DSAG-Positionspapier

Künftige SAP-Cloud-Lösungen für das Personalwesen in der öffentlichen Verwaltung

Standpunkte der DSAG

Stand: August 2021

Vorwort

Der Einsatz von Human-Resources-Cloud-Lösungen im öffentlichen Dienst ist an besondere Bedingungen geknüpft. Das von SAP initial vorgeschlagene Cloud-in-Country-Modell kann sie noch nicht vollständig erfüllen.

Inhaltsverzeichnis

1. SAP-Cloud-Strategie beim Human-Capital-Management

Die Zukunft im Human-Capital-Management (HCM) liegt für SAP in der Cloud. Zwar gibt es für die bisherige ERP-Lösung für das Personalwesen (SAP HCM) eine Wartungszusage bis mindestens 2027, optional bis 2030. Zudem erhalten SAP-Kunden, die in diesem zeitlichen Umfeld noch nicht in die Cloud wechseln wollen oder können, Planungssicherheit: Ihnen wird weiterhin eine HCM-On-Premise-Lösung im Kontext von SAP S/4HANA angeboten. Mit Umstieg auf S/4HANA gilt für HCM die Wartungszusage aktuell bis mindestens 2040. Strategisch konzentriert sich SAP jedoch klar auf SuccessFactors; Investitionen erfolgen in Innovationen in der Cloud und in den hybriden Betrieb.

Nicht für alle Branchen stellt SuccessFactors allerdings zum jetzigen Zeitpunkt eine gangbare Alternative zur bewährten On-Premise-Lösung dar. Dazu gehört in Deutschland in besonderem Maße die öffentliche Verwaltung. Gründe dafür finden sich in den Bereichen Datenschutz, Sicherheit und Funktionalität. Dort gelten für öffentliche Verwaltungen zum Teil schärfere Bedingungen als in anderen Branchen.

2. Die Initiative „Einsatz von HR-Cloud-Lösungen im öffentlichen Dienst“

Aus diesem Grund ist die DSAG seit längerem mit SAP in Gesprächen, wie für die öffentliche Verwaltung eine SAP-HR-Cloud-Lösung so bereitgestellt werden kann, dass sie für die Branche geeignet ist. Dies erfordert eine breite Abstimmung von Anforderungen der Kundenseite durch strategische Produktverantwortliche auf Entscheidungsebene von Bund und Ländern. Beteiligt sind deshalb insgesamt acht Organisationen, das sind alle Bundesländer und Teile des Bundes, die SAP-Verfahren heute einsetzen bzw. den Einsatz planen. Die Vertreter aus den zuständigen Ministerien von Bund und Ländern haben sich als Strategiegruppe zusammengefunden, um sich abzustimmen. Somit ist sichergestellt, dass die Rechtslagen und die Spezifika von Bund und Ländern, von Gemeinden und Gemeindeverbänden sowie von sonstigen der Aufsicht eines Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts abgedeckt sind.

Zum Vorgehen: In Arbeitsgruppen erarbeiten fachkundige Vertreter der Länder und des Bundes unter Beteiligung der Rechenzentren und großen IT-Dienstleister zusammen mit SAP-Entscheidungsvorschläge zu bestimmten Themenkomplexen. Sie werden dann in einem übergreifenden Gremium (Strategiegruppe) zwischen SAP und öffentlicher Verwaltung (insbesondere Vertretern auf ministerieller Ebene) abschließend abgestimmt.

Ziel dieser Initiative „Einsatz von HR-Cloud-Lösungen im öffentlichen Dienst“ ist es, öffentlichen Verwaltungen eine strategische Empfehlung bezüglich des Cloud-Einsatzes von HCM-Lösungen an die Hand zu geben. Auf deren Basis können sie dann entscheiden, ob und wie sie die Lösungen zukünftig einsetzen. Für SAP bieten die Gespräche die Grundlage und Chance, unter Berücksichtigung der Produktstrategie von SuccessFactors eine zielgerichtete Lösung für die öffentliche Verwaltung (Bund, Länder, Kommunen und Körperschaften des öffentlichen Rechts) zu entwickeln.

3. SAP SuccessFactors Cloud-in-Country – das Konzept

SAP hat im Rahmen der Initiative nach ersten Gesprächen mit DSAG und Anwenderkreis zunächst das so genannte Cloud-in-Country-Modell für SuccessFactors vorgestellt. Cloud-in-Country sieht eine datensouveräne, physisch abgetrennte Public Cloud für die öffentliche Verwaltung vor. Alle Daten bleiben im Land, wobei „Land“ in diesem Sinne eine Nation ist, aber auch die EU sein kann, „wenn dies ausreicht“. Nach Konzeption von SAP befindet sich das primäre Rechenzentrum in Deutschland oder den Niederlanden, das Rückfallzentrum jeweils im anderen Land. Standort des sekundären Rechenzentrums (Backup-Server) ist im Europäischen Wirtschaftsraum oder der Schweiz.

Datenspeicherung (auch für Ersatz-, Backup- und Disaster-Recovery) und Datenverarbeitung (personenbezogen und geschäftlich) finden ausschließlich im „Land“ (der hier vorliegenden Definition folgend) statt. Der Support (1., 2., 3. Level) greift auf Kundensysteme und -daten nur vom Land aus zu, falls erforderlich nur durch Personal mit besonderer Staatsangehörigkeit und Sicherheitsfreigabe. Soweit zur Wahrung der Souveränität erforderlich, müssen Daten anonymisiert oder über das Konzept des Mittelmanns eingesetzt werden.

4. Untersuchung auf Tauglichkeit

Ist dieses Konzept geeignet, um alle Aspekte einer souveränen Cloud für die deutsche Verwaltung abzudecken? Dieser Frage sind DSAG und Anwender nachgegangen. Gemeinsam mit SAP wurden die Anforderungen analysiert, um daraus ein rechtskonformes, technisch machbares und wirtschaftlich sinnvolles Cloud-Modell zu erstellen.

Im Einzelnen wurde Cloud-in-Country durch die Brille der drei Themenkomplexe Datenschutz, Sicherheit und Funktionalität beleuchtet. Ein weiterer Aspekt (der allerdings erst betrachtet werden kann, nachdem aussagekräftige Zahlen zur Verfügung stehen) ist das Thema Wirtschaftlichkeit. Denn wie auch immer ein funktionierendes Modell am Schluss aussehen kann:

Es muss für SAP und Kunden, also die öffentliche Verwaltung, unter Berücksichtigung der bisherigen Investitionen wirtschaftlich tragfähig sein.

Die aus den drei Themengruppen resultierenden Ergebnisse wurden im Laufe des ersten Halbjahres 2021 von einer übergreifenden Strategiegruppe mit Entscheidungsträgern aus verschiedenen Organisationen auf Landes- und Bundesebene bewertet und zu einem Gesamturteil verdichtet.

Insbesondere wurde dabei geprüft, ob das vorgesehene Modell den Anforderungen der Kunden aus der öffentlichen Verwaltung genügt bzw. auf welche Anwendungsfälle es passt. Reichen Europa oder ein weltweiter Cloud-Service, wann muss es Deutschland und deutsches Personal sein? Kann man für Cloud-in-Country auch die EU als Land definieren? Wie unterscheidet sich Datenschutz für Beamte, Angestellte, Drittpersonal und Bewerberinnen und Bewerber? Dabei zogen die Beteiligten verschiedene rote Linien. Das von SAP vorgeschlagene Modell käme demnach nicht in Frage, wenn Landes- und Bundesgesetze, Verordnungen, Beschlüsse des IT-Planungsrats oder BSI-Vorgaben dagegen sprächen oder sich sonstige funktionale, praktische und politische Hinderungsgründe ergäben.

Auf dieser Basis wurde jedes an der DSAG-Initiative beteiligte Bundesland/jede Bundesbehörde gebeten, für sich eine erste Einschätzung zu treffen, ob Cloud-in-Country die Anforderungen des Datenschutzes erfüllt und an welchen Stellen Anpassungen notwendig sind.

5. Die Bewertung

... aus Datenschutzsicht

Alle vorliegenden Bewertungen der Länder und Bundesbehörden bestätigen übereinstimmend die datenschutzrechtliche Rechtsbeziehung zwischen der öffentlichen Verwaltung und SAP. Maßgebliche Rechtsgrundlage ist Art. 28 DSGVO („Auftragsverarbeiter“) i. V. m. Art. 32 DSGVO („Sicherheit der Verarbeitung“), da SAP in seiner Rolle als Cloud-Anbieter als Auftragsverarbeiter i. S. v. Art. 4 Nr. 8 DSGVO agiert. Die Mindestanforderungen dieser Vorschriften müssen bei einem Cloud-in-Country-Modell vollumfänglich erfüllt werden, die öffentliche Verwaltung muss Herr der Daten bleiben.

Aus verschiedenen Landesgesetzen ergibt sich (jeweils graduell unterschiedlich ausgestaltet) eine besondere Schutzwürdigkeit der verarbeiteten Personalaktendaten. Nach dem Berliner Landesbeamtengesetz, dem hessischem Beamtengesetz und dem bayerischen Beamtengesetz dürfen nur Beschäftigte Zugang zur Personalakte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

Auftragsdatenverarbeitung ist im Freistaat Bayern nur zulässig zur Realisierung erheblich wirtschaftlicherer Arbeitsabläufe (Art. 108 Abs. 3 BayBG). Das hessische Landesrecht ermächtigt explizit nur landeseigene Dienstleister als Auftragsverarbeiter. Durch Auslagerung an einen Auftragsdatenverarbeiter sehen die befragten Fachleute und Experten in den Behörden im vorgelegten Modell eine potenzielle Gefährdung der gesetzlich geforderten Daten- bzw. digitalen Souveränität.

Eine besondere Schutzwürdigkeit der verarbeiteten Personalaktendaten resultiert rechtlich zudem aus

- § 50 Satz 3 des Beamtenstatusgesetzes (BeamtStG), der den vertraulichen Umgang mit Personalaktendaten („Personalaktengeheimnis“) ausdrücklich regelt, und
- Art. 9 Abs. 1 DSGVO, da zumindest z. T. auch besondere Kategorien von personenbezogenen Daten (z. B. Gesundheitsdaten) verarbeitet werden.

Hinzu kommt die Fürsorgepflicht des Arbeitgebers/Dienstherrn. Ausdrücklich hervorzuheben ist, dass die Verarbeitung personenbezogener Daten besonders exponierter Personenkreise wie Politiker, verdeckte Ermittler, Steuerprüfer, Richter und Staatsanwälte in Personaladministration, Zeitwirtschaft oder Personalabrechnung das entscheidende Kriterium bildet für den „sehr hohen“ Schutzbedarf hinsichtlich des Schutzguts Vertraulichkeit.

Laut IT-Planungsrat muss zudem der Ort der Datenverarbeitung zwingend in Deutschland liegen. Wörtlich heißt es dort: „Von den Einrichtungen der öffentlichen Verwaltung gehaltene schützenswerte Informationen (z. B. Informationen aus Verfahren mit hohem oder sehr hohem Schutzbedarf, Betriebs- und Geschäftsgeheimnisse sowie sensible Daten über IT-Infrastrukturen) dürfen ausschließlich in Deutschland gespeichert und verarbeitet werden. Cloud-Anbieter sollen ein dafür geeignetes Betriebsmodell vorweisen...“. Dass sich unter „Land“ laut SAP-Konzeption auch die EU verstehen lässt, stellt demnach einen nicht akzeptablen Verstoß gegen diese Regelung dar.

Dass Daten nicht ins Ausland transferiert werden dürfen, wurde im Juli 2020 durch das sog. „Schrems II“-Urteil des EuGH bestätigt. Es besagt, dass der EU-US-Datenschutzschild (Privacy-Shield) eben kein angemessenes Schutzniveau bei Datenübermittlungen in die USA bietet. Damit hob der EuGH einen Durchführungsbeschluss der Europäischen Kommission vom 12. Juli 2016 auf, infolgedessen eine Übermittlung an US-Unternehmen tragbar sei, sofern sich diese den Bedingungen dieses Schutzschildes unterworfen haben.

Selbst wenn man aber nun den Ort der Datenverarbeitung auf die EU beschränkt (auch dies geht dem IT-Planungsrat allerdings bereits zu weit, s. o.), ergibt sich ein datenschutzrechtliches Problem. Es resultiert aus dem US-Cloud-Act, der im Rechtskonflikt mit der EU-DSGVO steht.

Rechtskonflikt zwischen EU-DSGVO und Cloud-Act

Der Cloud-Act trat 2018 in Kraft. US-Behörden dürfen demnach auf personenbezogene Daten zugreifen, die im Besitz oder unter der Kontrolle von US-Unternehmen sind, auch wenn sich die Daten außerhalb der USA befinden. SAP ist, wenngleich ein deutsches Unternehmen, in vielfältiger Weise mit den USA verflochten: über seine amerikanische Gesellschaft SAP America Inc. ebenso wie über die Zusammenarbeit in der Cloud mit Microsoft, Amazon und Google. Die EU hingegen betrachtet sämtliche personenbezogenen Daten in ihrem Hoheitsgebiet als durch EU-Recht vor Zugriffen Dritter geschützt. Art. 48 der EU-DSGVO erlaubt einen solchen Zugriff nur im Falle eines Rechtshilfeabkommens zwischen dem Drittland und der EU bzw. einem EU-Mitgliedstaat. Ein solches Abkommen sieht den Austausch der personenbezogenen Daten über zwischengeschaltete staatliche Stellen vor, nicht aber ihre direkte Herausgabe. Unternehmen mit US-amerikanischem Hauptsitz befinden sich damit in einem Rechtskonflikt zwischen EU-DSGVO und Cloud-Act.

Verantwortliche, die personenbezogene Daten in der Cloud verwalten, müssen daher zu einem Dienstleister in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau wechseln; für Behörden wird der Ort nochmals eingeschränkt auf Deutschland. SAP muss jetzt nachweisen, dass es die Anforderung erfüllt, personenbezogene Daten nur in Deutschland speichert bzw. verarbeitet und keine Daten in andere Länder (insb. USA) überträgt. Letzteres ist – trotz Schrems II – noch immer möglich, sofern vertraglich vereinbart. Offen ist außerdem, wie mit den Daten durch die Hyperscaler Microsoft, AWS und Google umgegangen wird.

Wie aber nun gleichzeitig der Cloud-Act-Problematik begegnen (die stets droht, wenn eine Rechtsbeziehung zu einem Unternehmen mit US-Sitz besteht)? Die Lösung ist ein Cloud-Modell, bei dem der Betrieb allein in der Hoheit der Verwaltung verbleibt (siehe unten Punkt 6. „Lösungsansatz für die öffentliche Verwaltung“). Damit wäre die geforderte Datensouveränität gewahrt und der Zugriff auf Daten aus den USA nicht möglich.

...aus funktioneller Sicht

SuccessFactors für die öffentliche Verwaltung muss eine Reihe von Kernfunktionalitäten abdecken, die das Produkt zum jetzigen Zeitpunkt noch nicht bietet. So fehlt in der Grundausprägung die Stellenwirtschaft, die jedoch unverzichtbar zur Personalplanung und -entwicklung sowie gesetzlichen Haushaltsdokumentation ist. Funktionale Defizite gibt es außerdem bei der Versorgungsadministration und beim Modul SuccessFactors Employee Central Payroll, das den öffentlichen Dienst nicht abrechnen kann. Auch die Anpassbarkeit für die Umsetzung aller Landesgesetze ist aktuell nicht gegeben und ein wesentliches Argument (s. u. Punkte 2. und 3.).

Als gemeinsame Haltung der öffentlichen Verwaltung hat sich aus den genannten Gründen herauskristallisiert, dass Cloud-in-Country im initial vorgelegten Entwurf kein geeignetes Betriebsmodell für die öffentliche Verwaltung darstellt.

Konkrete Begründung:

- Sämtliche datenschutzrechtliche Vorschriften (unabhängig davon, ob solche aus der DSGVO oder aus Bundes- bzw. Landesrecht) sowie entsprechende einschlägige Rechtsprechung müssen zwingend höchste Relevanz haben.
- Analog gilt dies hinsichtlich der Vorgaben zu IT-Sicherheit aus Gesetzgebung und BSI.
- Die gesetzlichen Anforderungen sind vor dem Hintergrund der Gesetzesbindung der Verwaltung und im Hinblick auf Datenschutzkonformität zwingend und unabhängig von der Aufwandsintensität umzusetzen.
- Insbesondere die Sicherheit der besonders schutzwürdigen Personaldaten kann im vorliegenden Entwurf nicht ausreichend garantiert werden.
- Ort der Datenverarbeitung darf wegen der Schutzbedarfsfeststellung „sehr hoch“ nur Deutschland sein, was im Erstentwurf so explizit nicht genannt wird.
- Fehlende Funktionalitäten: Die Software-Lösung muss
  1. die für die öffentliche Verwaltung notwendigen Kernfunktionalitäten bereitstellen und
  2. gesetzliche Anforderungen aus länderspezifischem Dienstrecht (Beamten- und Besoldungsrecht) und Tarifrecht (verschiedene Tarifverträge) technisch zur Aufgabenerfüllung unterstützen sowie
  3. die Möglichkeit zur individuellen Anpassung bieten.
- Die Wahrung der digitalen Souveränität der öffentlichen Verwaltung (u.a. Wechselmöglichkeiten und Gestaltungsfähigkeit i. S. v. Art. 28 DSGVO Datenhoheit/Vertragsgestaltung) ist nicht gewährleistet, solange durch US-Cloud-Act ein Zugriff möglich ist.

6. Lösungsansatz für die öffentliche Verwaltung

Parallel zur Bewertung hat die Strategiegruppe aus den genannten Kritikpunkten einen Lösungsansatz skizziert, wie die Unzulänglichkeiten des Erstentwurfs von Cloud-in-Country ausgeräumt werden können. Ziel muss es sein, am Ende zu einem zukunftsfähigen Ansatz zu kommen, wie sich SAP-Personalfunktionen aus der Cloud für die öffentliche Verwaltung unter Einhaltung aller branchentypischer Anforderungen bereitstellen lassen.

Der Ansatz sieht ein öffentlich-rechtliches Rechenzentrum in Deutschland als Private Cloud für den Betrieb von allen SAP-HCM-Cloud-Lösungen für die öffentliche Verwaltung unter staatlicher Hoheit vor. Dem Zugriff über US-Cloud-Act wäre damit ein Riegel vorgeschoben. Der Betrieb erfolgt in eigener Hoheit und in eigener Betriebsverantwortung durch staatlich Beschäftige, ggf. mit Betriebsunterstützung und Nutzung von Dienstleistungen durch Externe. Die SAP-SuccessFactors-Lösungen müssen der öffentlichen Verwaltung den vollständigen von ihr benötigten Funktionsumfang bieten und sich kundenspezifisch erweitern lassen können.

Schlüsselfaktoren:

- Die Datenverarbeitung – also Betrieb, Übertragung, Administration, Speicherung und Backup – finden ausschließlich in Deutschland statt. Dedizierte Rechenzentren für die öffentliche Verwaltung bedeuten gleichzeitig: keine Auftragsdatenverarbeitung!
- Die digitale Souveränität der öffentlichen Verwaltung (u. a. Wechselmöglichkeit und Gestaltungfähigkeit) wird gewahrt.
- Vollständige Konformität der Lösung zu Art. 28 DSGVO (insb. die Vorgaben von Abs. 3) und Art. 32 DSGVO, sowohl in vertraglicher als auch in tatsächlicher Hinsicht.
- Um den besonderen Schutzbedarf von Personaldaten zu gewährleisten, muss es möglich sein, einzelne öffentliche Arbeitgeber netztechnisch zu trennen.
- Gesetzliche und behördenspezifische Anforderungen für Bund, Länder und Kommunen werden durch die Software unterstützt.
- Bisherige Kernfunktionalitäten (z. B. Stellenwirtschaft, Versorgungsadministration, EC-Payroll für den öffentlichen Dienst) stehen auch im Cloud-Standard bereit.
- Die Cloud-Lösung kann hinsichtlich der Umsetzung von Gesetzen und Vorschriften ausreichend angepasst werden.

7. Fazit

Das vorgestellte und mit der DSAG diskutierte neue Deployment-Modell Cloud-in-Country, welches die nationale Datenhaltung inklusive aller relevanten rechtlichen Rahmenbedingungen garantieren soll, ist für DSAG und Anwenderorganisationen aus verschiedenen Gründen noch nicht tragfähig. Im Wesentlichen bestehen Defizite in den Bereichen Datenschutz, Sicherheit und Funktionalität. Die DSAG hat deshalb verschiedene Lösungsansätze aufgezeigt, die über Cloud-in-Country hinausgehen und die Basis für eine Zukunft von SAP-Personalfunktionen in der Cloud für die öffentliche Verwaltung darstellen können.

Impressum

Wir weisen ausdrücklich darauf hin, dass das vorliegende Dokument nicht jeglichen Regelungsbedarf sämtlicher DSAG-Mitglieder in allen Geschäftsszenarien antizipieren und abdecken kann. Insofern müssen die angesprochenen Themen und Anregungen naturgemäß unvollständig bleiben. Die DSAG und die beteiligten Autoren können bezüglich der Vollständigkeit und Erfolgsgeeignetheit der Anregungen keine Verantwortung übernehmen.

Deutschsprachige SAP® Anwendergruppe e.V.
Altrottstraße 34 a
69190 Walldorf | Deutschland
Telefon +49 6227 35809-58
Telefax +49 6227 35809-59
E-Mail info@dsag.de
dsag.de