Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Bereich Digitale Transformation und IKT-Lenkung DTI

AR009 – Architekturrichtlinie Microsoft 365 im SD-Büroautomation Beilage 2

Beilage zu einer IKT-Vorgabe

Sachtitel (der Beilage):	**Governance Microsoft Power Platform**
Ausgabedatum dieser Beilage:[1]	01.03.2026
Gehört zu:	AR009, Version 1.0
Status der Weisung:	Genehmigt

[1] Das *Ausgabedatum* stimmt bei der Erstpublikation einer Beilage mit dem *Beschlussdatum* der genehmigten Version einer Weisung zur Bundesinformatik überein. Bei einer geringfügigen Änderung in der Beilage wird auf eine Anpassung der Version der Weisung verzichtet. Es ist lediglich das *Ausgabedatum* der Beilage anzupassen sowie die Änderung in *Anhang A der Beilage* festzuhalten.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1. Dieses Dokument definiert die Governance für die Microsoft Power Plattform Services und stellt sicher, dass die Nutzung effizient, sicher und in einer für die Bundesverwaltung geregelten Form erfolgen kann.

1.1 Geltungsbereich

1. Der Geltungsbereich für die Governance gilt für alle Tenants des Typ-1 «gemeinsamer Tenant BA & FA» im SD-Büroautomation (SD/BA).
2. In diesen Geltungsbereich DÜRFEN KEINE eGOV Power Platform Services angeboten werden.
3. Die Governance regelt die «Power Apps, Power Automate und Power BI Pro»[2] inkl. deren Backend Services wie z.B. Data connectors.

1.2 Begriffe

1. In dieser Weisung bedeuten
   a. *Tenantverantwortlicher (TAV):* nach innen gerichtete Rolle der Regelungs- und Sourcing Kompetenz sowie Eskalationsinstanz.
   b. *Tenantowner (TO):* Microsoft-Definition ihrer Erwartungen und Verantwortlichkeiten an eine Cloud-Services-beziehende (oder konkret tenant-besitzende) Organisation. Der Organisationsrahmen ist «die Bundesverwaltung».
   c. *Tenantbetreiber (TB):* verantwortet den vorgaben- und gesetzeskonformen Betrieb der Tenant-Services gegenüber dem Tenantowner primärer Ansprechpartner für Fachanwendungsverantwortliche und sonstigen Servicebetreiber und Servicekonsumenten in allen Fragen betrieblicher Natur.
   d. *Anwendungsverantwortliche (AV):* Fachlich und technisch verantwortliche Person für das Angebot der Power Platform Services.
   e. *Fachanwendungsverantwortlicher (FAV):* Fachlich und technisch verantwortliche Person für die fachliche Lösung. Er sorgt dafür, dass genügend Budget vorhanden ist, um die Powerlösung kontinuierlich weiterzuentwickeln. Der FAV ist auch für die datenschutzkonforme Lösung und Einhaltung des ISG und DSG verantwortlich und für die entsprechende Sicherheitsdokumentation. Der FAV ist im Normalfall eine Leistungsbezüger Rolle.
   f. *Microsoft Power Platform:* Die Microsoft Power Platform ist eine Low-Code-Plattform, mit der Benutzer Geschäftsprozesse automatisieren, Daten analysieren, Apps erstellen und Chatbots entwickeln können – alles ohne tiefgehende Programmierkenntnisse.
   g. *Solutions:* Solutions sind der Mechanismus zur Implementierung des Application Lifecycle Management (ALM) in Power Apps und Power Automate. Solutions unterstützen den

[2] Momentaufnahme, Microsoft ändert regelmässig ihre Bezeichnungen

ALM bei der Erstellung, Aktualisierung, Upgrades und Patches von fachlichen Lösungen. Der Transfer der fachlichen Lösung durch Solutions wird erheblich vereinfacht. Solutions werden für spezifische Anforderungen eingesetzt, wenn der Standard nicht mehr genügt.

h. *Microsoft Dataverse:* Microsoft Dataverse ermöglicht das sichere Speichern und Verwalten von durch Geschäftsanwendungen genutzte Daten. Dataverse-Daten werden in Tabellen gespeichert. Eine Tabelle besteht aus einer Reihe von Zeilen und Spalten.

i. *Standard-Konnektoren:* Ein Konnektor ermöglicht die Verbindung zu Datenquellen – möchte z.B. Power Automate eine E-Mail über Outlook senden, dann braucht es den Office 365 Outlook-Konnektor.

j. *Premium-Konnektoren:* Im Prinzip wie Standard-Konnektoren, jedoch benötigt es für die Nutzung zusätzliche Lizenzen – z.B. mit Daten in einer SQL-Datenbank arbeiten.

2 Strukturen der Microsoft Power Platform

2.1 Use Cases

1. Mit Power Platform Services lassen sich verschiedene Arten von Use Cases effizient entwickeln und implementieren. Im Normalfall bezieht die Power Platform Daten aus Datenquellen und generiert keine neuen:
   a. **Benutzerdefinierte Apps mit Power Apps** – Ermöglicht die Entwicklung von massgeschneiderten Anwendungen oder einer bestimmten Geschäftsanforderung ohne tiefgehende Programmierkenntnisse.
   b. **Automatisierung von Geschäftsprozessen mit Power Automate** – Reduziert manuelle Aufgaben durch automatisierte Workflows.
   c. **Datenanalyse und Visualisierung mit Power BI Pro** – Hilft bei der Analyse und Darstellung von Unternehmensdaten für bessere Entscheidungen.
2. **Fachanwendung mit Geschäftsprozessen und Datenquellen** – Fachanwendung die verschiedenen Komponenten der Power Platform nutzt (Apps, Tabellen, Flows, Premium-Konnektoren, etc.).

2.2 Einstufung der fachlichen Lösung

1. Folgende Stufen MUSS der Tenant Betreiber gemäss (vgl. Anhang E) anbieten – davon ausgeschlossen sind Datenanalysen und Visualisierungen mit Power BI Pro:
   a. **Solutions** – Diese Stufe ist darauf ausgelegt, Lösungsspezifische Anforderungen umzusetzen. Sie ist ausschliesslich für den internen Gebrauch innerhalb des Departements oder Bundeskanzlei vorgesehen. Für jede Solutions MUSS eine Entwicklung-, Integration- und Produktion-Umgebung aufgebaut werden.
   b. **Bund** – Diese Stufe ist darauf ausgelegt, Lösungen für den ganzen Bund oder Departement anzubieten. Sie ist ausschliesslich für den internen Gebrauch innerhalb der ganzen Bundesverwaltung oder Departement vorgesehen. Für Bund und Departement MUSS jeweils eine Entwicklung- und Produktion-Umgebung aufgebaut werden.
   c. **Amt** – Diese Stufe ist darauf ausgelegt, Lösungen für ein Amt, Bereich oder Team anzubieten. Sie ist ausschliesslich für den internen Gebrauch innerhalb des Amtes, Bereich oder Team vorgesehen. Für ein Amt, Bereich oder Team MUSS jeweils eine Entwicklung- und Produktion-Umgebung aufgebaut werden.
   d. **Geteilte Produktivität** – Diese Stufe ist darauf ausgelegt Innovation und Know-how innerhalb der Bundesverwaltung zu fördern. Versierte Benutzer oder Citizen Developer, die über entsprechende Erfahrung verfügen, tauschen sich mit anderen aus und sind besonders aktiv in der Community. Diese Stufe hat keinen produktiven Charakter. Für diese Stufe MUSS eine Entwicklung- und Integration-Umgebung aufgebaut werden.
   e. **Persönliche Produktivität** – Diese Stufe ist darauf ausgelegt, die individuelle Effizienz und Produktivität zu optimieren. Sie ist ausschliesslich für den internen Gebrauch zu verwenden und dient dem persönlichen Gebrauch. Auf dieser Stufe MUSS die Default Power Platform Umgebung eingesetzt werden.
2. Die fachliche Lösung MUSS in einer der Stufen integriert werden können, um eine konsistente und effiziente Umsetzung zu gewährleisten.

3. Es DÜRFEN NUR kompatible Fachanwendungen in Anerkennung der Co-Existenz und gegenseitigen Rücksichtnahme zwischen der Büroautomation und Fachanwendungen betrieben werden – dies nach den Vorgaben der [AR015].
4. Die fachliche Lösung DARF auf einer oberen Stufe betrieben werden, indem weitere Benutzerkreise davon profitieren können. Dabei MÜSSEN die Regelungen der oberen Stufe eingehalten werden.
5. Es liegt in der Verantwortung der Departemente und der Bundeskanzlei, ob sie alle Stufen anbieten wollen.
6. Die Bestellung der Power Platform Services (z.B. Umgebung, Rechte, Services) MUSS über den Integrationsmanager (IM) erfolgen und vom jeweiligen GS bewilligt werden.
7. Daten Policies MÜSSEN gemäss Kap. 3.3 beantragt werden.
8. Falls die Lösung keiner Stufe zugeordnet werden kann, MUSS gemäss [AR015] vorgegangen werden.

2.3 Datenanalyse und Visualisierung mit Power BI Pro

1. Die Funktion «Publish to Web» SOLLTE eingeschränkt werden, um eine unkontrollierte Freigabe von Daten zu verhindern.
2. Der Zugriff auf Arbeitsbereiche (Workspaces) SOLLTE durch rollenbasierte Zugriffskontrolle (RBAC) geregelt werden.
3. Zur Unterstützung von Data Loss Prevention (DLP) SOLLEN Sensitivitätskennzeichnungen aktiviert werden.
4. Der Einsatz von Microsoft Purview SOLL für die Klassifizierung und Überwachung der Daten eingesetzt werden, zur Einhaltung von Compliance-Richtlinien.
5. Es KÖNNEN keine Sourcen geblockt werden, daher gelten die IAM-Berechtigungen aus der zugreifenden Datenquelle.
6. Ansonsten sind die Tenant Richtlinien gemäss Kap. 3.2 zu berücksichtigen.

3 Regelungen und Verantwortlichkeiten

3.1 Allgemeines

1. Der Anwendungsverantwortliche (AV) ist fachlich und technisch für das Angebot der Power Platform Services verantwortlich.
2. Der Leistungsbezüger MUSS sicherstellen, dass jederzeit ein FAV ernannt ist.
3. Der AV stellt mindestens sicher,
   a. dass die Power Platform Services für die Leistungsbezüger genutzt werden können.
   b. dass die Architektur- und Sicherheitsunterlagen erstellt und durch das zuständige Gremium freigegeben werden.
   c. dass die Governance gemäss Kap. 4Sicherstellen der Governance sichergestellt wird.
4. Der Fachanwendungsverantwortliche (FAV) ist
   a. verantwortlich, dass die Lösung gemäss departamentalen Vorgaben abgenommen wird.
   b. für die korrekte Lizenzierung seiner fachlichen Lösung verantwortlich.
   c. verantwortlich, dass nach Best Practices, Security by Design und Privacy by Default entwickelt wird. Der FAV ist auch für die datenschutzkonforme Lösung und Einhaltung des ISG und DSG verantwortlich.
   d. verantwortlich für das Application Lifecycle Management (ALM). Das Deployment SOLL, wenn möglich automatisiert Abfolgen.
   e. verantwortlich für das Testmanagement.
   f. für das Kapazitäts- und Kostenmanagement verantwortlich und trägt, wenn Limiten erreicht sind die Zusatzkosten, und leitet die nötigen Schritte ein.
   g. verantwortlich, dass für unerwartete Changes Budget vorhanden ist.
   h. für das fortlaufende Qualitätsmanagement für die Powerlösung verantwortlich.
   i. verantwortlich, dass bei Entdeckung von Sicherheitslücken diese umgehend geschlossen werden.
   j. verantwortlich, dass die fachliche Lösung keine negativen Auswirkungen hat auf den Tenant (z.B. Verschlechterung der Sicherheit oder zusätzliche Risiken, die damit eingegangen werden).
   k. verantwortlich, dass die erstellten Lösungen immer auf den aktuellen Stand gehalten werden. Dabei gilt, dass die Standard-Anpassungen aus dem SD-Büroautomation immer vorrangig sind.
   l. verantwortlich, dass bei der Entwicklung die Kriterien gemäss Checkliste (vgl. Anhang D) berücksichtigt werden. Bei Bedarf MÜSSEN die Unterlagen dem TAV offengelegt werden.
   m. verantwortlich, dass keine eGOV-Lösungen gebaut werden. Für diesen Use Case MUSS ein anderer Tenant-Typ gemäss der [AR015] eingesetzt werden.
5. Der Leistungserbringer oder Tenant Betreiber MUSS
   a. entsprechende Prozesse für die Nutzung der Power Platform Services für die Leistungsbezüger anbieten (Self Service Portal oder MAC) und verursachergerecht verrechnen.

b. ein Namens- und Rollenkonzept (RBAC) erstellen und durch das zuständige Gremium freigeben lassen.

c. sicherstellen, dass die Power Platform Umgebungen in der Region Schweiz betrieben werden.

d. die Bereitstellung der Lizenzen sicherstellen.

e. sicherstellen, dass die fachliche Lösung inventarisiert wird, um ggf. Redundanzen zu erkennen. Der Tenant Betreiber MUSS zudem sicherstellen, dass für die fachliche Lösung ein Fachanwendungsverantwortlicher (FAV) inkl. Stellvertreter benannt wird.

f. sicherstellen, dass die beteiligten nach dem «Least Privilege Prinzip» die nötigen minimalen Rechte bekommen.

g. die nötigen Monitoring- und Reportingwerkzeuge zur Verfügung stellen, damit die Leistungsbezüger ihr Portfolio, Sicherheit und Kosten überwachen können.

h. die FAVs entsprechend über vorgesehene Patches und Releases der genutzten Power Platform Services vorgängig und umfassend informieren.

i. Der TAV DARF fachliche Lösungen verbieten oder ausser Betrieb nehmen, wenn es negative Auswirkungen auf den Tenant hat.

3.2 Sicherheitsaspekte

1. Es gelten die Architekturrichtlinien aus der [AR009, Hauptdokument] gemäss Kap. 2.9 (Überwachung und Protokollierung der Umgebungen).
2. Tenant Richtlinien der Power Platform Services MÜSSEN durch das zuständige Gremium freigegeben werden.
3. ALM-Prozesse MÜSSEN definiert und eingehalten werden (vgl. 3.4).
4. Freigegebene Datenquellen MÜSSEN dokumentiert werden.

3.3 Einsatz und Nutzung von Konnektoren

1. Die Freigabe von Konnektoren (Data Policy) MUSS über das zuständige Gremium erfolgen. Dies betrifft alle Stufen der Pyramide (vgl. Anhang E). Die Regelung gilt auch für Daten Gateways, die auf On-Premises Daten zugreifen wollen.
2. Für die Stufe Persönliche Produktivität, Geteilte Produktivität, Amt und Bund gilt die gleiche Daten Policy. Auf diesen Stufen DÜRFEN NUR Standard-Konnektoren verwendet werden. Es SOLLEN Datenquellen erlaubt werden, die für alle nützlich sind.
3. In einem Sicherheitsvorfall DARF der Leistungserbringer oder Tenant Betreiber in eigenem Ermessen Konnektoren per sofort blockieren.

3.4 Application Lifecycle Management (ALM)

1. Der ALM MUSS gemäss Anhang G erfolgen.
2. Der Leistungserbringer und die Departemente MÜSSEN Genehmigungsprozesse oder Tollgates (Prüfung Architektur, Sicherheit, Abhängigkeit, Machbarkeit, betriebliche Readyness) implementieren, wenn die fachliche Lösung in die nächste Umgebung portiert wird.

3. Für die Stufe Geteilte Produktivität DARF KEINE PROD-Umgebung bereitgestellt werden.

4 Sicherstellen der Governance

1. Die Sicherstellung der Governance MUSS durch den Anwendungsverantwortlichen (AV) erfolgen.
2. Der AV MUSS folgende minimale Aufgaben wahrnehmen:
   a. Einhalten der Governance, Sicherheit und technische Standards.
   b. Unterstützen von Fachabteilungen bei der Entwicklung und Skalierung der fachlichen Lösung, allenfalls in Zusammenarbeit mit dem Gemeinsamen Fachdienst Business Process Automation.
   c. Bereitstellen von Umgebungen, Plattformzugriffen, Lizenzen und Infrastruktur.
   d. Bereitstellen von Berichten, damit die Departemente / BK ihre fachlichen Lösungen effektiv überwachen und verwalten können.
   e. Die FAVs entsprechend über vorgesehene Patches und Releases der genutzten Power Platform Services vorgängig und umfassend informieren (z.B. über eine Power Platform Community).
   f. Die FAVs darüber informieren – wenn die Anwendung aufgrund Nichtnutzung (z. B. keine berechtigten Benutzer, keine Aktivität während einer bestimmten Zeit) – ihre fachliche Lösung wieder löschen.
   g. Beim Ausserbetriebnehmen der fachlichen Lösung unterstützen.

Anhänge

A. Referenzen

ID	Referenz[3]
VDTI	Verordnung über die digitale Transformation und die Informatik, VDTI vom 25. November 2020; SR 172.010.58
AR015	AR015 - Architekturvorgaben bei Nutzung von Cloud Ressourcen des Microsoft Ökosystems
IAMV	Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes

B. Abkürzungen

Kürzel	Bedeutung
SD/BA	Standarddienst Büroautomation
M365	Microsoft 365
LE	Leistungserbringer
LB	Leistungsbezüger

C. Prinzipien

Die Governance basiert auf den folgenden Prinzipien.

Prinzip 1	Schutz und Kontrolle der Daten
Aussage	Der Schutz und die Kontrolle von Daten haben oberste Priorität.
Begründung	Daten sind ein kritisches Gut. Ihr Schutz ist essenziell für Vertrauen, Compliance und Geschäftskontinuität.
Implikationen	• Mehrschichtige Sicherheitsmassnahmen (DLPs, Zugriffskontrollen, usw.) • Einsatz von Microsoft Purview, Sentinel und CoE Toolkit zur Überwachung • Umsetzung des «Least Privilege»-Prinzips

Prinzip 2	Einheitliche Datenschutzrichtlinien
Aussage	Datenschutzrichtlinien gelten konsistent über alle Ebenen und Umgebungen hinweg.
Begründung	Einheitliche Regeln verhindern Inkonsistenzen und Sicherheitslücken.

[3] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. Bei einer referenzierten Weisung zur Bundesinformatik wird die zum Ausgabedatum dieser Beilage gültige Version angegeben.

Prinzip 2	**Einheitliche Datenschutzrichtlinien**
Implikationen	• Durchsetzung von Data Policies • Änderungen gelten tenantweit • Governance muss regelmässig überprüft und angepasst werden

Prinzip 3	**Gesteuerte Ausnahmenbehandlung**
Aussage	Ausnahmen werden strukturiert über Solutions behandelt.
Begründung	Geschäftskritische oder sicherheitsrelevante Anforderungen erfordern Flexibilität bei gleichzeitiger Kontrolle.
Implikationen	• Ausnahmen bedürfen zusätzlicher Genehmigungen • Dokumentation und Risikobewertung sind verpflichtend

Prinzip 4	**Klare Verantwortlichkeiten bei Bereitstellung und Nutzung**
Aussage	Jede Umgebung muss definierte Anforderungen erfüllen und die Verantwortlichkeiten müssen klar geregelt sein.
Begründung	Transparenz und Verantwortlichkeit sind essenziell für sicheren Betrieb.
Implikationen	• Die fachliche Lösung muss eingestuft werden • Dokumentation von Verantwortlichkeiten • Dokumentation von Datenquellen und Klassifizierungen • ALM-Prozesse müssen definiert und eingehalten werden • Risikobewertung ist verpflichtend

Prinzip 5	**Übergabe an Integrationsmanager**
Aussage	Nach Bereitstellung der Umgebung erfolgt die Übergabe an zuständige Integrationsmanager (IMs).
Begründung	Klare Zuständigkeiten fördern effizienten Betrieb und Support.
Implikationen	• IMs müssen geschult und informiert sein • Übergabeprozesse müssen dokumentiert sein und erfolgen den departamentalen Vorgaben

Prinzip 6	**Betrieb durch Tenant Betreiber**
Aussage	Die Power Platform wird zentral durch den Tenant Betreiber [gemäss AR015] bereitgestellt und betrieben.
Begründung	Zentrale Bereitstellung ermöglicht Standardisierung und Sicherheit.

Prinzip 6	**Betrieb durch Tenant Betreiber**
Implikationen	• Der Tenant Betreiber ist für Plattformbetrieb, Sicherheit und Überwachung verantwortlich • Nutzung des Power Platform Admin Centers (PPAC) und Center of Excellence Kit (CoE)

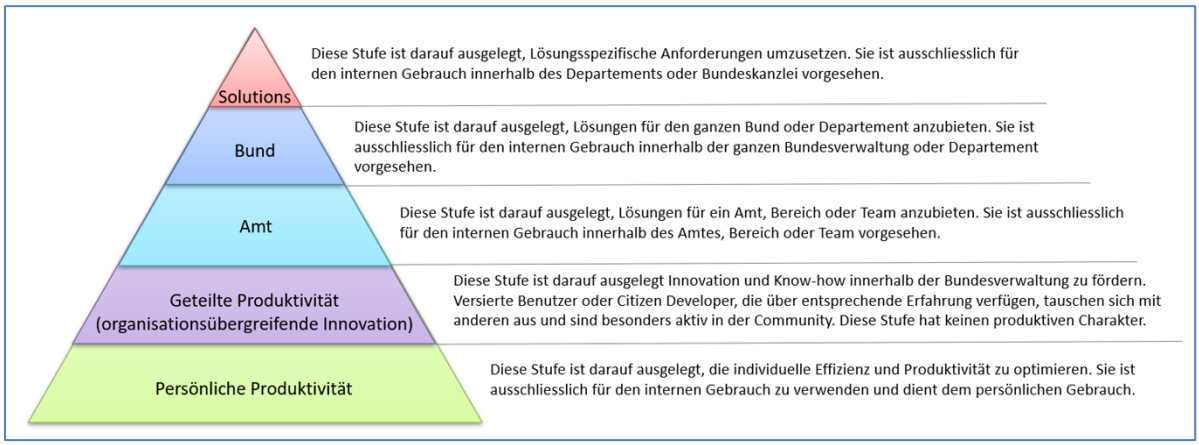
Prinzip 7	**Least Privilege Prinzip**
Aussage	Zugriffsrechte werden nach dem Prinzip der minimalen Rechte vergeben
Begründung	Minimierung von Risiken durch unnötige Berechtigungen
Implikationen	• Regelmässige Überprüfung von Rollen und Berechtigungen • Automatisierte Tools zur Rechtevergabe und -überwachung

D. Checkliste

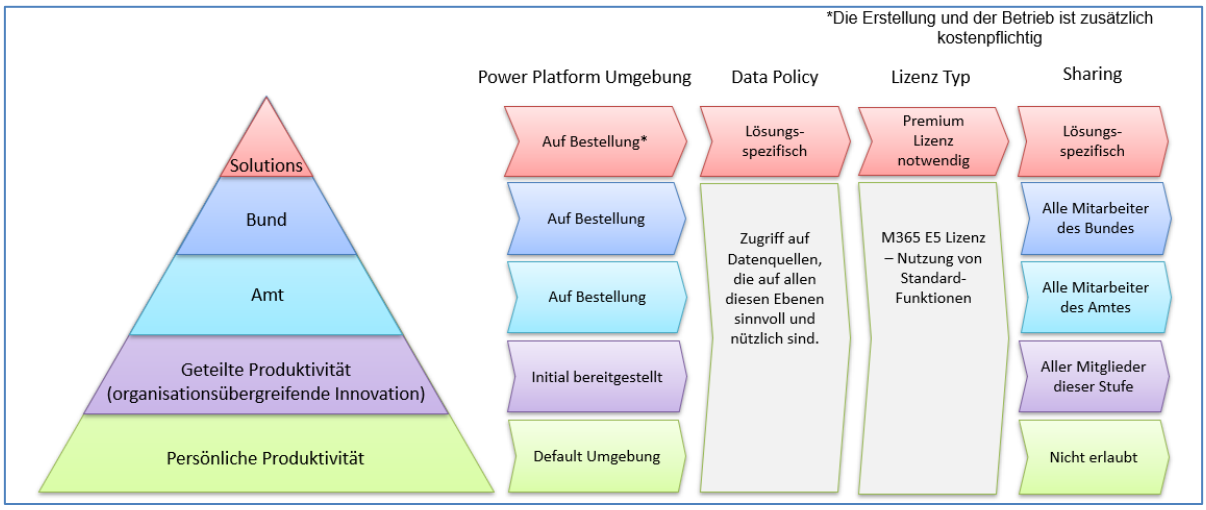
	Persönliche Produktivität	**Geteilte Produktivität**	**Teilen innerhalb des Amts oder BV**	**Solutions**
Bestellung und Einbezug Integrationsmanager (IM)		X	X	X
Definierter AV inkl. Stv. AV		X	X	X
Schutzbedarfsanalyse, Risikovorprüfung		(X)	X	X
Minimale Dokumentation	(X)	X		
Umfangreiche Dokumentation mit Architektur- und Sicherheitsunterlagen			X	X
Supportregelung			X	X
PFCT Bund Objekt			X	X
Finanzplanung			X	X

(X) Abhängig, welche Daten mit der Powerlösung verarbeitet werden.

E. Einstufung der fachlichen Lösung



F. Power Platform Pyramide



G. Application Lifecycle Management (ALM)