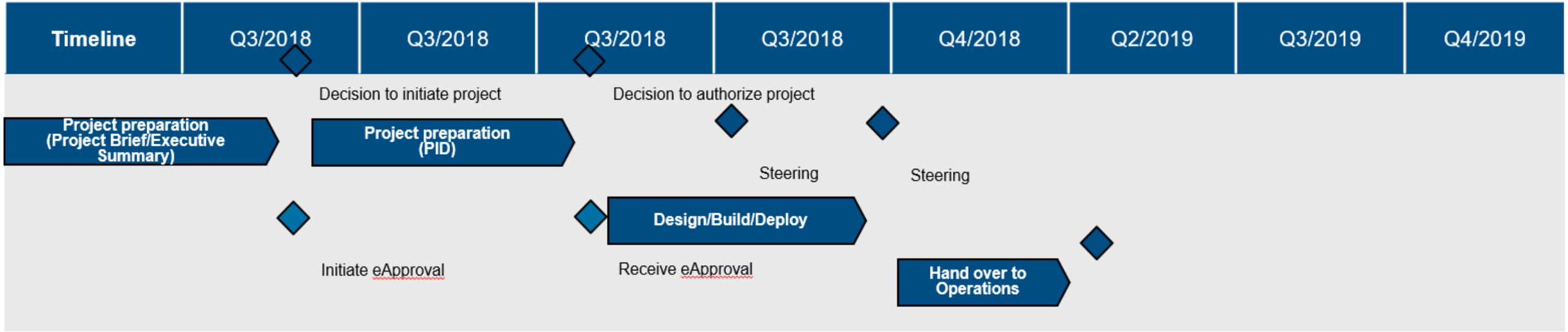
- Betrifft reaktiv das Recht auf Löschung (Art. 17 DSGVO)
- Intelligentes Entfernen oder Verfremden von sensiblen Daten
- Selektives Entfernen garantiert Datenintegrität

Testsysteme

- Sensible Daten in Testsystemen gemäß DSGVO schützen
- Flexible, anpassbare Maskierungsregeln
- Optimiert für die Massenverarbeitung

PwC & EPI-USE & GEA

Erste Projektannäherung bereits in 2018



- Analyse in Q2 & Q3/2019 mit einem großen Anbieter
- Erster Kontakt mit EPI-Use in Q3/2019
- Marktsondierung und Anbieterbewertung in Q4/2019 und 2020 mit vier weiteren Dienstleistern

Ergebnis: automatisierter Löschansatz personenbezogener Daten bei 5 Dienstleistern nicht ausreichend unterstützt

GEA SAP Systeme

Ranking	System	SAP Application Release	SAP Netweaver	Database Type	Size	Anzahl Buchungskreise
1	PPE	ECC 600 EHP 8 SP 03	750 SP 04	HANA DB	203 GB	7
2	P01	ECC 600 EHP 7 SP 04	740 SP 06	SAP ASE	126 GB	64
3	PHC	HR 600 SP 190	700 SP 36	MaxDB	334 GB	1
4	PEM	ECC 600 EHP 8 SP 04	750 SP 05	SAP ASE	1,2 TB	6
5	P30	ECC 600 EHP 7 SP 05	740 SP 07	MaxDB	501 GB	1
6	C11	ECC 600 EHP 3 SP 20	700 SP 36	MaxDB	1 TB	3
7	P11	ECC 600 EHP 8 SP 04	750 SP 05	HANA DB	2,2 TB	37
8	PL1	ECC 600 EHP 6 SP 05	731 SP 05	SAP ASE	4 TB	55
9	P16	ECC 600 EHP 5 SP 05	702 SP 09	SAP ASE	1 TB	18
10	PLB	ECC 600 SP 30	700 SP 35	MaxDB	123 GB	4
11	PCP	ECC 600 EHP 5 SP 14	702 SP 17	SAP ASE	106 GB	2
12	P21	ECC 600 EHP 6 SP 04	731 SP 04	SAP ASE	465 GB	1
13	P18	ERP 470 SP 35	620 SP 70	SAP DB	171 GB	1
14	globalSAP	S4CORE 104 SP 02	754 SP 02	HDB 2.00.046		tbd
15	PCE	S4CORE 104 SP 00 (S/4 1909 SP 00)	754 SP 00	HDB 2.00.048	154 GB	1
16	PMD	S4CORE 1909 SP 02 (MDG 804 SP 02)	754 SP 02	HDB 2.00.044	231 GB	1
17	PAM	SCM / APO 700 EHP 4 SP 04	750 SP 05	HDB 2.00.048	234 GB	1
18	PRM	CRM 700 EHP 4 SP 14	750 SP 17	SAP ASE	1,3 TB	1
19	PSM	ST 720 SP 11	740 SP 22	HDB 2.00.048	347 GB	1
20	PBW	BW 750 SP 16	750 SP 16	HDB 2.00.044	931 GB	1

Wo kommt die gesetzliche Löschungsverpflichtung her?

Grundsätze des Datenschutzes mit besonderer Löschrelevanz

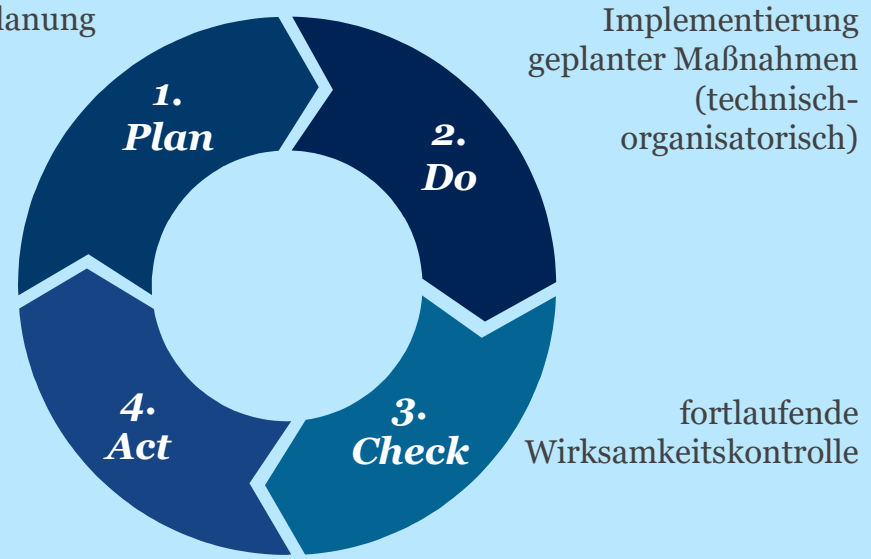
	Speicherbegrenzung von Daten	Daten-minimierung
Die Datenverarbeitung muss so gestaltet sein, dass …	personenbezogene Daten in einer Form gespeichert werden, die die **Identifizierung** der betroffenen Personen **nur so lange** ermöglicht, **wie es für die festgelegten Zwecke erforderlich** ist *(vgl. Art. 5 Abs. 1 lit. e) DSGVO)*.	• sie für die festgelegten Zwecke **angemessen und erheblich** ist und • **auf das** für die Erreichung dieser Zwecke **notwendige Maß** (quantitativ und qualitativ) **beschränkt** ist *(vgl. Art. 5 Abs. 1 lit. c) DSGVO).*
Hieraus folgen die Pflichten …	zur rechtzeitigen und planmäßigen Anonymisierung oder Löschung personenbezogener Daten (→ „**Löschkonzept & Umsetzung**“).	zur Sperrung, wenn Daten nur noch aufbewahrt werden müssen.

Warum nicht einfach löschen und „gut ist“?

Rechenschafts-
pflicht

Der Verantwortliche … muss … **Einhaltung jederzeit nachweisen** können *(vgl. Art. 5 Abs. 2 DSGVO)*.

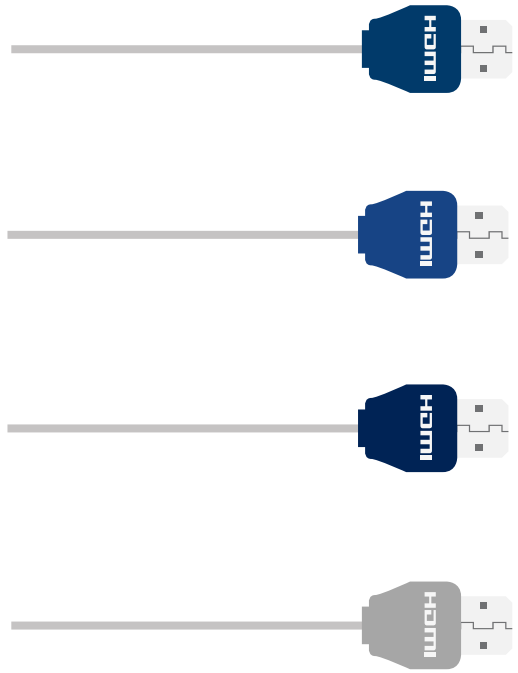
Umsetzung durch „PDCA“-Prozesszyklus



Dokumentation Löschprozesse & Löschung

Zeitpunkt und Umstände eines Zweckfortfalls und Anonymisierung oder Löschung der betreffenden Daten (oder aber Gründe für deren fortgesetzte Speicherung).

Wie kommt man drauf? – „Sichtbarkeit“ von Löschfristen



Datenschutzhinweise

Verzeichnis von Verarbeitungstätigkeiten

Auskunftsrecht

Überprüfungen der Datenschutz-Compliance *(Rechenschaftspflicht)*

Wer will es wissen? z.B.

- Betroffene
- Arbeitnehmer-vertreter / Betriebsrat
- Aufsicht

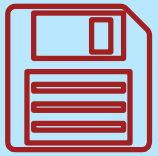
Grenzen der Löschungsverpflichtung: Aufbewahrungspflichten & -rechte

Typische Aufbewahrungsfristen – AO und HGB

Beispiele

- Handelsbriefe: 6 Jahre
  Schriftstücke, die ein Handelsgeschäft (bzw. dessen Vorbereitung, Durchführung oder Rückgängigmachung) betreffen: z.B. Angebot, Annahme, Kostenvoranschlag, Mängelrüge, Reklamation, Vertrag
- Buchungsbelege: 10 Jahre
  z.B. Rechnungen, Lieferscheine, Quittungen, Auftrags- und Bestellscheine, Bankauszüge, Betriebskostenabrechnungen, Lohn- und Gehaltslisten, Eigenbelege und interne Buchungsanweisungen
- Sonstige steuerrelevante Unterlagen: 6 Jahre
  Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind.
- Bücher, Aufzeichnungen, Bilanzen: 10 Jahre

Fristbeginn: Schluss des Kalenderjahres, in dem das Dokument aufgestellt/empfangen/abgesandt wurde.



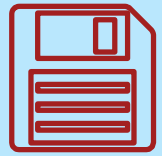
Vorhaltefrist

Typische Aufbewahrungsfristen – Personalbereich

Beispiele

- Unterlagen Mindestlohn: 2 Jahre ab dem für die Aufzeichnung maßgeblichen Zeitpunkt aufzubewahren (§ 17 Abs. 1 MiLoG)
- Mutterschutz-Unterlagen: 2 Jahre ab letzter Eintragung (§ 27 Abs. 5 MuSchG)
- Dokumentation über Erste-Hilfe-Leistungen: 5 Jahre ab Ende des Jahres der Erstellung (§ 24 Abs. 6 DGUV)

- Bewerbungsunterlagen (Ablehnung): Aufbewahrungs**recht**: 6 Monate ab Ablehnung (Art 6 DSGVO i. V. m. § 21 Abs. 5 AGG)
- Bewerbungsunterlagen (Einstellung): Dauer des Arbeitsverhältnisses



Vorhaltefrist

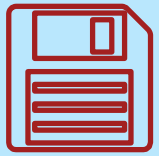
Typische Aufbewahrungsfristen – Diverses

Beispiele

Vertragsdaten
- Laufzeit des Vertrages
- Behandlung etwaiger (Gewährleistungs-)Ansprüche

Daten auf Basis einer Einwilligung
- Dauer der zulässigen Verarbeitung der Daten
- Bei Nichtnutzung „Halbwertszeit“ umstritten

Daten auf Basis eines berechtigten Interesses
- Dauer der zulässigen Verarbeitung der Daten umstritten



Vorhaltefrist

Spannungsverhältnis Löschung und Aufbewahrung

Aufbewahrungs-pflichten

z.B. HGB, AO

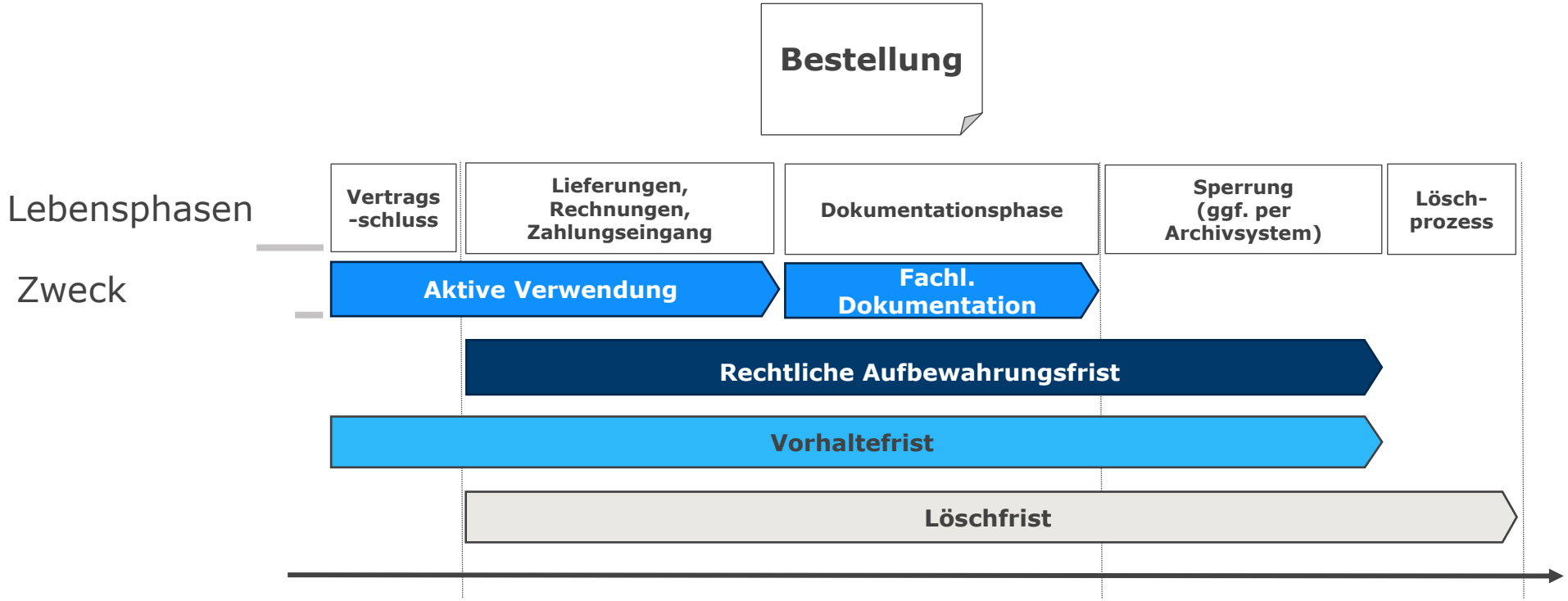
Mittel zur Auflösung des Spannungs-verhältnisses:

- Einschränkung der Verarbeitung
- Anonymisierung
- "Schwärzen”
- …

Löschungs-anforderungen

Art. 5 Abs. 1 lit. e) DSGVO

Wie spielt das zusammen?
Lebenszyklus von Daten und relevante Fristen am Beispiel einer Bestellung

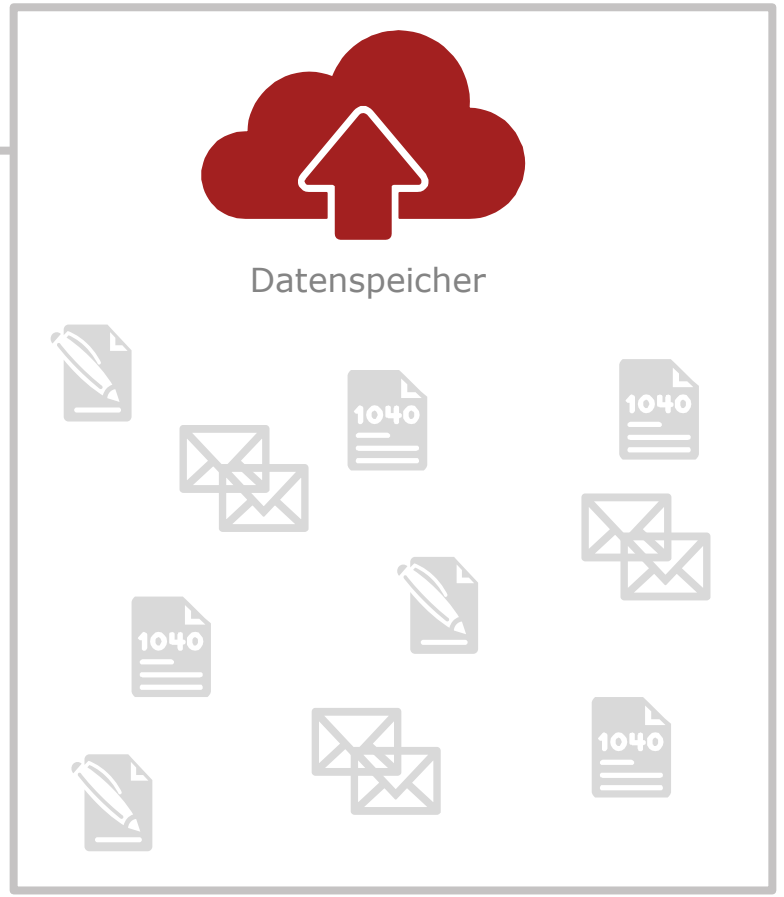


Darstellung nach DIN 66398:2016-05

Praxis: Umsetzung der Löschpflicht in SAP

Praktische Herausforderungen (1/2)

- **Fortwährendes Speichern von Daten als Normalfall**



- Gewachsene Datenbestände
- Leistungsfähige Hard- und Software; → Speicherkapazitäten
- (Meist) vollständige Datenübertragung bei Migration ohne Datenbereinigung
- Mehrfachnutzung verlinkter Datenfelder (Vorsysteme)
- Wesentliche Software-Leistung: „revisionssichere Langzeitarchivierung“
- Diverse gesetzliche Anforderungen zur Aufbewahrung von Informationen
- Geringes Bewusstsein über strenge Löschvorgaben

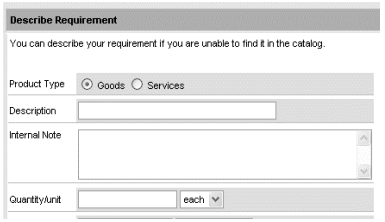
Praktische Herausforderungen (2/2)

Auffindbarkeit

- Wo sind die Daten gespeichert?
- Welche Systeme tauschen Daten aus? Wie?
- Welcher Empfänger hat die Daten erhalten?

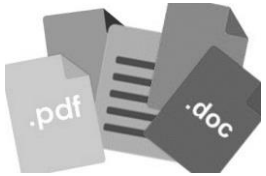
Backups

- Konträres Ziel: Sicherung vollständiger Inhalte.



Freitextfelder

- Dateneingabe nicht kontrollierbar
- Löschen von (Einzel-)Angaben nicht oder nur mit hohem Aufwand möglich



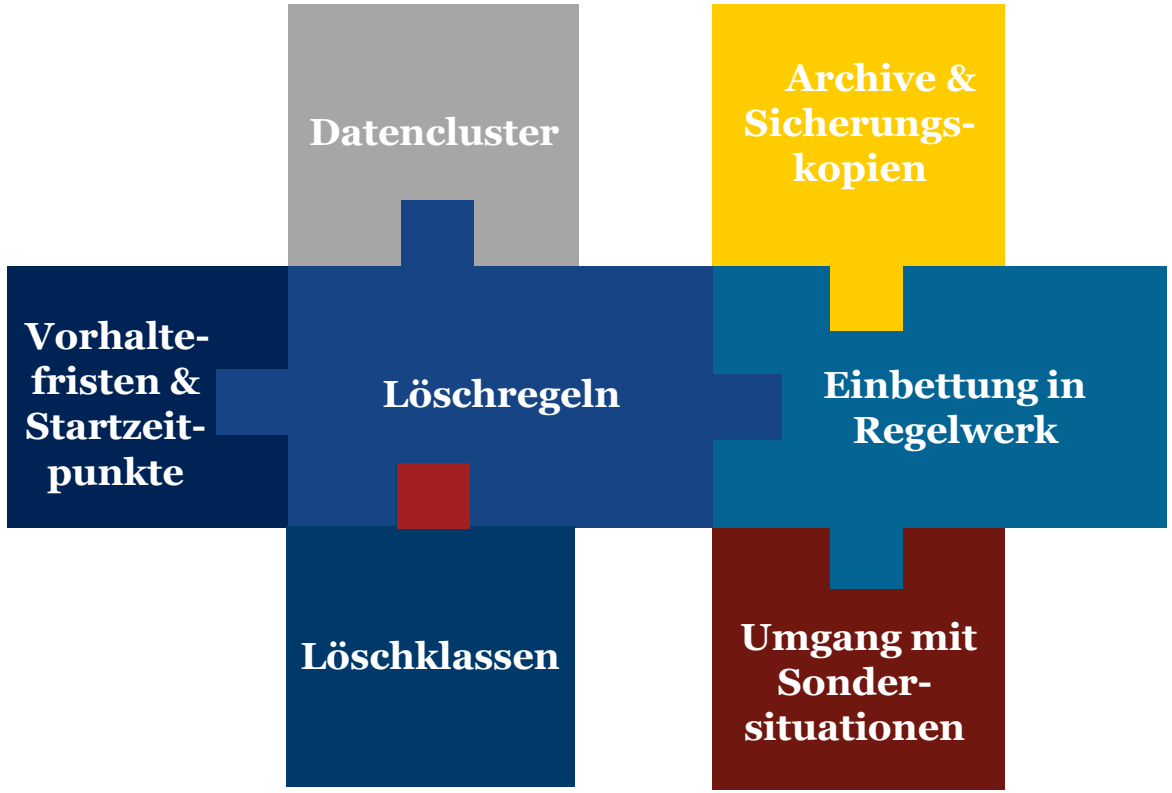
Kaum SAP-Relevanz

Schatten-IT

- Lokale Datenablage
- Außerhalb der Reichweite des Löschkonzepts

Fachliche Lösung
Anforderungen an Löschkonzepte nach DIN 66398:2016-05

- ***„In einem Löschkonzept legt die verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von pbD erfüllt."***



Effektives Datenschutzmanagement

- Präzise und umfassende Festlegung der Zwecke der Datenverarbeitung
- Klare Dokumentation der Verarbeitungsprozesse im Verzeichnis der Verarbeitungstätigkeiten
- Transparenz über Datenflüsse; Datenlandkarten
- Richtlinien und Arbeitsanweisungen, insbes. zum Umgang mit personenbezogenen Daten, zur Verwendung von Freitextfeldern und zur Dokumentenablage
- Systematisches Löschen: **Löschkonzepte für Produktivsysteme, Archivsysteme und Backups**

Fachliche Lösung
Bildung von Löschregeln und Löschklassen

Daten(-art) 1 ⟹ Löschfrist 1 ⟹ Startzeitpunkt 1 ⟹ Löschregel 1

Daten(-art) 2 ⟹ Löschfrist 2 ⟹ Startzeitpunkt 1 ⟹ Löschregel 2

Daten(-art) 3 ⟹ Löschfrist 3 ⟹ Startzeitpunkt 2 ⟹ Löschregel 3

Löschklassenmatrix

		Vorhaltefrist							
		Sofort	**3 Monate**	**6 Monate**	**2 Jahre**	**3 Jahre**	**6 Jahre**	**10 Jahre**	**Unbegrenzt**
Startzeitpunkt	**Ab Erstellung**	Web-Logs	Dokumen-tation		SGB	Gesetzl. Verjäh-rungsfrist	Handels-briefe	Buchungs-belege	
	Ende des Vorgangs/ Vertragsende			AGG				Verträge	Rechts-streitigkeiten
	Zeitpunkt des letzten Audits								

Fachliche Lösung
Bildung von Löschregeln und Löschklassen

Bonus-Material

Aufbewahrungs-frist	Zeitraum, innerhalb dessen die Objekte einer Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein müssen.
Vorhaltefrist	Zeitraum, innerhalb dessen die Objekte einer Datenart in der verantwortlichen Stelle aufgrund der fachlichen Verwendung oder gesetzlicher Aufbewahrungspflichten mindestens verfügbar sein sollten.
Löschfrist	Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden sollte.
Löschregel	Kombination aus einer Löschfrist und einer konkreten Bedingung für den Startzeitpunkt des Fristlaufs.
Löschklasse	Kombination aus einer Standardlöschfrist und einem abstrakten Startzeitpunkt für den Fristlauf.

Fachliche Lösung
Ergebnis: Beispiel Implementierungstabelle EPI-USE

Please list your data fields / records here and complete all blue colums.

<Legal entity>

STANDARD DELETION RULES FRAMEWORK for personal data

Grew columns will be completed by Data Protection Team.

IT System	Data Field (Information) / Data Object (Record)	SAP Process (Transaction)	File name of the Screenshot	Process Owner / Process Manager	Description of Data Field / Data Object	Comment	Data Subjects	Categories of Personal Data	Purpose of Processing	Period of Active Use and Trigger Event	Period of Documentation and Trigger Event	Local Statutory Retention Period and Trigger Event	Local Legal Basis for Statutory Retention Period	Evaluation (Reasoning regarding the statutory retention period)	Standard Deletion Period + Trigger Event	Restriction of Processing + Trigger Event	Evaluation (Reasoning regarding the standard deletion period and the restriction of processing)
<Department>																	
SAP PPE (100)	**Customer Invoice** (Debitorenrechnung)	VF01, VF02, VF03	Screenshots VF01_001.jpg	Tom Tomson	Invoices that were issued in the name of Company or on Company's behalf for services and goods offered by Company.	n/a	Customers	Full name, Company / entity, Company Address, Contact Data, Cost Center, Customer ID, Bank account information, Invoice number, Tax Data, Tax Identification Number	Purchase of Goods and Services	6 months after creation of invoice	6 years after creation of invoice	10 years from the end of the calendar year in which the invoice has been created	Sec. 147 AO, 257 HGB; Sec. 14b (l) German Value Added Tax Act (Umsatzsteuergesetz)	This document is defined as booking voucher according to Sec. 147 (1) no. 4 AO, 257 (1) no. 4 HGB, so that a retention period of 10 years applies in accordance with Sec. 147 (3) S. 1 AO, 257 (4) HGB.	10 years from the end of the calendar year in which the invoice has been created	1 year after end of the calendar year in which the invoice has been created	The deletion period is based on the statutory retention period. Since the period of active use is less than the retention period, it can be deleted after the retention period has expired. Once the business needs have expired, the processing must be restricted.

<u>Relevanz</u>:

- Implementierungsfähig
- PDCA taugliche Dokumentation der Maßnahme

Vorgehensweise im Projekt

Phase 1: *Prozesse & Datenerhebung*

- Wieviele Löschkonzept sind erforderlich (pro Gesellschaft, Gruppe …)? → Art & Menge der Systeme
- Auswahl der zu untersuchenden Prozesse (Ausgangspunkt: VVT)
- Weitere Erhebung pro Prozess durch Interviews und Fragebögen: Identifizierung der Datenbestände (Datenobjekte/-felder), der Verarbeitungszwecke und der Datenempfänger etc.
- Abhängigkeiten der Systeme beachten !!!

z.B. per Interview mit Fachbereich durch PwC

Phase 2: *Datenanalyse & -bewertung*

- Bestimmung der nationalen gesetzl. Aufbewahrungsfristen (Einbeziehung der PwC-Netzwerkgesellschaften)
- Erarbeitung von Empfehlungen zu Sperr- und Löschfristen
- Ggf. Durchführung von Workshops zur Herbeiführung von Entscheidungen zu Sperr- und Löschfristen (Kleingruppen)
- Festlegung der Löschregeln, Bildung von Löschklassen und Datenarten

Fachbereich, IT, PwC, Datenschutz, (Recht)

Phase 3: *Dokumentation*

- Dokumentation der Datenbewertung aus Phase 2

Regelwerk soweit nicht vorhanden:

- Erstellung Richtlinie „Löschen"
- Erstellung Verfahrensanweisungen

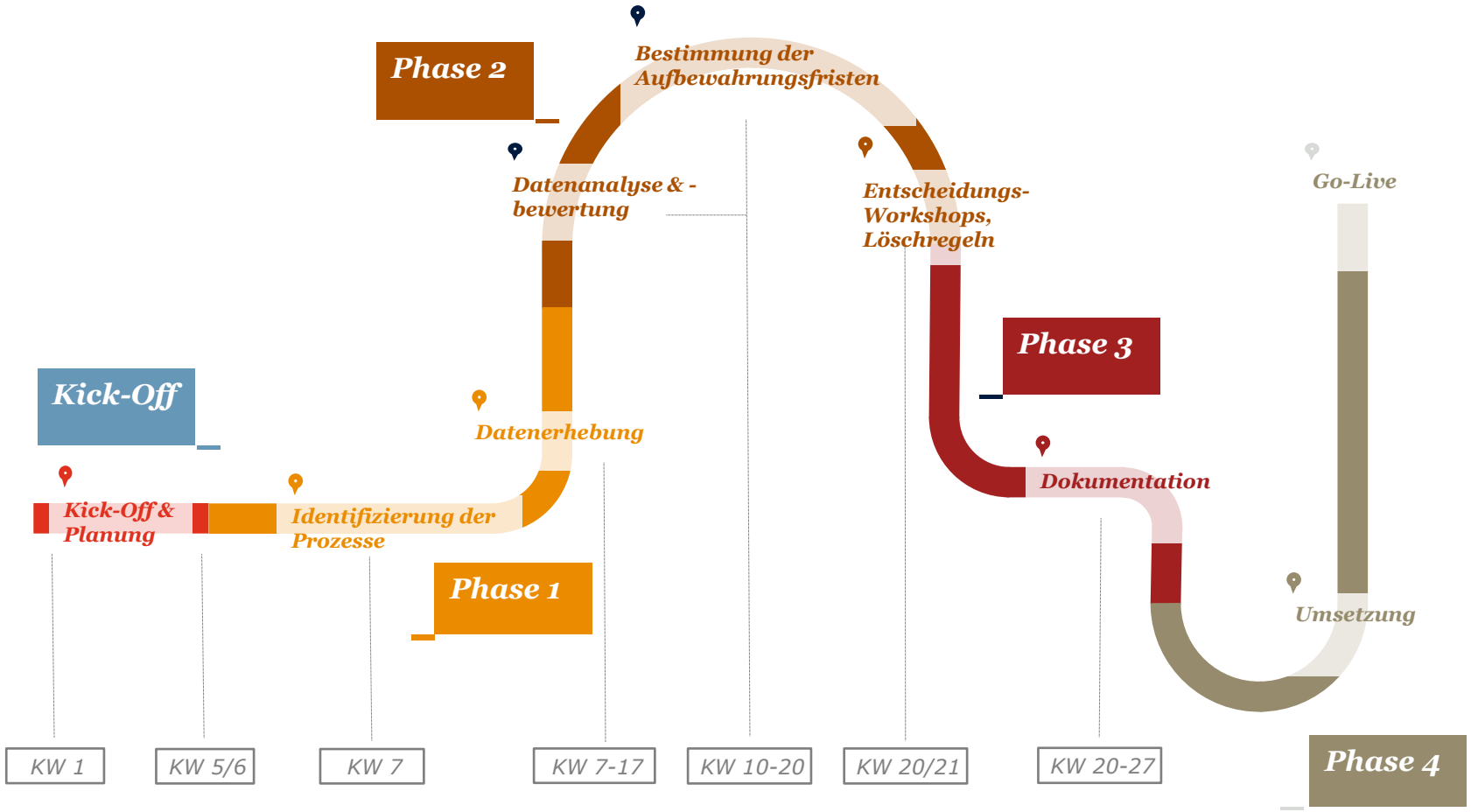
Datenschutz, (Recht), PwC

Phase 4: *Umsetzung*

- Erstellung (technischer) Feinkonzepte zur Umsetzung der Löschverpflichtungen
- Umsetzung des Konzeptes
- Tests zur Funktionsfähigkeit &-weise der Löschroutinen

IT

Vorgehensweise im Projekt (Visualisiert Beispiel)



Fachliche Lösung
Beispiel: Fachkonzept und Feinkonzept Löschen

1. Zusammenfassung
2. Datenbestände
   - Eingesetzte IT-Systeme / Anwendungen
   - Datenbestände
   - Prozess(e) der Datenverarbeitung
3. Lösch-, Sperr- und Anonymisierungsvorgaben
   - Bestimmung der Aufbewahrungsfristen
   - Festlegung von Lösch- und Sperrfristen ((datenschutz)rechtliche Bewertung)
   - Beschreibung der Löschregeln und Übersicht der Löschklassen
4. Umsetzung
   - Definition der Löschmechanismen (Lösch-/Anonymisierungsprozess, Initiierung der Löschung, verantwortlicher Mitarbeiter, Nachweis der Löschung/Sperrung/Anonymisierung), Nachweis der Löschung und Dokumentation
5. Umgang mit Sondersituationen
   - Außerordentliche Löschung/Sperrung wg. Recht auf Löschung/Einschränkung
   - Recht auf Vergessenwerden: Benachrichtigung von Empfängern
   - Aussetzung der Löschung, z.B. rechtliche Auseinandersetzungen
   - Regeln für Backups
6. Kontrolle/Audit
7. Pflege und Weiterentwicklung
8. Verantwortlichkeiten

Sonstige Anforderungen

Verantwortung für Löschkonzept 1	Rolle des Verant-wortlichen für Datenschutz 2	Verantwortung für Umsetzungs-vorgaben 3	Organisatorische Einbettung 4	Interne Melde-pflichten 5
Zuweisung der Verantwortlichkeiten für die Erstellung und Pflege des Löschkonzeptes • Projektverantwor-tung • Fortschreibung bei neuen/geänderten Datenarten.	Zu konsultieren bei • Prüfung von Löschregeln • Freigabe-Beteiligung (Umsetzungs-vorgaben für Löschmaßnahmen) • Audit.	Klare Zuweisung der Verantwort-lichkeiten für die IT-seitige Umsetzung • Tests und fachliche Freigabe • Initiierung der Löschung • Umsetzung von Anfragen Betroffener • Dienstleister-management.	Klare Anweisungen an Mitarbeiter • zur Aufbewahrung/ Löschung von Daten • zur Dokumentation der Löschung.	Verpflichtung jeder Organisationseinheit • Unregelmäßigkei-ten bei Löschmaß-nahmen • Bestände mit pbD, für die keine oder eine falsche Lösch-regel besteht, • neue Datenarten / Verarbeitungs-prozesse zu melden.

Technische Lösungsmöglichkeiten

	EPI-USE	SAP ILM
Adressierte Systeme	• SAP-Systeme • Non-SAP-Systeme (über Schnittstellen)	• ILM-fähige SAP-Systeme (z.B. ERP)
Identifizierung der Daten	• Hinterlegung eines Regelwerks für jedes einzelne Datenfeld	• Daten werden in ILM-Objekten geclustert
Löschung der Daten	• Daten können gelöscht, verfremdet oder auf Initialwert zurückgesetzt werden → Fokus Stammdaten / Anpassung	• Löschung orientiert sich an ILM-Objekten

Questions

Dr. Jan-Peter Ohrtmann

PwC Legal

Partner IT & Datenrecht

jan-peter.ohrtmann@pwc.com

0171 761 4597