Eine bayerische Infrastrukturkomponente für alle aus der Cloud

René Käker

Sophie Eberl

Daniela Schleder

1. Einleitung

1.1 Motivation

Einen einfachen Verwaltungsantrag wollen wir alle – Bürgerinnen und Bürger sowie Sachbearbeiterinnen und Sachbearbeiter: kein Beamtendeutsch, keine doppelte Datenerfassung, keine fehlenden oder überflüssige Angaben. Ein Online-Antrag soll der Start in ein vollständig digitales Verwaltungsverfahren sein. Das ist auch das Ziel des Onlinezugangsgesetzes (OZG). Über 575 Verwaltungsleistungen mit fast 10-mal so vielen Online-Anträgen sollen digitalisiert werden. Diese Aufgabe teilen sich Bund, Länder und Kommunen.

Viele Verwaltungsprozesse werden bereits von Fachverfahren unterstützt. Auf der Weiterentwicklung dieser Verfahren lag in der Vergangenheit sehr oft der Fokus bzw. die Kompetenz. Prozessoptimierungen oder Überlegungen zur nutzerfreundlichen Bedie-

nung wurden häufig nur nachrangig mitgedacht. Aber gerade hier schlummert Potential. Insbesondere mit der Nutzung zentral bereitgestellter Querschnittskomponenten können Verwaltungsprozesse effizienter und fokussierter bearbeitet werden. Der Freistaat Bayern hat sich im Rahmen des OZG zum Ziel gesetzt, einen solchen Querschnittservice bereitzustellen.

Zahlreiche Verwaltungsleistungen haben einen Raumbezug, sei es für die Genehmigung einen Brunnen zu bohren, einen Baum zu fällen oder eine Biertischgarnitur für das Volksfest aufzustellen. Die verbale Beschreibung der räumlichen Lage des Antragsgegenstandes führt oft zu vielen Rückfragen. Karten können helfen, die Sache auf den Punkt, die Linie oder die Fläche zu bringen.

Die Geodateninfrastruktur (GDI) – also digitale Geodaten mit ihrer technischen Infrastruktur zur Erfassung und Bereitstellung – ist ein Querschnittangebot, das viele Verwaltungsverfahren nutzen. Geoexperten unterstützen Fachdisziplinen bei der Erfüllung ihrer Aufgaben. Und nun zieht die GDI auch in die Schnittstelle des Bürgers zur Verwaltung ein. Mit einer Lageskizze zu einem Antrag – oder genauer – mit einer Geodigitalisierungskomponente.

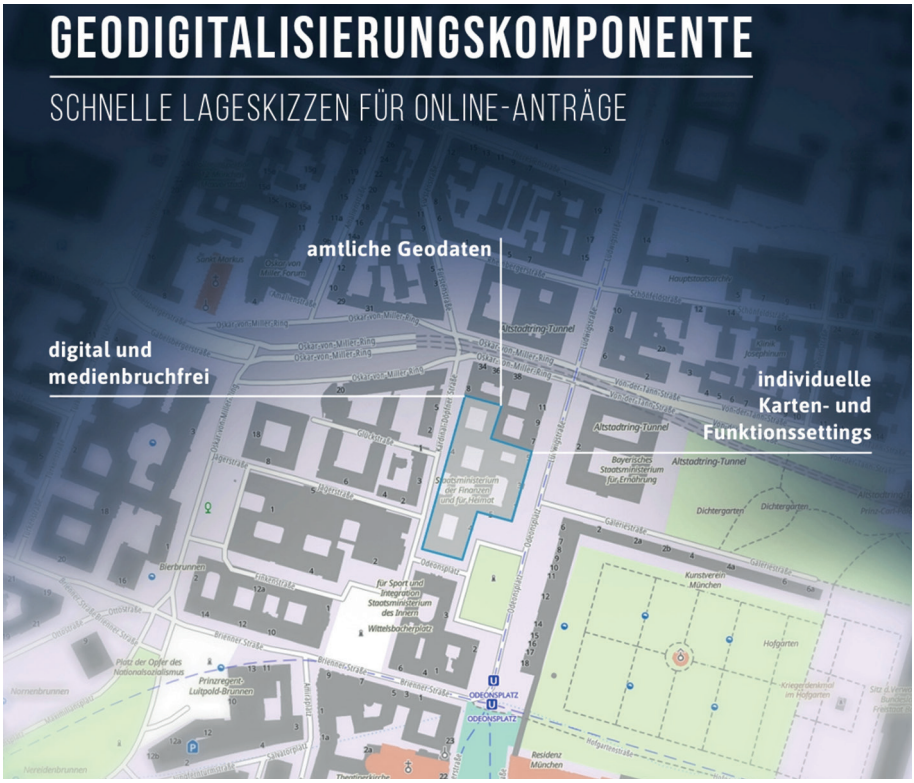

Abbildung 1: Die Geodigitalisierungskomponente

Die Geodigitalisierungskomponente – GDIK – wurde im Kontext des OZG als eine „Einer für Alle" (EfA)-Lösung entwickelt. „Einer für Alle-Services sind flächendeckend einsetzbare Lösungen, die einmal nutzerzentriert konzipiert und entwickelt, fachlich betreut und technisch betrieben werden".[1] Unter diese Definition fallen also nicht nur konkrete Anträge, sondern auch zentral, bereitgestellte verwaltungsübergreifende Infrastrukturangebote.

1.2 Geodigitalisierungskomponente – Eine Skizze zum Antrag

Amtliche Geodaten werden auf vielfältige Art und Weise zur Wahrnehmung öffentlicher Aufgaben benötigt. Auch zahlreiche Leistungen nach dem OZG-Umsetzungskatalog benötigen Geodaten in ihren Verwaltungsprozessen, z. B. bei der Beantragung einer Baugenehmigung, der Denkmalförderung, der Bodenrichtwertauskunft, der Baumfällgenehmigung oder bei Beteiligungsverfahren zu Planaufstellungen.

Sehr oft werden schon bei der Antragsstellung Geodaten benötigt. Mit der GDIK wird ein einheitliches Werkzeug zur Erfassung von geografischen Informationen auf Basis amtlicher Geodaten zur Einbindung in Verwaltungsanträge bereitgestellt. So kann der Antragsgegenstand auf Grundlage digitaler Geodaten visualisiert und konkretisiert werden (s. Abbildung 1). Die zusätzliche Darstellung von bereits vorhandenen Fachinformationen während eines Antragsprozesses fördert zudem die Transparenz und steigert die Antragsqualität. Die GDIK unterstützt den nutzerfreundlichen, digitalen Zugang zu Verwaltungsleistungen und eine effiziente Prozessgestaltung innerhalb der Verwaltung.

Die Einbindung der GDIK in Verwaltungsanträge bietet Vorteile für Bürgerinnen und Bürger:

- Sie gibt ein „gutes Gefühl" bei der Antragstellung, da das Anliegen konkretisiert werden kann.
- Sie enthält zusätzliche Informationen für mehr Transparenz rund um das Antragsthema.
- Sie ist medienbruchfrei und kann in vielen digitalen Anträgen verwendet werden.
- Sie ist übersichtlich gestaltet und intuitiv bedienbar.

In einem Verwaltungsprozesse trägt die GDIK insb. dazu bei,

- mit Zusatzinformationen durch Verknüpfung mit Geodaten Rückfragen zu minimieren und
- Verwaltungsverfahren durch standardisierte und qualifizierte Antragsbeilagen zu beschleunigen.

1 Mindestanforderungen an „Einer für Alle"-Services, Stand 08.12.2020, https://leitfaden.ozg-umsetzung.de/display/OZG/OZG-Leitfaden?preview=/4621478/12588603/EfA-Mindestanforderungen_Version%201.0.pdf

Der zentral angebotene Querschnittsservice kann einfach genutzt werden, da

- mittels standardisierter Schnittstellen viele Geodaten eingebunden werden können.
- besondere Kenntnisse über Geodaten, Geodateninfrastrukturen oder Geoinformationssystemen nicht nötig sind.
- eigene Entwicklungs- oder Infrastruktur-Ressourcen entfallen.

Je nach Anforderungen eines OZG-Antrags kann die GDIK aus dem Antragsprozess heraus mit einem individuellen Karten- und Funktionssetting an einer Lokalität (Adresse, Flurstück, Koordinate) über standardisierte Schnittstellen aufgerufen werden. Die erfassten Daten werden im Schnittstellenformat an den Antrag bzw. ein Fachverfahren übergeben (s. Abbildung 2).

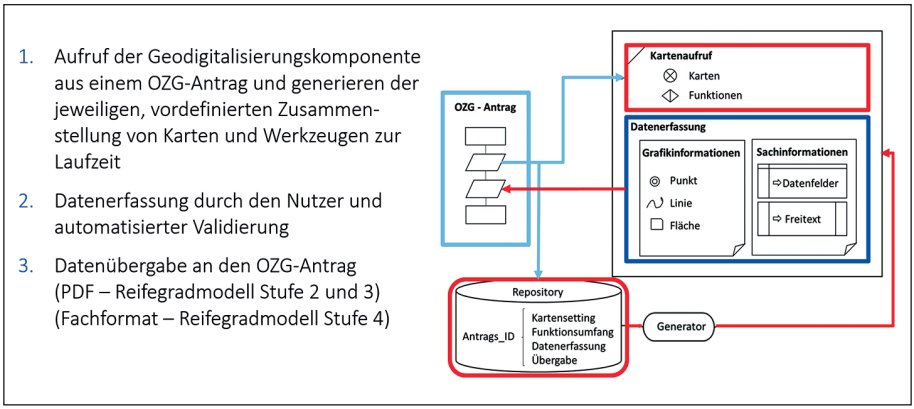

Abbildung 2: Prozessskizze der Geodigitalisierungskomponente

1.3 Aus der Cloud für alle

Die GDIK wurde im Rahmen der Umsetzung des OZG unter der Federführung des StMFH, in Zusammenarbeit mit dem Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) sowie dem Landesamt für Sicherheit in der Informationstechnik (LSI) länderübergreifend mit dem Land Niedersachsen als Kooperationspartner entwickelt. Insbesondere die Entwicklung einer zeitgemäßen und zukunftsorientierten Cloud-Lösung stellt eine stetige Verfügbarkeit und hohe Leistungsfähigkeit sicher. Künftig nutzbare Infrastrukturen und Technologien, die u. a. mit dem Vorhaben der Deutschen Verwaltungscloud (DVC) formuliert sind, wurden bei der Umsetzung in einem Proof of Concept (PoC) frühzeitig berücksichtigt.

Da die GDIK eine Querschnittskomponente ist, muss ihre Nutzung aus vielen Perspektiven betrachtet werden. Als Nachnutzungsszenarien wurden daher Web-Services aus einer Cloud-Infrastruktur gewählt. So ist eine zukunftsgerichtete und weitreichende Nutzung sichergestellt. Die Entwicklung und der Betrieb der Services geschehen unter Anwendung der agilen DevOps-Methodik.

Für die weitere Bekanntmachung der GDIK wurde einerseits eine Webseite www.gdik.de erstellt, die allgemein, technisch und über die Nachnutzung informiert. Ein Video und ein Musterantrag[2] zeigen die Funktionsweise der GDIK und laden zum Ausprobieren ein. Über die Webseite können registrierte Nutzer die GDIK antragsindividuell konfigurieren.

Eine Leistungsbeschreibung sowie das Vertragswerk zur Nachnutzung der GDIK ist im FIT-Store der Föderalen IT-Kooperation (FITKO) bzw. dem Marktplatz für EfA-Leistungen[3] der govdigital eingestellt. Der Vertrag zur Nachnutzung wird über den Marktplatz geschlossen und die Nutzerregistrierung über die Servicestelle der GDIK angestoßen (s. Abbildung 3).

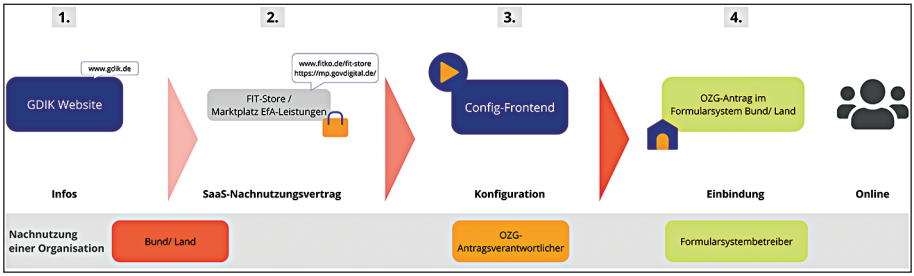

Abbildung 3: Schritte zur Nachnutzung

Im Umsetzungsprojekt der Servicebereitstellung im Cloud-Service-Portal (CSP) der Deutschen Verwaltungscloud (DVC) hat die GDIK aufgrund ihrer technischen Konzeption nun auch einen hohen Stellenwert („Top 10“) zuerkannt bekommen. Die Einstellung der GDIK als ein erster bayerischen Service wird durch das IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) unterstützt.

2. Umsetzung

2.1 Grundprinzipien

Das Konzept der bedingungslosen Einfachheit für alle Nutzer sowie die Anforderung, die Komponente über das Internet und über Standard-Web-Browser nutzbar zu machen, erforderte auch andere Wege in der Umsetzung:

- Die Entwicklung erfolgte Cloud-Native. Die Komponente ist prinzipiell in jeder modernen Cloudinfrastruktur nach nur minimalen Anpassungen lauffähig und nutzt im hohen Maße skalierbare Services bzw. ist selbst skalierbar.
- Die Applikation folgt einer modernen Cloud-Service-Architektur (Microservices); Teilkomponenten werden unabhängig voneinander entwickelt und betrieben und sind mit unterschiedlichen Parametern individuell über API-Standards nutzbar.

2 https://formsrv-test-neu.bayern.de/intelliform/forms/entwicklung/test/test/kartentest/index
3 https://mp.govdigital.de/

- Das Verfahren erfüllt alle Compliance-Anforderungen bzgl. Informationssicherheit, Datenschutz und Barrierefreiheit. Diese Anforderungen sind für Cloud-Anwendungen nicht geringer als in klassischen Betriebsumgebungen, sondern tendenziell höher aber vor allem anders, z. B. fordert die Informationssicherheit eine gehärtete Entwicklungsumgebung und für alle Grundkomponenten BSI C5-Zertifikate.
- Das Verfahren wird nach dem DevOps-Prinzip entwickelt und betrieben.

2.2 Vorgehen und Struktur

Das Projekt verfolgte mit dem Entwicklungsansatz Minimum Viable Product (MVP – kleinste bereits tragfähige und funktionierende Lösung) ein schnelles Ergebnis, um innerhalb des ersten Jahres einen einsatzfähigen Service bereitzustellen. Das MVP wird kontinuierlich weiterentwickelt.

Im Projekt wurde zunächst ein klassischer Rahmen mit nur wenigen Meilensteinen, Projektphasen und Arbeitspaketen gewählt, um mit einem extrem schlanken Projektmanagement schnell ein Ergebnis zu erzielen. Dieser Ansatz wurde nun in ein agiles Vorgehen nach Scrum überführt und langfristige Strukturen für Weiterentwicklung und Betrieb geschaffen. Neben dem DevOps-Team wurden Gremien zur Koordinierung und fachlichen Steuerung (s. Abbildung 4) gebildet.

Abbildung 4: Projektstruktur

Der Lenkungsausschuss setzt sich aus den nachnutzenden Ländern zusammen und steuert die Weiterentwicklung der GDIK sowie den Ressourceneinsatz.

Die Nahtstelle zwischen der strategischen und operativen Ebene ist das Produktmanagement. Neben der Koordinierung der Nachnutzung sind hier das Releasemanagement sowie die Koordination der technischen Umsetzung, die Organisation des Supports und die Maßnahmen zur Bekanntmachung der GDIK verortet.

2.3 Servicearchitektur

Durch Verwendung offener Standards (OGC, REST, HTML oder JSON) wird die Interoperabilität, grundlegend für die breite Nachnutzung sichergestellt. Darüber hinaus werden aber auch weitere nutzerspezifische Schnittstellen abgestimmt. Mit der Umsetzung einer Micro-Frontend-Architektur mit optionalen Hilfsservices wird ein modulares Baukastenprinzip (Microservice-Architektur) verfolgt.

Für jede in dem Nachnutzungsprozess beteiligte Stelle, wird ein individuell benötigter Service angeboten (s. Abbildung 5):

- Für Antragsverantwortliche: Config-Web-Service – zur antragsindividuellen Konfiguration der GDIK und der Bereitstellung für die Formularserverbetreiber
- Für Formularserverbetreiber: Config-Code-Service – konfigurierter Quellcode zur Einbindung in das Antragsformular
- Für Entwicklung: Open-Source-Code – Bereitstellung des Quellcodes auf GitHub
- Für Nachnutzungsverantwortliche: Webseite mit Musterantrag, Anleitungen und Dokumentation sowie Wegen zur Nachnutzung

Die funktionalen und qualitativen Merkmale der Produkte umfassen auch Anforderungen an die Nutzerfreundlichkeit (User Experience und Usability), den Datenschutz, die IT-Sicherheit und Barrierefreiheit.

Die Cloud-Infrastruktur bringt gerade für diese bundesweit zur Verfügung stehende Querschnittskomponente erhebliche Vorteile. Neben der 24/7/365 Verfügbarkeit können so auch unterschiedlichste Bedarfe hinsichtlich der Skalierbarkeit (hochverfügbar) abgedeckt werden. Die zentral angebotenen Services (Config-Web-Service und Config-Code-Service) stehen den Nutzern verlässlich zur Verfügung. Die Verfügbarkeitsklassen für EfA-Onlinedienste[4] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden jeweils in „Gold" erfüllt. Auch gelten die Service Level Agreements (SLA) for Online Services[5] der Betriebsumgebung von Microsoft Azure. Daher wird eine Cloud-Infrastruktur als die geeignetste Lösung für die Weiternutzung der GDIK gesehen.

Hinsichtlich der Entwicklung wurden die Hauptqualitätsmerkmale der ISO 25010 beachtet: Funktionalität, Effizienz/Performance, Kompatibilität, Benutzbarkeit, Zuverlässigkeit, Sicherheit, Wartbarkeit und Portabilität.

4 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G2_Definitionen.pdf?__blob=publicationFile&v=1

5 https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1

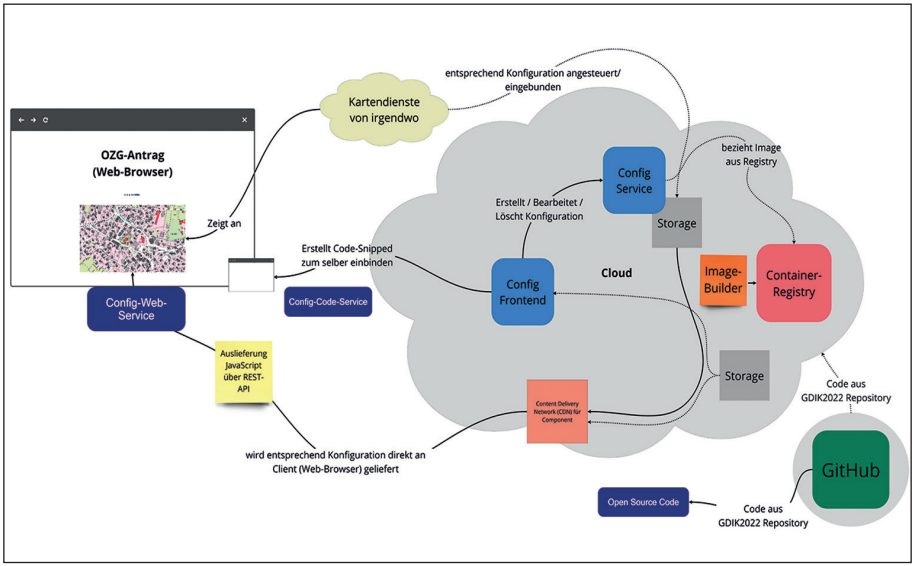

Abbildung 5: Grobarchitektur mit Services

2.4 Nachnutzung

Es bestehen drei Möglichkeiten, die GDIK über das Internet nachzunutzen. Als präferiertes Lösungsszenario wird der GDIK Config-Web-Service angeboten. Für die jeweilige Verwaltungsleistung wird ein vorkonfiguriertes (Nutzung des GDIK Konfigurators) JavaScript über ein REST-Interface (HTTP-Standard, einfache API) als Cloud-Service an einen Web-Browser ausgeliefert (statischer Web-Content). Dieser Weg entspricht dem OZG-Nachnutzungsmodell „Einer für Alle". Über das Identity and Access Management (IAM) werden die Mandanten jeweils sicher zugeordnet und verwaltet.

Eine weitere Möglichkeit ist die Nutzung des GDIK Config-Code-Service. Das für die jeweilige Verwaltungsleistung vorkonfigurierte (Nutzung des GDIK Konfigurators) Code-Snippet wird über einen zu einer Konfiguration (Standard Web-Component) generierten Link abgerufen und lokal in das genutzte Formularsystem implementiert. Im Gesamtkontext ist diese Möglichkeit mit der Anbindung der GDIK nicht gleichzusetzen, da hier noch die lokale Implementierung des erhaltenen Code-Snippet notwendig ist. Das entspricht dem OZG-Nachnutzungsmodell „Nachnutzbare Software dezentral betrieben".

Bei der dritten Variante handelt es sich letztlich um die Verwendung des GDIK Open Source-Code aus GitHub und entspricht ebenfalls dem Nachnutzungsmodell „Nachnutzbare Software dezentral betrieben".

Veröffentlicht wird die GDIK unter der European Union Public License V1.2 (EUPL 1.2)[6]. Diese wurde von der Europäische Kommission im Rahmen der Open Source-Software-Strategie[7] zur Förderung des Einsatzes und der Entwicklung von Open Source-Software entwickelt.

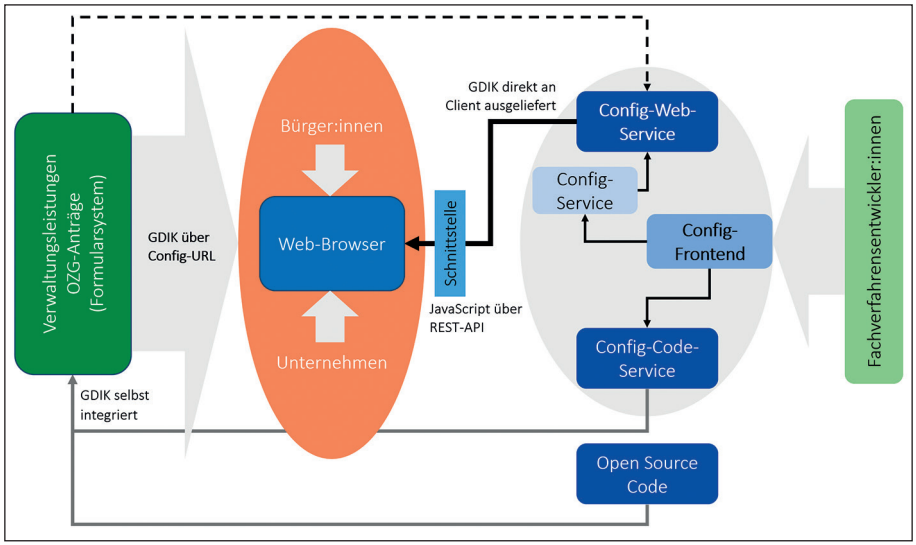

Abbildung 6: Nutzungsszenarien der GDIK

Mit dem Config-Web-Service und dem Config-Code-Service werden zwei Software-as-a-Services (SaaS) angeboten. Um die Konnektivität zu unterschiedlichen Web-Browser-Anwendungen zu gewährleisten, wird die GDIK zunächst im gebräuchlichsten Web-Standard ausgeliefert (s. Abbildung 6). Die Lauffähigkeit in den am Markt relevanten Web-Browsern wird sichergestellt. Im Abstimmungsprozess mit den Softwarefirmen der Formularserver und den Entwicklerinnen und Entwicklern der Fachverfahren in den Ländern können ggf. notwendige weitere Schnittstellen diskutiert und umgesetzt werden.

2.5 Code und Ressourcen

Der Betrieb erfolgt in einer Cloud-Infrastruktur von Microsoft (Azure). Es werden drei voneinander getrennte Bereiche für Entwicklung (Dev), Test und Produktion (Ops/ Prod) vorgehalten.

Gerade auch die konsequente Umsetzung von Infrastructure-as-Code (IaC) mit Nutzung von Plattform-as-a-Service (PaaS) in einer Cloud erzeugt einen Paradigmenwechsel in

6 https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_de.pdf
7 https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en

Entwicklung und Betrieb. Neben der Umsetzung von Sicherheitsanforderungen (u. a. Transparenz und Nachvollziehbarkeit, wer hat was wann getan) oder der jederzeitigen Wiederherstellung vorheriger Versionsstände und der nahezu vollständig gemanagten Cloud-Services durch den Provider, werden hierdurch die erheblichen Ressourceneinsparungen in Entwicklung und vor allem im Betrieb realisiert.

3. Releaseprozess

Das Releasemanagement befasst sich damit, wie Weiterentwicklungen den DevOps-Prozess des Teams durchlaufen. Ziel ist ein jeweils erfolgreiches Release und Deployment der Weiterentwicklung in die Produktions-Umgebung zu gewährleisten. Releasewechsel beeinflussen bzw. unterbrechen die bestehende Nutzung nicht; die einmal eingebundene Komponente wird ununterbrochen ausgeliefert. Neue Funktionalitäten können hinzu konfiguriert werden. Die registrierten Nutzer werden über die eingerichtete Kommunikationsplattform informiert. Einen festen Releasezyklus gibt es nicht, diese werden vom Bedarf bestimmt.

Das Release-Management startet mit dem stetigen Sammeln von Anforderungen. Über einen koordinierten Planungsprozess werden die Anforderungen (Funktionen, Optimierungen, usw.) für das nächste Release mit dem DevOps-Team zusammengestellt. Das DevOps-Team setzt anschließend die im Backlog befindlichen Anforderungen um und stellt den getesteten Code als Release bereit. Hierbei werden u. a. Unit-, Integrations- und Systemtests durchgeführt und der Code zu einem Build (bereitstellbarem Paket oder einer ausführbaren Datei) kompiliert.

Nach dem fachlichen Review und Test folgt die fachliche Freigabe für das Release (s. Abbildung 7).

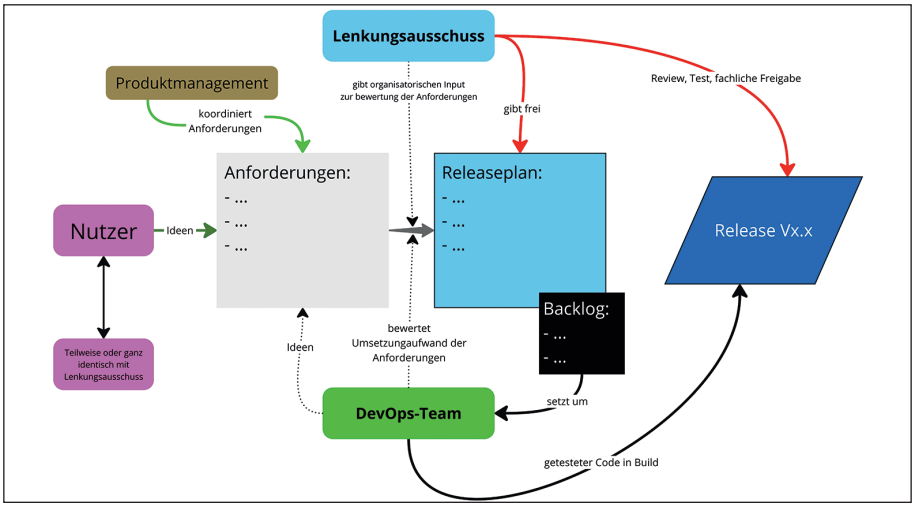

Abbildung 7: Releasemanagement – Prozess

3.1 Rolloutprozess

Der Rolloutprozess konzentriert sich auf die Bereitstellung (Produktion) und IT-Sicherheit der GDIK und ihrer Weiterentwicklung. Ungeachtet der Inhalte des Releases werden immer die gleichen Anforderungen angelegt.

Ein kompletter Deployment-Prozess (Produktion) wird in einer Testumgebung aufgebaut und bereitgestellt. Diese Umgebung und die Prozesse sind identisch mit den Prozessen und der Umgebung der späteren Produktion. Neben funktionalen Tests des Releases erfolgt gegen die Testumgebung auch ein zwingend erforderlicher externer Penetrationstest, um eine Freigabe hinsichtlich der IT-Sicherheit zu erreichen. Diese Freigabe wird durch das LSI entsprechend den Richtlinien des Landes und des Bundes durchgeführt.

Sollten während dieses Prozesses Fehler auftreten, wird das potentielle Release als fehlerhaft betrachtet und ein neues Release muss den Rolloutprozess nach vorheriger Fehlerbehebung erneut durchlaufen. Es erfolgt auch eine Bewertung hinsichtlich der Notwendigkeit einer Fortschreibung von relevanten Konzepten, wenn das Release hier Anpassungen verlangt.

Nach erfolgreicher Testung liegen Code, Pipelines, Container, Infrastruktur usw. für den Betrieb vor. Die Produktionsumgebung wird automatisiert erstellt und das neue Release ersetzt nach Gesamtfreigabe die aktuelle Version (s. Abbildung 8).

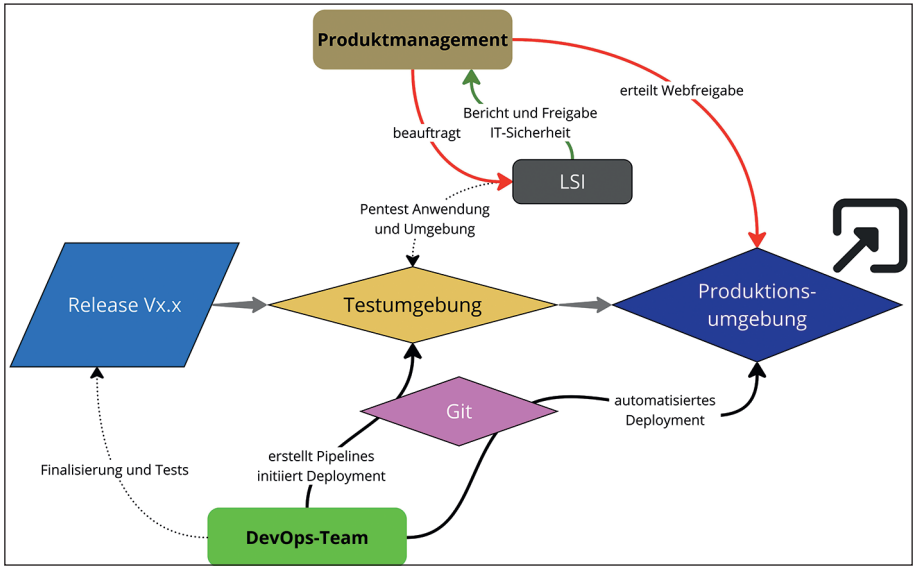

Abbildung 8: Rollout- und Freigabeprozess

3.2 Supportorganisation

Die Nutzerinnen und Nutzer sowie der „Provider“ (hier Freistaat Bayern) des Service sollen eine auf gegenseitigen Vorteil bedachte Beziehung eingehen. Die Nutzerinnen und Nutzer ziehen die Mehrwerte aus den bereitgestellten Produkten und stellen dabei gewisse Anforderungen an die bereitgestellten Produkte. Sie erwarten, dass diese über einen unbefristeten Zeitraum mit einem angemessenen Qualitätsniveau zur Verfügung gestellt werden. Dies umfasst auch Aktivitäten der Anleitung von neuen Nutzerinnen und Nutzern, einen Service Desk für auftretende Störungen und die Aufnahme von sich über die Zeit ändernden Anforderungen. Der Provider erhält im Gegenzug eine für die Leistungserbringung notwendige Vergütung.

Jedoch haben auch die nachnutzenden Länder und der Bund eine gewisse Mitverantwortung. So muss es in jedem nachnutzenden Land eine koordinierende Stelle geben, die die zentrale Verantwortung für die Vertretung der Interessen des Landes hinsichtlich des Supports und der Weiterentwicklung des EfA-Onlinedienstes innehat.

Diese Anforderungen an die Serviceorganisation sind über eine robuste Organisation abgebildet, mit zwei leistungserbringenden Einheiten für Produktmanagement, Kundenbetreuung und Governance Aufgaben sowie für Entwicklung und Betrieb (s. Abbildung 9).

Abbildung 9: Supportstruktur

3.3 Sicherheitsbetrachtung

Die GDIK erfüllt die Mindestanforderungen des BSI-Grundschutzes. Zur Erfüllung der Sicherheitsanforderungen sind umfangreiche organisatorische und technische Maßnahmen für die Gewährleistung der Informationssicherheit nach innen und außen um-

zusetzen. Die Berücksichtigung von Sicherheit in der Softwaresystemarchitektur ist von entscheidender Bedeutung, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Ressourcen zu gewährleisten.

Aufbauend auf einer Risikoanalyse zu möglichen Bedrohungsszenarien erfolgte die Planung der Architektur und Anforderungen an das System. Die herausgearbeiteten Bedrohungen, Schwachstellen und Angriffsvektoren sind in einer Risikoausweisung sichtbar gemacht und nach Schutzbedarf, Eintrittsrisiko und zu erwartendem Schaden klassifiziert. Das DevOps-Team ergreift – soweit technisch möglich – entsprechende Gegenmaßnahmen, um den aufgezeigten Risiken zu entgegnen.

Risikoanalyse und Risikoausweisung sind sogenannte lebende Dokumente und werden während der gesamten Laufzeit stetig aktualisiert. Zusätzlich kommen organisatorische Maßnahmen zum Einsatz, um Risiken zu minimieren, wie z. B. das Prinzip der geringsten Rechte. Es ist sichergestellt, dass die Webservices vor unberechtigter (automatisierter) Nutzung geschützt werden, da die Zugriffsberechtigungen eine Mehrfaktorauthentifizierung (MFA) erzwingen. Für Administratoren sind hier zudem nur FIDO2-Sicherheitsschlüssel und E-Mail-OTP zugelassen. Der IT-Betrieb stellt sicher, dass Zugangsdaten zum jeweiligen Webservice sowie Zertifikate vor unbefugtem Zugriff geschützt werden.

Die GDIK wurde nach einem erfolgreichem Webfreigabeverfahren (Penetrationstest gemäß IKT-Sicherheitsrichtlinie "BayITSiR-14 - Sicherheit von Webanwendungen im Bayerischen Behördennetz") vom LSI für den Betrieb freigegeben.

3.4 Datenschutzbetrachtung

Die GDIK selbst verarbeitet keine personenbezogenen oder sensiblen Daten. Die über die GDIK durch die Antragstellerinnen und Antragsteller erfassten Informationen verbleiben ausschließlich im Client der Nutzerinnen und Nutzer bzw. werden an das umgebende Formularsystem oder Fachverfahren übergeben.

Personenbezogene Daten treten ggf. im Gesamtprozess beim Login-Prozess zum Config-Web-Service auf. Hier wird derzeit der Login über Microsoft Entra ID mit anonymisierten E-Mail-Adressen angeboten. Künftig wird der Login ggf. über BundID möglich sein.

Nach einer umfassenden Bewertung ist nach der aktuellen Konzeption und aktuellem Umsetzungsstand der GDIK mit den enthaltenen Daten keine Datenschutzfolgeabschätzung durchzuführen. Bei der Weiterentwicklung von Funktionalitäten oder der Hinzunahme weiterer Daten ist diese neu zu bewerten. Ziel dabei ist jedoch der datenschutzkonforme Betrieb der Komponente im Allgemeinen. Betrachtungen der Prozesse in angebundenen Fachverfahren sind nicht Teil der folgenden Ausführungen.

4. Digitale Souveränität

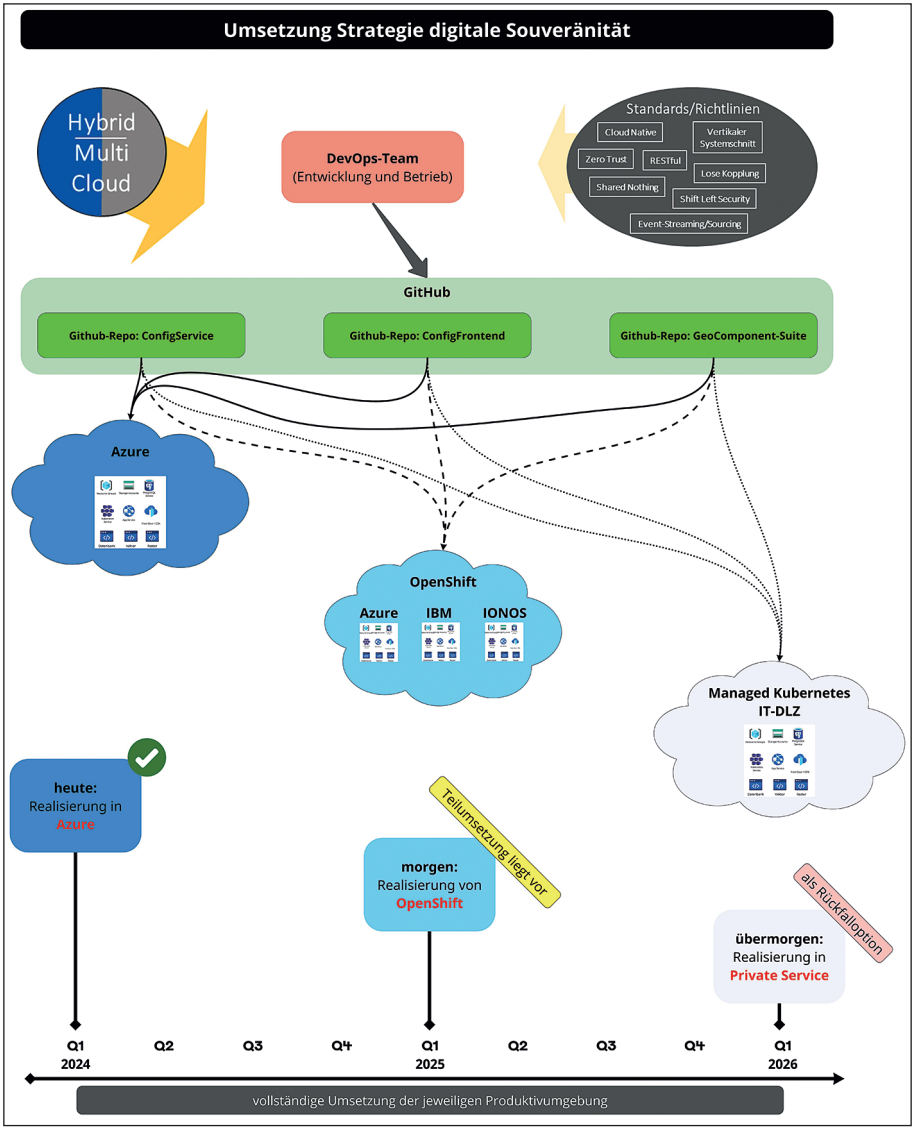

Abbildung 10: hybrider-Multi-Cloud-Ansatz

Im Rahmen der digitalen Souveränität (Eigenständigkeit bei der Gestaltung des Einsatzes digitaler Technologien) werden die modernsten und für einen Anwendungsfall

passendsten Technologien umfassend bewertet, um diese praxistauglich, effektiv sowie flexibel einsetzen zu können. Durch die verstärkte Nutzung von hybriden Multi-Cloud-Angeboten im Sinne eines „Cloud-First-Prinzips" verringert sich außerdem der staatliche Aufwand bei Entwicklung und Betrieb.

Die digitale Souveränität wird im Cloud-Umfeld stark befördert bzw. ist überhaupt erst vorhanden. Tatsächlich innovative Services für Bürger, Unternehmen und Verwaltung lassen sich nur mit modernen Prozessen und Applikationen schaffen, zahlreiche Werkzeuge bietet die Cloud. Es gilt sichere und verlässliche Services in die bundesweite Nutzung zu bringen. Mit Cloud-Computing lassen sich zahlreiche Themenfelder deutlich effizienter oder überhaupt erst umsetzen. Stark vorangetrieben und operational einsetzbar werden die Themenfelder Künstliche Intelligenz (KI) oder Big Data.

Zur sicheren und funktionalen Nutzung werden bestimmte Services vorkonfiguriert (z. B. Härtung) und orchestriert in sogenannten Landing Zones vorgehalten. Dies gilt auch für die genutzten Ressourcen der Azure-Cloud des bayerischen IT-Dienstleistungszentrums. Der genutzte Azure-Tenant hat erste Härtungsmaßnahmen erfahren, die aktuell noch deutlich erweitert werden.

Die häufig geführte Diskussion über die digitale Souveränität mit Augenmerk auf europäische oder gar deutsche Datenräume ist wenig zielführend, da hier insbesondere der vermeintlich sichere Verbleib von oder die Zugriffsmöglichkeit auf Daten im Fokus steht. Für Daten die ohnehin redundant bei den Ländern und dem Bund lokal vorliegen und zudem noch Open Data sind, stehen andere Punkte im Fokus. Der Cloudbegriff ist heute erheblich mehr als nur der Zusammenhang mit dem Ort der Datenspeicherung, es geht vor allem um die Nutzung und Verknüpfung von Services. Aktuelle Veröffentlichungen des BSI oder der Deutschen Verwaltungscloud orientieren sich ebenfalls an dieser geänderten Betrachtung.

Die Abbildung 10 zeigt die Strategie eines hybriden-Multi-Cloud-Ansatzes auf und interpretiert die digitale Souveränität insbesondere als technologische Weiterentwicklung und ökonomische Flexibilität. So sollen neuartige oder kosteneffizientere Services einzelner Provider schnell angebunden werden können; mit OpenShift bietet sich hierzu aus heutiger Sicht eine erste Lösung. Die Entwicklung einer Rückfalloption ist weniger durch die Besorgnis vor der Abhängigkeit von international tätigen Providern getrieben, sondern vielmehr als Möglichkeit einer künftigen Einbindung datenschutzrelevanter Daten oder des Betriebs von Services mit besonderen Sicherheitsanforderungen in den hybriden-Multi-Cloud-Ansatz. Aktuell finden sich im Projekt GDIK keinerlei derartige Daten oder Dienste.

Neben der primären Betriebsinfrastruktur in der Azure-Cloud ist im Sinne der digitalen Souveränität bei der GDIK auch ein Deployment aller Komponenten auf OpenShift-Basis in die IBM-Cloud als Proof of Concept (PoC) umgesetzt und als sekundäres Szenario einsetzbar. Als Rückfallszenario soll bis Ende 2024 auch noch der Betrieb im Managed Kubernetes des IT-DLZ getestet werden. Als dauerhafte Variante wird dies nicht ange-

strebt, da es für das vorliegende Projekt deutlich vorteilhafter ist, in einer Public-Cloud-Infrastruktur zu verbleiben.

5. Ausblick

Neben dem Bund und einzelnen Ländern warten auch schon die bayerischen Kommunen auf die Einbindung der GDIK in kommunale Antragsprozesse. Die GDIK wurde für die Nachnutzung in die BayernPackages aufgenommen. Unter allen verfügbaren EfA-Leistungen der BayernPackages wurde die GDIK als Einzige sowohl von den Bezirken als auch vom Städte-, Landkreis- und Gemeindetag zur Nachnutzung ausgewählt. Dies ist ein erfreuliches Signal und verdeutlicht die vielfältige Einsetzbarkeit der GDIK.

Zum derzeitigen Stand wollen drei Länder die GDIK nachnutzen, sechs weitere Länder sind an einer Nachnutzung interessiert.

Die GDIK – konzipiert mit Gedanken aus der GDI, Daten standardisiert in eine Nutzung zu bringen – macht die Geodateninfrastruktur mit all ihren Bereichen sichtbar. Das Lenkungsgremium der GDI-DE hat eng die Entwicklung der GDIK begleitet und befürwortet deren Nutzung. Die moderne Architektur der GDIK wurde durch die GDI-DE untersucht und als kompatibel und zukunftstauglich bewertet.

Die GDIK ist ein Werkzeug von Experten für die einfache Geodatennutzung in vielen Anwendungen und schafft vielerlei Mehrwerte.