Das SAP (HCM) System und die personenbezogenen Daten auf EU-DSGVO Konformität prüfen. “

Thomas KASTNER, smarterSec GmbH

SAP System/HR Daten auf DSGVO Konformität prüfen

Agenda

- Datenschutzgrundverordnung
- Bußgelder / Datenpannen
- Relevante Bereiche der EU-DSGVO

- Bereiche der EU-DSGVO in Verbindung mit SAP

- Bin ich EU-DSGVO konform?
  - Die SAP HCM Konfiguration / Berechtigungen
  - Die SAP HCM Daten (gesetzliche Aufbewahrungsfristen)
  - Das SAP System (ohne Sicherheit keine Konformität)

Datenschutzgrundverordnung EU-DSGVO

Rechtliche Grundlagen: EU-DSGVO, BDSG-Neu

- Datenschutzgrundverordnung trat am 25.05.2016 in Kraft
- Datenschutzgrundverordnung wurde am **25.05.2018** verbindlich
- EU-DSGVO engl. GDPR General Data Protection Regulation

- Jeder EU-Staat hat ein eigenes Datenschutzrecht
- Ergänzend für Österreich:
  Datenschutzgesetz – DSG (Das Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 idgF., ist das geltende österreichische Datenschutzgesetz und ergänzt die Datenschutz-Grundverordnung (DSGVO))

Datenschutzgrundverordnung EU-DSGVO

EU-DSGVO Bußgelder, Datenpannen

- Bei Nichteinhaltung der EU-DSGVO sind Strafen von bis zu
  20 Millionen EUR
  oder bis zu 4% des gesamten Vorjahresumsatzes möglich

- 2020: **26.057** gemeldete Datenpannen nach §33 DSGVO

- Notebooksbilliger.de AG (Dezember 2020) **10,4 Millionen EUR**

- Höchstes Bußgeld 2020: H&M **35 Millionen EUR**

Datenschutzgrundverordnung EU-DSGVO

Datenpannen, Beispiele: Top 5 aus März 2021

- Fahrlässige Verletzung der datenschutzrechtlichen Rechenschaftspflicht
  - **300.000** EUR (Art. 5 Abs. 2 DSGVO)
- Verspätete Meldung einer schweren Datenschutzverletzung
  - **475.000** EUR (Art. 33 Abs. 1 DSGVO)
- Identifizierbarkeit von Fahrzeughaltern wegen fehlerhafter QR-Codes
  - **350.000** EUR
    (Art. 5 DSGVO, Art. 6 DSGVO, Art. 28 DSGVO, Art. 32 DSGVO)
- Unzulässige Werbung trotz Widerspruch der Betroffenen
  - **8.150.000** EUR
    (Art. 21 DSGVO, Art. 24 DSGVO, Art. 28 DSGVO, Art. 44 DSGVO)
- Unzulässige Verarbeitung von Gesundheitsdaten
  - **195.000** EUR
    (Art. 5 Abs. 1 DSGVO, Art. 6 Abs. 1 DSGVO, Art. 9 Abs. 2 DSGVO)

Relevante Bereiche der EU-DSGVO

- Zugangskontrolle
  - "Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren"
- Zugriffskontrolle
  - "zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können"
- Weitergabekontrolle
  - "zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist"
- Eingabekontrolle
  - "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personen-bezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind"
- Auftragskontrolle
  - "zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können"

Betroffene Bereiche der EU-DSGVO

- Verfügbarkeitskontrolle
  - "zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"
- Datentrennung
  - "zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können"
- Auskunftsrecht
  - Art 15 DSGVO über Verarbeitungszweck; Kategorien personenbezogenen Daten, an wen weitergegen …
- Sperren und Löschen
  - Art 17 Abs. 1 DSGVO sind personenbezogene Daten künftig unverzüglich zu löschen, wenn … Zweckbestimmung, Einwilligung widerruft, …
- Verschlüsselung
  - Art 32 DSGVO; Mail, Schnittstellen
- Einwilligung
  - Art 7 DSGVO; explizite schriftliche Einwilligungserklärung zur Verarbeitung der Daten

Datenschutzgrundverordnung EU-DSGVO

Und was hat das mit SAP und SAP HCM zu tun?

- Zugangskontrolle
  - 2FA, Passwortrichtlinien, alte Passworthashes, SSO, Benutzerverwaltung
- Zugriffskontrolle
  - SAP_ALL, SoD, Schutz vor internen und externen Angreifern, P_DURATION nicht gepflegt
- Weitergabekontrolle
  - Keine Übersicht aller Schnittstellen und der Relevanz, Keine Verschlüsselung von (HR) Schnittstellen; Schnittstellenempfänger nicht bekannt, welcher Zweck nicht bekannt
- Eingabekontrolle
  - Änderungsbelege PA, Änderungsbelege OM, Änderungsbelege PB, Protokollierung Reportstarts
- Auskunftsrecht
  - Auskunft gemäß Artikel 15 DSGVO im SAP HCM nicht umgesetzt, innerhalb 14 Tagen, Mitarbeiterauskunft (RPLERDX0)
- Sperren und Löschen
  - Aufbewahrungsfristen für ausgetretene Mitarbeiter nicht definiert, 25 Jahre produktiv, noch nie etwas gelöscht, Infotyp 3246 Vernichtungssperre nicht gepflegt

Datenschutzgrundverordnung EU-DSGVO

Zusammenfassung: Relevante Bereiche der EU-DSGVO vs. Realität

Zugangskontrolle	in aller Regel umgesetzt; unzulänglich
Zugriffskontrolle	in aller Regel umgesetzt; unzulänglich
Weitergabekontrolle	nur teilweise umgesetzt bspw. B2A
Eingabekontrolle	in aller Regel umgesetzt; unzulänglich
Auftragskontrolle	in aller Regel umgesetzt
Verfügbarkeitskontrolle	in aller Regel umgesetzt
Datentrennung	in aller Regel umgesetzt
Auskunftsrecht	selten umgesetzt
Sperren und Löschen	fast nicht umgesetzt
Verschlüsselung	Siehe auch Weitergabekontrolle
Einwilligung	in aller Regel umgesetzt

Bin ich EU-DSGVO konform?

SAP HCM Konfiguration und Berechtigungen

- Mitarbeiterauskunft
  - Konfiguriert?
  - Ausgeführt?
- Änderungsprotokollierung (wer?, wann?, was?)
  - Änderungsprotokollierung PA
  - Änderungsprotokollierung PB
- Protokollierung von Reportstarts
- Prüfung auf Ende des Verwendungszwecks
- Zeitabhängiges Sperren von Daten
- Vorhandensein Infotyp 0283 Archivierung/Datenvernichtung
- Vorhandensein Infotyp 3246 Vernichtungssperre

Bin ich EU-DSGVO konform?

SAP HCM Konfiguration und Berechtigungen

- Mitarbeiterauskunft (RPLERDX0)
  - Konfiguriert? (V_T77PADERD_FLDS)
  - Ausgeführt? (THRPAD_ERD_LOG)
- Änderungsprotokollierung (wer?, wann?, was?)
  - Änderungsprotokollierung PA (V_T585A, V_T585B, V_T585C)
  - Änderungsprotokollierung PB (V_T585A, V_T585B, V_T585C)
- Protokollierung von Reportstarts (V_T599R)
- Prüfung auf Ende des Verwendungszwecks (V_T77HREOP_PER)
- Zeitabhängiges Sperren von Daten (P_DURATION)
- Vorhandensein Infotyp 0283 Archivierung/Datenvernichtung (SE16)
- Vorhandensein Infotyp 3246 Vernichtungssperre (SE16)

Bin ich EU-DSGVO konform?

SAP HCM Daten (gesetzliche Aufbewahrungsfristen/-pflichten)

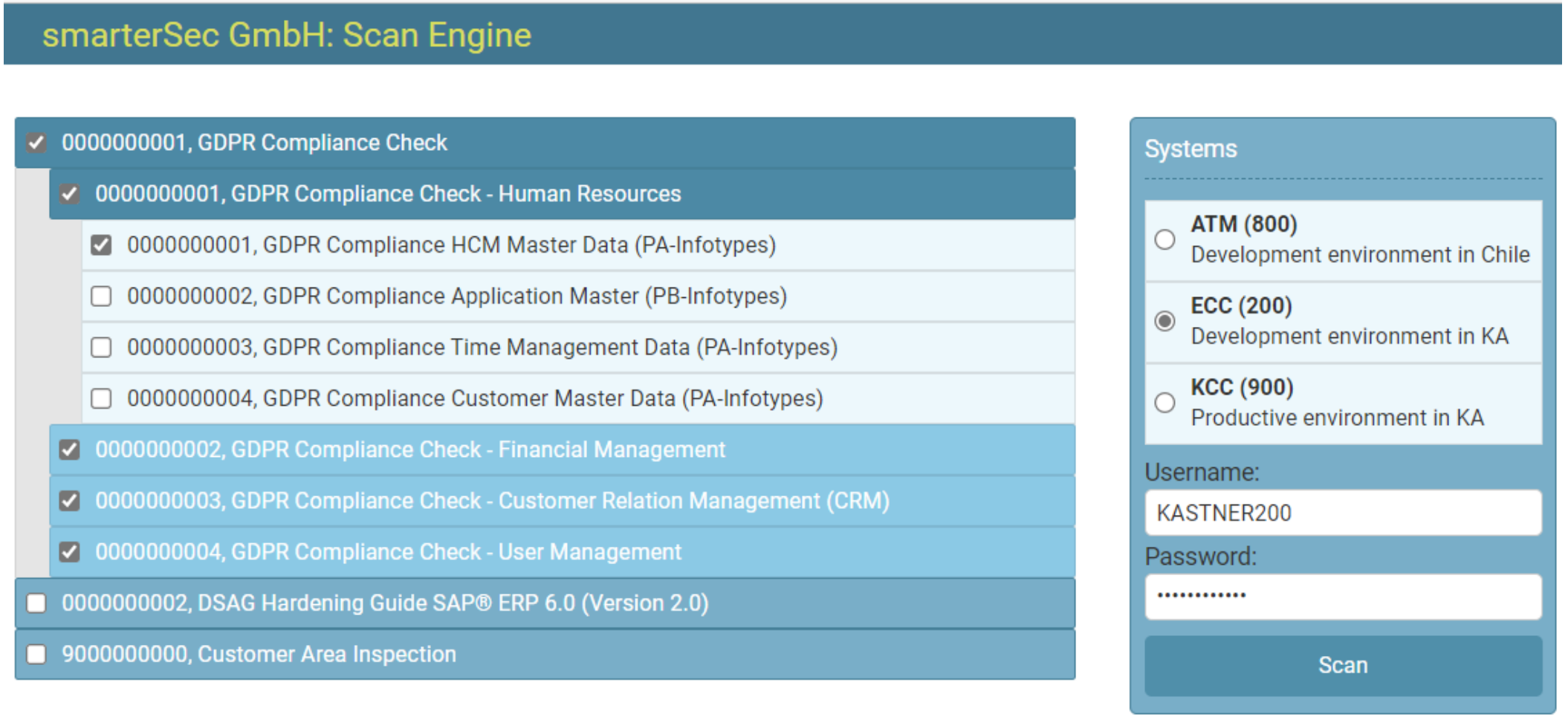
Prüfung auf gesetzliche Aufbewahrungsfristen:

- Die Aufbewahrungsfristen/-pflichten in der Personalbrechnung liegen zwischen 3 und 30 Jahren (BAO, ASVG, AVRAG, ASchG, AÜG, ABGB)
- SAP liefert keine Regeln zu den Aufbewahrungsfristen/-pflichten, diese sind vom Kunden selbst zu definieren, ebenso die Abhängigkeiten zwischen den Infotypen, bspw. den Abwesenheiten
- Prüfung der gesetzlichen Aufbewahrungsfristen/-pflichten aller vorhandenen Infotypen im SAP System automatisch ermitteln

→ SAP DSGVO Assessment by smarterSec GmbH (SDA)

Bin ich EU-DSGVO konform?

SAP HCM Daten (gesetzliche Aufbewahrungsfristen/-pflichten)



Bin ich EU-DSGVO konform?

SAP HCM Daten (gesetzliche Aufbewahrungsfristen/-pflichten)

- Grün: alles konform nach den gesetzlichen Aufbewahrungsfristen
- Rot: „längere“ Zeit aufbewahrt, d.h. länger als die gesetzlichen Aufbewahrungsfristen
  Angabe wieviel Sätze mit drill-down Möglichkeit

smarterSec GmbH: Scan Results

Testcase	Index	Datasource	Details
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	1	PA0005	▪ occurrences: 1
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	2	PA0006	▪ occurrences: 60
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	3	PA0007	▪ occurrences: 53
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	4	PA0008	▪ occurrences: 55
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	5	PA0009	▪ occurrences: 11
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	6	PA0010	▪ occurrences: 2
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	7	PA0011	
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	8	PA0012	▪ occurrences: 15
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	9	PA0013	▪ occurrences: 16
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	10	PA0014	▪ occurrences: 20
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	11	PA0015	▪ occurrences: 94
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	12	PA0016	▪ occurrences: 5
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	13	PA0030	▪ occurrences: 1 ▪ inconsistencies: 1
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	14	PA0040	▪ occurrences: 9
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	15	PA0111	
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	16	PA0112	
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	17	PA0113	
0000000001, GDPR Compliance HCM Master Data (PA-Infotypes)	18	PA0114	

Löschung von Daten – dezidierte Infotypen

- SAP Information Lifecycle Management (SAP ILM)
  - Löschung der Infotypen / Infotyp-Sätze
  - Infotyp 0283 Archivierung/Datenvernichtung
  - Beispiele von SAP_ILM Objekten:
    - HRPA_TASK HR (Terminverfolgung)
    - HRTIM_MAT HR (Mutterschutz)
    - PA_PDOC HR (Abrechnungsbelege für die Buchung ins RW)
    - PA_CALC HR (Personalabrechnungsergebnisse)
  - Liste
    - 2122906 - ILM: Liste von ILM Objekten mit zugeordneten Archivierungs- / Data Destruction Objekten - SAP ONE Support Launchpad

Löschung von Daten – komplette Personalnummern

- Löschung kompletter P# (RPUDELPP; RPUDELPN)
  - HRPAD_DELPN
  - Mehrstufige Löschung

Status	Kurzbeschreibung
00	Kein Status für Personalnummer gespeichert
01	Vernichtung der Personalnummer wurde beantragt
02	Vernichtungsantrag der Personalnummer wurde zurückgezogen
03	Vernichtung der Personalnummer wurde angestoßen
04	Vernichtung der Personalnummer wurde durchgeführt

Bin ich EU-DSGVO konform?

Das SAP System (ohne Sicherheit keine Konformität)

Wirtschaftsprüfer attestieren, aber …

RSURS003	SAP Standardpassworte
SAP_ALL	Generalrechte
BCODE	Schwache (alte) Passwort-Hashes
Client 001/066	SAP Standard Mandanten immer noch im SAP System
Security Patches	monatliche Updates fehlen
U. v. a. m	DSAG Prüfleitfaden, SAP Netweaver Hardening Guide, BSI Grundschutzhandbuch etc.

→ SAP Risk Assessment by smarterSec GmbH (SRA)

Ihre Fragen

Danke für Ihr Interesse!

Haben Sie irgendwelche Fragen?
Bitte kontaktieren Sie uns!

info@smartersec.com
+49 (0)721-1608000
www.smartersec.com

FOLLOW US ON SOCIAL MEDIA

smarterSec GmbH | Albert-Nestler-Str. 21 | 76131 Karlsruhe | Germany