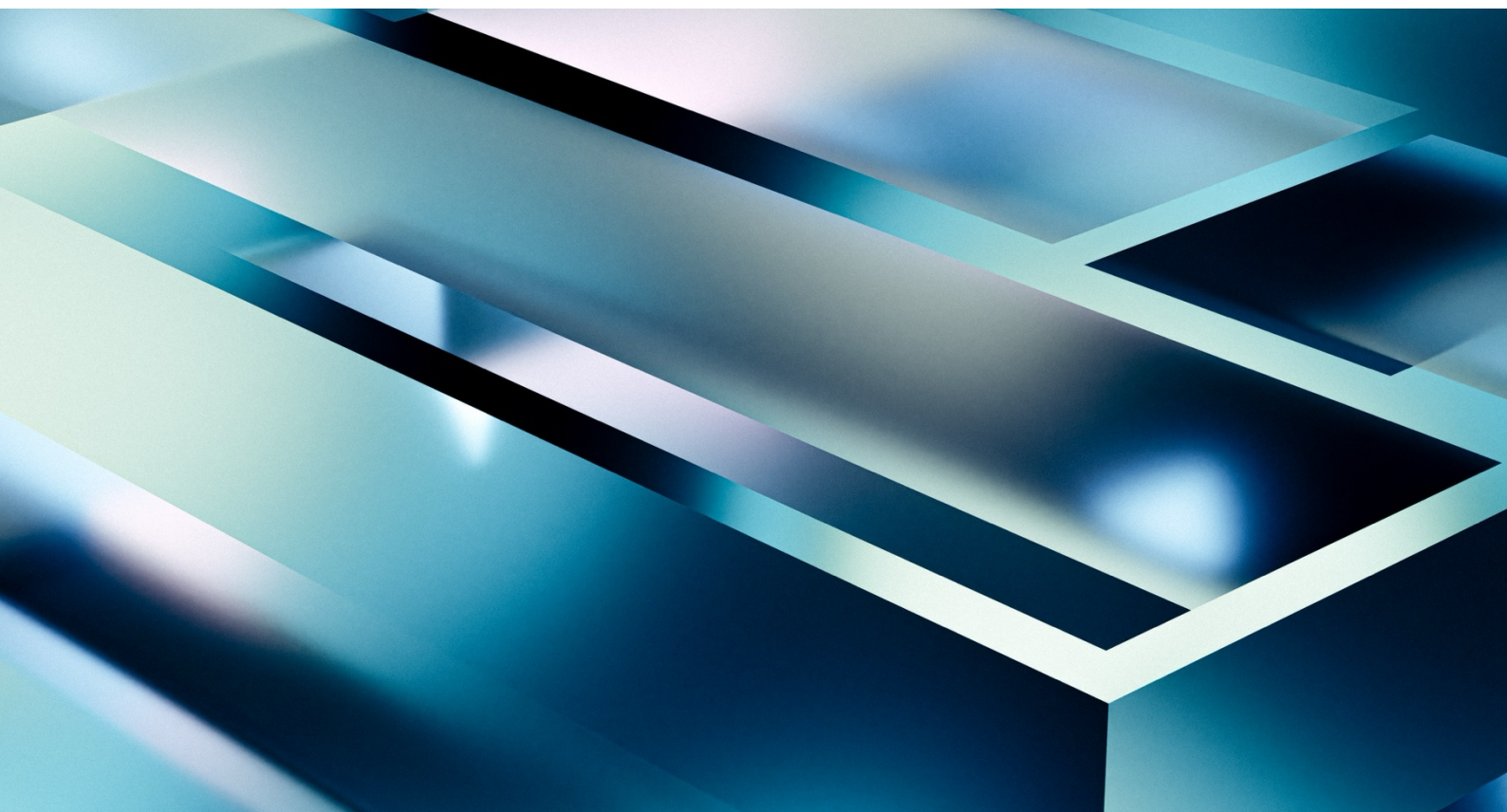


GovTech-Framework

Gemeinsame technische Grundlage für die produktiven
Ende-zu-Ende-Entwicklungs- und Betriebsumgebungen
Deutschlandplattform und MEDI:CUS auf Basis standardisierter,
modularer Multi-Cloud-Laufzeitumgebungen

Version 2.0

Author: GovTech Deutschland



Inhaltsverzeichnis

Executive Summary	4
1 Einleitung	5
2 Motivation	8
3 Konzept des GovTech-Frameworks	11
3.1 Zielsetzung und Rahmenbedingungen.....	11
3.2 Zielgruppen	12
3.3 Instanziierungen des GovTech-Frameworks: Deutschlandplattform und MEDI:CUS..	15
3.3.1 Deutschlandplattform	15
3.3.2 MEDI:CUS.....	16
3.4 Architekturübersicht: GovTech-Framework	17
3.5 Grundsätze und Designprinzipien	18
3.6 Alleinstellungsmerkmale und Mehrwerte	20
4 Konzeption und Operationalisierung der Plattformschichten	24
4.1 Infrastruktur-Schicht: GovTech Infrastructure	24
4.1.1 DevOps Services (DO).....	25
4.1.2 Virtuelle Infrastruktur Services (VI)	25
4.1.3 Organisatorische Eckpunkte von GovTech Infrastructure	27
4.1.4 Technische Eckpunkte von GovTech Infrastructure	27
4.1.5 Wirtschaftliche Eckpunkte von GovTech Infrastructure	28
4.2 Plattformkern: GovTech Core.....	28
4.2.1 Secure Multi-Cloud Abstraction Layer (CAL)	28
4.2.2 Basisdienste (BD).....	30
4.2.3 Organisatorische Eckpunkte von GovTech Core.....	33
4.2.4 Technische Eckpunkte von GovTech Core	33
4.2.5 Wirtschaftliche Eckpunkte von GovTech Core	35
4.3 Anwendungs- und Marktplatzschicht: GovTech Store	35
4.3.1 Querschnittsdienste (QD)	36
4.3.2 Fachdienste (FD)	40
4.3.3 Fachanwendungen (FA)	40
4.3.4 Organisatorische Eckpunkte von GovTech Store.....	42
4.3.5 Technische Eckpunkte von GovTech Store.....	43
4.3.6 Wirtschaftliche Eckpunkte von GovTech Store	45

5	Eckpunkte zur Souveränität	46
6	IT-Sicherheit und Datenschutz.....	49
6.1	<i>IT-Sicherheit</i>	49
6.1.1	Sicherheitsarchitektur des GovTech Core.....	49
6.1.2	Sicherheitskonzepte für Anwendungen im GovTech Store	50
6.2	<i>Datenschutz</i>	51
6.2.1	Datenschutzkonzept des GovTech Core.....	51
6.2.2	Datenschutzkonzepte für Anwendungen im GovTech Store.....	52
6.3	<i>Sicherheitszonen</i>	53
7	Fazit und Ausblick	55

Executive Summary

Die digitale Transformation der öffentlichen Verwaltung und des Gesundheitswesens benötigt eine belastbare, skalierbare und souveräne technische Grundlage. Mit dem GovTech-Framework steht hierfür eine einheitliche Plattformarchitektur zur Verfügung, die die Entwicklung, Bereitstellung und den Betrieb digitaler Fachanwendungen unterstützt.

Das GovTech-Framework ist eine standardisierte, modulare Multi-Cloud-Plattform, die technische Architektur, Betrieb, Governance und Beschaffung zu einem integrierten Plattformansatz verbindet. Über die Plattform werden wiederverwendbare und sichere digitale Lösungen bereitgestellt, ohne dass Bedarfsträger oder Anbieter jeweils eigene Infrastrukturen oder Betriebsmodelle aufbauen müssen. Zugleich werden zentrale Anforderungen und Vorarbeiten für Sicherheitskonzepte bereits plattformseitig erbracht.

Die Plattform ermöglicht die Bereitstellung und Nutzung digitaler, produktbasierter Lösungen unterschiedlicher Anbieter, unter anderem über standardisierte, vorqualifizierte Bezugswege. Öffentliche Institutionen können Anwendungen schnell und inhouse beziehen, während Wettbewerb, Nachnutzbarkeit und Innovation systematisch gefördert werden. Kern der Plattform ist das GovTech-Framework mit einer klar geschichteten Architektur. Eine Cloud-Abstraktionsschicht entkoppelt Anwendungen von einzelnen Infrastrukturanbietern und ermöglicht echte Wechselfähigkeit. Zentrale Basisdienste wie Identitäts- und Zugriffsmanagement, Logging, Monitoring, Sicherheits- und Abrechnungsdienste werden plattformweit bereitgestellt und verbindlich genutzt. Auf dieser Grundlage können Querschnittsdienste, Fachdienste und vollständige Fachanwendungen effizient entwickelt, integriert, betrieben und sukzessive erweitert werden.

Sicherheit, Datenschutz und digitale Souveränität sind dabei integrale Bestandteile der Plattform („by design“). Durch Multi-Cloud-Abstraktion, offene Standards, den Einsatz von Open Source und Confidential Computing wird ein hohes Maß an Kontrollierbarkeit, Schutz sensibler Daten und langfristiger Wechselfähigkeit erreicht.

Das GovTech-Framework kann in verschiedenen produktiven Instanziierungen betrieben werden. Initial liegen zwei produktive Instanziierungen vor: die **Deutschlandplattform** für Bund, Länder und Kommunen sowie die **MEDI:CUS-Plattform** für das öffentliche Gesundheitswesen. Beide basieren auf dem GovTech-Framework und unterscheiden sich in ihrer fachlichen Ausprägung und den regulatorischen Anforderungen.

1 Einleitung

Die digitale Transformation der öffentlichen Verwaltung und des Gesundheitswesens ist eine zentrale Voraussetzung für den handlungsfähigen Staat von morgen. In den vergangenen Jahren wurden zahlreiche Initiativen, Programme und Einzelvorhaben angestoßen, um Verwaltungsleistungen zu digitalisieren und Prozesse zu modernisieren. Trotz dieser Fortschritte bestehen weiterhin strukturelle Herausforderungen, insbesondere im Hinblick auf Skalierbarkeit, Wiederverwendbarkeit, Wirtschaftlichkeit und Sicherheit digitaler Lösungen. Häufig entstehen isolierte Einzellösungen, deren Betrieb und Weiterentwicklung hohe Aufwände verursachen und die nur begrenzt über Organisations- oder Ebenengrenzen hinweg nachgenutzt werden können.

Vor diesem Hintergrund schafft das **GovTech-Framework** eine gemeinsame, souveräne und skalierbare Grundlage für die Digitalisierung der öffentlichen Hand. Sie dient als operative Ende-zu-Ende-Betriebsumgebung, auf der digitale Anwendungen sicher, effizient und standardisiert entwickelt, bereitgestellt und betrieben werden können. Ziel ist es, die Digitalisierung nicht als Abfolge einzelner Projekte, sondern als dauerhaft nutzbares Plattformmodell zu etablieren, das Wiederverwendung fördert, Komplexität reduziert und Innovation beschleunigt.

Kern des GovTech-Frameworks ist eine standardisierte, modulare **Multi-Cloud-Laufzeitumgebung**. Sie stellt Infrastruktur, zentrale Basisdienste sowie marktplatzfähige Anwendungen in einem integrierten Betriebsmodell bereit. Dadurch werden technische und organisatorische Grundlagen vor die Klammer gezogen, sodass sich Bedarfsträger und Anbieter auf fachliche Inhalte und Mehrwerte konzentrieren können, ohne jeweils eigene Infrastrukturen, Betriebsmodelle oder Sicherheitskonzepte aufbauen zu müssen. Die Plattform ist dabei von Beginn an auf hohe Sicherheits- und Datenschutzanforderungen sowie auf föderale und sektorale Anschlussfähigkeit ausgelegt. Die Plattform schafft durch den Multi-Cloud-Ansatz und den verstärkten Einsatz von Open-Source-Technologien die Voraussetzungen für digitale Souveränität, insbesondere durch Offenheit und Wechselfähigkeit.

Das GovTech-Framework ist schichtenbasiert aufgebaut und gliedert sich in drei Ebenen. Die **Infrastruktur-Schicht** (*GovTech Infrastructure*) stellt virtualisierte, Multi-Cloud-fähige Ressourcen für Rechenleistung, Speicher und Netzwerk bereit. Der **Plattformkern** (*GovTech Core*) umfasst einen Cloud-Abstraktionslayer sowie zentrale Basisdienste, die plattformweit einheitlich genutzt werden. Die oberste Schicht bildet

eine **Anwendungs- und Marktplatzebene** (*GovTech Store*), über die Querschnittsdienste, Fachdienste und vollständige Fachanwendungen bereitgestellt und bezogen werden können. Dieses Architekturmodell ermöglicht eine klare Trennung von Verantwortlichkeiten, hohe Wiederverwendbarkeit und die unabhängige Weiterentwicklung einzelner Komponenten.

Der Marktplatzansatz der Plattform schafft einen einfachen, standardisierten Bezugsweg für digitale Lösungen. Öffentliche Institutionen können Anwendungen über bestehende Rahmenverträge direkt beziehen, ohne eigene Ausschreibungen durchführen zu müssen. Anbieter von Fachverfahren und digitalen Lösungen erhalten zugleich eine geprüfte, standardisierte Entwicklungs- und Betriebsumgebung sowie Zugang zu einem breiten Anwenderkreis. Damit verbindet die Plattform technologische Standardisierung mit wirtschaftlicher Effizienz und wettbewerblicher Offenheit.

Die Verantwortung für Aufbau, Betrieb und Weiterentwicklung des GovTech-Frameworks liegt bei **GovTech Deutschland** in der Rolle als Plattformbetreiber. Als gemeinsame Organisation von Bund, Ländern und Kommunen stellt GovTech Deutschland die technischen, organisatorischen und wirtschaftlichen Rahmenbedingungen bereit, verantwortet den Plattformbetrieb und sorgt für die kontinuierliche Weiterentwicklung des Angebots. Dazu zählen insbesondere der Betrieb des Multi-Cloud-Abstraktionslayers, die Bereitstellung zentraler Basisdienste, die Integration von Querschnitts- und Fachdiensten sowie die Ausgestaltung des Marktplatz- und Beschaffungsmodells. Durch Rahmenverträge und ein zentrales Abrechnungsmodell wird ein wirtschaftlicher, transparenter und inhouse-fähiger Bezug der Leistungen ermöglicht.

Das vorliegende Dokument beschreibt das GovTech-Framework aus strategischer, organisatorischer, technischer und wirtschaftlicher Perspektive. Es definiert die zentralen Leitplanken für Aufbau, Betrieb und Nutzung der Plattform und dient als Referenzrahmen für nachgelagerte Umsetzungs- und Fachkonzepte. Ziel ist es, ein gemeinsames Verständnis der Zielsetzung, der Architektur und der Nutzungsmöglichkeiten der Plattform zu schaffen. Das Dokument adressiert Entscheidungsträgerinnen und Entscheidungsträger auf Bundes-, Landes- und Kommunalebene, für die die Plattform ein strategisch relevantes Instrument der Verwaltungsdigitalisierung darstellt. Ebenso richtet es sich an öffentliche Institutionen und Einrichtungen des Gesundheitswesens als potenzielle Nutzer der Plattform sowie an externe Anbieter von Fachverfahren, Anwendungen und Diensten, die ihre Lösungen über die Plattform bereitstellen möchten.

Das GovTech-Framework liegt initial in zwei produktiven Instanziierungen vor: der **Deutschlandplattform** als verwaltungsspezifische Plattformausrprägung für Bund, Länder und Kommunen sowie der **MEDI:CUS-Plattform** als domänenspezifische Ausprägung für das öffentliche Gesundheitswesen. Beide Instanziierungen basieren auf dem gemeinsamen Framework, unterscheiden sich jedoch in ihrer fachlichen Ausprägung, ihrer Governance und den jeweils adressierten regulatorischen Anforderungen. Das zugrunde liegende GovTech-Framework stellt dabei bereits heute eine implementierte Referenz für zentrale Elemente des geplanten **Deutschland-Stacks** dar.

Die nachfolgenden Kapitel erläutern zunächst die Motivation für das Plattformmodell und die dahinterstehenden Herausforderungen. Anschließend wird das Konzept des GovTech-Frameworks detailliert beschrieben. Dabei werden die Zielgruppen, die Architektur, die Designprinzipien sowie die Alleinstellungsmerkmale und Mehrwerte erläutert.

2 Motivation

Die Digitalisierung der öffentlichen Verwaltung und des Gesundheitswesens wird seit Jahren durch zahlreiche Programme und Initiativen vorangetrieben. Dazu zählen unter anderem das Onlinezugangsgesetz, Maßnahmen zur Registermodernisierung, Konsolidierungsvorhaben sowie spezifische Digitalisierungsprogramme im Gesundheitswesen. Diese Initiativen adressieren wichtige fachliche und rechtliche Anforderungen, entfalten ihre Wirkung jedoch häufig nur begrenzt. Ein wesentlicher Grund dafür ist das Fehlen einer gemeinsamen, dauerhaft nutzbaren technischen und organisatorischen Grundlage, auf der digitale Lösungen effizient entwickelt, betrieben und übergreifend nachgenutzt werden können.

- In der Praxis zeigt sich, dass viele Digitalisierungsprojekte mit **langen Entwicklungs- und Bereitstellungszyklen** konfrontiert sind. Planungs-, Vergabe- und Umsetzungsphasen erstrecken sich häufig über mehrere Jahre. In dieser Zeit verändern sich technologische Standards, Sicherheitsanforderungen und Nutzererwartungen erheblich, sodass ursprünglich moderne Konzepte zum Zeitpunkt der Produktivsetzung bereits veraltet sind. Die fehlende Standardisierung von Infrastruktur, Betrieb und Basisdiensten erschwert zudem eine iterative Weiterentwicklung und eine schnelle Reaktion auf neue Anforderungen.
- Ein weiterer zentraler Hemmfaktor ist die **geringe Wiederverwendung bestehender Lösungen**. Digitale Anwendungen und Komponenten werden meist für einzelne Institutionen oder Vorhaben entwickelt und nur selten über Organisations- oder Ebenengrenzen hinweg nachgenutzt. Technische Inkompatibilitäten, fehlende gemeinsame Betriebsmodelle sowie organisatorische und rechtliche Hürden verhindern eine systematische Wiederverwendung. Dies führt zu parallelen Entwicklungen ähnlicher Funktionalitäten, erhöhten Kosten und einer insgesamt geringen Skalierung digitaler Lösungen.
- Die bestehenden IT-Landschaften in Verwaltung und Gesundheitswesen sind zudem stark **fragmentiert und historisch** gewachsen. Viele Systeme wurden als monolithische Insellösungen konzipiert, die auf spezifische institutionelle Anforderungen zugeschnitten sind. Unterschiedliche Softwareprodukte, proprietäre Schnittstellen und heterogene Datenmodelle erschweren die Integration, Interoperabilität und Wartung erheblich. Moderne Architekturansätze

wie modulare Services, standardisierte APIs oder containerbasierte Betriebsmodelle werden bislang nur punktuell genutzt.

- Diese technischen Defizite werden durch **organisatorische Rahmenbedingungen** weiter verstärkt. Institutionell gewachsene Strukturen, individuelle Zuständigkeiten und isolierte Entscheidungsprozesse erschweren eine übergreifende Koordination und Standardisierung. Regulatorische Fragestellungen, insbesondere zu Datenschutz und IT-Sicherheit, werden häufig dezentral und projektbezogen gelöst, anstatt auf gemeinsame, vorab geprüfte Konzepte zurückzugreifen. Dadurch entstehen zusätzliche Aufwände, Verzögerungen und Unsicherheiten in der Umsetzung digitaler Vorhaben.
- Auch wirtschaftlich stoßen bestehende Ansätze an ihre Grenzen. **Lange Projektlaufzeiten, hohe Betriebs- und Wartungskosten** sowie fehlende Skaleneffekte beeinträchtigen die Wirtschaftlichkeit digitaler Lösungen. Starre Vertragsmodelle und individuelle Ausschreibungen erschweren den flexiblen Bezug bedarfsgerechter Leistungen. Gleichzeitig fördern proprietäre Technologien und der Einsatz spezifischer Cloud-Services Abhängigkeiten von einzelnen Anbietern und erhöhen das Risiko langfristiger **Vendor Lock-ins**.
- Infrastrukturseitig sind viele Organisationen weiterhin durch **wenig flexible On-Premise-Strukturen** oder begrenzte Kapazitäten öffentlicher IT-Dienstleister geprägt. Lange Vorlaufzeiten, geringe Elastizität und hohe Fixkosten behindern den Einsatz moderner Entwicklungs- und Betriebsmodelle bereits auf der Infrastrukturebene. Dies wirkt sich unmittelbar auf die Geschwindigkeit, Qualität und Innovationsfähigkeit digitaler Lösungen aus.

In der Summe führen diese Rahmenbedingungen zu Doppelentwicklungen, ineffizientem Ressourceneinsatz und einer hohen operativen Komplexität. Eine durchgängige Ende-zu-Ende-Digitalisierung sowie die konsequente Umsetzung des Once-Only-Prinzips lassen sich unter diesen Voraussetzungen nur eingeschränkt realisieren. Gleichzeitig steigt der politische und gesellschaftliche Erwartungsdruck, digitale Leistungen schneller, nutzerfreundlicher und sicherer bereitzustellen.

Vor diesem Hintergrund bedarf es einer integrierten Plattform, die technische, organisatorische und wirtschaftliche Anforderungen zusammenführt. Das GovTech-Framework schafft hierfür eine standardisierte und souveräne Grundlage für Entwicklung, Betrieb und Beschaffung digitaler Lösungen. Es reduziert Fragmentierung, ermöglicht systematische Nachnutzung, beschleunigt die Umsetzung und trägt zu einer

nachhaltigen, föderal anschlussfähigen Digitalisierung in Verwaltung und Gesundheitswesen bei.

3 Konzept des GovTech-Frameworks

Dieses Kapitel beschreibt das konzeptionelle Fundament des GovTech-Frameworks. Es stellt die zentralen Rahmenbedingungen und Gestaltungsprinzipien dar und zeigt deren Ausprägung für unterschiedliche Zielgruppen und Anwendungsbereiche.

3.1 Zielsetzung und Rahmenbedingungen

Ziel des GovTech-Frameworks ist es, eine gemeinsame, souverän betriebene und dauerhaft nutzbare Plattform bereitzustellen, auf der digitale Lösungen für Verwaltung und Gesundheitswesen sicher, effizient und wiederverwendbar entwickelt und betrieben werden können. Es adressiert damit gezielt die strukturellen Defizite bestehender Digitalisierungsansätze und schafft eine einheitliche Grundlage für eine skalierbare und nachhaltige digitale Transformation.

- Die Plattform verfolgt den Anspruch, Fragmentierung zu reduzieren und **Wiederverwendung** systematisch zu fördern. Durch die Bereitstellung zentraler Infrastrukturkomponenten, eines einheitlichen Betriebsmodells sowie verbindlicher Basisdienste werden technische und organisatorische Grundlagen standardisiert. Digitale Fachanwendungen können modular aufgebaut, interoperabel betrieben und über institutionelle Grenzen hinweg nachgenutzt werden. Gleichzeitig sinkt die Komplexität für einzelne Bedarfsträger erheblich, da grundlegende Aufgaben vorab zentral gelöst sind.
- Ein wesentliches Ziel der Plattform ist die **Beschleunigung von Entwicklungs- und Bereitstellungsprozessen**. Standardisierte Schnittstellen, klare Architekturrichtlinien und vorkonfigurierte Dienste ermöglichen eine schnelle Integration neuer Anwendungen und Dienste. Self-Service-Ansätze und ein Marktplatzmodell tragen zusätzlich dazu bei, Time-to-Market-Zeiten zu verkürzen und Skaleneffekte zu realisieren.
- Der föderale Aufbau der öffentlichen Verwaltung wird im Plattformdesign ausdrücklich berücksichtigt. Die Plattform verbindet zentrale technische Grundlagen mit dezentraler fachlicher Verantwortung. Mandantenfähigkeit, rollenbasierte Zugriffskonzepte und klar definierte Trennungen zwischen Organisationen ermöglichen eine gemeinsame Nutzung der Plattform bei gleichzeitiger Wahrung institutioneller Autonomie. Die Plattform stärkt damit die **föderale Zusammenarbeit**, ohne dass zentrale Steuerungspflichten oder

rechtliche Anpassungen, etwa am Artikel 91c des Grundgesetzes, erforderlich sind.

- **Regulatorische Anforderungen**, insbesondere in den Bereichen Datenschutz, IT-Sicherheit und Compliance, sind integraler Bestandteil der Plattformkonzeption. Anstatt diese Anforderungen in jedem Projekt neu zu adressieren, werden sie zentral vorab umgesetzt und als verbindlicher Rahmen bereitgestellt. Gleichzeitig bleibt Raum für zusätzliche, fach- oder institutionsspezifische Anforderungen, die über Konfigurationen oder ergänzende Maßnahmen berücksichtigt werden können. Dies erhöht sowohl die Umsetzungsgeschwindigkeit als auch die Rechtssicherheit für alle Beteiligten.
- Die Plattform ist bewusst so gestaltet, dass sie langfristig weiterentwickelt und auf neue fachliche und technologische Anforderungen angepasst werden kann. **Modularität, Offenheit und Wechselfähigkeit** sind daher zentrale Rahmenbedingungen. Abhängigkeiten von einzelnen Anbietern oder Technologien werden gezielt vermieden, um digitale Souveränität und Investitionssicherheit zu gewährleisten.

Insgesamt versteht sich das GovTech-Framework als strategisches Fundament für eine moderne, vernetzte und nutzerorientierte Digitalisierung. Sie schafft stabile Rahmenbedingungen für Innovation, fördert Wettbewerb und Zusammenarbeit und ermöglicht es öffentlichen Institutionen, digitale Lösungen schneller, wirtschaftlicher und sicherer bereitzustellen und zu betreiben.

3.2 Zielgruppen

Die auf dem GovTech-Framework basierenden Instanzen richten sich an diverse Akteure im öffentlichen Sektor und im Gesundheitswesen, die jeweils in unterschiedlicher Rolle an der Entwicklung, Bereitstellung, Nutzung und dem Betrieb digitaler Lösungen beteiligt sind. Als gemeinsames Plattformmodell schafft das Framework ein **integriertes Ökosystem**, das sowohl Synergien zwischen den Akteuren hebt als auch deren spezifische Anforderungen berücksichtigt. Zur gezielten Ausgestaltung der Mehrwerte werden drei zentrale Zielgruppen unterschieden.

1. Anbieter von Fachverfahren, Fachanwendungen sowie Fach- und Querschnittsdiensten

Private und öffentliche Anbieter digitaler Lösungen erhalten mit der Plattform eine standardisierte, geprüfte und wirtschaftliche Entwicklungs- und Betriebsumgebung. Sie können ihre Lösungen direkt auf der Plattform entwickeln, testen und betreiben, ohne eigene Infrastrukturen oder individuelle Betriebsmodelle aufbauen zu müssen. Zentrale Basisdienste wie Identitätsmanagement, Logging, Monitoring oder CI/CD-Pipelines stehen sofort zur Verfügung und reduzieren den Entwicklungs- und Integrationsaufwand. Durch den Marktplatzansatz erreichen Anbieter mit einem einheitlichen technischen und vertraglichen Onboarding einen breiten Nutzerkreis in Verwaltung und Gesundheitswesen. Sicherheits- und Datenschutzanforderungen sind auf Plattformebene bereits berücksichtigt, sodass sich Anbieter auf die fachliche Ausgestaltung ihrer Lösungen konzentrieren können. Gleichzeitig ermöglicht die Plattform die Nutzung vorhandener Querschnitts- und Fachdienste anderer Anbieter, was Wiederverwendung fördert und Innovationszyklen verkürzt. Insgesamt profitieren Anbieter von kürzeren Time-to-Market-Zeiten, geringeren Betriebskosten, klaren technischen Standards und einem erweiterten adressierbaren Markt. Damit schafft das GovTech-Framework attraktive Rahmenbedingungen für Wettbewerb, Kooperation und nachhaltige Innovation im öffentlichen Sektor.

Beispiel: Ein Fachverfahrenshersteller stellt ein Verfahren zur steuerlichen Anmeldung von Hundehaltung auf der Plattform bereit und nutzt dabei einen bereits im Marktplatz verfügbaren Workflow- und Formularbuilder. Mehrere Bundesländer können die Lösung direkt und ohne erneute Ausschreibungsverfahren beziehen und mit minimalem Anpassungsaufwand produktiv einsetzen, während sich für den Hersteller der Entwicklungsaufwand durch die Nachnutzung bestehender Dienste deutlich reduziert.

2. Bedarfsträger der öffentlichen Verwaltung und des Gesundheitswesens

Öffentliche Institutionen, insbesondere Behörden, Verwaltungen und Einrichtungen des Gesundheitswesens, profitieren von einem stark vereinfachten Zugang zu digitalen Lösungen. Über den Marktplatz der Plattform können Fachanwendungen, Fachdienste und Querschnittsdienste ohne eigene Ausschreibungsverfahren direkt bezogen und genutzt werden. Dies reduziert Beschaffungsaufwände und verkürzt Einführungszeiten erheblich. Gleichzeitig ermöglicht der Plattformansatz den Wechsel zwischen alternativen Lösungen und fördert damit Wettbewerb, Innovation und Souveränität. Für

Mitarbeiterinnen und Mitarbeiter in Fachbereichen stehen moderne, standardisierte Anwendungen zur Verfügung, die Prozesse automatisieren und die tägliche Arbeit unterstützen. Technische Verantwortliche und IT-Abteilungen profitieren von klar definierten Entwicklungs- und Betriebsgrundlagen, zentral bereitgestellten Basisdiensten sowie vorgeprüften Sicherheits- und Datenschutzmechanismen. Der Aufwand für Integration, Betrieb und Wartung sinkt, während Skalierbarkeit, Stabilität und Sicherheit steigen. Auf Ebene von Führungskräften, Projektleitungen und Steuerungsgremien schafft die Plattform Transparenz und Steuerungsfähigkeit. Einheitliche Governance-Strukturen, definierte Rollenmodelle sowie zentrale Auswertungs- und Reportingmöglichkeiten ermöglichen eine datenbasierte Steuerung von Nutzung, Kosten und Weiterentwicklung digitaler Lösungen über die gesamte Organisation hinweg.

Beispiel: Eine Kommune bezieht eine Fachanwendung über die Plattform, passt sie an eigene Vorgaben an und setzt sie innerhalb weniger Tage produktiv ein. Sachbearbeiterinnen und Sachbearbeiter erhalten ein modernes Werkzeug zur automatisierten Fallbearbeitung, während technische Verantwortliche auf zentrale Basisdienste und vorgeprüfte Sicherheitsbausteine zurückgreifen, ohne eigene Infrastruktur oder zusätzliche Integrationen aufbauen zu müssen. Die Anbindung bestehender Identitätslösungen erfolgt über standardisierte Schnittstellen.

3. Endnutzer: Bürgerinnen und Bürger, Patientinnen und Patienten, Unternehmen

Auch die Endnutzer, wie Bürgerinnen und Bürger, profitieren von der Plattform durch gesteigerte Qualität und Nutzbarkeit digitaler Leistungen. Sie nutzen die bereitgestellten Anwendungen und durchgängige, medienbruchfreie Services mit einheitlichen Zugängen und konsistenter Benutzerführung. Dies führt zu kürzeren Bearbeitungszeiten, höherer Transparenz und einer insgesamt besseren Nutzererfahrung bei der Inanspruchnahme öffentlicher Leistungen. Gleichzeitig steigert die effizientere Leistungserbringung die Verwaltungseffizienz insgesamt und trägt so mittelbar zu einer leistungsfähigeren, bürgernäheren Verwaltung bei.

Beispiel: Ein Unternehmen erhält über ein zentrales, benutzerfreundliches Portal direkten Zugang zu einer auf der Plattform betriebenen Fachanwendung und kann Anträge, Nachweispflichten oder Meldungen vollständig digital und ohne Systembrüche erledigen.

3.3 Instanziierungen des GovTech-Frameworks: Deutschlandplattform und MEDI:CUS

Das GovTech-Framework ist als **übertragbares Plattformmodell** aufgebaut, auf dessen Grundlage mehrere fachlich spezialisierte Instanziierungen betrieben werden, die unterschiedliche Zielgruppen, Anwendungsdomänen und regulatorische Anforderungen adressieren. Allen Instanziierungen gemeinsam sind die zugrunde liegende Architektur, das Betriebsmodell sowie zentrale Prinzipien wie Multi-Cloud-Fähigkeit, Modularität, Wiederverwendbarkeit und hohe Sicherheitsstandards. Unterschiede ergeben sich in der fachlichen Ausprägung, der Governance sowie in spezifischen rechtlichen und regulatorischen Rahmenbedingungen.

Die Instanziierungen werden technisch getrennt und logisch separiert betrieben. Dabei ist die fachliche und regulatorische Abgrenzung bei gleichzeitiger Nutzung eines gemeinsamen Frameworks maßgeblich. Dieses wird über Konfigurationen und instanzspezifische Serviceausprägungen angepasst. Dieses Modell ermöglicht es, domänenspezifische Anforderungen zu erfüllen, ohne die Vorteile einer gemeinsamen Plattformbasis aufzugeben. Neben den bestehenden Instanziierungen sind weitere Ausprägungen für zusätzliche Fachdomänen grundsätzlich möglich.

Aktuell existieren zwei **produktive Instanziierungen**: die Deutschlandplattform für die öffentliche Verwaltung sowie die MEDI:CUS-Plattform für das öffentliche Gesundheitswesen.

3.3.1 Deutschlandplattform

Die Deutschlandplattform ist die **verwaltungsspezifische Instanziierung** des GovTech-Frameworks. Sie richtet sich an Bedarfsträger aus Bund, Ländern und Kommunen und dient als operative Entwicklungs- und Betriebsplattform für digitale Verwaltungsanwendungen, Fachverfahren, Fachdienste und Querschnittsdienste. Ziel ist es, eine souverän betriebene, föderal anschlussfähige und standardisierte Laufzeitumgebung bereitzustellen, die die Nachnutzung digitaler Lösungen über Ebenen und Institutionen hinweg ermöglicht.

Die Deutschlandplattform befindet sich im produktiven Betrieb und ist bereits Bestandteil laufender Digitalisierungsprojekte. Sie dient unter anderem als zentrale Plattform im Kontext der Planungs- und Genehmigungsbeschleunigung und wird schrittweise bundesweit ausgerollt. Architekturprinzipien, Betriebsprozesse und organisatorische Strukturen sind erprobt und lassen sich unmittelbar für weitere

Vorhaben der Verwaltungsdigitalisierung nachnutzen. Sie stellt dabei bereits heute eine funktionierende Referenz für zentrale Elemente des geplanten **Deutschland-Stacks** dar.

Die Plattform ist dabei so ausgelegt, dass Fachverfahren und Dienste ohne erneute infrastrukturelle Grundsatzentscheidungen integriert und betrieben werden können. Sie unterstützt explizit die Nachnutzung bestehender Lösungen und ist anschlussfähig an bestehende und zukünftige Strukturen wie den Deutschland-Stack, die Deutsche Verwaltungscld sowie den Marktplatz Deutschland Digital. Zusätzliche Anforderungen, etwa Umsetzung spezifischer Standards und Vorgaben, können schrittweise ergänzt werden.

3.3.2 MEDI:CUS

Die MEDI:CUS-Plattform ist die **gesundheitswesensspezifische Instanziierung** des GovTech-Frameworks. Sie adressiert die besonderen fachlichen, organisatorischen und regulatorischen Anforderungen des öffentlichen Gesundheitswesens und wird insbesondere von Krankenhäusern und weiteren medizinischen Einrichtungen genutzt. Die Plattform wurde im Auftrag des Landes Baden-Württemberg aufgebaut und wird schrittweise auch für weitere Länder geöffnet.

MEDI:CUS befindet sich im produktiven Betrieb. Mehrere Kliniken sind bereits angebunden und nutzen die Plattform aktiv für den Betrieb und die Integration digitaler Anwendungen, etwa zur Unterstützung der Patientenversorgung, zur Telemedizin oder zur einrichtungsübergreifenden Zusammenarbeit. Träger und Betreiber ist eine eigene Betriebsgesellschaft, die den technischen und organisatorischen Rahmen für die angebundenen Einrichtungen verantwortet.

Sowohl in der Architektur und im Betrieb berücksichtigt MEDI:CUS die hohen Anforderungen an Datenschutz, Informationssicherheit und Interoperabilität im Gesundheitswesen. Durch die Nutzung desselben zugrunde liegenden Frameworks wie bei der Deutschlandplattform wird eine hohe technologische Konsistenz erreicht, während fachliche Anwendungen, Dienste und Standards gezielt auf die Anforderungen des Gesundheitsbereichs zugeschnitten sind. MEDI:CUS zeigt damit exemplarisch, wie das GovTech-Framework domänenspezifisch instanziiert und gleichzeitig für einen länderübergreifenden Ausbau genutzt werden kann.

3.4 Architekturübersicht: GovTech-Framework

Das GovTech-Framework beschreibt die technische Architektur der Plattform. Es definiert die strukturellen und technologischen Leitplanken für Aufbau, Betrieb und Weiterentwicklung der Plattform und bildet die gemeinsame Grundlage für alle Instanziierungen. Die Architektur folgt einem klar **geschichteten Modell**, in dem jede Ebene eine eindeutig abgegrenzte Aufgabe erfüllt und über standardisierte Schnittstellen mit den angrenzenden Schichten verbunden ist.

Das Framework ist in drei komplementäre Schichten gegliedert. Alle Dienste und Komponenten werden grundsätzlich innerhalb der Plattform betrieben, um konsistente Sicherheits-, Betriebs- und Governance-Standards sicherzustellen.

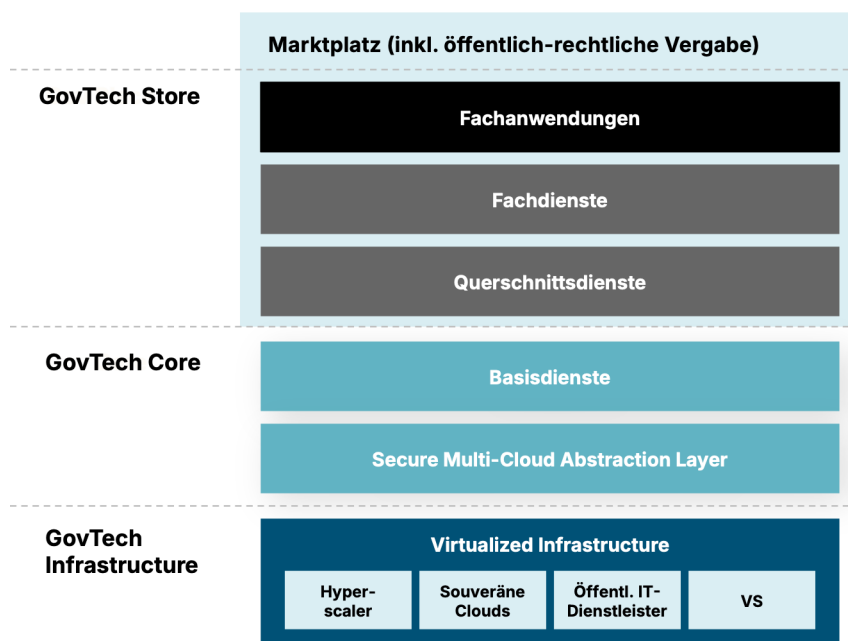


Abbildung 1: Architekturschichten des GovTech-Frameworks

GovTech Infrastructure bildet die unterste Schicht und stellt cloudfähige Infrastrukturressourcen für Rechenleistung, Speicher und Netzwerk bereit und ermöglicht einen hochverfügbaren, skalierbaren und Betrieb von der Plattform inkl. zentraler Plattformdiensten. Standardisierte Schnittstellen gewährleisten eine einheitliche Nutzung der Infrastruktur über verschiedene Anbieter hinweg.

GovTech Core stellt den technologischen Kern der Plattform dar. Er besteht aus einem **sicheren Multi-Cloud-Abstraktionslayer** sowie zentral bereitgestellten **Basisdiensten**. Der Abstraktionslayer vereinheitlicht den Zugriff auf Infrastrukturressourcen

unterschiedlicher Anbieter, reduziert Abhängigkeiten und ermöglicht echte Wechselfähigkeit. Gleichzeitig schafft er die Grundlage für den Einsatz von Confidential Computing, indem Daten auch während der Verarbeitung in isolierten, vertrauenswürdigen Ausführungsumgebungen geschützt werden können. Die Basisdienste, darunter Identitäts- und Zugriffsmanagement, Logging, Monitoring, Sicherheits- und Abrechnungsdienste, werden plattformweit verbindlich bereitgestellt und stellen sicher, dass Anwendungen interoperabel, sicher und effizient betrieben werden können.

GovTech Store bildet die oberste Schicht und fungiert als Anwendungs- und Marktplatzebene der Plattform. Hier werden Querschnittsdienste, Fachdienste und vollständige Fachanwendungen integriert und bereitgestellt. **Querschnittsdienste** sind übergreifende Funktionsbausteine, etwa Low-Code-Engines, Dokumentenmanagement oder KI-Plattformen, die in unterschiedlichen Ausprägungen verfügbar sind und – im Gegensatz zu Basisdiensten – auch von (mehreren) Drittanbietern bereitgestellt werden können. **Fachdienste** sind modulare, generische oder spezialisierte Dienste ohne eigene Benutzeroberfläche, darunter auch von Dritten bereitgestellte Angebote wie KI-Agenten oder weitere 3rd-Party-Komponenten. **Fachanwendungen** sind vollständige, nutzerorientierte digitale Lösungen bzw. Fachverfahren mit direkter Schnittstelle zu Endanwendenden, die Basis-, Querschnitts- und Fachdienste nutzen und über den Marktplatz der Plattform bereitgestellt und direkt gestartet werden. Der Store schafft einen standardisierten Zugang zu digitalen Lösungen unterschiedlicher Anbieter und unterstützt deren einfache Bereitstellung, Nutzung und Skalierung. Anwendungen können dabei sowohl plattformnativ entwickelt als auch aus externen Umgebungen in die Plattform integriert werden, sofern sie den definierten technischen und organisatorischen Anforderungen entsprechen.

Die klare Trennung zwischen Infrastruktur, Plattformkern und Anwendungsebene erlaubt eine unabhängige Weiterentwicklung der einzelnen Schichten. Neue Dienste können integriert, bestehende Komponenten ausgetauscht und Anwendungen skaliert werden, ohne andere Ebenen zu beeinträchtigen. Gleichzeitig gewährleisten die einheitlichen Basisdienste und der gemeinsame Abstraktionslayer konsistente Sicherheits- und Betriebsstandards über alle Instanziierungen hinweg.

3.5 Grundsätze und Designprinzipien

Der Aufbau und Betrieb des GovTech-Frameworks folgen klar definierten Grundsätzen und Designprinzipien. Sie stellen sicher, dass die Plattform nicht nur konzeptionell

schlüssig ist, sondern auch dauerhaft konsistent, interoperabel, sicher und wirtschaftlich betrieben werden kann. Die Prinzipien bilden den verbindlichen Rahmen für Architekturentscheidungen, Betriebsmodelle und die Weiterentwicklung der Plattform über alle Instanziierungen hinweg.

Zentrales Leitmotiv ist das Prinzip des „**Vor-die-Klammer-Ziehens**“. Grundlegende technische, organisatorische und regulatorische Aufgaben werden zentral gelöst und plattformweit einheitlich bereitgestellt. Dazu zählen insbesondere Infrastrukturabstraktion, Basisdienste, Sicherheits- und Datenschutzkonzepte, technische Standards sowie vergaberechtliche und wirtschaftliche Rahmenbedingungen. Durch diese Vorab-Standardisierung werden Redundanzen vermieden, Komplexität reduziert und die Einstiegshürden für Bedarfsträger und Anbieter deutlich gesenkt.

- Ein wesentliches Gestaltungsprinzip ist die Sicherstellung **digitaler Souveränität** durch konsequente **Wechselfähigkeit**. Nutzende behalten jederzeit die Kontrolle über Daten, Technologien und Betriebsentscheidungen. Abhängigkeiten von einzelnen Anbietern werden bewusst begrenzt, transparent gemacht und aktiv gesteuert. Anwendungen und Dienste sind so gestaltet, dass sie innerhalb eines Multi-Cloud-Ansatzes migriert oder durch alternative Lösungen ersetzt werden können. Alle wesentlichen Komponenten sind austauschbar ausgelegt, Schnittstellen offen und dokumentiert. Providerspezifische, proprietäre Funktionen werden nur eingesetzt, wenn sie zwingend erforderlich sind. So werden **Vendor Lock-ins** wirksam vermieden.
- Die Plattform folgt dem Prinzip der **Offenheit**. Der Einsatz von Open-Source-Software stärkt Transparenz, Auditierbarkeit und technologische Unabhängigkeit. Gleichzeitig bleibt die Plattform für proprietäre Lösungen offen, sofern diese die definierten technischen, organisatorischen und regulatorischen Anforderungen erfüllen. Wettbewerb und Innovation werden so gezielt gefördert.
- Ein weiteres zentrales Prinzip ist die **Datenportabilität und Interoperabilität**. Standardisierte, herstellerunabhängige Schnittstellen ermöglichen die Migration von Daten, den Austausch von Komponenten und die Nachnutzung bestehender Lösungen über Organisations- und Ebenengrenzen hinweg. Dadurch wird eine flexible Weiterentwicklung der Plattform und der darauf betriebenen Anwendungen unterstützt.

- Die Architektur des GovTech-Frameworks ist konsequent **modular** aufgebaut. Funktionen, Dienste und Anwendungen können schrittweise integriert, erweitert oder ersetzt werden, ohne bestehende Strukturen zu beeinträchtigen. Diese Modularität ermöglicht eine kontinuierliche Weiterentwicklung bei gleichzeitiger Stabilität des Gesamtsystems.
- Die Plattform folgt einem **Cloud-First- und Cloud-Native-Ansatz**. Alle Komponenten werden grundsätzlich in Cloud-Umgebungen realisiert und nach cloud-nativen Prinzipien entwickelt. Dazu zählen containerbasierte Architekturen, automatisierte Bereitstellungsprozesse, API-Zentrierung sowie das Konzept der unveränderbaren Infrastruktur. Dies ermöglicht eine hohe Skalierbarkeit, Ausfallsicherheit und eine effiziente Betriebsführung.
- **Sicherheit, Datenschutz und Compliance** sind integraler Bestandteil der Plattformarchitektur und werden nach dem Prinzip „by Design“ umgesetzt. Einheitliche Sicherheits- und Datenschutzstandards werden zentral definiert und plattformweit umgesetzt. Gleichzeitig können fach- oder institutionsspezifische Anforderungen über Konfigurationen berücksichtigt werden. Durch diesen Ansatz werden Umsetzungsaufwände reduziert und ein hohes, konsistentes Sicherheitsniveau gewährleistet.
- Schließlich wird die **Betriebskomplexität bewusst begrenzt**. Der Plattformbetrieb setzt auf Standardisierung, Automatisierung und den gezielten Einsatz etablierter Komponenten. Eigenentwicklungen erfolgen ausschließlich dort, wo sie für den Betrieb der Plattform zwingend erforderlich sind. Auf individuelle Sonderlösungen wird zugunsten eines stabilen, wartbaren und wirtschaftlichen Gesamtbetriebs weitgehend verzichtet.

In ihrer Gesamtheit stellen diese Grundsätze und Designprinzipien sicher, dass die Plattform als souveräne, offene und zukunftsfähige digitale Basis für Verwaltung und Gesundheitswesen betrieben werden kann.

3.6 Alleinstellungsmerkmale und Mehrwerte

Auf Basis der beschriebenen Architektur und Designprinzipien weist das GovTech-Framework eine Reihe von Alleinstellungsmerkmalen auf, die sie klar von bestehenden Einzelplattformen, projektbezogenen Betriebsmodellen und rein infrastrukturellen Cloud-Angeboten abgrenzt. Diese Merkmale bilden die Grundlage für spezifische Mehrwerte für Verwaltung, Gesundheitswesen und Anbieter digitaler Lösungen.

Ein zentrales Alleinstellungsmerkmal ist die **Multi-Cloud-Abstraktionsschicht**. Sie ermöglicht einen einheitlichen, anbieterunabhängigen Zugriff auf Cloud-Ressourcen unterschiedlicher Herkunft – von öffentlichen IT-Dienstleistern über souveräne europäische Anbieter bis hin zu Hyperscalern. Technische Unterschiede zwischen den Anbietern werden abstrahiert, sodass Ressourcen flexibel genutzt, verschoben oder ausgetauscht werden können, ohne Anwendungen neu entwickeln oder anpassen zu müssen. Dadurch entsteht echte Wechselfähigkeit auf Infrastrukturebene.

Ein weiteres wesentliches Merkmal ist die durchgängige Verankerung von **Confidential Computing** in der Plattformarchitektur. Auf Infrastruktur- und Betriebsebene ist Confidential Computing fester Bestandteil der Gesamtarchitektur. Durch Laufzeitverschlüsselung werden Daten nicht nur bei Speicherung und Übertragung, sondern auch während der Verarbeitung geschützt. Lösungsanbieter sind verpflichtet, ausschließlich Confidential-Computing-fähige Lösungen bereitzustellen und zu betreiben. Dies gewährleistet ein besonders hohes Sicherheits- und Vertrauensniveau und ermöglicht den sicheren Einsatz von Cloud-Technologien auch für hochsensible Daten im öffentlichen Sektor und im Gesundheitswesen.

Die Plattform verfolgt eine **Open-Source-Strategie**. Zentrale Plattformkomponenten und Basisdienste auf Ebene des Plattformkerns setzen bevorzugt auf offene Standards und quelloffene Software, um Transparenz, Auditierbarkeit und technologische Unabhängigkeit sicherzustellen. Sofern im begründeten Ausnahmefall auf Plattformkernebene proprietäre Komponenten eingesetzt werden, wird hierfür ein geeignetes Escrow-Modell (Treuhandmodell zur Hinterlegung von Quellcode) vorgesehen, um langfristige Wartbarkeit, Weiterentwicklungsfähigkeit und digitale Souveränität abzusichern. Proprietäre Lösungen auf Anwendungs- oder Marktplatzebene bleiben hiervon unberührt und folgen den jeweils definierten Integrations- und Zulassungskriterien. Diese Ausgestaltung stärkt Wettbewerb und Innovationsfähigkeit bei gleichzeitiger Wahrung der Souveränitätsanforderungen.

Ein weiteres Merkmal ist der **wettbewerbs- und innovationsorientierte Marktplatzansatz**. Die Plattform ermöglicht die parallele Bereitstellung vergleichbarer Fachanwendungen, Fach- und Querschnittsdienste unterschiedlicher Anbieter. Bedarfsträger können Lösungen frei auswählen und wechseln, während Anbieter im bundesweiten Wettbewerb stehen. Der Marktplatz ist dabei integraler Bestandteil des Betriebsmodells und nicht lediglich ein vorgelagerter Katalog.

Besonders hervorzuheben ist der stark **vereinfachte Beschaffungs- und Bereitstellungsweg**. Alle über den Marktplatz verfügbaren Lösungen sind vorqualifiziert und können von Bedarfsträgern **unmittelbar** über GovTech Deutschland

im Rahmen der **Inhouse-Fähigkeit** bezogen werden. Dadurch entfällt der Umweg über individuelle Ausschreibungen. Digitale Lösungen können so ohne zusätzlichen Vergabeaufwand in kurzer Zeit produktiv eingesetzt werden.

Schließlich stellt die **zentrale Bereitstellung von Basisdiensten und Entwicklungsinstrumenten** ein wesentliches Unterscheidungsmerkmal dar. Dienste wie Identitäts- und Zugriffsmanagement, Logging, Monitoring oder Abrechnung werden plattformweit einheitlich und einmal bereitgestellt und sind verbindlich zu nutzen. Ergänzt wird dies durch ein Angebot an Querschnittsdiensten, die von verschiedenen Anbietern bereitgestellt und von Entwicklern einfach nachgenutzt werden können. Dies reduziert Entwicklungsaufwände, verhindert Doppelentwicklungen und beschleunigt Innovationszyklen.

Aus diesen Alleinstellungsmerkmalen ergeben sich **konkrete Mehrwerte** für alle beteiligten Akteure.

- Technisch schafft die Plattform ein hohes Maß an **Souveränität, Sicherheit und echte Wechselfähigkeit**. Offene Schnittstellen, Multi-Cloud-Fähigkeit und Laufzeitverschlüsselung ermöglichen eine zukunftssichere Nutzung von Cloud-Technologien ohne strukturelle Abhängigkeiten.
- Organisatorisch führt die Plattform zu einer **massiven Beschleunigung von Beschaffungs- und Umsetzungsprozessen**. Standardisierte Betriebsmodelle, vorgeprüfte Sicherheits- und Datenschutzkonzepte sowie der Marktplatzansatz reduzieren Koordinations- und Verwaltungsaufwände erheblich und entlasten insbesondere Länder und Kommunen.
- Ökonomisch steigert die Plattform die **Wirtschaftlichkeit digitaler Lösungen**. Durch die gemeinsame Nutzung von Infrastruktur und Basisdiensten, die Vermeidung von Doppelentwicklungen und bessere Verhandlungspositionen gegenüber Anbietern sinken sowohl Einzel- als auch Gesamtkosten. Gleichzeitig werden Skaleneffekte und nachhaltige Investitionen ermöglicht.
- Darüber hinaus fördert die Plattform **Innovation und Wettbewerb**. Anbieter können neue Lösungen schneller entwickeln, bereitstellen und skalieren, während Bedarfsträger frühzeitig von innovativen Angeboten profitieren. Der offene Marktplatz schafft Transparenz und Vergleichbarkeit und stärkt die Angebotsvielfalt.
- Nicht zuletzt erfüllt die Plattform die hohen **Anforderungen des öffentlichen Sektors und des Gesundheitswesens** in Bezug auf Datenschutz, IT-Sicherheit,

Compliance und föderale Anschlussfähigkeit. Sie verbindet gemeinsame technische Standards mit institutioneller Autonomie und schafft damit eine tragfähige Grundlage für eine nachhaltige digitale Transformation.

4 Konzeption und Operationalisierung der Plattformschichten

Im Folgenden werden die Plattformschichten konzeptionell erläutert und ihre technischen, organisatorischen sowie wirtschaftlichen Aspekte dargestellt.

4.1 Infrastruktur-Schicht: GovTech Infrastructure

Das Fundament der Architektur bildet die virtualisierte Infrastruktur. Sie stellt die Multi-Cloud-Fähigkeit sicher und ermöglicht den Betrieb in unterschiedlichen Cloud-Umgebungen, darunter die von (souveränen) europäischen Anbietern, Hyperscalern, öffentlich-rechtlichen Anbietern sowie spezialisierten Cloud-Angeboten, beispielsweise Air-Gapped-Angeboten bei Hochsicherheitsanforderungen. Diese Offenheit schafft die Grundlage dafür, Anwendungen flexibel auf der Plattform zu betreiben. Die Infrastrukturschicht abstrahiert technische Ressourcen wie Rechenleistung, Speicher und Netzwerk von verschiedenen Anbietern und stellt diese bereit. Auch DevOps-Services, die der Entwicklung und dem Betrieb der Plattform dienen, sind Teil dieser Architekturschicht.

Beispielhafte, herstellerneutrale Technologien sind unter anderem:

- **Compute:** Virtual Machines (VMs), Kubernetes, Bare Metal
- **Storage:** S3-kompatibler Objektspeicher, Block/File Storage
- **Netzwerk:** Software Defined Networking (SDN), Virtual Private Networks (VPN), Gateway-Funktionen

Die Übergabe dieser Ressourcen an die höheren Architekturschichten erfolgt über standardisierte APIs, z. B. OpenStack- oder Kubernetes-kompatible Schnittstellen. Diese gewährleisten, dass Ressourcen plattformübergreifend provisioniert, skaliert und überwacht werden können.

Im Folgenden werden Leistungen und Services beschrieben, die Bestandteil der Umsetzung der Infrastruktur-Schicht sind.

4.1.1 DevOps Services (DO)

DevOps-Services umfassen interne Dienste, die für den Aufbau, Betrieb, das Testing und die Auslieferung von Plattformkomponenten sowie für das Anforderungs- und Qualitätsmanagement eingesetzt werden. Sie unterstützen die Entwicklungs- und Betriebsteams bei der kontinuierlichen Verbesserung der Plattform.

Zu den DevOps-Services der gehören unter anderem:

- **Dev/Ops Management** – automatisiert das Deployment und Lifecycle-Management von Plattform-Komponenten über deklarative GitOps-Ansätze.
- **Operative Test-Plattform für 3rd Party** – stellt eine isolierte Umgebung für externe Anbieter bereit, um ihre Fachanwendungen gegen die Plattform zu testen.
- **Operative Staging Plattform** – ermöglicht produktionsnahe Tests zur finalen Validierung neuer Releases vor der Liveschaltung.
- **Test- und Dev Plattform** – bietet interne Entwicklungs- und Testressourcen für Plattformteams.
- **Testautomatisierung** – automatisiert Testabläufe zur kontinuierlichen Qualitätssicherung.
- **Testmanagement** – verwaltet Testfälle, Testpläne und Ergebnisse im Rahmen der Qualitätssicherung.
- **Anforderungsmanagement** – erfasst, priorisiert und dokumentiert technische und fachliche Anforderungen.
- **Patch- und Schwachstellenmonitoring** – überwacht eingesetzte Software auf bekannte Schwachstellen und notwendige Sicherheitsupdates.
- **Dokumentation** – stellt technische und organisatorische Informationen zentral über ein Wiki bereit.

4.1.2 Virtuelle Infrastruktur Services (VI)

Diese Dienste bilden die technische Basis der Plattform. Hier werden Rechenressourcen, Speicher und Netzwerk als virtuelle Ressourcen bereitgestellt, auf

denen höhere Dienste aufsetzen. Die Plattform nutzt dabei, wo möglich, bestehende Cloud-Infrastrukturen, bleibt jedoch durch den Abstraktions-Layer unabhängig vom konkreten Infrastrukturanbieter.

Der primäre Fokus liegt auf Public-Cloud-Anbietern (europäische, souveräne Cloud-Anbieter, Bare-Metall-Anbieter und Hyperscaler). Hervorzuheben ist dabei, dass die genutzten Rechenzentren und Regionen innerhalb des Europäischen Wirtschaftsraums betrieben werden. Bei besonderen Anforderungen können auch Private-Cloud-Anbieter sowie Cloud-Angebote öffentlicher IT-Dienstleister oder anderer spezialisierter Anbieter, z.B. von Air-Gapped-Lösungen, zum Einsatz kommen.

Die Auswahl der Cloud-Delivery-Modelle sowie die Zuordnung zu entsprechenden Anbieter-Clustern erfolgt auf Basis der fachlichen, technischen und regulatorischen Anforderungen der jeweiligen Use Cases und der beteiligten Organisationen, insbesondere unter Berücksichtigung von Sicherheits- und Souveränitätsanforderungen. Die konkrete Auswahl der Cloud-Anbieter wird im Rahmen des Plattformbetriebs vorgenommen; organisationsspezifische und regulatorische Anforderungen fließen dabei in die Entscheidungs- und Betriebsprozesse ein (siehe hierzu auch [Kapitel 6](#)).

Zu den virtuellen Infrastruktur Services, die die Plattform bereitstellt, gehören:

- **Virtual Machines** – ermöglicht die Bereitstellung von VMs und Compute-Instanzen zur Laufzeitumgebung von Services.
- **Persistent Storage** – speichert dauerhaft Daten und Backups in Form von Blockspeicher oder Objekten.
- **Database Storage** – stellt strukturierte Datenbanklösungen für persistente Fachanwendungsdaten bereit.
- **Container** – stellt virtuelle Maschinen oder Containerumgebungen bereit, verwaltet deren Nutzung und sorgt für Abrechnungsfähigkeit.
- **LLM-Resource** – stellt Ressourcen (z. B. GPU/TPU) für den Betrieb großer Sprachmodelle bereit.

Die GovTech Infrastructure-Schicht ist durch organisatorische, technische und wirtschaftliche Rahmenbedingungen und Merkmale determiniert.

4.1.3 Organisatorische Eckpunkte von GovTech Infrastructure

Cloud-Service-Provider müssen festgelegte Zulassungskriterien erfüllen, die vom Plattformbetreiber vorgegeben werden. Maßgeblich hierzu sind zum Beispiel Leistungsangebot, Zertifizierungen, Firmensitz und Besitzverhältnisse. Die Auswahl der eingesetzten Cloud-Service-Provider erfolgt zentral durch GovTech Deutschland auf Basis der fachlichen, technischen und regulatorischen Anforderungen der jeweiligen Use Cases und Organisationen, insbesondere unter Berücksichtigung von Sicherheits- und Souveränitätsanforderungen. Nutzende können entsprechende Anforderungen einbringen.

Auf dieser Grundlage bündelt GovTech Deutschland Rahmenverträge mit den qualifizierten Cloud-Service-Providern und verhandelt einheitliche Konditionen, von denen alle Nutzenden der Plattform profitieren. Im Rahmen des Plattformbetriebs übernimmt GovTech Deutschland zudem die operative Abwicklung von Abrechnung, Kostenaufbereitung und Reporting der Cloud-Ressourcen.

4.1.4 Technische Eckpunkte von GovTech Infrastructure

Über den GovTech Infrastructure-Layer werden vor allem Infrastrukturangebote im Sinne von IaaS (Infrastructure as a Service) bezogen und genutzt. In der Regel werden dabei virtuelle Maschinen der Cloud-Anbieter für den Betrieb der Plattform genutzt. Für spezielle Anforderungen, etwa im Bereich Confidential Computing (siehe hierzu auch [Kapitel 4.2](#)), oder aus wirtschaftlichen Gründen kann jedoch auch auf Bare-Metal-Anbieter zurückgegriffen werden.

Höherwertige Services (z. B. PaaS) der Cloud-Anbieter werden nach Möglichkeit vermieden, um Abhängigkeiten und Vendor Lock-ins zu reduzieren. Stattdessen werden notwendige Dienste vom Plattformbetreiber selbst entwickelt oder von unabhängigen Dritten bezogen und über den GovTech Core Layer bereitgestellt und betrieben.

Auch bei Storage- und Networking-Komponenten wird bewusst auf die gemanagten Angebote der Cloudanbieter verzichtet. Stattdessen kommen eigene Lösungen zum Einsatz, beispielsweise ein S3-kompatibler, auf Disks basierender (Block-)Storage-Service sowie der Einsatz von Open-Source-Netzwerkprodukten.

Cloud-Service-Provider müssen die vom Plattformbetreiber definierten, technischen Zertifizierungen sowie die technischen und organisatorischen Maßnahmen (TOMs)

nachweisen. Maßgeblich sind dabei insbesondere anerkannte Standards und Vorgaben wie BSI C5, ISO/IEC 27001 und der BSI-Mindeststandard. Abhängig vom jeweiligen Einsatzszenario können darüber hinaus weitere Anforderungen, etwa aus dem IT-Grundschutz oder eine VS-NfD-Zertifizierung, erforderlich sein.

4.1.5 Wirtschaftliche Eckpunkte von GovTech Infrastructure

GovTech Deutschland schließt mit den gebündelten Cloud-Service-Providern Rahmenverträge ohne Abnahmeverpflichtung ab. Diese beinhalten vorab vereinbarte pauschale Rabatte und bilden damit die wirtschaftliche Grundlage für das Angebot von Anwendungen auf der Plattform zu attraktiven Konditionen. Initial steht ein festgelegtes Set an Cloud-Service-Providern zur Verfügung, das bedarfsgerecht um weitere Anbieter ergänzt werden kann.

Die Abrechnung der Cloud-Leistungen gegenüber den Endnutzern erfolgt durch den Plattformbetreiber auf nutzungsbasierter Grundlage im Rahmen einer Gesamtrechnung. Die Cloud-Kosten sind dabei bereits im Preis der jeweiligen, über den Marktplatz vertriebenen Anwendung berücksichtigt und werden den Endnutzern nicht separat in Rechnung gestellt.

4.2 Plattformkern: GovTech Core

GovTech Core stellt den technologischen Kern der Plattform dar. Die einzelnen Komponenten des GovTech Core Layers sind wie folgt konzipiert:

4.2.1 Secure Multi-Cloud Abstraction Layer (CAL)

Der Secure Multi-Cloud Abstraction Layer bildet die Schnittstelle zu den Infrastrukturdiensten und stellt als zentrale Abstraktionsschicht cloudanbieterübergreifende Funktionen bereit, die Betrieb und Verwaltung der Plattform automatisieren und vereinheitlichen. Ziel ist es, die Plattform unabhängig von einzelnen Infrastruktur-Anbietern zu gestalten und Cloud-Funktionen standardisiert bereitzustellen.

Durch die Abstraktion der Unterschiede zwischen den Anbietern ermöglicht die Schicht einen konsistenten und sicheren Zugriff auf Ressourcen in verschiedenen Cloud-Umgebungen. Sie ist entscheidend, um echte Wechselfähigkeit zu gewährleisten und

eine konsequente Multi-Cloud-Strategie umzusetzen. Der Übergang zu den Basisdiensten erfolgt über interne, serviceorientierte Schnittstellen (z. B. REST), ergänzt durch ein zentrales Identity Management. Dadurch wird eine sichere, einheitliche und standardisierte Nutzung der abstrahierten Ressourcen sichergestellt.

Zum Cloud Abstraction Layer gehören folgende Dienste:

- **Load Balancing** – verteilt Anfragen auf mehrere Instanzen eines Services zur Lastverteilung und Hochverfügbarkeit.
- **Nameservice** – verwaltet interne Namensauflösung und Verwendung von Zertifikaten.
- **Container-Orchestrierung** – automatisiert Deployment, Skalierung und Verwaltung von containerisierten Anwendungen.
- **Infrastructure Provisioning** – ermöglicht die automatisierte Bereitstellung von Infrastrukturkomponenten über deklarative Vorlagen.
- **Policy Service** – setzt Sicherheits- und Betriebsrichtlinien für Infrastrukturressourcen und Workloads durch.
- **Admin Portal** – Grafische Oberfläche zur zentralen Steuerung, Überwachung und Verwaltung mehrerer Cloud-Umgebungen.
- **Connector** – ermöglicht die sichere Anbindung und Kommunikation zwischen mehreren Cloud-Infrastrukturen und Kunden.
- **Netzwerk-Isolation** – isoliert Netzwerksegmente durch cloud-native Sicherheits-mechanismen wie Firewalls und Security Groups.
- **Backup** – ermöglicht regelmäßige, automatisierte Sicherungen von Plattformdaten zur Wiederherstellung im Fehlerfall.
- **Laufzeitverschlüsselung (Confidential Computing)** – schützt Daten und Verarbeitungscode auch während der Ausführung durch hardwarebasierte, vertrauenswürdige Ausführungsumgebungen (Trusted Execution Environments), sodass ein Zugriff selbst durch Cloud-Anbieter oder Plattformbetreiber ausgeschlossen ist.
- **Federated Cluster Management** – ermöglicht die zentrale Verwaltung, Orchestrierung und Überwachung mehrerer logisch oder physisch getrennter

Kubernetes-Cluster über Cloud- und Infrastrukturgrenzen hinweg, einschließlich einheitlicher Richtlinien, Konfigurationen und Lifecycle-Management.

4.2.2 Basisdienste (BD)

Die Basisdienste stellen zentrale Funktionen bereit, die vom GovTech-Framework entwickelt und aktiv betrieben werden und somit **„vor die Klammer gezogen“** sind. Ziel ist es, Mehrfachimplementierungen zu vermeiden und Wiederverwendung von Beginn an zu fördern. Aus diesem Grund sind bestimmte Basisdienste, wie das IAM, auch als verbindlicher Rahmen für alle Plattformnutzer zu verstehen.

Sie folgen konsequent offenen Standards und unterstützen die Interoperabilität sowohl zwischen Anwendungen als auch über föderale und sektorale Grenzen hinweg. Anbieter und Nutzende profitieren von stabilen Schnittstellen, gesicherter Kompatibilität und klar definierten Betriebsverantwortlichkeiten. Die Architektur der Basisdienste ist gezielt auf Wechselfähigkeit und die Vermeidung von Vendor Lock-ins ausgelegt.

Die Basisdienste werden bewusst grundsätzlich auf Grundlage etablierter Open-Source-Frameworks entwickelt und betrieben. Um Abhängigkeiten von einzelnen Infrastrukturprovidern zu reduzieren und eine einheitliche, multi-cloudfähige Betriebslogik sicherzustellen, wird der Einsatz cloudanbieterspezifischer Managed Services vermieden. Sofern im begründeten Ausnahmefall proprietäre Komponenten auf Ebene der Basisdienste eingesetzt werden, wird hierfür ein geeignetes Escrow-Modell vorgesehen, um langfristige Wartbarkeit, Weiterentwicklungsfähigkeit und digitale Souveränität abzusichern.

Insbesondere werden die Basisdienste von Herstellern von Fachverfahren und Softwarelösungen genutzt, um ihre Angebote auf der Plattform sicher und performant betreiben zu können und zentrale, anwendungsübergreifende Funktionen zu integrieren. Die Entwicklung und Bereitstellung durch den Plattformbetreiber stellen sicher, dass diese Funktionen unabhängig von spezifischen Cloud-Anbietern verfügbar sind und plattformweit konsistent genutzt werden können.

Die Basisdienste interagieren über klar definierte Schnittstellen mit den Querschnittsdiensten, Fachdiensten und Fachanwendungen. Diese Übergänge werden durch standardisierte API-Gateways, Event-Busse und Service-Mesh-Komponenten realisiert. Die Basisdienste des GovTech-Frameworks umfassen unter anderem zentrale Funktionen wie:

- **Schnittstellenmanagement** – steuern, sichern und überwachen die Nutzung von APIs zwischen Frontend- und Backend-Komponenten.
- **Eventgetriebene Kommunikation / Event Bus** – verwaltet und listet alle verfügbaren Dienste zum Auffinden durch Entwickler.
- **Datenbank-Service** – stellt Datenbankdienste bereit, einschließlich Provisionierung, Betrieb, Backup, Wiederherstellung und Zugriffskontrolle, beispielsweise auf Basis von PostgreSQL.
- **Monitoring** – erfasst Systemmetriken und stellt Visualisierungen zur Überwachung der Plattform bereit.
- **Logging** – erfasst Protokolldaten in einheitlichen Formaten, um Betrieb, Fehlersuche, Sicherheit und Compliance nachvollziehbar zu unterstützen.
- **Service Registry** – ermöglicht Auffindbarkeit, Versionierung und kontrollierte Nutzung innerhalb von Diensten und Anwendungen der Plattform.
- **3rd Party Application provisioning** – ermöglicht das standardisierte Onboarding, die Bereitstellung und den Lebenszyklusbetrieb von Anwendungen externer Anbieter innerhalb der Plattformumgebung.
- **Billingsservice** – erfasst und analysiert Ressourcennutzung zur internen Verrechnung und Kostenkontrolle.
- **Authentifizierung und Autorisierung / Identity and Access Management (IAM)** – verwaltet Identitäten, Rollen und Zugriffsrechte für fachliches, technisches, administratives Personal und Endanwender.
- **Marktplatzservice (Provider)** – erlaubt Fachanwendungsanbietern, ihre Services auf der Plattform zu veröffentlichen und zu verwalten.
- **Marktplatzservice (Nutzer)** – bietet Nutzern einen Zugangspunkt zur Auswahl und Nutzung verfügbarer Dienste.
- **Service Access Management** – steuert und überwacht den Zugriff auf Plattformdienste und Anwendungen über rollenbasierte Berechtigungen, Policies und Freigabemechanismen.
- **Wallet ID / EUID Connector** – Verwaltung und Nutzung einer digitalen Identitäts-Wallet gemäß der EU-Verordnung EUDI.

- **Zertifikatsmanagement / PKI** – stellt und verwaltet digitale Zertifikate zur Absicherung von Diensten.
- **Schlüsselverwaltung / Secrets Vault** – verwaltet und schützt vertrauliche Zugangsinformationen und Secrets zentral.
- **Security Event Monitoring** – erkennt sicherheitsrelevante Ereignisse durch kontinuierliche Analyse von Logdaten.
- **Penetration Testing** – ermöglicht die strukturierte Durchführung von Sicherheitstests zur Überprüfung der Widerstandsfähigkeit von Anwendungen.

Vertiefung zum IAM-Service

Der Basisdienst „Identitäts- und Zugriffsmanagement“ (IAM) stellt die zentrale Infrastruktur zur Verwaltung von Identitäten und Berechtigungen auf der Plattform bereit. Er ermöglicht eine strikt mandantengetrennte Abbildung von Nutzerkonten und Rollen, sodass Organisationen und Fachanwendungen eindeutig zuordenbare, sichere und voneinander getrennte Identitätsräume nutzen können. Anwendungen werden grundsätzlich isoliert betrieben. Für Szenarien, in denen eine organisationsübergreifende Nutzung notwendig ist, unterstützt der Basisdienst eine kontrollierte und standardkonforme Föderation gemeinsam genutzter Anwendungen.

Der IAM-Basisdienst folgt etablierten offenen Standards und ermöglicht die Anbindung heterogener organisationsseitiger IAM-Infrastrukturen über Protokolle wie OpenID Connect. Dadurch können bestehende Identitätsquellen integriert und konsistent auf der Plattform abgebildet werden. Für Systeme, die über kein eigenes IAM verfügen, stellt der Basisdienst zusätzlich einen dedizierten AD-Connector bereit, über den Active-Directory-basierte Identitätsbestände sicher und interoperabel eingebunden werden können.

Durch diese einheitliche und interoperable Identitäts- und Berechtigungsverwaltung bildet der IAM-Basisdienst einen zentralen Baustein der Plattformarchitektur und stellt sicher, dass Fachanwendungen auf konsistente, sichere und skalierbare Authentifizierungs- und Autorisierungsmechanismen zugreifen können.

4.2.3 Organisatorische Eckpunkte von GovTech Core

Der GovTech Core Layer, bestehend aus Basisdiensten und Cloud Abstraction Layer, wird vom Plattformbetreiber betrieben und kontinuierlich weiterentwickelt. Die übergreifende fachliche, technische und organisatorische Gesamtverantwortung liegt bei ihm.

Sofern im begründeten Ausnahmefall proprietäre Komponenten auf Ebene des GovTech Core statt Open-Source-Frameworks eingesetzt werden, wird hierfür ein geeignetes Escrow-Modell vertraglich vorgesehen. Dieses stellt sicher, dass dem Plattformbetreiber im Bedarfsfall der Zugriff auf Quellcode, Dokumentation und notwendige Betriebsartefakte möglich ist und die langfristige Wartbarkeit, Weiterentwicklungsfähigkeit sowie digitale Souveränität der Plattform gewahrt bleiben.

Anbieter von Fachverfahren und -diensten nutzen den Core Layer und insbesondere die Basisdienste als verbindlichen Rahmen für Entwicklung und Betrieb ihrer Lösungen auf der Plattform. Erforderliche Anpassungen an bestehende Systeme erfolgen im Einklang mit den definierten Plattformstandards. Abweichungen hiervon sind nur in begründeten Ausnahmefällen möglich und bedürfen einer vorherigen Prüfung sowie ausdrücklichen Freigabe durch den Plattformbetreiber.

Der Betrieb des GovTech Core wird durch ein zentrales IT-Service-Management des Plattformbetreibers unterstützt, das einheitliche Prozesse für Betrieb, Support und Weiterentwicklung sicherstellt.

4.2.4 Technische Eckpunkte von GovTech Core

Basisdienste und Cloud Abstraction Layer basieren überwiegend auf Open-Source-Komponenten, um Transparenz, Sicherheit und langfristige Unabhängigkeit von proprietären Herstellern zu gewährleisten. Dies reduziert Abhängigkeiten von Anbietern proprietärer Lösungen, verringert Lizenzkosten, erleichtert Audits und unterstützt die aktive Weiterentwicklung durch die Community.

Der Cloud Abstraction Layer nutzt Kubernetes-Container-Technologien, die durch ein zentrales Container-Management orchestriert werden. Damit wird eine einheitliche, skalierbare und hochverfügbare Betriebsumgebung geschaffen, die sowohl die Automatisierung als auch die einfache Portierbarkeit von Anwendungen über verschiedene Cloud-Umgebungen hinweg ermöglicht.

Aufgrund der besonders schützenswerten Daten im öffentlichen Sektor und Gesundheitswesen setzt das GovTech-Framework auf Confidential Computing. Dabei werden hardwarebasierte, vertrauenswürdige Ausführungsumgebungen (Trusted Execution Environments, TEE) genutzt.

Vertiefung zu Confidential Computing

Confidential Computing (auch „Laufzeitverschlüsselung“) erweitert den klassischen Datenschutz („at rest“ – verschlüsselt gespeichert, „in transit“ – verschlüsselt übertragen) um den Schutz „in use“: Daten bleiben auch während der Verarbeitung vor unbefugtem Zugriff geschützt – selbst gegenüber Cloud-Anbietern oder Systemadministratoren.

Technisch wird dies durch Trusted Execution Environments (TEEs) realisiert: hardwaregestützte, isolierte Ausführungsumgebungen im Prozessor, die Code und Daten abschotten, unbefugten Zugriff verhindern und über kryptografische Remote Attestation die Integrität der ausgeführten Software belegen.

Auf der GovTech Plattform erfolgt die Umsetzung mit **Confidential VMs (cVMs)** sowie optional auf **Bare-Metal-Instanzen** mit eigenem Confidential-Computing-Stack. Dabei werden folgende Anforderungen umgesetzt:

Anforderungen bei Nutzung der Angebote der Cloud-Anbieter (cVMs):

- Volle Kontrolle durch die Nutzerseite über die Gast-VM (z. B. Root-Zugriff).
- Isolationsschutz von Speicher, Registern und Paging-Dateien gegenüber dem Host und Dritten.
- Remote Attestation der cVM mit Einsicht in Boot- und Firmware-Messwerte.
- Firmware-Transparenz: Einsicht in verwendete Firmware durch eine der folgenden Varianten:
 - Open-Source-Komponenten
 - Offene Dokumentation
 - Einsicht unter NDA auf Aufforderung
 - Prüfung durch eine vertrauenswürdige dritte Partei (z. B. BSI)

Anforderungen bei Umsetzung mit Bare-Metal-Instanzen:

Zusätzlich müssen die Anbieter den Betrieb auf Bare-Metal-Instanzen mit eigener Confidential-Computing-Laufzeitumgebung und mit Hardware-Technologien Intel TDX (ab 4. Generation Xeon Scalable) oder AMD SEV-SNP (ab 3. Generation Epyc 7003 Series) oder gleichwertig ermöglichen. Hierfür gelten folgende Anforderungen:

- Volle Kontrolle über Hardware und Software-Stack (inkl. Hypervisor, Firmware, Betriebssystem)
- Unterstützung zur Integration externer Confidential-Computing-Technologien
- Remote Attestation über die gesamte Stack-Kette (Firmware bis Applikation)
- Transparenzanforderungen analog zu cVMs

4.2.5 Wirtschaftliche Eckpunkte von GovTech Core

Die Basisdienste und der Cloud Abstraction Layer werden vom Plattformbetreiber bereitgestellt und betrieben. Die Entwicklungs- und Betriebskosten trägt dabei zunächst der Betreiber. Kosten für Betrieb und Weiterentwicklung werden anteilig an die Endnutzer in vorab definierten Kostenrahmen verrechnet.

GovTech Infrastructure und Core bilden somit gemeinsam die technische Grundlage für nutzerzentrierte Angebote, die im Rahmen des folgenden Unterkapitels beschrieben werden.

4.3 Anwendungs- und Marktplatzschicht: GovTech Store

Der GovTech Store bildet die oberste Schicht der Plattform und bündelt konkrete digitale Lösungen für Verwaltung und Gesundheitswesen. Dazu zählen vollständige Fachanwendungen, wiederverwendbare Fachdienste sowie Querschnittsdienste. Herzstück dieser Schicht ist der Store, der den Zugang zu bestehenden und neuen Anwendungen ermöglicht und kontinuierlich weiterentwickelt wird. Dabei spielt es keine Rolle, ob die Lösungen nativ auf der Plattform entwickelt oder aus externen

Umgebungen portiert wurden. Der Marktplatz bietet Anbietern und Nutzern einen zentralen, leicht zugänglichen Vertriebs- und Bezugsweg für digitale Lösungen. Alle Lösungen im GovTech Store folgen standardisierten API-Konzepten, Serviceverträgen und Zugriffsmechanismen.

Der GovTech Store Layer besteht dabei aus Querschnittsdiensten, Fachdiensten und Fachanwendungen.

4.3.1 Querschnittsdienste (QD)

Querschnittsdienste sind generische, fachübergreifend nutzbare Funktionsbausteine, die in verschiedenen Fachanwendungen wiederverwendet werden können. Sie stellen Mehrwertfunktionen insbesondere für Entwicklung, Datenverarbeitung und Interoperabilität bereit und dienen als Enabling-Dienste für die Umsetzung digitaler Lösungen auf der Plattform.

Institutionen der öffentlichen Verwaltung und des Gesundheitswesens erhalten über die Plattform einen direkten, standardisierten Zugang zu diesen Diensten. Auf dieser Grundlage können sie beispielsweise eigene Anwendungen entwickeln und konfigurieren oder mit eigenen Daten KI-Modelle trainieren, ohne hierfür separate Infrastrukturen oder individuelle Betriebsmodelle aufbauen zu müssen.

Die Plattform stellt Querschnittsdienste in unterschiedlichen Ausprägungen bereit. Dazu zählen unter anderem KI-Plattformen, High-Performance-Computing, Formulardienste, Dokumentenerzeugung oder Low-Code-Engines. Das parallele Angebot vergleichbarer Lösungen unterschiedlicher Anbieter ist ausdrücklich vorgesehen, um Innovation und Wettbewerb zu fördern, Wechselmöglichkeiten zu erhalten und unterschiedliche fachliche Schwerpunkte und Stärken der Anbieter zu berücksichtigen. Zu den Querschnittsdiensten gehören beispielhaft¹:

- **KI-Workbenches/KI-Plattform** – stellen Infrastruktur und Werkzeuge für das Training, Hosting und den Betrieb von KI-Modellen bereit (weitere Details siehe unten).
- **Low Code Service** – ermöglicht die Erstellung von Anwendungen über visuelle Oberflächen mit minimalem Programmieraufwand (weitere Details siehe unten)

¹ Die Aufzählung der Querschnittsdienste ist nicht abschließend. Einzelne Dienste befinden sich noch in Planung oder Umsetzung und werden schrittweise ergänzt.

- **Fit-Connect und OSCI** – standardisierte Konnektor zur Anbindung föderaler IT-Systeme und Register, der den sicheren, strukturierten und nachvollziehbaren Datenaustausch zwischen Verwaltungssystemen unterstützt.
- **(weitere) Konnektor-Services** – Technische Dienste, die als Schnittstelle zwischen unterschiedlichen IT-Systemen fungieren, z.B. zwischen einer Fachanwendung, einem Formularesystem, einem Register oder einer externen Komponente (z.B. IAM Connector für OICD).
- **Dokumentenmanagementsystem (DMS)** – stellt Funktionen zur strukturierten Ablage, Versionierung, Verwaltung und revisionssicheren Speicherung von Dokumenten bereit und kann von Fachanwendungen als integrierter Dienst genutzt werden.
- **Datenaustauschplattform** – ermöglicht einen sicheren, medienbruchfreien Austausch von Daten zwischen berechtigten Organisationen (weitere Details siehe unten).
- **Messenger Adressdienste** – ermöglicht die Adressierung von Einrichtungen über das Verzeichnisdienstsystem
- **Register-as-a-Service (RaaS)** – ermöglicht cloud-basierten dezentralen Registerzugriff (abgeschlossenes Projekt mit der FITKO im Rahmen der Registermodernisierung).
- **GIS-Services** – ermöglichen Zugriff auf Daten aus verschiedenen grafischen Informationssystemen.
- **OZG-Portale** – stellen zentrale Integrations- und Bereitstellungskomponente für OZG-Leistungen dar und unterstützen die Bündelung, Nachnutzung und Skalierung digitaler Verwaltungsleistungen (weitere Details siehe unten).
- **Vorgangsraumlösungen** – bieten zentrale Arbeits- und Prozessumgebungen zur strukturierten Bearbeitung von Verwaltungsvorgängen, in der Informationen, Dokumente, Beteiligte und Prozessschritte zusammengeführt werden.

Ausgewählte Vertiefungen von Querschnittsdiensten

1. KI-Workbenches / KI-Plattform

Die KI-Workbenches stellen zentrale Infrastruktur und Werkzeuge für das Training, Hosting und den Betrieb von KI-Modellen bereit. Sie bieten sichere, hochverfügbare Umgebungen, die auf die Anforderungen der öffentlichen Verwaltung und des Gesundheitswesens zugeschnitten sind. Unterstützt werden unterschiedliche Anwendungsfälle, darunter RAG-gestützte Chatbots, automatisierte Dokumentenverarbeitung, Entscheidungsunterstützung, Multiagenten-Systeme sowie Sprach- und Bilderkennung.

Die Bereitstellung erfolgt modular über vorkonfigurierte Templates und standardisierte Schnittstellen. Eigene Fachmodelle und Drittkomponenten können integriert werden. Durch die Nutzung der KI-Workbenches als Querschnittsdienst entfällt für Fachanwendungen und Anbieter der Aufbau eigener, isolierter KI-Infrastrukturen. Stattdessen steht ein geprüfter, vertrauenswürdiger und plattformkonformer Service zur Verfügung.

2. Low-Code-Service

Der Low-Code-Service stellt eine oder mehrere Entwicklungsumgebungen bereit, in denen Anwendungen vorwiegend über visuelle Modellierung und vorkonfigurierte Bausteine erstellt werden. Dadurch wird der Programmieraufwand deutlich reduziert, sodass auch Nutzende ohne tiefgehende Softwareentwicklungskenntnisse, etwa aus Fachbereichen, in die Lage versetzt werden, eigenständig digitale Prozesse und Anwendungen umzusetzen. Das Ziel besteht darin, Fachbereichen die Möglichkeit zu geben, flexibel und zeitnah auf fachliche Anforderungen zu reagieren, ohne auf langwierige klassische IT-Projekte angewiesen zu sein.

Der Low-Code-Service unterstützt kurze Entwicklungszyklen, fördert die Standardisierung von Prozessen auf Basis etablierter Modellierungsstandards wie BPMN oder DMN und ermöglicht die Integration externer Systeme über standardisierte Schnittstellen. Wiederverwendbare Oberflächenkomponenten sowie die Einbindung von KI-Funktionen, etwa zur automatisierten Datenerfassung oder Entscheidungsunterstützung, ergänzen das Angebot. Die Entwicklungs- und Laufzeitumgebungen sind geprüft, sicher und vollständig in

die Plattformarchitektur integriert und eignen sich sowohl für einfache Workflowlösungen als auch für komplexere Geschäftsprozesse.

3. Subplattformen und OZG-Portale

Subplattformen und OZG-Portale sind Lösungen, die selbst als Plattformen ausgelegt sind und mehrere Dienste oder Fachanwendungen bündeln. Sie bilden spezialisierte Ökosysteme innerhalb des Plattformangebots und ermöglichen es, komplexe fachliche Angebote strukturiert bereitzustellen, ohne die Vorteile der gemeinsamen Plattformbasis aufzugeben.

Die Integration solcher Subplattformen erweitert das Angebotsportfolio, stellt einen standardisierten Betrieb sicher und ermöglicht eine nahtlose Interoperabilität mit bestehenden Fachverfahren. Zentrale Basisdienste wie Identitäts- und Zugriffsmanagement, Logging, Monitoring, Datenschutz und Compliance werden plattformweit genutzt. Beispiele hierfür sind der OZG-Hub, der (VOIS-)Vorgangsraum, Serviceportale der Länder oder spezialisierte Fachportale im Gesundheitswesen. Für Betreiber reduziert sich der Infrastruktur- und Betriebsaufwand, während Nutzende von einer einheitlichen Nutzerführung, Single-Sign-On und konsistenten Datenflüssen profitieren.

4. Datenaustauschplattform

Die Datenaustauschplattform stellt eine standardisierte, sichere und interoperable Infrastruktur für den organisationsübergreifenden Austausch strukturierter Daten bereit. Sie bildet das technische Fundament für digitale Fachprozesse, bei denen Informationen zwischen Behörden, Kliniken, Fachanwendungen oder weiteren öffentlichen Einrichtungen zuverlässig übertragen werden müssen. Ziel ist es, prozesskritische Daten medienbruchfrei bereitzustellen und damit eine durchgängige Digitalisierung staatlicher und öffentlich-rechtlicher Leistungen zu ermöglichen.

Der Datenaustauschdienst ist vollständig in die Sicherheitsarchitektur des GovTech-Frameworks eingebettet und auf die performante Verarbeitung auch großer Datenmengen ausgelegt. Er bildet damit einen zentralen Baustein für eine vernetzte, interoperable Verwaltungslandschaft.

4.3.2 Fachdienste (FD)

Fachdienste sind 3rd-Party-Dienste, die generische oder spezifische Anforderungen des öffentlichen Sektors oder des Gesundheitswesens unterstützen. Sie stellen zentrale Funktionen bereit, die von Fachanwendungen genutzt werden können, und bilden damit eine wesentliche Grundlage für die Beschleunigung und Unterstützung von Abläufen und Prozessen innerhalb von Anwendungen. Fachdienste verfügen über keine eigene grafische Nutzeroberfläche, sondern werden über klar definierte technische Schnittstellen in Anwendungen integriert.

Beispiele für Fachdienste sind u.a.:

- **OCR-Dienste** – ermöglicht die automatisierte Texterkennung und -extraktion aus gescannten Dokumenten und Bildern zur Weiterverarbeitung in Fachanwendungen.
- **Zertifizierungsdienste** – unterstützen die Prüfung, Ausstellung und Verwaltung fachlicher oder technischer Zertifikate und Nachweise gemäß definierter Standards.
- **Stempel- und Signaturdienst** – Dienste, mit denen Anwendungen elektronische Dokumente signieren oder behördlich siegeln können. Die Dienste unterstützen relevante Standards, übernehmen die sichere Schlüsselverwaltung und bieten einheitliche, auditierbare Verfahren.

4.3.3 Fachanwendungen (FA)

Fachanwendungen sind voll funktionsfähige digitale Lösungen für Endnutzer in Verwaltung und Gesundheitswesen – von bestehenden Fachverfahren für Bund, Länder und Kommunen bis hin zu modernen KI-Anwendungen. Sie unterstützen konkrete Prozesse, etwa von der Antragsbearbeitung bis zur Fallbearbeitung, und stellen damit den direkten Mehrwert für die Endnutzer der Plattform sicher.

Fachanwendungen werden in der Regel von Drittanbietern bereitgestellt – etwa von Fachverfahrensherstellern, Independent Software Vendors (ISV) oder Software-as-a-Service-Anbietern. Sie bringen das fachliche Know-how und die Domänenexpertise ein, die für leistungsfähige digitale Lösungen in Verwaltung und Gesundheitswesen unverzichtbar sind, und bilden damit das Rückgrat des Fachanwendungs-Ökosystems der Plattform. Heute erfolgt der Betrieb dieser Lösungen sehr heterogen: auf eigener

Infrastruktur, in Kundensystemen (On-Premise oder in der Cloud) oder in durch die Anbieter gemanagten Cloud-Umgebungen im SaaS-Modell.

Zukünftig werden Fachanwendungen innerhalb der zentralen Cloud-Umgebung auf Basis des GovTech-Frameworks bereitgestellt und betrieben. Dadurch werden Datenschutz, IT-Sicherheit, Skalierbarkeit und Interoperabilität durch die Plattform selbst sichergestellt. Gleichzeitig können Fachanwendungen auf die vorhandenen Basis- und Fachdienste der Plattform zurückgreifen und diese nahtlos integrieren. So entstehen vollständige digitale Lösungen, die modular aufgebaut und wiederverwendbar sind.

Ein Krankenhaus kann zum Beispiel eine digitale Patientenaufnahme nutzen, die Formulardienste, Identifizierungslösungen und ein Zeitfenstermanagement integriert. Eine Landesbehörde kann ein Reha-Antragssystem betreiben, das Dokumentenmanagement, Rollen- und Rechteverwaltung sowie sichere Kommunikationsdienste umfasst. Für die Endnutzer, wie Bürgerinnen und Bürger, Patientinnen und Patienten, ebenso wie Mitarbeitende in Verwaltung und Gesundheitswesen, ermöglicht dies konkrete Mehrwerte durch moderne, nutzerfreundliche Services, die rechtssicher, datenschutzkonform und effizient sind.

Fachanwendungen und digitale Dienste werden sukzessive auf die Plattform überführt. Bereits heute dient die Plattform als Betriebs-, Entwicklungs- und Umsetzungsumgebung für eine wachsende Zahl fachlicher Anwendungen und Pilotvorhaben aus unterschiedlichen Domänen. Dazu zählen sowohl produktive als auch in Umsetzung befindliche Lösungen, unter anderem aus den Bereichen digitale Verwaltungsverfahren, Zusammenarbeit, Wissensmanagement, Archivierung, Gesundheit sowie KI-gestützte Assistenzsysteme. Der Umsetzungsstand zeigt sich an folgenden Eckpunkten:

- Betriebs- und Umsetzungsumgebung für eine zweistellige Zahl abgeschlossener, laufender oder pilotierter Projekte und Vorhaben von GovTech Deutschland.
- Darüber hinaus befinden sich bereits Lösungen vielzähliger Fachverfahrenshersteller und Technologieanbieter im Test- und Pilotbetrieb auf der Deutschlandplattform.

Der GovTech Store ist durch folgende organisatorische, technische und wirtschaftliche Rahmenbedingungen und Merkmale determiniert:

4.3.4 Organisatorische Eckpunkte von GovTech Store

Das Angebot im GovTech Store orientiert sich an der Nachfrage öffentlicher Stellen sowie am konkreten Mehrwert für die Endanwenderinnen und Endanwender. Zentrales Kriterium ist die Nachnutzbarkeit: Es werden keine individuellen Einzellösungen onboardet, sondern ausschließlich Lösungen, die übergreifend für mehrere Organisationen oder Nutzergruppen übergreifend einsetzbar sind.

Die Auswahl Lösungsbereiche sowie das Portfoliomanagement erfolgen durch den Plattformbetreiber anhand kontinuierlicher Markt- und Bedarfsanalysen, die sowohl fachliche Anforderungen als auch erwartete Nutzenpotenziale berücksichtigen.

Auf dieser Basis führt der Plattformbetreiber Markterkundungen durch. Im Anschluss führt GovTech Deutschland ein Zulassungsverfahren durch bei dem festgelegte Anforderungskriterien validiert werden. Hierzu gehören das Erfüllen von technischen übergeordneten Anforderungen beispielsweise aus Vorgaben des IT-Planungsrates, mit dem Deutschland-Stack oder zwingende Betriebsanforderungen des GovTech-Frameworks. Zur Sicherstellung von Wettbewerb und Auswahlmöglichkeiten werden Verträge mit einer Vielzahl von Anbietern in einem Leistungsbereich geschlossen.

Bei der Festlegung der Anforderungen an Lösungsanbieter berücksichtigt der Plattformbetreiber insbesondere die technologische Architektur, die Integrationsfähigkeit in die Plattform, die Einhaltung sicherheits- und datenschutzrechtlicher Anforderungen sowie die Konformität mit den definierten Plattformstandards. Öffentliche Organisationen können dann ohne eigene Vergabeverfahren im Rahmen der Inhouse-Vergabe (siehe unten) direkt von GovTech Deutschland Unterlizenzen beziehen und so die auf der Plattform verfügbaren Lösungen nutzen.

Zwischen dem Plattformbetreiber und den Lösungsanbietern werden verbindliche Regelwerke vereinbart. Dazu zählen insbesondere Service Level Agreements (SLA) mit definierten Mindeststandards, Auftragsverarbeitungsvereinbarungen (AVV) sowie Allgemeine Geschäftsbedingungen (AGB).

Die Bereitstellung von Lösungen erfolgt initial über das IT-Service-Management des Plattformbetreibers. Anfragen werden geprüft und bereitgestellt; dieser Prozess wird schrittweise automatisiert und in einen vollumfänglichen Marktplatzbetrieb überführt.

Die betriebliche Verantwortung für Qualität, Performance und Verfügbarkeit der Lösungen liegt bei den jeweiligen Lösungsanbietern. Erforderliche Anpassungen an Anwendungen, Verfahren und Diensten werden durch die Anbieter selbst

vorgenommen und getragen. Der Plattformbetreiber unterstützt die Anbieter bei der Integration ihrer Lösungen in die Plattformumgebung, begleitet erforderliche Anpassungen und stellt die Einhaltung verbindlicher Betriebs-, Sicherheits- und Qualitätsstandards sicher.

Vertiefung „Inhouse-Vergabe“

Das Prinzip der Inhouse-Vergabe ermöglicht es öffentlichen Organisationen, digitale Leistungen unmittelbar über GovTech Deutschland zu beziehen, ohne eigene Ausschreibungsverfahren durchführen zu müssen. Grundlage hierfür ist, dass Bund, Länder und Kommunen – letztere über GovTech Kommunal – ordentliche Mitglieder von GovTech Deutschland sind und damit in einem inhouse-fähigen Verhältnis zum Plattformbetreiber stehen. Öffentliche Auftraggeber können GovTech Deutschland somit unmittelbar mit der Erbringung von Leistungen beauftragen.

Auf dieser Basis führt GovTech Deutschland zentrale Bedarfsanalysen durch und ist für die einheitliche, deutschlandweite Beschaffung digitaler Leistungen verantwortlich. Dies betrifft insbesondere Lösungen von Anbietern von Fachanwendungen sowie Herstellern von Querschnitts- und Fachdiensten.

Der Vertragsschluss zwischen GovTech Deutschland und den nutzenden öffentlichen Organisationen erfolgt im Wege der Inhouse-Vergabe, sofern ein entsprechendes inhouse-fähiges Verhältnis besteht. Für die Endnutzer bedeutet dies, dass digitale Lösungen direkt über den Marktplatz der Plattform bezogen werden können, ohne selbst zeit- und ressourcenintensive Vergabeverfahren durchführen zu müssen.

Darüber hinaus wird dieses Modell in einem eigenständigen organisatorischen Rahmen auch für den Gesundheitsbereich nachgebildet. Ziel ist es, im Rahmen von MEDI:CUS sicherzustellen, dass öffentliche Einrichtungen des Gesundheitswesens digitale Lösungen ebenfalls im Inhouse-Verhältnis und auf Basis zentraler Rahmenverträge beziehen können.

4.3.5 Technische Eckpunkte von GovTech Store

Anwendungen, Verfahren und Dienste müssen cloudfähig sein und vollständig durch den Anbieter innerhalb der Plattformumgebung betrieben werden können. Die

Architektur ist cloudagnostisch auszugestalten und muss ohne Anpassungen in einer heterogenen Multi-Cloud-Umgebung betrieben werden können. Die Nutzung cloud-spezifischer Managed Services, proprietärer Microservices oder sonstiger providerspezifischer Plattformdienste ist unzulässig, sofern nicht im Einzelfall begründete Ausnahmen gelten.

Anwendungen müssen vollständig auf der Plattform betreibbar sein. Der vorgesehene Bereitstellungsweg sind OCI-konforme Container-Images mit standardisierten Deployment-Artefakten (Helm Charts oder gleichwertige Kubernetes-Manifeste). Weitere Bereitstellungsformen werden sukzessive ermöglicht und können nach Abstimmung mit dem Plattformbetreiber genutzt werden. Unabhängig vom gewählten Modell gilt, dass Deployment, Updates und Rollbacks vollständig automatisiert und reproduzierbar erfolgen, während manuelle Eingriffe auf Hostsystemen oder Plattform-Infrastruktur ausgeschlossen sind.

Zentrale Plattformdienste wie Identitäts- und Zugriffsmanagement, Logging, Monitoring, Messaging, Storage und Datenbanken werden durch die Plattform bereitgestellt. Anwendungen müssen diese Basisdienste über offene, standardisierte Schnittstellen integrieren (z. B. OIDC, standardisierte Log-Ausgaben) und dürfen keine eigenen, abweichenden Implementierungen voraussetzen. Die Integration in das Identitäts- und Zugriffsmanagement der Plattform muss OIDC-kompatibel erfolgen. Sofern fachlich erforderlich, ist eine standardisierte Anbindung an Verzeichnisdienste wie Active Directory oder LDAP zu unterstützen.

Anwendungen können die von der Plattform bereitgestellten Datenbanksysteme, insbesondere PostgreSQL, nutzen, sind hierzu jedoch nicht verpflichtet. Sofern eigene oder externe Datenbanklösungen eingesetzt werden, sind proprietäre Datenbankeerweiterungen oder enginespezifische Abhängigkeiten nicht zulässig.

Das Betriebs- und Zugriffsmodell ist strikt getrennt. Lösungsanbieter erhalten keinen administrativen Zugriff auf die Cloud- oder Plattforminfrastruktur. Support- und Wartungsleistungen erfolgen ausschließlich auf Applikations- und Container-Ebene über definierte Schnittstellen, Logs und bereitgestellte Laufzeitumgebungen.

Die Architektur der Anwendungen muss hochverfügbar und resilient ausgelegt sein. Single-Point-of-Failure-Architekturen sind zu vermeiden; zustandsbehaftete Komponenten müssen Pod-Neustarts, Rolling Updates und horizontale Skalierung ohne Datenverlust oder Funktionsbeeinträchtigung unterstützen. Anwendungen müssen vollständig automatisierbar sein und sich in Infrastructure-as-Code- und CI/CD-Prozesse integrieren lassen. Sämtliche Konfigurationen sind über Parameter, Variablen

und deklarative Mechanismen steuerbar; manuelle Konfigurations- oder Betriebsmaßnahmen sind ausgeschlossen.

Darüber hinaus gelten verbindliche Vorgaben in Bezug auf IT-Sicherheit und Datenschutz. Diese sind plattformweit einheitlich definiert und in Kapitel 6 detailliert beschrieben.

Weiterführende technische Anforderungen, Architekturrichtlinien sowie detaillierte Angaben zu Schnittstellen, Deployments und Betriebsmodellen sind in der Entwicklerdokumentation des GovTech-Frameworks festgelegt.

4.3.6 Wirtschaftliche Eckpunkte von GovTech Store

Der GovTech Store wird über nutzungsabhängige Entgelte für die bereitgestellten SaaS-Angebote finanziert.

Die Abrechnung erfolgt in Form einer Gesamtrechnung gegenüber den Endnutzern und setzt sich in der Regel aus mehreren Komponenten zusammen. Dazu zählen insbesondere die Lizenzkosten der jeweiligen Anwendung sowie, wie die eingerechneten Kosten für die Nutzung der Basisdienste und der genutzten Cloud-Infrastruktur. Das zugrunde liegende Lizenz- und Entgeltmodell kann je nach Anwendung und Nutzungsszenario unterschiedlich ausgestaltet sein, etwa **fallbasiert**, **nutzerbasiert**, **arbeitsplatzbezogen** oder **ressourcenbasiert**. Die konkrete Ausgestaltung wird vom Plattformbetreiber anhand der Nutzeranforderungen festgelegt und vertraglich geregelt.

In diesem Rahmen setzt GovTech Deutschland zentrale Konditionen und Rabatte mit den Anbietern fest. Durch die Bündelung der Nachfrage und die zentrale Beschaffung können Lizenzkonditionen erzielt werden, die regelmäßig unter den marktüblichen Preisen liegen.

Für die Endnutzer ergeben sich dadurch Gesamtkosten, die aufgrund von Skaleneffekten, verhandelten Preisnachlässen sowie der enthaltenen Infrastruktur- und Plattformleistungen in der Regel marktgerecht oder günstiger sind als vergleichbare Einzelbeschaffungen. Gleichzeitig entfallen eigene Aufwände für Infrastruktur, Betrieb und Vergabeverfahren.

5 Eckpunkte zur Souveränität

Digitale Souveränität ist ein zentrales Ziel des GovTech-Frameworks, wird jedoch nicht als im Sinne von Autarkie, sondern als **steuerbare, risikobewusste Kontrolle über zentrale Abhängigkeiten** verstanden. Der öffentliche Sektor und das Gesundheitswesen müssen dauerhaft in die Lage versetzt werden, technologische, organisatorische und rechtliche Entscheidungen eigenständig zu treffen, Weiterentwicklungen aktiv zu steuern und Anbieterwechsel kurzfristig und aufwandsarm umzusetzen.

Das Kapitel führt keine neuen Architekturprinzipien ein, sondern definiert **strategische Leitplanken** für Technologie-, Betriebs-, Anbieter- und Beschaffungsentscheidungen. Diese orientieren sich an **fünf komplementären Dimensionen**:

- **Technologische Souveränität:** Sicherstellung von Austauschbarkeit und Weiterentwicklungsfähigkeit durch modulare Architekturen, offene Schnittstellen und klar dokumentierte Abhängigkeiten. Ziel ist nicht der Ausschluss proprietärer Technologien, sondern deren beherrschbare Einbindung.
- **Daten- und Informationssouveränität:** Kontrolle über Datenstandorte, Zugriffsrechte, Schlüsselverwaltung und Datenportabilität. Verarbeitung erfolgt grundsätzlich im Europäischen Wirtschaftsraum. Daten müssen jederzeit exportierbar und bei Anbieterwechseln rückführbar sein.
- **Betriebliche Souveränität:** Transparenter, überprüfbarer Plattformbetrieb mit klar definierten Betriebsprozessen, Verantwortlichkeiten und Exit-Szenarien. Lückenlose Nachvollziehbarkeit aller Betriebsaktivitäten.
- **Organisatorische Souveränität:** Öffentliche Steuerungsfähigkeit über Plattformbetrieb und Weiterentwicklung durch definierte Rollen, Governance-Strukturen und institutionalisierte Mitwirkung von Bund, Ländern und weiteren Trägern.
- **Rechtliche Souveränität:** Einhaltung europäischer Datenschutz-, Sicherheits- und Vergabenormen sowie Schutz vor extraterritorialen Zugriffen durch technische, organisatorische und vertragliche Maßnahmen.

Souveränitätsstufen

Digitale Souveränität wird im Plattformkontext bewusst **abgestuft** umgesetzt. Zwischen vollständiger Eigenkontrolle und vollständiger Fremdabhängigkeit existieren unterschiedliche, jeweils zweckmäßige Ausprägungen. Die Plattform verfolgt daher eine **risikoorientierte Differenzierung nach Plattformebene**.

Zur Einordnung wird ein vierstufiges Modell genutzt:

- **Stufe 1 – Niedrige Souveränität:** Abhängigkeit von proprietären Diensten, keine Kontrolle über Infrastruktur, Verarbeitung oder Datenstandorte; potenzielle Verarbeitung außerhalb der EU.
- **Stufe 2 – Grundlegende Souveränität:** Teilweise Kontrolle über Konfigurationen und Verantwortlichkeiten. Datenhaltung im EWR und Austauschbarkeit muss vertraglich, technisch und organisatorisch abgesichert werden.
- **Stufe 3 – Erweiterte Souveränität:** Transparente und kontrollierbare Abläufe auf nachvollziehbar vertrauenswürdiger Infrastruktur, klare steuerbare Exit- und Wechseleigenschaften, Einsatz offener Standards und interoperabler APIs.
- **Stufe 4 – Hohe Souveränität:** Umfassende Kontrolle über Architektur, Software, Betrieb und Daten. Einsatz weitgehend offener Technologien und Modelle unter öffentlicher Governance.

Die praktische Umsetzung der Souveränitätsstrategie erfolgt **differenziert nach Plattformschicht**:

- **Infrastruktur & Cloud-Abstraktion:** Orientierung an Stufe 2-3. Externe Cloud-Infrastrukturen werden genutzt, Abhängigkeiten jedoch durch Multi-Cloud-Ansätze, Abstraktion und Wechseloptionen begrenzt.
- **Basisdienste und Plattformkern:** Orientierung an Stufe 3-4. Zentrale Funktionen unterliegen erhöhter Kontrollanforderung. Hier werden Offenheit, Austauschbarkeit und langfristige Gestaltungsfähigkeit priorisiert, sodass GovTech Deutschland die technische und operative Kontrolle behält.
- **Querschnittsdienste (Stufe 2-4) sowie Fachdienste und Fachanwendungen (Stufe 1-4):** Proprietäre Lösungen sind zulässig, sofern sie verbindliche Anforderungen an Interoperabilität, Datenportabilität, Sicherheit und Exit-Fähigkeit erfüllen. Wettbewerb und Mehrfachvergabe sichern Wechseleigenschaften

Vertiefung zu Open Source und Lizenzstrategie

Open Source ist ein zentrales Element der Plattform. Offene Software schafft Transparenz, ermöglicht unabhängige Prüfungen und reduziert strukturelle Abhängigkeiten. Daher werden für den Multi-Cloud-Abstraction-Layer sowie für die Basisdienste des GovTech-Frameworks bevorzugt permissiv lizenzierte Open Source-Lösungen eingesetzt.

Diese Präferenz schließt alternative Modelle nicht aus. Steht für einen erforderlichen Basisdienst keine geeignete Open-Source-Lösung zur Verfügung, können auch proprietäre Technologien eingesetzt werden, sofern entweder mehrere vergleichbare Anbieter existieren oder die Architektur einen Anbieterwechsel ohne unverhältnismäßige Abhängigkeiten ermöglicht. Ergänzend kann ein Escrow-Treuhandmodell genutzt werden, um langfristige Wartbarkeit und Weiterentwicklungsfähigkeit abzusichern. Ist weder eine geeignete Open-Source- noch eine austauschbare proprietäre Lösung verfügbar, kann eine gezielte Eigenentwicklung in Betracht gezogen werden.

In den höheren Architekturschichten, insbesondere im GovTech Store, ist Open Source ebenfalls willkommen, jedoch keine zwingende Voraussetzung. Hier stehen funktionale Vielfalt, Wettbewerb und ein breites Marktangebot im Vordergrund. Proprietäre Lösungen sind ausdrücklich zulässig, sofern sie die verbindlichen Anforderungen an Sicherheit, Interoperabilität und Datenportabilität erfüllen.

Die Lizenzstrategie der Plattform folgt damit einem klaren, pragmatischen Prinzip: maximale Offenheit und Unabhängigkeit dort, wo sie für den stabilen Kernbetrieb erforderlich sind, und größtmögliche Flexibilität dort, wo Vielfalt, Innovation und Marktbreite im Fokus stehen.

Die Eckpunkte zur Souveränität sind verbindlicher **Bewertungsmaßstab** für Architektur- und Technologieentscheidungen, Auswahl und Einbindung von Anbietern, Beschaffungs- und Vertragsmodelle und Weiterentwicklung des Plattformbetriebs. Sie wirken **querschnittlich**, ersetzen jedoch keine konkreten Sicherheits-, Datenschutz- oder Betriebsanforderungen. Diese werden in den nachfolgenden Kapiteln detailliert.

6 IT-Sicherheit und Datenschutz

IT-Sicherheit und Datenschutz sind grundlegende Voraussetzungen für den Betrieb des GovTech-Frameworks. Sie sind nicht nachgelagerte Anforderungen einzelner Anwendungen, sondern integraler Bestandteil von Architektur, Betrieb und Governance der Plattform. Ziel ist es, ein einheitliches, hohes und dauerhaft tragfähiges Sicherheits- und Datenschutzniveau bereitzustellen, auf dem digitale Lösungen für Verwaltung und Gesundheitswesen rechtssicher und vertrauenswürdig betrieben werden können.

Die Plattform verfolgt dabei einen zentralisierten, standardisierten Ansatz: Wesentliche Sicherheits- und Datenschutzanforderungen werden plattformseitig vorab umgesetzt und verbindlich bereitgestellt. Dadurch entfällt die Notwendigkeit, grundlegende Konzepte in jedem einzelnen Projekt neu zu entwickeln, zu prüfen oder zu genehmigen. Gleichzeitig bleibt ausreichend Flexibilität erhalten, um fach- oder institutionsspezifische Schutzbedarfe gezielt abzubilden.

Dieses Kapitel beschreibt dieses Vorgehen in zwei Teilen. Abschnitt 6.1 erläutert die Grundsätze und Mechanismen der IT-Sicherheit auf Plattform- und Anwendungsebene. Abschnitt 6.2 konkretisiert die datenschutzrechtlichen Rahmenbedingungen und Rollenmodelle. Beide Themen sind eng miteinander verzahnt, werden jedoch aus Gründen der Klarheit getrennt dargestellt.

6.1 IT-Sicherheit

Die Maßnahmen zur IT-Sicherheit des GovTech-Frameworks haben das Ziel, die sichere und regelkonforme Bereitstellung aller Plattform-Services zu gewährleisten sowie die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen sicherzustellen. Die technischen und organisatorischen Maßnahmen sorgen für Risikominimierung, klare Verantwortlichkeiten und Prozesse für ein durchgängiges Sicherheitsniveau. Die Plattform verfolgt hierzu einen zweistufigen Sicherheitsansatz, der sowohl den GovTech Core als auch die im GovTech Store betriebenen Anwendungen adressiert.

6.1.1 Sicherheitsarchitektur des GovTech Core

Für den Plattformkern wird eine einheitliche Sicherheitsarchitektur definiert, die unabhängig von der einzelnen Anwendung gilt. Sie stellt sicher, dass grundlegende Sicherheitsanforderungen konsistent, überprüfbar und skalierbar umgesetzt sind.

Zentrale Sicherheitsfunktionen werden plattformweit bereitgestellt und sind verbindlich zu nutzen. Dazu zählen insbesondere ein zentrales Identitäts- und Zugriffsmanagement, durchgängige Verschlüsselungsmechanismen, einheitliche Logging- und Monitoringverfahren sowie standardisierte Backup- und Wiederanlaufkonzepte. Ergänzt wird dies durch eine strikte Netzwerksegmentierung und klar definierte Sicherheitszonen, die es ermöglichen, Anwendungen mit unterschiedlichem Schutzbedarf getrennt und angemessen abzusichern.

Die Logging- und Monitoringfunktionen werden durch ein zentrales Security Information and Event Management (SIEM) sowie ein Security Operations Center (SOC) ergänzt. Das SIEM aggregiert und korreliert sicherheitsrelevante Ereignisse und Log-Daten über alle Plattformschichten hinweg und bildet damit die technische Grundlage für deren Erkennung und Auswertung. Das SOC fungiert als operative Überwachungs- und Steuerungsinstanz für die Plattform und stellt auf dieser Grundlage die kontinuierliche Erkennung, Bewertung und koordinierte Behandlung sicherheitsrelevanter Ereignisse sicher. Es verbindet präventive Sicherheitsmaßnahmen mit einer strukturierten Incident-Response und gewährleistet einen einheitlichen, nachvollziehbaren Umgang mit Sicherheitsvorfällen.

Die Sicherheitsarchitektur des Plattformkerns erfüllt die maßgeblichen gesetzlichen und normativen Anforderungen, insbesondere aus DSGVO, IT-Sicherheitsgesetz und BSI-Grundschutz. Diese Anforderungen werden plattformseitig umgesetzt und müssen nicht für jede Anwendung neu nachgewiesen werden. Dadurch entsteht ein konsistentes Basissicherheitsniveau, das Genehmigungs- und Freigabeprozesse deutlich vereinfacht.

6.1.2 Sicherheitskonzepte für Anwendungen im GovTech Store

Aufbauend auf dem plattformseitigen Sicherheitsfundament wird für jede Anwendung ein eigenes, anwendungsspezifisches Sicherheitskonzept erstellt. Dieses orientiert sich am konkreten Schutzbedarf der Anwendung und beschreibt, wie die bereitgestellten Sicherheitsmechanismen genutzt und gegebenenfalls ergänzt werden.

Zentraler Ausgangspunkt ist die Einordnung der Anwendung in eine **Schutzklasse**, entweder anhand bestehender behördlicher Kategorien (z. B. öffentlich, behördenintern, VS-NfD, VS-Vertraulich, VS-Geheim) oder durch eine strukturierte **Schutzbedarfsanalyse**. Daraus werden die relevanten Schutzziele abgeleitet und die erforderlichen Sicherheitsmaßnahmen bestimmt (technische und organisatorische Maßnahmen, TOMs). Diese umfassen sowohl die Nutzung der plattformseitigen

Sicherheitsfunktionen als auch gegebenenfalls zusätzliche Maßnahmen auf Anwendungsebene.

Die Plattform stellt hierfür **standardisierte Vorlagen, Prozesse und Prüfmechanismen** bereit. Dadurch bleibt der Aufwand für die Erstellung und Pflege anwendungsspezifischer Sicherheitskonzepte beherrschbar, während gleichzeitig ein hohes Maß an Vergleichbarkeit, Transparenz und Prüfbarkeit gewährleistet wird. Anwendungen mit erhöhtem Schutzbedarf können in speziell dafür vorgesehenen Sicherheitszonen betrieben werden, ohne dass hierfür individuelle Sonderlösungen notwendig sind.

Durch dieses zweistufige Modell verbindet das GovTech-Framework zentrale Standardisierung mit fachlicher Differenzierung. Sie schafft damit die Voraussetzungen für einen sicheren, skalierbaren und wirtschaftlichen Betrieb digitaler Lösungen über Organisations- und Ebenengrenzen hinweg.

6.2 Datenschutz

Der Datenschutz auf der Plattform ist integraler Bestandteil von Architektur, Betrieb und Governance. Ziel ist eine rechtmäßige, transparente und kontrollierbare Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung (DSGVO) sowie den einschlägigen nationalen Regelungen. Die Plattform schafft hierfür einen einheitlichen, vorgeprüften Rahmen, der den datenschutzrechtlichen Aufwand für einzelne Anwendungen deutlich reduziert und gleichzeitig ein hohes, konsistentes Schutzniveau sicherstellt.

Grundprinzip ist auch im Datenschutz ein **zweistufiges Vorgehensmodell**. Zentrale datenschutzrechtliche Anforderungen werden plattformseitig umgesetzt und verbindlich bereitgestellt. Darauf aufbauend werden anwendungsspezifische Datenschutzkonzepte erstellt, die sich auf die jeweilige Fachlogik und die konkreten Verarbeitungsvorgänge beziehen.

6.2.1 Datenschutzkonzept des GovTech Core

Für den Plattformkern gilt ein übergreifendes Datenschutzkonzept, das die datenschutzrechtlichen Grundlagen für alle zentralen Dienste und Betriebsprozesse definiert. Es regelt insbesondere Rollen und Verantwortlichkeiten, den Einsatz von

Unterauftragnehmern, die Verarbeitung von Protokoll- und Metadaten sowie grundlegende Verfahren zur Wahrnehmung von Betroffenenrechten.

Die Plattform berücksichtigt die datenschutzrechtlichen Grundsätze systematisch im Design ihrer Komponenten. Datenverarbeitungen sind auf das notwendige Maß begrenzt, Zugriffe rollenbasiert und mandantentrennt umgesetzt, und technische Schutzmaßnahmen wie Verschlüsselung und Zugriffskontrollen sind plattformweit verbindlich integriert. Logging- und Monitoringdaten werden ausschließlich zu Betriebs- und Sicherheitszwecken verarbeitet und unterliegen klar definierten Lösch- und Aufbewahrungsregeln.

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich innerhalb des Europäischen Wirtschaftsraums. Der Plattformbetrieb ist so ausgestaltet, dass Datenportabilität, Nachvollziehbarkeit und Auditierbarkeit jederzeit gewährleistet sind. Damit schafft der Plattformkern einen stabilen datenschutzrechtlichen Rahmen, auf den alle Anwendungen aufsetzen können.

6.2.2 Datenschutzkonzepte für Anwendungen im GovTech Store

Für jede Anwendung im GovTech Store wird ein eigenes, anwendungsspezifisches Datenschutzkonzept erstellt. Dieses beschreibt die konkreten Verarbeitungsvorgänge, Zwecke, Datenkategorien und Rechtsgrundlagen der jeweiligen Fachanwendung und legt fest, wie die datenschutzrechtlichen Vorgaben umgesetzt werden.

Verantwortlicher im Sinne der DSGVO ist stets die jeweilige nutzende Organisation. Der Plattformbetreiber agiert als Auftragsverarbeiter und verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Verantwortlichen. Etwaige Unterauftragnehmer, etwa Lösungsanbieter oder Cloud-Dienstleister, werden vertraglich eingebunden und unterliegen den gleichen datenschutzrechtlichen Anforderungen. Die Plattform stellt hierfür standardisierte Vorlagen, Prozesse und Vertragsgrundlagen bereit. Dadurch wird sichergestellt, dass Datenschutzkonzepte vergleichbar, prüfbar und effizient erstellt werden können. Soweit erforderlich, werden Datenschutz-Folgenabschätzungen durchgeführt. Die Plattform unterstützt diesen Prozess durch vorstrukturierte Verfahren und bereits bewertete technische Rahmenbedingungen.

Soweit eine Verarbeitung voraussichtlich mit hohen Risiken für die Rechte und Freiheiten natürlicher Personen verbunden ist, wird für die jeweilige Anwendung eine **Datenschutz-Folgenabschätzung** gemäß Art. 35 DSGVO durchgeführt. Die Plattform

unterstützt diesen Prozess durch vorstrukturierte Verfahren und vorab bewertete technische Rahmenbedingungen, wodurch der Aufwand für die Durchführung der DSFA deutlich reduziert wird.

Durch die Kombination aus zentralem Plattform-Datenschutzkonzept und anwendungsspezifischen Datenschutzregelungen entsteht ein abgestimmtes, skalierbares Datenschutzmodell. Zentrale Risiken werden plattformseitig adressiert, während fachliche Besonderheiten gezielt auf Anwendungsebene berücksichtigt werden können. Dieser Ansatz ermöglicht es, digitale Lösungen schnell bereitzustellen, ohne datenschutzrechtliche Anforderungen zu vernachlässigen. Gleichzeitig bleibt die Verantwortung klar zugeordnet, die Verarbeitung transparent nachvollziehbar und der Plattformbetrieb dauerhaft auditfähig.

6.3 Sicherheitszonen

Basierend auf Datenschutz- und IT-Sicherheitsanforderungen unterscheidet die Plattform mehrere Sicherheitszonen mit zunehmendem Schutzniveau. Insgesamt werden vier Zonen definiert, die von niedrigem bis zu sehr hohem Schutzbedarf reichen und als praxisnahe Orientierung für den Betrieb und die Platzierung von Anwendungen dienen. Die nachfolgenden Ausführungen stellen **typische Beispiele für die Ausgestaltung dieser Zonen dar und dienen als Orientierung**, ohne eine starre oder abschließende Zuordnung einzelner Anwendungsfälle vorzugeben:

- Anwendungen mit geringem Schutzbedarf, etwa Informationsangebote oder Webanwendungen zur Bereitstellung öffentlicher Inhalte, können in hochskalierbaren Cloud-Umgebungen betrieben werden, beispielsweise bei Hyperscalern.
- Für Anwendungen mit begrenztem Schutzbedarf, etwa zur Verarbeitung interner oder weniger sensibler Daten, können kontrollierte Cloud-Umgebungen von deutschen oder europäischen Anbietern mit klar definierten Datenlokalisationen zum Einsatz kommen.
- Anwendungen mit erhöhten Anforderungen an Vertraulichkeit, etwa bei der Verarbeitung personenbezogener, behördeninterner Daten oder VS-NfD, können in besonders kontrollierten Umgebungen betrieben werden, beispielsweise bei öffentlich-rechtlichen IT-Dienstleistern oder in dedizierten Rechenzentren der öffentlichen Hand.

- Für Anwendungen mit sehr hohem Schutzbedarf, etwa bei höheren Einstufungen, stehen auch isolierte Betriebsumgebungen zur Verfügung, etwa hochgesicherte, abgeschottete oder air-gapped Infrastrukturen mit erweiterten technischen und organisatorischen Schutzmaßnahmen.

Innerhalb jeder Sicherheitszone bestehen abgestufte Ausprägungen, um fachliche Besonderheiten und unterschiedliche Risikoprofile angemessen berücksichtigen zu können. Auf dieser Grundlage wird für jede Anwendung ein individuelles Sicherheits- und Datenschutzkonzept abgeleitet, das überwiegend auf den plattformseitig bereitgestellten Funktionen aufsetzt. Dadurch werden einheitliche, skalierbare und auditierbare Standards gewährleistet, ohne den Betrieb oder die Weiterentwicklung der Anwendungen unnötig zu verkomplizieren.

7 Fazit und Ausblick

Das GovTech-Framework begegnet den eingangs beschriebenen Herausforderungen der Verwaltungs- und Gesundheitsdigitalisierung auf mehreren Ebenen zugleich: Technisch verkürzt die standardisierte Multi-Cloud-Architektur Entwicklungs- und Bereitstellungszyklen und ermöglicht durchgängige Wiederverwendung statt paralleler Insellösungen. Organisatorisch schafft die Plattform mit einheitlichen Governance-Strukturen und vorgeprüften Sicherheits- und Datenschutzkonzepten eine gemeinsame Grundlage, die Koordinationsaufwände reduziert. Wirtschaftlich senken gebündelte Rahmenverträge, geteilte Basisdienste und der Marktplatzansatz sowohl Einzel- als auch Gesamtkosten. Föderal ist die Plattform von Beginn an so ausgelegt, dass sie über Ebenen und Institutionen hinweg – von Bund über Länder bis Kommunen – anschlussfähig ist und genutzt werden kann.

Die Plattform versteht sich dabei nicht als abgeschlossenes System, sondern als sich weiterentwickelnde Infrastruktur. Architektur, Basisdienste und Sicherheitskonzepte werden laufend erweitert und optimiert. Auch das Angebot im GovTech Store wird sukzessive aufgebaut: Mit wachsender Zahl an Anbietern, Fachdiensten und Fachanwendungen entsteht ein zunehmend vollständiges und vergleichbares Lösungsportfolio für Verwaltung und Gesundheitswesen.

Das GovTech-Framework ist dabei explizit anschlussfähig an bestehende und zukünftige nationale Strukturen. Die Deutschlandplattform dient bereits heute als funktionierende Referenz für zentrale Elemente des Deutschland-Stacks und ist auf die Anbindung an die Deutsche Verwaltungscld sowie den Marktplatz Deutschland Digital ausgelegt. Darüber hinaus können über die Plattform verbindliche Governance-Vorgaben, beispielsweise des IT-Planungsrates oder des Deutschland-Stacks gegenüber Anwendungen und Lösungen effizient durchgesetzt werden, unter anderem für Schnittstellen und Datenhaltung. Auch MEDI:CUS wird kontinuierlich ausgebaut und schrittweise für weitere Länder geöffnet, sodass die im Gesundheitswesen gewonnene Architektur- und Betriebserfahrung zunehmend nachgenutzt werden kann.

Erfahrungen aus dem produktiven Betrieb, aus Pilotvorhaben und aus konkreten fachlichen Anforderungen fließen systematisch in die strategische Weiterentwicklung des Frameworks ein. Über die bestehenden Instanziierungen hinaus sind grundsätzlich weitere, fachlich spezialisierte Instanziierungen für zusätzliche Domänen des öffentlichen Sektors möglich.

Mit dem GovTech-Framework steht eine tragfähige, souverän kontrollierte Grundlage zur Verfügung, die öffentlichen Institutionen die technologische Handlungsfähigkeit

gibt, digitale Lösungen selbstbestimmt und nachhaltig zu gestalten. Zugleich wächst mit jeder neuen Instanziierung, jedem neuen Anbieter und jeder neuen Anwendung ein gemeinsames digitales Ökosystem, von dem nicht nur Verwaltung und Gesundheitswesen, sondern letztlich auch Bürgerinnen und Bürger profitieren.

Ihr Kontakt

GovTech Deutschland
platforms@gov.tech

