Künftige Cloud-Lösungen für das Personalwesen in der öffentlichen Verwaltung

DSAG-Positionspapier

Stand: August 2022

Inhaltsverzeichnis

Einleitung

Künftige Cloud-Lösungen für das Personalwesen in der öffentlichen Verwaltung

Der Einsatz von Human-Resources-Cloud-Lösungen im öffentlichen Dienst ist an besondere Bedingungen geknüpft. Die Grundlagen für rechtskonforme Cloud-Lösungen im Bereich HCM in der öffentlichen Verwaltung wurden in der DSAG erhoben. Sie dienen anstehenden Bewertungsprozessen.

.

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

Eine HR-Cloud-Lösung, die für die öffentliche Verwaltung geeignet ist, erfordert eine breite Abstimmung von Anforderungen der Kundenseite durch strategische Produktverantwortliche auf Entscheidungsebene von Bund und Ländern. Die Vertreter aus den zuständigen Ministerien von Bund und Ländern haben sich als Strategiegruppe und in DSAG-Arbeitsgruppen zusammengefunden, um sicher zu stellen, dass die Rechtslagen und Spezifika von Bund und Ländern, 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 Vertreterinnen und Vertreter der Länder und des Bundes unter Beteiligung der Rechenzentren und großen IT-Dienstleister Entscheidungsvorschläge zu bestimmten Themenkomplexen. Sie werden dann in einem übergreifenden Gremium (Strategiegruppe), insbesondere mit Fachleuten auf ministerieller Ebene, abschließend abgestimmt.

Ziel der Initiative 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.

Die aus den drei Themengruppen resultierenden Ergebnisse wurden im Laufe des ersten Halbjahres 2021 von der übergreifenden Strategiegruppe mit Entscheidungsträgern aus verschiedenen Organisationen auf Landes- und Bundesebene bewertet und wie folgt festgelegt:

2 Die Anforderungen

2.1 …aus Datenschutzsicht

Alle vorliegenden Bewertungen der Länder und Bundesbehörden bestätigen übereinstimmend die datenschutzrechtliche Rechtsbeziehung zwischen der öffentlichen Verwaltung und dem Cloud-Anbieter. Maßgebliche Rechtsgrundlage ist Art. 28 DSGVO („Auftragsverarbeiter“) i. V. m. Art. 32 DSGVO („Sicherheit der Verarbeitung“), da der Cloud-Anbieter als Auftragsverarbeiter i. S. v. Art. 4 Nr. 8 DSGVO agiert. Die Mindestanforderungen dieser Vorschriften müssen 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 Auftragsdatenverarbeiter. Durch Auslagerung an einen solchen Verarbeiter sehen die befragten Fachleute und Experten in den Behörden 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 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.

2.2 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. 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. Der Cloud-Anbieter muss nachweisen, dass er 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.

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. Damit wäre die geforderte Datensouveränität gewahrt und der Zugriff auf Daten aus den USA nicht möglich.

2.3 …aus funktioneller Sicht

Die Cloud-Lösung für die öffentliche Verwaltung muss eine Reihe von Kernfunktionalitäten abdecken: Die Stellenwirtschaft ist unverzichtbar zur Personalplanung und -entwicklung sowie gesetzlichen Haushaltsdokumentation. Spezifisch sind die Versorgungsadministration und die komplexe Abrechnung des öffentlichen Dienstes. Auch die Anpassbarkeit der Software für die Umsetzung aller Landesgesetze muss gegeben sein. (s. u. Punkte).

2.4 Zusammenfassung der Anforderungen

- 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 muss ausreichend garantiert werden.

- Ort der Datenverarbeitung darf wegen der Schutzbedarfsfeststellung „sehr hoch“ nur Deutschland sein.

- Funktionalitäten: Die Software-Lösung muss

  1. die für die öffentliche Verwaltung notwendigen Kernfunktionalitäten bereitstellen,
  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.

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
https://dsag.de/