

SAP HCM EU-DSGVO (ILM)

im SAP HCM umsetzen und betreiben (AMS)



Hagen Bornemann
Senior Manager SAP HCM

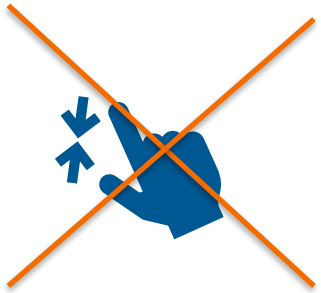
Organisatorisches

Unterlagen

Die Unterlagen werden im Anschluss per Mail verschickt

Fragen

Stellen Sie Ihre Fragen bitte per Chatfunktion

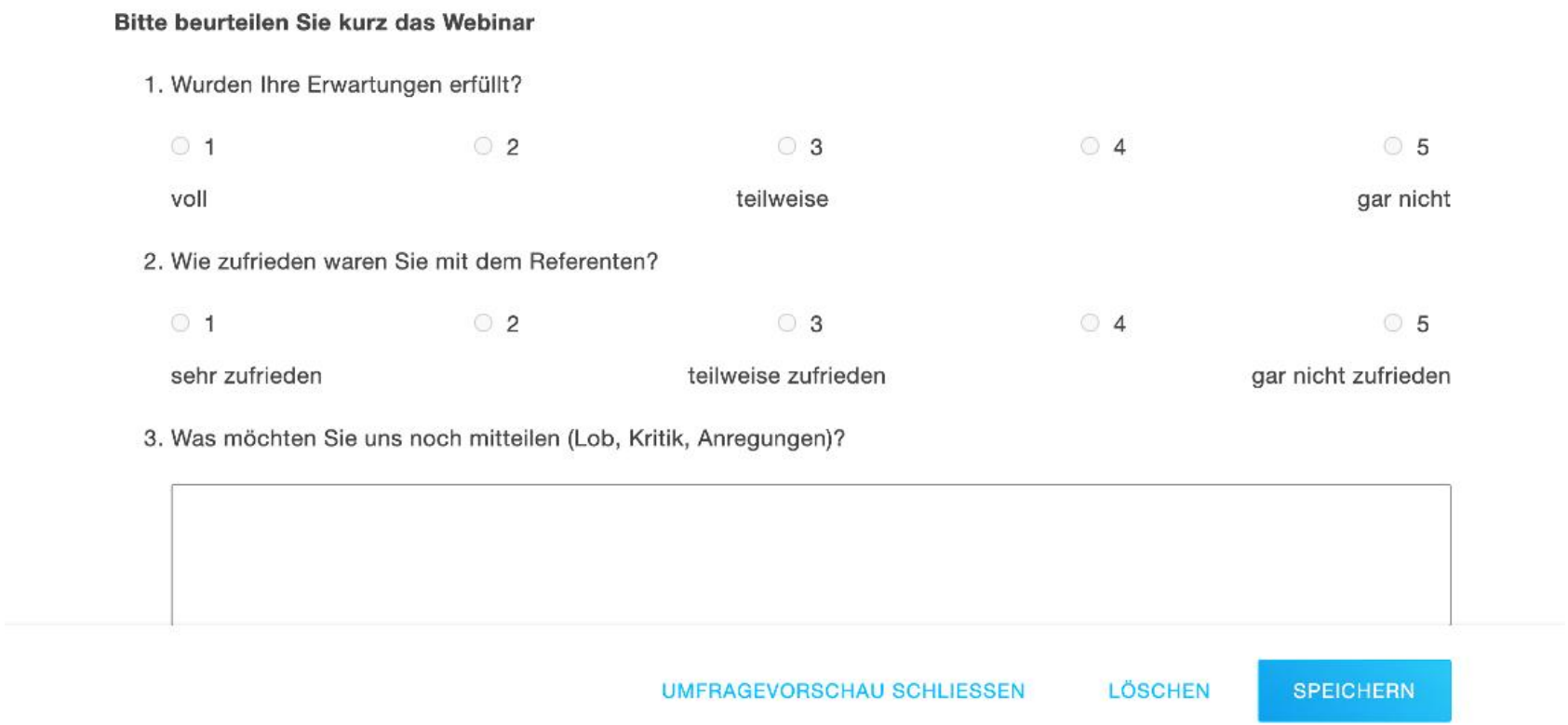


Handzeichen

Werden während des Webinars nicht registriert

Organisatorisches

Bitte geben Sie Feedback. Die Umfrage startet automatisch, wenn Sie das Webinar beenden!



ÜBER MICH



Hagen Bornemann

Senior Manager SAP HCM

hagen.bornemann@lmconsulting.de

- SAP HCM seit über 20 Jahren
- Spezialisierung im SAP ILM (DSGVO) seit 2017
- Entwicklung, Beratung, Projektleitung



AGENDA

01 Allgemeine Projektvorgehensweise

02 Zeitplan, Systemlandschaft, Module / Schnittstellen

03 SAP HCM EU-DSGVO im Application Management

Rechtliche Grundlagen

EU-DSGVO seit 25.05.2018	Zweckmäßige Verwendung von Daten in SAP HCM	Zeitlich begrenzte Verwendung von Daten	Vernichtung der Daten ohne rechtliche Verarbeitungsgrundlage	Hohe Strafen bei Verstößen gegen die Verordnung
Rechtsverbindlich für alle Unternehmen mit Sitz in der EU Ziel ist ein EU-weiter Schutz von personenbezogenen Daten.	Welche Daten dürfen von wem gelesen oder geändert werden? Wer darf wen sehen? Gibt es eine rechtliche Grundlage für die Verwendung?	Daten, die aufgrund gesetzlicher Vorgaben noch nicht gelöscht werden dürfen, sollen für die normale Datenverarbeitung zeitabhängig gesperrt werden.	Datensätze ohne Grundlage der Datenverarbeitung müssen vernichtet werden. Dies betrifft abgegrenzte Datensätze oder Daten von ausgetretenen Personen. .	Strafen bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes. Über 400 Millionen Euro Strafe im Jahr 2019.



01

Allgemeine Projektvorgehensweise

Allgemeine Vorgehensweise

Ist Aufnahme	Prozessanalyse	Verfahrensver-zeichnis & Dateninventur	Fristen der Datenhaltung definieren	Business Blueprint
Umsetzung	Sicherheits-analyse	Vernichten & Sperren von HCM Daten	Optimierung Berechtigungen	Optimierung Systemsicherheit
Betrieb	Tests und erstes Löschen	Compliance-konforme Prozesse	Regelmäßiges Datenvernichten	Regelmäßige Auditierung

Ist-Aufnahme

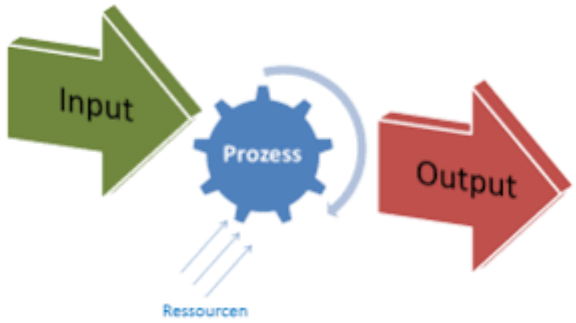
1. Prozessanalyse

Welche personal-wirtschaftlichen Prozesse gibt es im Unternehmen?

Wer ist für die einzelnen Prozesse verantwortlich?

Welche Systeme spielen für die Prozesse eine Rolle?

Wer ist für die Schnittstellen verantwortlich?



Ist-Aufnahme

2. Verfahrensverzeichnis & Dateninventur

Dokumentation der zuvor analysierten Prozesse und Verfahren

Verzeichnis von Verarbeitungstätigkeiten: Art. 30 DSGVO

Was für Daten liegen im SAP HCM-System vor? (RPDINF01)

Welche davon sind für eine Löschung relevant?

Gibt es Besonderheiten, die beachtet werden müssen?

Ist-Aufnahme

2. Verfahrensverzeichnis & Dateninventur

Unser Datenanalysetool:

Wie viele Datensätze liegen in den einzelnen IT/ST vor?

Wie viele davon müssten gelöscht werden?

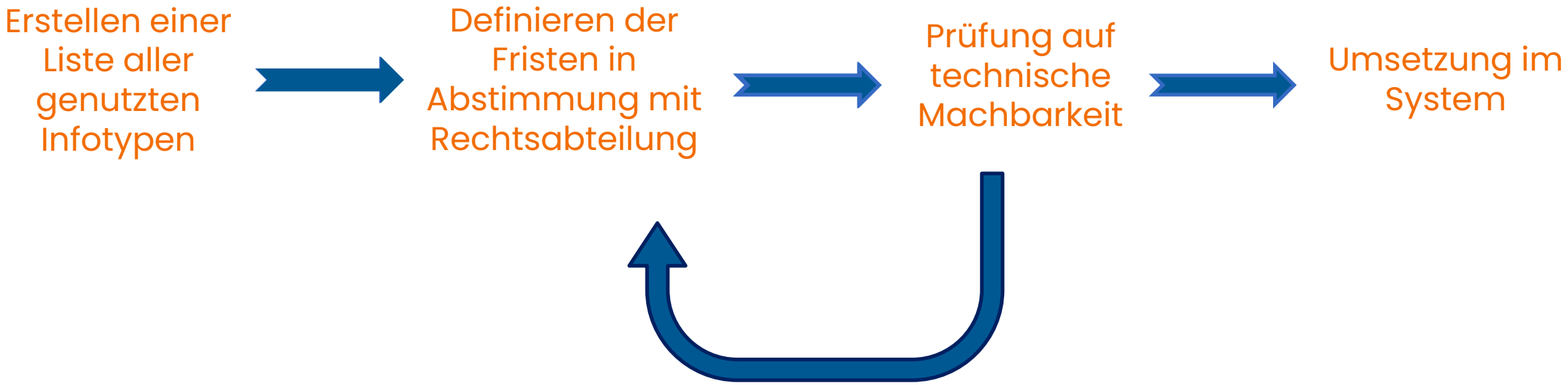
Welches Archivierungsobjekt greift jeweils?

Welche Tabellen sind von dem Archivierungsobjekt betroffen?

Auf welcher gesetzl. Grundlage basiert die Löschfrist?

Ist-Aufnahme

3. Fristen der Datenhaltung definieren



Ist-Aufnahme

4. Business Blueprint

Ausführliche Dokumentation der Umsetzung

Bietet dem Kunden die Möglichkeit, spätere Anpassungen selbst vorzunehmen

Kann zu Nachweiszwecken verwendet werden (bei Kontrollen o. Ä.)

Variiert von Kunde zu Kunde

Wird von uns in Abstimmung mit dem Kunden erstellt

Umsetzung



1. Sicherheitsanalyse

Wie ist der Schutz personenbezogener Daten gewährleistet?

Gibt es ein umfassendes Berechtigungs-konzept im SAP HCM?

Prüfung der allgemeinen IT-Sicherheit, wie z. B.:

- Software-Versionen (veraltet?, regelmäßige Updates? etc.)
- Verschlüsselungs-mechanismen
- Passwortregeln

Umsetzung



2. Vernichten & Sperren von HCM-Daten

Umsetzen der definierten Löschfristen im System

Durchführung und Dokumentation von Funktionstests

Daten, die nicht vernichtet werden, können gesperrt werden

Ausführliche Dokumentation der Umsetzung

Umsetzung mithilfe von SAP ILM

Umsetzung

3. Optimierung der Berechtigungen

Analyse des vorhandenen Berechtigungs-konzeptes:

- Haben alle Personen die „richtigen“ Berechtigungen?
- Werden im ILM-Zusammenhang weitere Berechtigungen bzw. Rollen benötigt?
- Sollte ein neuer Nutzer mit speziellen Berechtigungen angelegt werden?
- Müssen Transaktionen berechtigungsspezifisch angepasst werden?

Anlegen neuer Berechtigungen, Rollen, etc.

Umsetzung

4. Optimierung der Systemsicherheit

Identifizierung von Schwachstellen

Entwickeln von Verbesserungs-möglichkeiten

Umsetzung durch bspw.:

- Einführung/Verbesserung technisch-organisatorischer Maßnahmen
- Regelmäßige Sicherheitsprüfungen
- etc.

„Betrieb“

1. Tests und erstes Löschen

Von unserer Seite erfolgen Funktionstests

Die detaillierten Tests führt der Kunde selbst durch:

- Training der MA durch Schulungen, Workshops, etc.
- Support

Bei erfolgreichen Tests, kann mit dem produktiven Vernichten begonnen werden



„Betrieb“

2. Compliance-konforme Prozesse

- Anpassung der zuvor analysierten Prozesse an den Datenschutz
- Regelmäßige Überprüfung der Prozesse
- Ausführliche Dokumentation der Prozesse
- Bestimmen von Prozessverant-wortlichen

„Betrieb“

2. Compliance-konforme Prozesse

z. B. Anfrage auf Auskunft:	• Report: RPLERDX0 • Nachteile: Aufwand für Personalabteilung, Protokollierung der Ausführung, etc.
Unser Mitarbeiter-Auswertungstool:	• MA kann jederzeit selbstständig seine Daten einsehen (ESS/MSS) • Aufbereitung in einer verständlichen Form • Auswertung als PDF

„Betrieb“

3. Regelmäßiges Datenvernichten



Die Datenvernichtung sollte regelmäßig stattfinden

Unsere Empfehlung: 1x jährlich

Zwei Möglichkeiten:

- Einplanung als Joblauf (automatisiert)
- Anstoß durch einen Mitarbeiter (manuell)

Einige Daten können evtl. nicht regelbasiert vernichtet werden

- Dies muss dann manuell geschehen

„Betrieb“



4. Regelmäßige Auditierung

Zur Überprüfung auf Wirksamkeit und Angemessenheit getroffener Maßnahmen (bspw. TOM)

Beitrag zur Rechenschaftspflicht gemäß DSGVO

Sollten ebenfalls regelmäßig durchgeführt und dokumentiert werden

Das SAP System bietet zahlreiche Funktionen an:

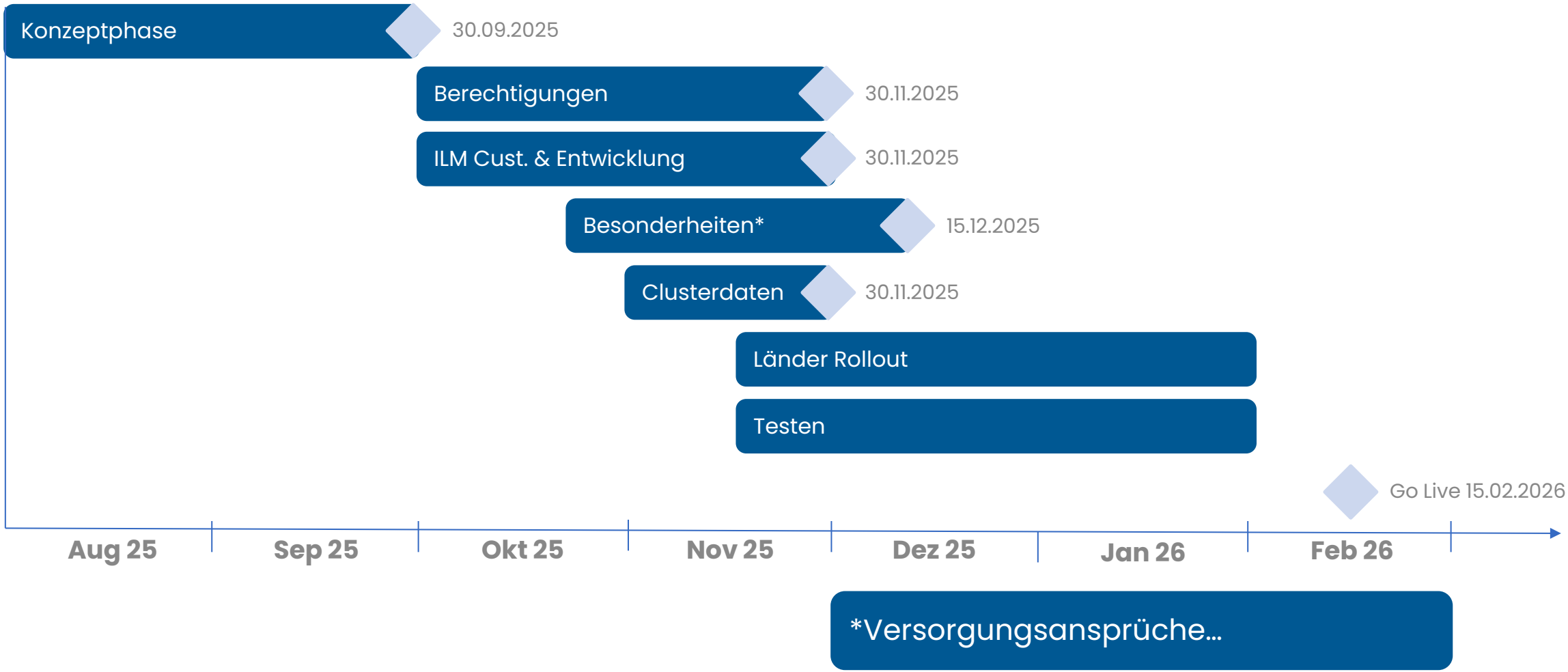
- SAP Audit Management
- SAP Process Control
- etc.



02

Zeitplan, Systemlandschaft, Module / Schnittstellen

Zeitplanung (Beispiel)



Systemlandschaft

Mehrere Möglichkeiten:

2-Systemlandschaft (Entwicklung & Produktion)

3-Systemlandschaft (Entwicklung, Test/Qualität, Produktion)

ein zusätzliches Sandboxsystem -> Vorteile:

- Tests finden auf einem gesonderten System statt
- Das eigentliche Testsystem wird nicht beeinflusst

Ideal: 3-Systemlandschaft + Sandboxsystem

Module / Schnittstellen

- Personaladministration
- Abrechnung
- Zeitwirtschaft
- Reisekostenabrechnung
- Personalkostenplanung
- Bewerberverwaltung (PB)
- Performance Management
- Veranstaltungsmanagement (LSO)

- Organisationsmanagement
- ESS/MSS Szenarien (Zeitbuchungs-korrekturen, Zeitnachweise, Abw.-Workflow)
- Meldedateien (P01*, EEL, AAG, Elster)
- Buchungsläufe
- Versorgungsansprüche
- Schnittstellen zu anderen SAP Systemen und Drittanbietersoftware



03

SAP HCM EU-DSGVO im Application Management

Ihre Ausgangssituation

Sie nutzen seit Jahren SAP HCM und sind verpflichtet …

… die DSGVO umzusetzen und regelmäßig zu Löschen
… stellen sich die folgenden Fragen vor jedem Löschlauf:

- Was muss gelöscht werden?
- Wie wird das Löschen dokumentiert?
- Wie hoch ist der personelle Aufwand?
- Wo muss gelöscht werden (Länder/Mandanten)?
- Bis zu welchem Zeitpunkt muss gelöscht werden?
- Bis zu welchem Zeitpunkt muss gelöscht werden?
- Wer übernimmt das Löschen?
- Wie löscht man?
- Wie hoch ist der zeitliche Aufwand?

Wir haben die Lösung für Sie…

Deletion **a**s **a** **S**ervice (DAAS) von der LM Consulting GmbH

Wir übernehmen die Löschaktivitäten in einem von Ihnen vorgegebenen Rhythmus

Festlegung des Zyklus - die meisten Kunden entscheiden sich für einen jährlichen Zyklus

Sollten wir das EU DSGVO Projekt bzw. das ILM nicht implementiert haben ist zunächst ein Transition Projekt erforderlich

Alle Rahmenbedingungen werden zu Beginn festgelegt

Sie müssen sich nicht mehr um die Löschaktivitäten kümmern

Etwaige Anpassungen, die aufgrund von Updates notwendig werden, übernehmen wir

Alle Löschungen werden von uns dokumentiert und Ihnen zur Verfügung gestellt

Ihr System ist jederzeit revisionssicher und datenschutzkonform

Sie gewinnen Freiräume für die wichtigen Dinge in Ihrem SAP HCM System

Deletion as a Service (DAAS) RoadMap



Regelmäßiges Löschen

04

Finales Löschen

Durchführung der Löschung
Dokumentation und Löschprotokoll
(Business Blueprint)

03

Löschvorbereitung

Anlegen von Testfällen
Durchführung von Testfällen
Dokumentation von Testfällen

02

Vorprojekt

Prüfung
Analyse der Anforderungen
Auffälligkeiten Ergebnis

01

Deletion as a Service (DAAS) - Ablauf

Vorprojekt	Löschvorbereitung	Löschen	Regelmäßiges Löschen	International
Wir prüfen das bestehende System, analysieren die Anforderungen, prüfen auf Auffälligkeiten und besprechen mit dem Kunden das weitere Vorgehen.	Wir besprechen mit dem Kunden ggf. veränderte Anforderungen, setzen diese um und prüfen & protokollieren diese mit Hilfe von Testfällen.	Wir führen die Löschung durch, und passen uns an den Zeitplan des Kunden an. Zudem wird alles dokumentiert, festgehalten und nach Bedarf präsentiert.	Nach Abschluss der Löschung planen wir mit dem Kunden ein regelmäßiges Folgelöschen, damit wir Ihn auch in Zukunft entlasten können.	Wir übernehmen den Service für alle Länder in denen die DSGVO gilt.

Transition/Vorprojekt

(ca 6 Monate vor dem Löschen)

Prüfung

- Konzept und Einrichtung des ILM

Ergebnis

- Transition Bericht

Inhalt des Berichts

- Basis ist der Business Blueprint
- Auffälligkeiten / ungewöhliche Sachverhalte
- Customizingfehler werden dokumentiert
- Regeln technisch plausibel und rechtskonform
- Badl's analysieren

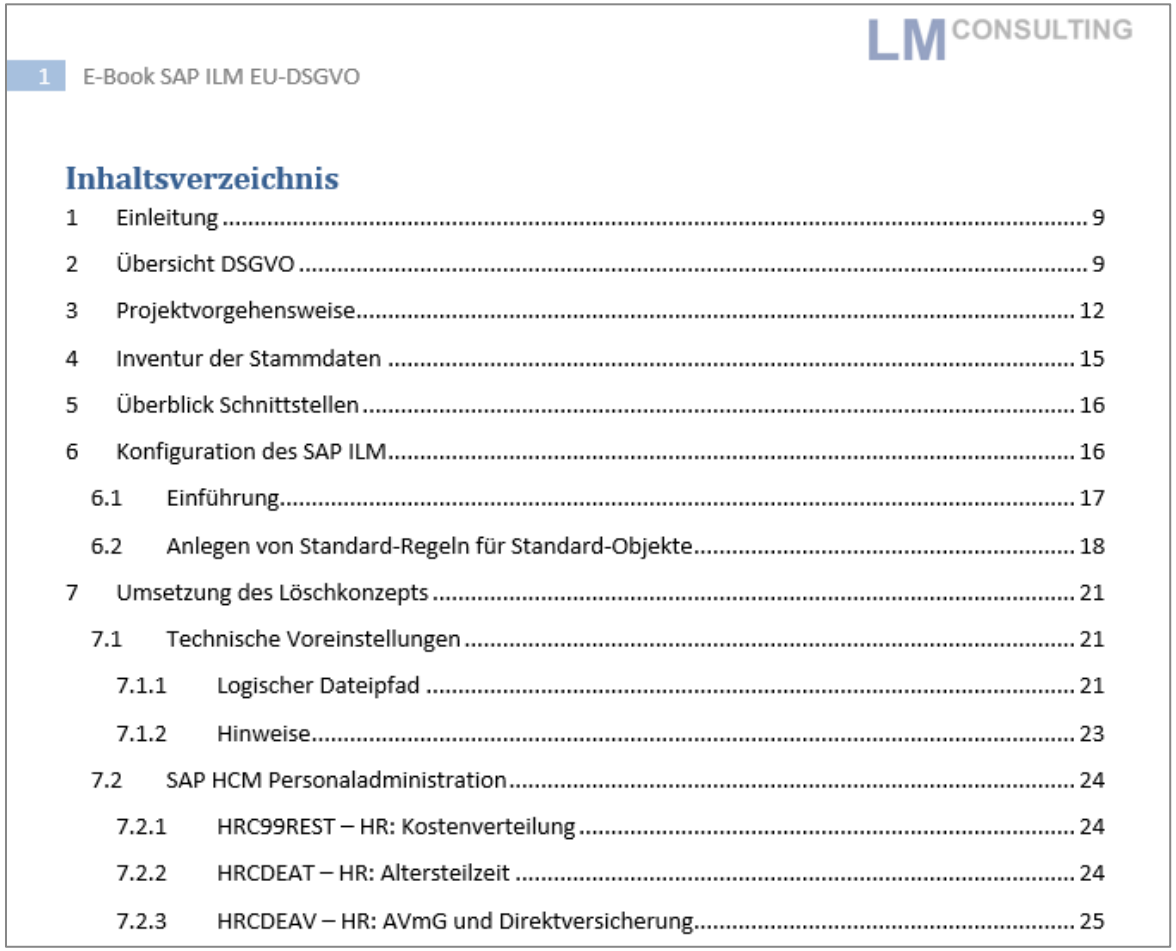
Voraussetzung

Aktuelles Abbild des Produktiv Systems oder einer Sandbox

Transition/Vorprojekt

(ca 6 Monate vor dem Löschen)

- Wir analysieren Ihr Konzept und die Einrichtung Ihres ILM und transferieren es in unseren standardisierten Business Blueprint
- Dieser dient als Dokumentation und Vorlage für die zukünftigen Löschzyklen
- Die Prüfung umfasst das allgemeine ILM Customizing, Regelwerke, BadI Implementierungen und weitere kundenspezifische Umsetzungen innerhalb des ILM sowie EU DSGVO spezifische Berechtigungen



LM CONSULTING

1 E-Book SAP ILM EU-DSGVO

Inhaltsverzeichnis

1 Einleitung 9
2 Übersicht DSGVO 9
3 Projektvorgehensweise 12
4 Inventur der Stammdaten 15
5 Überblick Schnittstellen 16
6 Konfiguration des SAP ILM 16
6.1 Einführung 17
6.2 Anlegen von Standard-Regeln für Standard-Objekte 18
7 Umsetzung des Löschkonzepts 21
7.1 Technische Voreinstellungen 21
7.1.1 Logischer Dateipfad 21
7.1.2 Hinweise 23
7.2 SAP HCM Personaladministration 24
7.2.1 HRC99REST – HR: Kostenverteilung 24
7.2.2 HRCDEAT – HR: Altersteilzeit 24
7.2.3 HRCDEAV – HR: AVmG und Direktversicherung 25

Transition/Vorprojekt

(ca 6 Monate vor dem Löschen)

- Die umgesetzten Regelwerke werden mit den ursprünglichen Anforderungen abgeglichen
- Es wird geprüft ob diese technisch plausibel und rechtskonform sind

ILM Objekt	Infotyp	Bezeichnung	Frist	Zeiteinheit	verfügbare Bedingungsfelder	verfügbare Zeitbezüge	Zeitversatz
HRPA_ADRGR	0006	Anschriften	6	Jahre	Archivierungsteilobjekt Ländergruppierung **Beschäftigungsstatus**	**Ende des Datensatzes** **Austrittsdatum**	**Ende des Jahres** **Ende des Jahres**

Regeln zum Regelwerk HRPA_ADRGR

Beschäftigung	bis	Kennz. für High-Date	bis	Min. Aufbew.zeitraum	Max. AufbewZeitraum	Einheit AufbZeitraum	Zeitbezug	Zeitversatz	ILM-Ablage	Regel-Priorität
0	3	N	N	6	6	Jahr	Ende des Datensatzes	Ende des Jahres		
0	0	Y	Y	6	6	Jahr	Austrittsdatum des Mita…	Ende des Jahres		

Protokoll (Zusammenfassun… | Protokoll (Details)

Typ	Meldungstext	Ltxt	Objektanz.	Objekt (Beispiel)
⚠	Vernichten nicht möglich; ständiger Wohnsitz muss im System bleiben		2	60000034 | 0006 | 1 | 01.01.2003 | 31.12.9999
■	Kriterien für die Datenvernichtung erfüllt		4	60000034 | 0006 | 2 | 01.01.2001 | 31.12.9999
■	Daten für ArchivTeilobjekt 1 bis zum 16.10.2008 vorbereitet zur Datenvernichtung	?	12	60000034 | 0283 | 1 | 01.01.1800 | 16.10.2008
●	Aufbewahrungsregel erlaubt keine Vernichtung der Daten	?	4	60004430 | 0006 | 2 | 01.01.2002 | 31.12.9999
●	Keine passende Regel gefunden für Prüfgebiet HCM_DP des ILM-Objekts HRPA_ADRS	?	36	60000034|CNHK
⚠	2 Mitarbeiter bearbeitet		1	
⚠	Dies war ein Testlauf; es wurden keine Daten vernichtet		1	HRPA_ADRS
⚠	Selektionsdatum "Daten selektieren bis" zurückgesetzt auf: 31.07.2017	?	2	60000034

- Badl's werden analysiert, Customizingfehler und sonstige Auffälligkeiten/ungewöhnliche Sachverhalte werden dokumentiert

Löschvorbereitung

(ca. 3 Monate vor dem Löschen)

Prüfung und Einspielen von Patches/SAP Hinweisen

Abgleich mit regelmäßigem Support

Prüfung und Klärung veränderter Prozesse und damit verbundene Anforderungen an die anstehenden Löschungen und zeitraumabhängigen Berechtigungen

Aufnahme der Anforderungen in den Business Blueprint

Anpassung Customizing, Entwicklung, Regelwerke und zeitraumabhängiger Berechtigungen an die veränderten Anforderungen

Vorbereitung von Testfällen durch den Kunden gemäß den Löschroutinen

Durchführung und ausführliche Dokumentation der Testfälle

Regelmäßiges Löschen beim Kunden

Durchführung der Löschung

Support bei Problemen

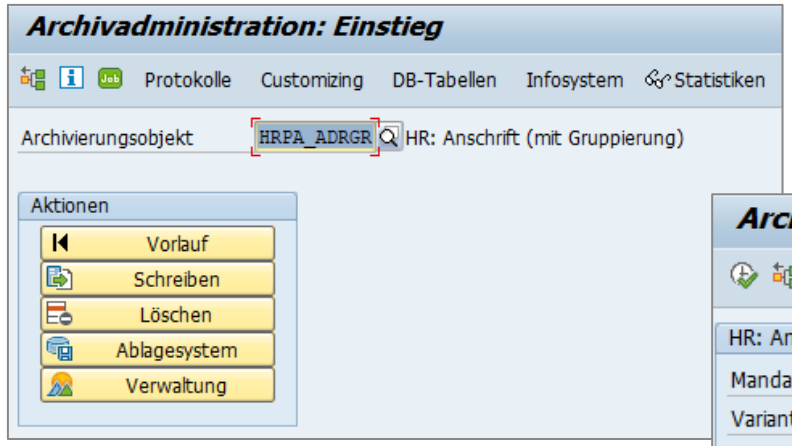
Dokumentation der Löschung:

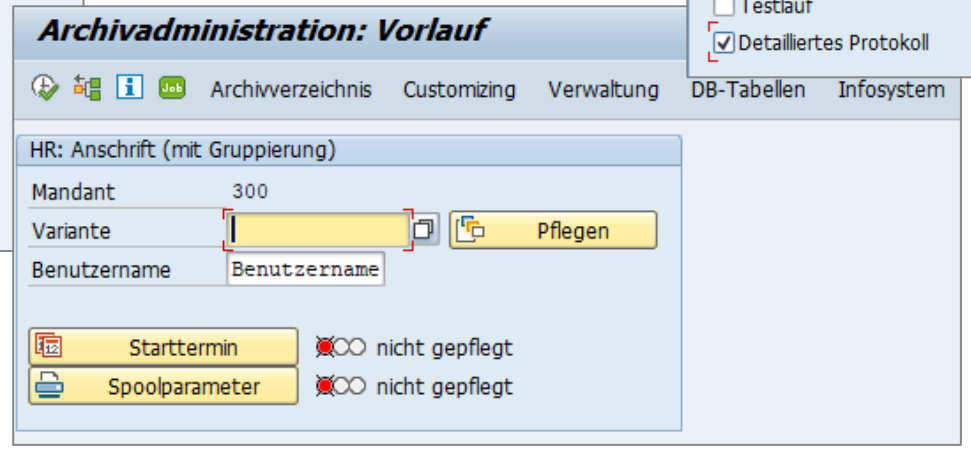
- Screenshots der Löschprotokolle
- Screenshots der aufkommenden Meldungen
- Anzahl der Löschungen pro ILM-Objekt
- Ergebnis: Löschprotokoll angelehnt an Business Blueprint

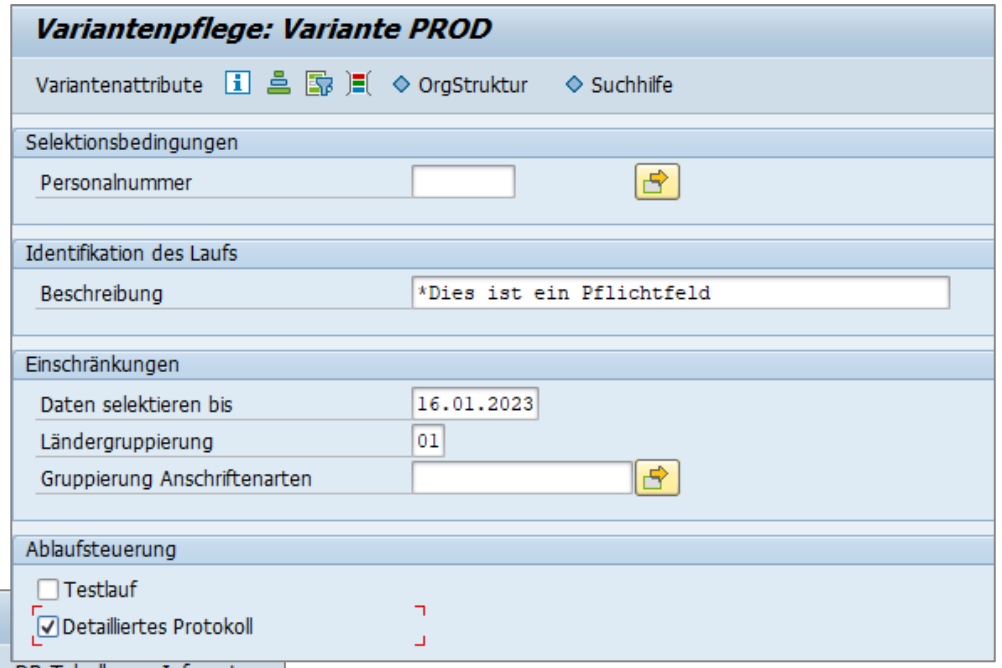


Regelmäßiges Löschen beim Kunden

- Die Löschung wird nach Terminabsprache von uns durchgeführt
- Dabei werden über die Transaktion SARA die Löschvarianten vorbereitet und ausgeführt







Regelmäßiges Löschen beim Kunden

- Die Dokumentation erfolgt mit Screenshots der Löschprotokolle und ggf. Erläuterung der Meldungen

Produktivlauf SARA – Protokoll (Detail):

Protokoll (Zusammenfassung) | Protokoll (Details)

0 | 25 | 195 | 72

T...	Meldungstext	Ltxt	Objekt
▲	Selektionsdatum "Daten selektieren bis" zurückgesetzt auf: 31.12.2022	?	03100031
▲	Vernichten nicht möglich; ständiger Wohnsitz muss im System bleiben		03100031 | 0006 | 1 | 01.05.2012 | 31.12.9999
■	Kriterien für die Datenvernichtung erfüllt		03100031 | 0006 | 1 | 01.01.2011 | 30.04.2012
▲	Selektionsdatum "Daten selektieren bis" zurückgesetzt auf: 31.07.2017	?	03100047
▲	Vernichten nicht möglich; ständiger Wohnsitz muss im System bleiben		03100047 | 0006 | 1 | 01.11.2012 | 31.12.9999
■	Kriterien für die Datenvernichtung erfüllt		03100047 | 0006 | 1 | 05.04.2011 | 31.10.2012
●	abrechnen bis darf nur in nichtaktivem Zeitraum liegen	?	03100031
●	Fehler beim Aktualisieren von IT0003; Personalnr. 03100031 wurde zu...	?	03100031
■	Daten bis 11.01.2013 vorbereitet zur Vernichtung	?	03100047 | 0283 | HRPA_ADRGR | 01.01.1800 | 11.01.2013

Abbildung 26: Sara Protokoll - Detail HRPA_ADRGR (Vorlauf)

Eingeschränkt auf die Personalnummern 3100031 und 3100047. Zu beiden gäbe es jeweils einen Datensatz zum Löschen.

PERNR: 3100031 → Austritt 01.12.2016
Fehler im IT0003 → Das „abrechnen bis“ Datum lag im aktiven Zeitraum.
Daher keine weitere Verarbeitung.

PERNR: 3100047 → Aktiv
Keine Fehler → Personalnummer kann verarbeitet werden.

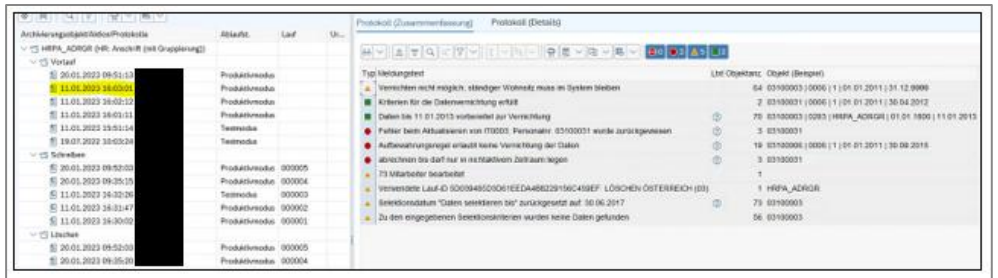


Abbildung 23: Sara Protokoll - Zusammenfassung HRPA_ADRGR (Vorlauf)

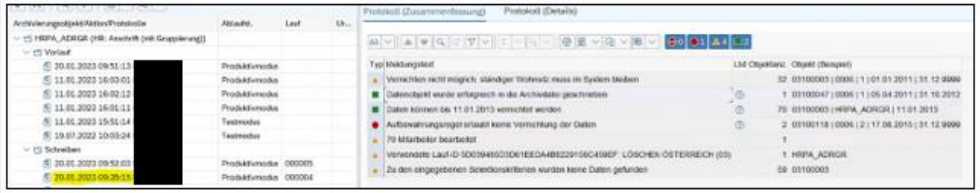


Abbildung 24: Sara Protokoll - Zusammenfassung HRPA_ADRGR (Schreiblauf)

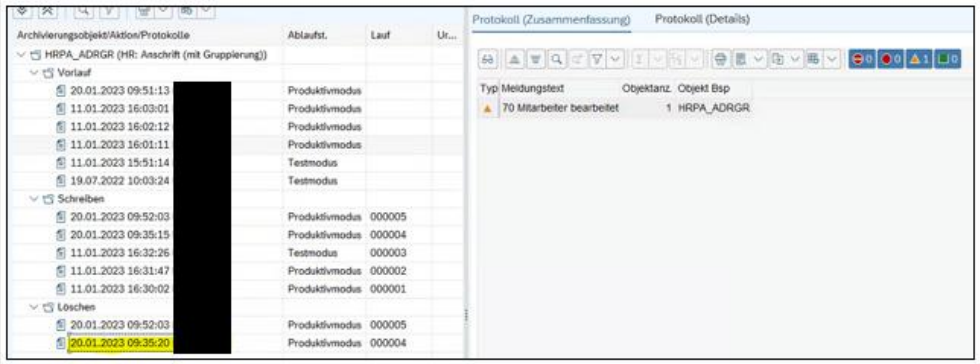


Abbildung 25: Sara Protokoll - Zusammenfassung HRPA_ADRGR (Löschlauf)



ILM Tools

HCM Regel DSGVO	• Zentrale Anzeige von implementierten Regeln • Anzeige von verknüpften Infotypen bzw. Datenbanktabellen • Anzeige zugeordneter Regelwerke • Anzeige der Fristen, Bedingungen und Zeitbezüge • Anzeige technisches Customizing
HCM Analyse DSGVO	• Analyse aller HCM-Daten im System • Unterteilt auf Länderorganisationen • Infotypen, Datenbanktabellen und Cluster • Exportierbar als Excel-Sheet • Nutzbar als Vollständigkeitskontrolle bei neuen HCM-Daten
HCM Legal Hold DSGVO	• Erstellen und Löschen von Vernichtungssperren • Ermöglicht das Behalten von Daten trotz gültigem Regelwerk • Setzt Sperren für alle ILM-Objekte • Ein Mausklick zum Setzen der Sperre für mehrere Personen

ILM Tools

HCM Custom Data DSGVO	• Löschen von beliebigen Daten aus transparenten Datenbanktabellen • Eingebettet in das ILM-Framework • Standard-Protokollierung • Berücksichtigung von Legal Hold • Aufruf über ILM_DESTRUCTION
HCM Accounting DSGVO	• Überprüft inkonsistente Werte in Infotyp 0003 • Rückrechnungswerte Payroll und Time • Überprüfung auf Werte, die das Löschen mit SAP ILM verhindern • Bereinigung separat mit Standardreport RPUTRBK0
HCM Automatic DSGVO	• Starten der Datenvernichtung der ILM-Objekte • Automatisch in der richtigen Reihenfolge • Eventgesteuerter Start • Protokollierung im ILM-Framework



Beispiel eines zeitlichen Ablaufes

September						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

October						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

November						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Events

Sep. 1st Vorprojekt/Transition Kick off
Sep. 11-12th Analyse
Sep. 25-26th Analyse / Ergebnis

Oct. 16-17rd Löschvorbereitung / Anlegen von Testfällen
Oct. 23rd Durchführung der Tests
Oct. 30-31th Durchführung der Tests

Nov. 7-8th Dokumentation der Tests
Nov. 14th Dokumentation der Tests

Beispiel eines zeitlichen Ablaufes

December						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

January						
S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

Events

Dez. Jahreswechsel Aktivitäten

Jan. Systemupdates

Feb. 5–12th Durchführung der Löschung
Feb. 13–14th Dokumentation
Feb. 15th Löschprotokoll
Regelmäßiges Löschen



Vielen Dank!



Hagen Bornemann
Senior Manager SAP HCM
hagen.bornemann@lmconsulting.de