All for One

SAP API Policy – und jetzt?

Eine pragmatische Einordnung vom 16.7.2026

Vor ein paar Wochen war das Thema SAP API Policy ziemlich heiß. Da war schnell die Rede davon, dass SAP den Zugriff auf Daten einschränkt, externe Plattformen nicht mehr vernünftig an SAP-Systeme herankommen und Unternehmen ihre ganze Daten- und Integrationsarchitektur umbauen müssen.

Wenn man sich die Situation heute mit etwas Abstand anschaut, muss man sagen: Mit etwas Abstand zeigt sich: Es ist kein pauschales Abschotten von SAP-Daten. Für bestimmte Zugriffsmuster, insbesondere ODP-RFC und nicht veröffentlichte APIs, ist die Lage aber deutlich konkreter und operativ relevant.

Die Richtung ist klar: SAP möchte stärker steuern, wie Anwendungen auf SAP-Systeme zugreifen, welche Schnittstellen genutzt und wie Daten- und KI-Szenarien umgesetzt werden. Aus Sicht von Governance, Sicherheit und Systemstabilität ist das grundsätzlich nachvollziehbar. Gleichzeitig stärkt SAP damit natürlich auch die eigenen Architekturpfade und Plattformen. Beides kann man nicht ganz voneinander trennen.

Wichtig ist deshalb, die Themen auseinanderzuhalten. Sonst werden KI-Agenten, Datenextraktion, BDC Connect und nicht veröffentlichte APIs vermischt – und man landet schnell bei Aussagen, die zwar griffig sind, technisch aber so nicht stimmen.

Im Kern geht es aus unserer Sicht um drei Bereiche:

1.

den Zugriff von KI-Systemen und Agents auf SAP,

2.

die Nutzung und Replikation von SAP-Daten auf anderen Plattformen,

3.

und die Frage, welche APIs langfristig als veröffentlicht und unterstützt gelten.

KI-Systeme und Agents: Ganz ohne Regeln wird es nicht gehen

Der erste Teil betrifft Agents, Bots, MCP-basierte Anwendungen und andere KI-Lösungen, die über APIs mit einem SAP-System kommunizieren. Bei einer klassischen Schnittstelle ist relativ gut vorhersehbar, wie oft sie aufgerufen wird und welche Last entsteht. Bei einem Agenten sieht das anders aus. Der kann in kurzer Zeit sehr viele Requests erzeugen. Aus einem sinnvollen Use Case wird dann im schlechtesten Fall ein Performanceproblem im operativen System.

Dass SAP an der Stelle Leitplanken einzieht, ist deshalb keine große Überraschung. KI-Zugriffe sollen über definierte Architekturpfade laufen, überwacht werden können und nicht unkontrolliert auf produktive Systeme losgelassen werden. SAP spricht von sogenannten „endorsed pathways“, unter anderem über die SAP Business AI Platform und weitere vorgesehene Integrations- und Governance-Komponenten. Bei anderen Wegen kann SAP technische Begrenzungen wie Rate Limits oder Throttling vorsehen.

Jetzt kann man diskutieren, ob es nur um Sicherheit geht oder auch darum, die eigenen Plattformen stärker zu positionieren. Ehrlicherweise wird beides eine Rolle spielen. Für die technische Bewertung hilft das aber nur begrenzt weiter.

Entscheidend ist: Welche APIs nutzt die Anwendung? Wie viele Aufrufe entstehen? Welche Daten darf der Agent sehen? Und gibt es ein vernünftiges Berechtigungs- und Monitoringkonzept? Dann bleiben KI-Szenarien mit SAP-Daten natürlich möglich. Nur irgendeinen Agent anzuschließen und zu schauen, was passiert, wird auf Dauer nicht funktionieren.

Datenzugriff: Es gibt weiterhin Mittel und Wege

Beim zweiten Themenbereich ist in der öffentlichen Diskussion schnell der Eindruck entstanden, SAP wolle den Export von Daten in Non-SAP-Umgebungen grundsätzlich verhindern. So pauschal ist das nicht richtig. Es gibt weiterhin unterschiedliche Möglichkeiten, SAP-Daten bereitzustellen – etwa über veröffentlichte APIs, CDS Views, OData Services und weitere unterstützte Verfahren. Auch Drittanbieterwerkzeuge können weiterhin funktionieren, sofern sie freigegebene technische Wege nutzen.

Gleichzeitig werden bestimmte Zugriffspfade konkret eingeschränkt oder technisch abgesichert – besonders prominent ODP-RFC in SAP-to-Non-SAP-Szenarien. Das ist kein generelles Datenexportverbot, kann für betroffene Datenpipelines aber sehr relevant sein. Alternative Wege, zum Beispiel über OData, bestehen in diesem Fall aber weiterhin.

Für Unternehmen heißt das erst einmal: Man sollte wissen, welche Extraktionswege genutzt werden. Das klingt banal, ist es in der Praxis aber oft nicht. Viele Schnittstellen laufen seit Jahren, Reporting und Datenpipeline funktionieren – und solange nichts ausfällt, fragt niemand genau nach, ob darunter ODP-RFC, ein individueller ABAP-Baustein oder etwas anderes steckt.

Deshalb wäre ein groß angelegtes Prüfprogramm für alle Schnittstellen in vielen Fällen unverhältnismäßig. Sinnvoller ist eine pragmatische Betrachtung: Gibt es Abhängigkeiten von konkret betroffenen Technologien? Gibt es ohnehin instabile oder schwer wartbare Schnittstellen? Oder stehen neue Daten-, Analytics- oder KI-Szenarien an, bei denen man die Architektur sowieso neu denken muss? Dort sollte man ansetzen. Nicht überall gleichzeitig.

BDC Connect: Datenaustausch ja, klassischer Export nein

Im Zusammenhang mit der API Policy wird häufig SAP Business Data Cloud beziehungsweise BDC Connect als zukünftiger Weg für den Datenaustausch genannt. Auch hier lohnt es sich, genauer hinzuschauen.

BDC Connect ist nicht einfach ein neuer Exportadapter. Der Ansatz basiert auf Zero Copy beziehungsweise Delta Sharing: Die Daten bleiben grundsätzlich in der Ursprungsplattform und werden für definierte Szenarien bereitgestellt.

Das kann interessant sein, weil Daten nicht mehrfach physisch gespeichert werden müssen und Governance sowie Aktualität besser kontrollierbar sind. Trotzdem ist BDC Connect kein universeller Ersatz für jede Extraktionslösung.

Wenn Daten auf einer anderen Plattform dauerhaft gespeichert und unabhängig weiterverarbeitet werden sollen, muss man prüfen, welcher Weg tatsächlich passt. Und man muss unterscheiden: Brauche ich wirklich eine Kopie? Reicht ein kontrollierter Zugriff? Benötige ich den vollständigen Datenbestand oder nur ein klar definiertes Data Product für einen konkreten Use Case? Die Antwort fällt nicht überall gleich aus.

Veröffentlichte APIs und Clean Core: Was ist eigentlich sauber?

Der dritte Teil betrifft veröffentlichte und nicht veröffentlichte APIs. SAP möchte, dass neue Integrationen möglichst auf offiziell bereitgestellten und dokumentierten Schnittstellen aufbauen. Das passt zu Clean Core: Individuelle Tabellenzugriffe, nicht freigegebene Funktionsbausteine und kundenspezifische Sonderwege sollen reduziert werden.

Nicht veröffentlichte APIs sind deshalb aber nicht automatisch von heute auf morgen verboten oder unbrauchbar. Viele dieser Lösungen werden zunächst weiterlaufen. Sie bringen nur ein höheres Risiko mit – etwa bei Updates, beim Support oder bei einer späteren Migration in die Public Cloud. Damit wird die API Policy schnell zu einem Thema technischer Schulden. Und auch da gilt: Nicht jede technische Schuld muss sofort beseitigt werden. Das wäre wirtschaftlich meistens Unsinn. Man sollte aber wissen, wo sie liegt und wie kritisch sie ist. Eine Schnittstelle für einen monatlichen Nebenreport ist anders zu bewerten als ein zentraler Datenfluss, an dem Planung, Vertrieb und Produktion hängen.

Das Ziel ist also nicht Perfektion. Das Ziel ist Transparenz und eine vernünftige Priorisierung.

Was bedeutet das für bestehende SAP-Landschaften?

Für die meisten Unternehmen wird die API Policy kurzfristig keine dramatischen Folgen haben. Nicht jedes Reporting fällt plötzlich aus und nicht jede individuelle Schnittstelle muss sofort ersetzt werden.

Inzwischen lässt sich besser unterscheiden zwischen klar unterstützten Wegen, technischen Grauzonen und wenigen konkret eingeschränkten Verfahren. Vereinfacht gesagt: „endorsed pathway“, „use at your own risk“ und Wege, die tatsächlich nicht mehr vorgesehen sind.

Unterschiede gibt es je nach Betriebsmodell. In On-Premises- und Private-Cloud-Systemen bestehen heute häufig noch mehr technische Zugriffsmöglichkeiten. In der S/4HANA Cloud Public Edition ist der direkte Datenbankzugriff ohnehin nicht vorgesehen; dort müssen Unternehmen stärker über veröffentlichte APIs, CDS Views und die von SAP vorgesehenen Erweiterungsmechanismen arbeiten.

Mittelfristig wird sich dieser Unterschied stärker bemerkbar machen. Je mehr Unternehmen in standardisierte Cloud-Modelle wechseln, desto weniger funktionieren historisch gewachsene Umwege. Neue Integrationen sollte man deshalb so aufsetzen, dass sie nicht nur heute laufen, sondern auch zum Zielbild passen.

Was Unternehmen jetzt sinnvollerweise tun sollten

Aus unserer Sicht braucht es wegen der API Policy kein hektisches Großprojekt. Aber ein paar Fragen sollte man sich stellen.

Welche Anwendungen greifen auf SAP-Daten zu? Welche Schnittstellen, Extraktoren und individuellen Entwicklungen werden genutzt? Gibt es ODP-RFC-Abhängigkeiten? Und greifen KI-Systeme oder Agents direkt auf operative SAP-Systeme zu? Danach kommt die Bewertung: Ist der eingesetzte Weg offiziell unterstützt? Funktioniert er nur im aktuellen Betriebsmodell? Welche Datenmengen und Aufruffrequenzen entstehen? Und wie kritisch wäre eine Änderung bei einem Update oder einer Cloud-Migration?

Erst dann geht es um das Zielbild. Welche Daten müssen wirklich repliziert werden? Welche können in SAP bleiben? Wo ist Zero Copy sinnvoll? Wo braucht es ein Data Product? Und welche Plattform übernimmt in der gesamten Datenlandschaft welche Aufgabe?

Viele Unternehmen haben eben nicht die eine Plattform. Sie nutzen SAP für Kernprozesse, Microsoft Fabric oder Databricks für Daten und Analytics und weitere Lösungen für spezielle Anwendungsfälle. Das stellt die API Policy nicht grundsätzlich infrage. Der Austausch muss nur bewusster gestaltet werden.

Unsere Einordnung: nicht überreagieren, aber die Richtung ernst nehmen

Unterm Strich wird die SAP API Policy nicht so heiß gegessen, wie sie zunächst gekocht wurde. Es gibt kein pauschales Verbot, SAP-Daten auf anderen Plattformen zu nutzen. Es gibt weiterhin unterschiedliche technische Wege. Bei vielen gut dokumentierten Integrationen wird kurzfristig kein Handlungsdruck entstehen.

Trotzdem ist die Richtung klar: SAP stärkt veröffentlichte APIs, Clean Core, kontrollierte Datenzugriffe und die eigenen Governance-Mechanismen. Gerade mit Blick auf Agentic AI, Cloud-ERP und hybride Datenplattformen wird das Thema eher wichtiger als unwichtiger.

Aus unserer Sicht geht es nicht darum, bestehende Lösungen vorschnell auszutauschen oder aus der API Policy ein riesiges Transformationsprogramm zu machen. Es geht darum, zu wissen, was man im Einsatz hat, technische Schulden sichtbar zu machen und dort zu modernisieren, wo es notwendig oder ohnehin sinnvoll ist.

Oder etwas einfacher gesagt: Keine Panik. Aber auch nicht einfach ignorieren. Die API Policy ist vor allem ein Anlass, die eigene Daten- und Integrationsstrategie noch einmal vernünftig anzuschauen. Und dann Schritt für Schritt den Weg zu gehen, der zum Unternehmen, zur bestehenden Landschaft und zu den geplanten Use Cases passt.

AUTOREN:

Georg Krenn

Thomas Buchegger

Emily Celen

Dr. Torben Hügens

All for One Group SE
Rita-Maiburg-Str. 40
70794 Filderstadt

info@all-for-one.com

all-for-one.com