



# Open API – offene Daten professionell anbieten und nutzen

Leitfaden

### Herausgeber

Bitkom  
Bundesverband Informationswirtschaft,  
Telekommunikation und neue Medien e. V.  
T 030 27576-0  
bitkom@bitkom.org  
www.bitkom.org

### Ansprechpartner

Dr. Frank Termer | Bitkom e. V.  
T 030 27576-232 | f.termer@bitkom.org

### Verantwortliches Bitkom-Gremium

AK Open Data / Open API

### Projektleitung

Michael Binzen | DB Systel GmbH

### Satz & Layout

Katrin Krause | Bitkom e. V.

### Titelbild

© Markus Spiske – Unsplash

### Copyright

Bitkom 2019

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht KEIN Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom.

# Inhaltsverzeichnis

Danksagung	4
Autoren	5
<b>1 Bedeutung und Relevanz des Themas Open API</b>	<b>7</b>
<b>2 Hintergründe</b>	<b>10</b>
2.1 Einordnung – kontextuell und historisch	10
2.2 Open als Konzept	11
2.2.1 API Manifest	11
2.2.2 Definition	12
<b>3 Sektorspezifische Relevanz und Einsatzszenarien</b>	<b>14</b>
<b>4 Fünf Mythen zu OpenAPI</b>	<b>17</b>
Mythos 1: Alles offen, oder was?	17
Mythos 2: »API First« ist doch so 2002	19
Mythos 3: Um APIs kümmern sich eh nur Nerds	20
Mythos 4: Datenschutz verhindert Öffnung (Open Data und Open API)	21
Mythos 5: Öffnung bringt nur Google & Co etwas, wir schaden uns dadurch	21
<b>5 Digitale Geschäftsstrategien mittels Open API implementieren</b>	<b>24</b>
5.1 Von der Geschäftsstrategie bis zur Open API	24
5.2 Potenziale für digitale Geschäftsmodelle mit Open API und Aspekte der Rechtslage	26
5.3 Referenzmodelle für Open API: digitale Ökosysteme und Open API Programme	30
5.3.1 Praktische Betrachtung des Referenzmodells	34
5.3.2 Rollen im Open Ecosystem	35
5.3.3 Systemelemente im Open Ecosystem	37
<b>6 Technisches API-Design</b>	<b>40</b>
6.1 Wechselwirkung Technik – Geschäftsstrategie	40
6.2 Umsetzung der Steuerung und Kontrolle des Zugriffs auf die API/API-Management	40
6.3 Service-Implementierung und Anbindungsoptionen für verschiedene Datenquellen / Bestandssysteme und Szenarien	43
6.4 Security-Aspekte im API-Management	45
6.4.1 Dokumentation	47
6.4.2 Authentifizierung und Autorisierungen	47

<b>7</b>	<b>Fachliches API-Design: Metadaten für Datenkataloge</b>	<b>50</b>
	DCAT	50
	DCAT-AP	51
	GeoDCAT-AP	52
	OAI-PMH	52
	CKAN	52
<b>8</b>	<b>Rechtslage für Open API</b>	<b>54</b>
8.1	Schutz von personenbezogenen Daten	54
8.2	Freier Fluss von nicht-personenbezogenen Daten in der EU	55
8.3	Urheberrechtlicher Schutz von Datenbanken	56
8.4	Open Data Lizenzierung	59
<b>9</b>	<b>Aspekte des Veränderungsmanagements</b>	<b>61</b>
<b>10</b>	<b>Fazit/Zusammenfassung/Ausblick</b>	<b>64</b>

# Abbildungsverzeichnis

Abbildung 1: Open API als Dreh- und Angelpunkt von Bausteinen für Plattformen und Wertschöpfungsnetzwerke _____	7
Abbildung 2: Data Spectrum _____	18
Abbildung 3: Arbeitsschritte des strategischen Managements _____	25
Abbildung 4: Fraunhofer Smart Ecosystems Reference Model _____	31
Abbildung 5: API Management – Aufgaben _____	33
Abbildung 6: Rollen im Open Ecosystem _____	35
Abbildung 7: Systemelemente und Systemlandschaft im Open Ecosystem _____	37
Abbildung 8: »Donut«: Interne/externe Sicht auf API Management _____	41
Abbildung 9: Systematische Übersicht der Komponenten einer API-Management-Lösung _____	42
Abbildung 10: Übersicht verschiedener Implementierungsszenarien des Frontendservices _____	44
Abbildung 11: Absicherung offener APIs über ein Security Gateway _____	46
Abbildung 12: Transaktionsbasierte Autorisierung _____	48

# Tabellenverzeichnis

Tabelle 1: Unterscheidung verschiedener Öffnungsgrade von Daten _____	18
Tabelle 2: Metadaten für DCAT nach Dublin Core Standard _____	51

# Danksagung

Daten werden für Unternehmen, Wissenschaft und den Staat im Zuge der Digitalen Transformation immer wichtiger. So können externe Daten eine wertvolle Anreicherung eigener (Geschäfts-)tätigkeiten ermöglichen, und umgekehrt eigene veröffentlichte Daten einen Mehrwert für andere Akteure schaffen. Durch das Zusammenwirken vieler Organisationen in diesem Feld können so gänzlich neue Geschäftsmodelle umgesetzt werden, die der Gesellschaft zahlreiche Mehrwerte liefern, sowie Prozesse vereinfachen und verbessern. Häufig kann das volle Potenzial von Daten aber nur dann genutzt werden, wenn diese offen zugänglich und leicht nutzbar sind. Dieses Konzept von »Open Data« wiederum bedarf einer technischen Realisierung, die den Anforderungen moderner Systeme gerecht wird, d.h. Daten müssen maschinenlesbar und möglichst in Echtzeit bereitgestellt werden.

Durch den Arbeitskreis Open Data / Open API wurde mit dem Leitfaden »Open API – offene Daten professionell anbieten und nutzen« eine Publikation vorgelegt, welche die verschiedenen Facetten des Themas zugänglich aufbereitet. In Kapitel 1 wird das Thema motiviert und dessen Relevanz herausgestellt. Kapitel 2 liefert historische Hintergründe und stellt das grundlegende Konzept der Offenheit, die das Grundverständnis bei Open API darstellt, vor. Kapitel 3 beleuchtet Besonderheiten, die bei der Auseinandersetzung mit Open Data und Open API in verschiedenen Sektoren auftreten können. Dabei wird zwischen der Industrieperspektive und der Perspektive des Öffentlichen Sektors differenziert. Das Kapitel 4 greift explizit Mythen auf, die bei der praktischen Umsetzung von Open Data und Open API regelmäßig aufkommen und liefert mögliche Argumentationsketten, um diesen Mythen entgegenzutreten. Den Hauptteil des Leitfadens stellen die Kapitel 5 und 6 dar, in denen auf die verschiedenen Schritte der Entwicklung einer API-Strategie sowie deren technischen Konzeption und Realisierung eingegangen wird. Kapitel 7 stellt einige gängige Beschreibungsformen für Metadaten und Datenkataloge zusammen. Das Kapitel 8 stellt die aktuelle Rechtslage für Open API dar und betrachtet sowohl den rechtlichen Schutz von Daten, den freien Fluss von Daten sowie die Möglichkeiten einer Open Data Lizenzierung. Das abschließende Kapitel 9 liefert Ansatzpunkte, die bei der Umsetzung von Open Data und Open API durch ein geeignetes Veränderungsmanagement zu berücksichtigen sind, bevor das Kapitel 10 ein Fazit zieht und einen Ausblick gibt.

Der vorliegende Leitfaden liefert damit sowohl für die geschäftsseitige als auch für die technische Umsetzung von Open API einen Überblick und einen ersten Einstieg. Dabei wird sowohl die Perspektive der Daten-Konsumenten (Consumer) als auch die der Daten-Anbieter (Provider) aufgegriffen. Der Leitfaden soll damit einen Ausgangspunkt für die notwendige Diskussion zum Einsatz und zur Nutzung von Open API in Unternehmen und Institutionen der öffentlichen Hand darstellen.

An der Erstellung des Leitfadens waren über 20 Personen beteiligt: IT-Spezialist\*innen, Fachexpert\*innen, Jurist\*innen und Wissenschaftler\*innen. Dabei war allen wichtig, sowohl die Anbieter- als auch die Anwenderseite von Open Data abzudecken und vor allem auch die juristische Perspektive einzubeziehen. Denn gerade bei der Frage nach der Konzeption von Open-Data-basierten Geschäftsmodellen und dem urheberrechtlichen Schutz von Daten müssen entsprechende Überlegungen schon von Beginn an mit berücksichtigt werden.

Das gesamte Autoren- und Redaktionsteam wünscht Ihnen eine anregende Lektüre. Wir freuen uns über Ihr Feedback zum Leitfaden und sind für Anregungen zur Verbesserung der Publikation offen.

# Autoren

Johannes Abel | Sopra Steria Consulting

Michael Beutler | LionGate AG

Michael Binzen | DB Systel GmbH

Sebastian Böttger | Capgemini Deutschland GmbH

Lina Bruns | Fraunhofer Institut für Offene Kommunikationssysteme FOKUS

Christian Horn | Freie und Hansestadt Hamburg – Geschäfts- und Koordinierungsstelle GovData

Dr. Till Jaeger | JBB Rechtsanwälte

Marie Jansen | Capgemini Deutschland GmbH

René Kießling | Axway GmbH

Fabian Kirstein | Fraunhofer Institut für Offene Kommunikationssysteme FOKUS

Marc Kleemann | ISB AG

Wolfgang Ksoll | Viderum GmbH

Michael Leibfried | Red Hat GmbH

Tobias Maier | PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Markus Mayer | Axway GmbH

Jelena Mura | Capgemini Deutschland GmbH

Michael Ochs | Fraunhofer Institut für Experimentelles Software Engineering IESE

Cosmina Radu | Capgemini Deutschland GmbH

Dr. Gerald Ristow | Software AG

Antonia Schmidt | Bitkom e.V.

Thomas Sturm | ONEflow GmbH

Dr. Frank Termer | Bitkom e.V.

Dr. Göttrik Wewer | Deutsche Post AG

# 1 Bedeutung und Relevanz des Themas Open API

# 1 Bedeutung und Relevanz des Themas Open API

Ziel dieses Leitfadens ist es, praktische Überlegungen und Hinweise darüber zur Verfügung zu stellen, was Open API ist, wie dieses Konzept auf- und umgesetzt werden kann, um die Unternehmensstrategie zu schärfen, Zielgruppen klarer zu identifizieren und den Wertbeitrag einer Organisation positiv zu beeinflussen. Dieser Leitfaden richtet sich dabei sowohl an Unternehmen der Privatwirtschaft als auch an Behörden und Körperschaften des öffentlichen Rechts sowie zivilgesellschaftliche Organisationen.

Gesellschaftliches und unternehmerisches Handeln ist wie nie zuvor durch die Digitalisierung geprägt bzw. in seinem Erfolg von ihr abhängig. Das prägendste Merkmal der Digitalisierung besteht dabei in der ständigen Verfügbarkeit von digitalen Diensten zu jeder Zeit und an jedem Ort sowie eine fortschreitende Vernetzung der Dienste untereinander. Eine wesentliche Grundlage der Digitalisierung stellt dabei die Interoperabilität über technische Schnittstellen dar, die das Entstehen von neuen Organisations- und Kommunikationsbeziehungen sowie die Etablierung neuer Wertschöpfungsnetzwerke ermöglicht.

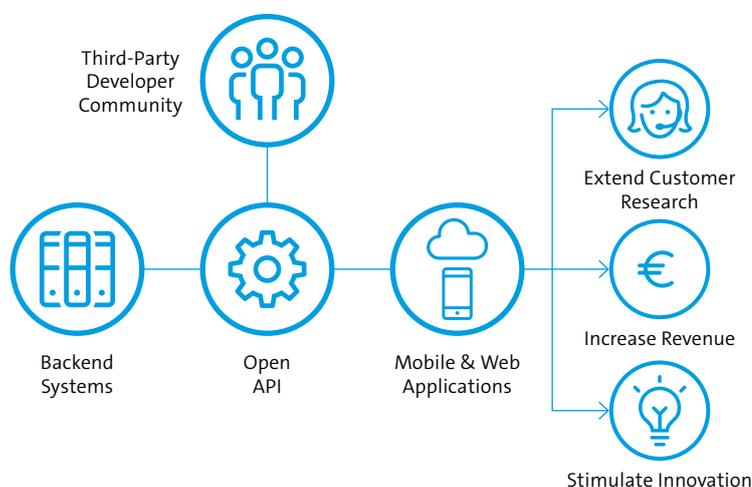


Abbildung 1: Open API als Dreh- und Angelpunkt von Bausteinen für Plattformen und Wertschöpfungsnetzwerke

Durch Open API werden bisher unsichtbare Backend-Systeme für Third-Party Developer sichtbar und nutzbar. Dadurch entsteht in externen App- und Web-Märkten **mehr Kundenreichweite**, die **Umsätze** mit über APIs bereitgestellten Daten können **gesteigert** werden und **Innovationen** werden **stimuliert**.

Die Entwicklung von Fähigkeiten zur Planung, Einrichtung und den Betrieb entsprechender Programmierschnittstellen (API), ist daher sowohl für Unternehmen als auch für Institutionen

der öffentlichen Hand von hoher strategischer Bedeutung. Nur so kann tatsächlich eine konsequente Orientierung an den Logiken der Digitalisierung erfolgen, eine nutzbringende Partizipation an deren Vorteilen erreicht und gleichzeitig die eigene Gestaltungsfähigkeit abgesichert werden. Auf der gesellschaftlichen Ebene ist dies gleichgestellt mit dem Erhalt der Wettbewerbsfähigkeit gegenüber Volkswirtschaften wie den USA oder China. Nur durch den konsequenten Ausbau der entsprechenden Fähigkeiten kann ein Wirtschaftsstandort bestehen, können gesellschaftliche Prinzipien und Regeln wie Datenschutz oder Schutz der individuellen Privatsphäre erhalten werden. »Platforms beat products any time« – dieses Zitat von Prof. van Alstyne beschreibt auf zugespitzte Weise, dass nicht nur durch neue Produkte Mehrwerte und Innovationen geschaffen werden können, sondern zunehmend auch durch die Verzahnung von Services über Sektoren und Organisationen hinweg Innovation und weitreichende Mehrwerte geschaffen werden können. Ähnlich wie in der Industriellen Revolution entstehen durch den Zusammenschluss einzelner Dienste digitale Wertschöpfungsnetzwerke. Der Unterschied in dieser Ausprägung der digitalen Transformation besteht allerdings in einer deutlich höheren Dynamik und Komplexitätszunahme, die organisiert werden muss. Wenn in den Nachrichten über KI – Künstliche Intelligenz, Digitalisierung, Smart (Home|Phone|\*), Predictive Maintenance und die vielschichtigen Diskussionen zu Digitalisierung etc. berichtet wird, dann geht es in der Regel immer um die Bildung dieser Wertschöpfungsnetzwerke im Sinne der Plattformökonomie: Services und die automatisierte Interpretation von Daten werden enger verzahnt, Innovationspotentiale und die Bedeutung von Daten für die Entwicklung unserer Wirtschaft nehmen zu und führen schlussendlich zu einer tiefgreifenden und nur teilweise vorhersagbaren Veränderung unserer Gesellschaft.

Um die Verzahnung, Dynamik und Komplexität digitaler Technologien handhabbar zu machen, werden in der Informationsverarbeitung seit jeher Schnittstellen/APIs (Application Programming Interface) verwendet, die organisatorische und technische Komplexität abstrahieren und zusätzlich einen Vertrag zwischen Konsument und Bereitsteller beinhalten. Der Zugriff auf und von APIs kann abgesichert und kontrolliert werden, was auch das Umsetzen rechtlicher und der genannten vertraglichen Aspekte erlaubt. Der Zusatz »Open« stellt zugleich eine Beschreibung und einen Appell dar. Der Allgemeinheit APIs zur Verfügung zu stellen bedarf einer strategischen Abwägung und folglich einer Entscheidung dahingehend, welche APIs und Services der Allgemeinheit bereitgestellt und welche nicht öffentlich verfügbar gemacht werden sollen. Schlussendlich gehört auch die Überlegung dazu, wie eine API bekannt gemacht wird, wie sie publiziert wird. Dazu werden im Leitfaden in der Folge Möglichkeiten wie Verzeichnisdienste und Bibliotheken beschrieben, die diverse APIs nach Themen und Relevanz such- und auffindbar machen.

Um zu diesen Themen hinsichtlich der Bewertung aus Sicht der Politik, Verbänden, Gesellschaft und Unternehmen diskurs- und handlungsfähig zu werden, soll dieser Leitfaden einen grundsätzlichen Überblick und vertieftes Verständnis schaffen.

# 2 Hintergründe

## 2 Hintergründe

### 2.1 Einordnung – kontextuell und historisch

Unter »Open API« wird das Konzept einer offenen »Application Programming Interface« (Programmier-Schnittstelle; oft auch als öffentlich zugängliche API bezeichnet) verstanden, d. h. eine öffentlich verfügbare Anwendungsprogrammierschnittstelle, die Entwicklern programmgesteuerten Zugriff auf eine Softwareanwendung oder einen Webservice bietet. Spezifikationen von APIs sind Anforderungen, die festlegen, wie eine Anwendung mit einer anderen kommunizieren und interagieren kann. Im Gegensatz zu einer privaten API steht eine offene API grundsätzlich allen Entwicklern öffentlich zur Verfügung. Das Konzept einer offenen API besteht darin, dass die API in erster Linie aus Open-Source-Modulen besteht oder zumindest für eine Überprüfung und Verwendung offen sein sollte. Eine offene API kann auseinander-genommen, zu neuen Dingen (weiter-) entwickelt oder auf freie Weise ge- und verändert werden. Sie ermöglicht Entwicklern außerhalb einer Organisation z. B. den Zugriff auf Backend-Daten, die in deren eigenen Anwendungen verwendet werden können, etwa zur Anreicherung von Informationen.

Seitens der technischen Spezifikation von OpenAPI, die ursprünglich als »Swagger-Spezifikation« bekannt geworden ist, reicht die Historie bis ins Jahr 2010 zurück.

OpenAPI<sup>1</sup> ist in diesem Kontext eine Spezifikation für maschinenlesbare Schnittstellendateien zum Beschreiben, Produzieren, Konsumieren und Visualisieren von RESTful-Webdiensten. Ursprünglich Teil des Swagger-Frameworks, wurde es 2016 zu einem separaten Projekt, das von der OpenAPI-Initiative, einem Open Source-Verbundprojekt der Linux Foundation, betreut wurde.

Während also einige öffentlich zugängliche, offene APIs möglicherweise die OpenAPI-Spezifikation verwenden, ist OpenAPI demnach kein Synonym für offene APIs.

Es ist empfehlenswert Open APIs generell als Open Source zu deklarieren. Dies ist aus juristischer Sicht notwendig, weil sonst eine unklare Rechtslage provoziert wird (siehe aktuellen Rechtsstreit zwischen Oracle und Google<sup>2</sup>). Hierzu gibt es noch keine höchstrichterlichen oder gar internationalen Entscheidungen.

---

1 Also ist **OpenAPI** (zusammengeschrieben) die aktuelle Bezeichnung für die ursprüngliche Swagger-Spezifikation. **Open API** (mit Leerzeichen dazwischen) wird in diesem Leitfaden als die allgemeine Bezeichnung von offenen Schnittstellen verstanden.

2 [https://en.wikipedia.org/wiki/Application\\_programming\\_interface#Copyright\\_controversy](https://en.wikipedia.org/wiki/Application_programming_interface#Copyright_controversy)

## 2.2 Open als Konzept

In diesem Leitfaden wird Open im Sinne der Definition aus dem Leitfaden »*Open Data – Neue Konzepte erfolgreich umsetzen*« vom 17.01.2018<sup>3</sup> verwendet.

### 2.2.1 API Manifest

Wir greifen die im ursprünglichen Open-Data-Manifest<sup>4</sup> formulierten Aussagen auf und beleuchten die folgenden Aspekte:

1. Offene Schnittstellen schaffen Interesse, Verständnis und Vertrauen, wenn dadurch Entscheidungen nachvollziehbar, d. h. transparent werden. Wenn Entscheidungsprozessen zugrunde liegende Daten offengelegt werden, werden offene Schnittstellen damit dem wachsenden Interesse in der Gesellschaft nach einer möglichst frühen und ganzheitlichen Mitsprache gerecht und können die Mündigkeit der beteiligten Bevölkerung stärken.
2. Offene Schnittstellen beschleunigen Modernisierung und Innovationen, indem hierarchie- und organisations-unabhängig über offene Schnittstellen innovative Lösungen schnell prototypisch umgesetzt und wieder zurück in die eigene Organisation gespielt werden können. Offene Schnittstellen sind damit ein wichtiger Wirtschaftsmotor, der auf Basis der zugrundeliegenden Daten völlig neue Geschäftsmodelle ermöglicht, die wiederum die Digitalisierung voranbringen.
3. Offene Schnittstellen schaffen Raum für diskriminierungsfreie Mehrwertdienste für alle, indem auch Dritte in die Lage versetzt werden, für eigene Zielgruppen spezialisierte Dienstleistungen anbieten zu können. Offene Schnittstellen ermöglichen damit auch für solche Nutzerkreise neue Mehrwerte, indem an die Stelle eines wirtschaftlichen Zwecks ehrenamtliche Ziele treten können.
4. Offene Schnittstellen demokratisieren Datenhoheit für offene Ökosysteme, indem Daten offen für jedermann, entgeltfrei und ohne Einschränkung verfügbar sind und damit die Basis für robustere und nachhaltige Lösungen darstellen. Offene Schnittstellen hebeln damit bereits im Kern mögliche Monopolbildung aus, in dem durch die Verfügbarmachung von Daten ein freier, wettbewerblicher Markt ermöglicht wird.
5. Offene Schnittstellen machen Funktionen von Backend-Systemen nutz- und sichtbar. So schaffen diese, genau wie Open Data, die Grundlage für neue digitale Märkte und Services und sind so Basis für eine digitale Plattformökonomie.

---

3 siehe <https://www.bitkom.org/Bitkom/Publikationen/Open-Data-Neue-Konzepte-erfolgreich-umsetzen.html>

4 <https://www.bitkom.org/Bitkom/Publikationen/Open-Data-Neue-Konzepte-erfolgreich-umsetzen.html>

## 2.2.2 Definition

»Open API sind offene Schnittstellen für ungefilterte und maschinenlesbare elektronische Daten, die jedem öffentlich, zweckfrei und unverbindlich zur Verfügung gestellt werden. Der Zugriff ist jederzeit und ohne Begründung möglich. Sie werden unverzüglich und entgeltfrei zur uneingeschränkten Weiterverwendung für jedermann einfach angeboten.«<sup>5</sup>

Die Schlüsselaspekte dieser Definition sind hierbei:

- **Ungefiltert und maschinenlesbar:** Die Daten liegen digitalisiert vor und sind entweder noch gar nicht bearbeitet, oder die Art und der Umfang der Bearbeitung (z. B. einfache und offensichtliche Fehlerbehebungen) sind explizit gemacht.
- **Öffentlich und zweckfrei:** Die nicht schutzwürdigen Daten (d. h. unbedenklich aus Sicht des Urheberrechts, ohne Personenbezug oder Sicherheitsbedenken) werden im Internet offen und nicht auf einen unmittelbaren Nutzen ausgerichtet angeboten.
- **Uneingeschränkte Weiterverwendung:** Die Nutzer von offenen Schnittstellen können beliebige Geschäftsmodelle auf Basis dieser Schnittstelle umsetzen, ohne dass es dafür einer Registrierung oder einer einschränkenden Lizenz bedarf.
- **Einfach angeboten:** Beim Angebot gilt es, zumindest zwei Aspekte zu berücksichtigen:
  - Einfach **auffindbar** – Die Schnittstelle sollten in entsprechenden Open API-Portalen gelistet und die nötige Beschreibung (z. B. Metadaten) ebenfalls direkt zugänglich sein.
  - Einfach **nutzbar** aus Sicht der Nutzer – die Schnittstelle sollte in gebräuchlichen Formaten (für Nicht-Fachleute) bereitgestellt werden.

Der Aspekt **unverzüglich** wird durch Open API besonders gut adressiert, weil technisch hier die geringste Verzögerung möglich ist. Dies wird häufig mit dem Begriff Echtzeit<sup>6</sup> adressiert. An dieser Stelle soll dem Lesenden klar werden: Der Aspekt unverzüglich ist ein primärer Treiber<sup>7</sup> für den Übergang von Open Data zu Open API.

Was an dieser Stelle explizit betont werden muss: Mit dieser Definition wird ausgeschlossen, dass über offene Schnittstellen **personenbezogene Daten** verarbeitet werden können. Diese fallen eindeutig unter die Kategorie schutzwürdig und sind per Definition keine offenen Daten.

Der Umgang in der Praxis bzw. was bei personenbezogenen Daten zu beachten ist, wird im Kapitel [↗ »Schutz von personenbezogenen Daten«](#) im Detail erörtert.

5 übernommen und angepasst auf offene Schnittstellen

6 Dieser Begriff bedeutet üblicherweise »unmittelbare Reaktion«, was aber im Sinne der Informatik für den jeweiligen Kontext genauer definiert werden muss. Genau dieser »Echtzeit«-Aspekt ist die funktionale Erweiterung zu Open Data, weil statische Daten im Download dies nicht bieten.

7 Dies ist sozusagen die Consumer-Sicht. Aus Provider-Sicht ist der Zugang zu neuen Märkten ebenfalls ein primärer Treiber.

# 3 Sektorspezifische Relevanz und Einsatzszenarien

## 3 Sektorspezifische Relevanz und Einsatzszenarien

Das Thema Open API kommt derzeit im öffentlichen Sektor getrieben durch Open Government Data im Zusammenhang mit Echtzeitbetrieb, d. h. der schnellen Verfügbarkeit von öffentlichen Daten, zum Tragen. In der Wirtschaft werden Geschäftsmodelle basierend auf der Idee der Plattformökonomie relevant, was ebenfalls Open API-Strategien erforderlich macht.

Insbesondere die Unterscheidung zwischen Privatwirtschaft und öffentlicher Hand ist bei der Betrachtung von Anwendungsfällen durchaus relevant und hilfreich, da sowohl Zielsetzungen als auch Rahmenbedingungen teilweise signifikant anders sind. Nachfolgende Beispiele sollen die Vielfalt an Anwendungsfällen illustrieren:

- **Industrie: Internet of Things / Industrie 4.0**

Im Bereich IoT / Industrie 4.0 sind besonders Aspekte der Echtzeitkommunikation zwischen einzelnen Objekten relevant und stellen das Design eines Open-API vor besondere Herausforderungen. Das Zusammenspiel von Software und Hardware, bspw. durch die Einbindung unterschiedlicher Devices wie Mobiltelefone, Sensoren, intelligente Geräte, Mikrocontroller, müssen bei der Konzeption und im täglichen Betrieb berücksichtigt werden. Hier ist Interoperabilität sehr wichtig, die durch offene Standards begünstigt wird.

- **Industrie: Open Banking**

Durch die Payment Services Directive 2 (PSD2) sind Banken verpflichtet, Dritten (bspw. Zahlungsdiensteanbietern) Zugang zu Konten und Kundendaten zu geben. Die dafür erforderlichen Schnittstellen sind offen im Sinne der Verfügbarkeit für alle Anbieter und können u. a. auch als Open API bereitgestellt werden. Hier liegen besondere Herausforderungen im Bereich der Autorisierung und Authentifizierung, da auf sehr sensible Daten zugegriffen wird.

- **Industrie: Telekommunikation**

Das Open API-Manifesto des Branchenverbands TM Forum bewegt führende Telekommunikationsanbieter und -ausrüster dazu offene Schnittstellen anzubieten, um bspw. die Prozesse um Customer Management, Bestellungen oder auch Produktkataloge verfügbar zu machen.

- **Öffentlicher Sektor: Open Government / Open Data**

Auf der EU-Ebene sind Open APIs ein wichtiger Teil der Vision um die Verwirklichung des digitalen Binnenmarktes und der Schaffung eines gemeinsamen europäischen Datenraumes. Durch die PSI-Richtlinie gelten spezifische Vorgaben für alle Länder der EU. Ergänzt durch bspw. das Open-Data-Gesetz in Deutschland und flankiert von entsprechenden Portalen für Open Data, bspw. GovData in Deutschland oder Data.gov in den USA, zeigt sich die hohe Relevanz im Bereich Public Sector.

- **Öffentlicher Sektor: Public Internet of Things**

Einsatzszenarien für IoT im öffentlichen Sektor bestehen grundsätzlich immer dann, wenn Daten, die von mit Sensoren ausgestatteten physischen Objekten bereitgestellt werden direkt oder indirekt in Arbeitsprozesse eingespeist werden können. Naheliegende Anwendungsfälle können dabei insbesondere in den Politikfeldern, die in hohem Maße mit der Aufsicht, Wartung und logistischen Steuerung von physischen Entitäten befasst sind (z. B. Umwelt, Verkehr, Bau, Verteidigung), jedoch auch darüber hinaus identifiziert werden (z. B. Gesundheit, innere Sicherheit/Katastrophenschutz).

- **Öffentlicher Sektor: Geodaten**

Geobasisdaten beschreiben die Topographie und sind die räumliche Bezugsbasis für unterschiedlichste Anwendungen, bspw. für eine Wander- oder Freizeitkarte. Geofachdaten im Speziellen sind fachliche oder thematische Informationen. Dazu zählen bspw. statistische Daten wie die Bevölkerungsdichte oder Geodaten der Umweltverwaltungen wie z. B. Kompensationsflächen oder Schutzgebiete. Mit der Umsetzung der europäischen INSPIRE Richtlinie wurde und wird seit 2007 ein sehr umfangreiches Geodateninventar geschaffen, in dem sowohl Datenbeschreibungen (sog. Metadaten) digital in Katalogdiensten registriert sind und Geodatendienste über Geodatenportale digital und öffentlich verfügbar gemacht werden.

- **Öffentlicher Sektor: Umsetzung des Onlinezugangsgesetz (OZG)**

Mit der Umsetzung des OZG sollen Bund, Länder und Kommunen 575 Verwaltungsleistungen bis 2022 über Verwaltungsportale digital anbieten und diese Portale zu einem Verbund verknüpfen. Damit aber digitale Verwaltungsangebote über alle föderalen Ebenen und fachlichen Grenzen hinweg funktionieren, bedarf es Schnittstellen. Wie diese konkret ausgestaltet werden sollen, ist momentan noch unklar und muss diskutiert werden. Open API bieten hier eine Möglichkeit, damit sich unterschiedliche Akteure (vom kommunalen IT-Dienstleister bis zum IT-Dienstleister des Bundes) flexibel anbinden können. Die Chancen, die dezentrale, innovations- und wettbewerbsfreundliche E-Government-Lösungen bieten, sind enorm und sollten dringend ergriffen werden.

# 4 Fünf Mythen zu OpenAPI

## 4 Fünf Mythen zu OpenAPI

Dass Open API ein mächtiges Konzept ist, davon zeugen bereits die Anfangskapitel. Doch welche Mythen ranken sich um »Open API«, was sollte berücksichtigt werden, bevor ein solches Konzept oder gar eine solche Handlungsmaxime bzw. Architektur-Entscheidung eingeführt wird?

Die nachfolgenden fünf Mythen lassen sich dabei unter dem Schlagwort »Open API falsch verstanden« subsumieren.

### Mythos 1: Alles offen, oder was?

*Man öffnet einfach seine kompletten Systeme. Damit bekommt man Innovation quasi umsonst, weil alle Welt sich auf diese offenen Schnittstellen stürzt. Es verbessert den Ruf, weil man das Image einer weltoffenen Organisation bekommt. Durch diese Schnittstellen-Fixierung werden alle Systeme auch besser strukturiert und das verbessert die Wartung und die Übersicht über alle Systembeziehungen. Wo Amazon damit erfolgreich war und ist, da kann das sicher nicht schaden.*

So naiv formuliert ist es sicher ein Mythos und die Öffnung wird wahrscheinlich scheitern.

Wer eine API der Öffentlichkeit und damit den Zugriff auf entsprechende Datenbestände freigibt, ohne sich vorab Gedanken über Auswirkungen und dadurch geschaffene Einfallstore zu machen, der denkt zu kurzfristig und wird die entstehenden Herausforderungen und Risiken nicht beherrschen können.

Es stellen sich grundsätzliche Fragen bei der Offenlegung und Nutzung öffentlicher APIs. Denn die Öffnung soll nicht alle anderen etablierten Geschäftsmodelle ersetzen, sondern sinnvoll ergänzen und damit neue Märkte und Innovation erschließen. In der Gesamtbetrachtung muss die Öffnung also als ein Aspekt in die bestehende Unternehmenslandschaft eingefügt werden.

Angelehnt an das »Data Spectrum« des Open Data Institute (ODI, London) kann bei der Veröffentlichung eine Abstufung des Zugriffs auf Daten und/oder Funktionen durch die API in folgende Stufen vorgenommen werden: Closed, Shared und Open. Damit lassen sich Aspekte von geheimhaltungsrelevant bis frei zugänglich einem klaren Schema zuordnen und durch entsprechende Detail-Abstufungen wie z. B. der nicht freien Zugänglichkeit (»closed«) mit einem personenbezogenen Zugriff (»named«) granular verwalten (siehe Abbildung 2).

Diese Zuordnung sollte nie durch technische Belange getrieben sein, sondern das Ergebnis einer strategischen Geschäftsentscheidung sein. Die Schnittstelle wird beim Prinzip »API First« (siehe nachfolgender Mythos) immer so entwickelt, das sie technisch einfach und schnell geöffnet werden kann. Faktisch werden die Zugriffsrechte dann in Abhängigkeit verschiedener Rahmenbedingungen wie z. B. Vertraulichkeit der Daten/Funktionen, der Marktsituation oder der Gesetzeslage festgelegt.

Die nachfolgende Grafik verdeutlicht die Abstufung nach ODI:

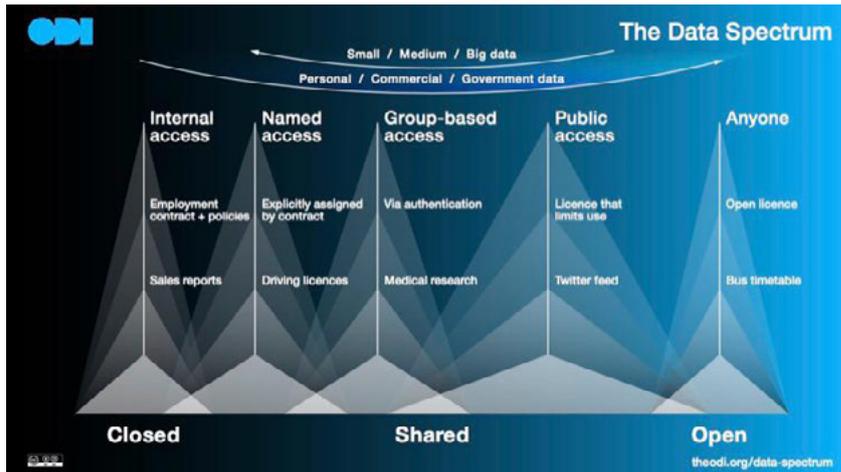


Abbildung 2: Data Spectrum (Quelle: Open Data Institute)

Mit dieser Struktur kann sichergestellt werden, dass sowohl der Geschäftszweck bzw. der hoheitliche Auftrag berücksichtigt wird als auch die positiven Auswirkungen der API-Economy voll genutzt werden können. Da einige wesentliche Aspekte dieser Abstufung aus dem Bild schwer erkennbar sind, werden diese in der nachfolgenden Tabelle erläutert:

Grad der Öffnung	Nutzung: Daten/API sind ...	Verwendung & Nutzer	Grundlage	Beispiel
<b>Open</b>	für jeden <i>umfassend</i> und <i>lizenzgebührenfrei</i> nutzbar	unbekannt	Offene Lizenz	Bus Fahrplan
<b>Public</b>	allgemein zugänglich	bekannt	Beschränkte Lizenz	»Datenhandel«
<b>Shared</b>	für <i>definierten Nutzerkreis</i> <sup>9</sup> frei zugänglich	bekannt	Lizenz beschränkt auf definierten Nutzerkreis	Medical Research
<b>Private</b>	nur dem Erzeuger und Ausgewählten bekannt und zugänglich (Kosten?)	bekannt	Einzelvertrag (Punkt zu Punkt)	individuelle Schnittstellenvereinbarung
<b>Closed</b>	nur Erzeuger bekannt und zugänglich	nur dem Erzeuger bekannt	»Besitz«	?

Tabelle 1: Unterscheidung verschiedener Öffnungsgrade von Daten

<sup>8</sup> Shared kann im Konzern zwischen Konzerngesellschaften implizit oder im Branchenverband durch Mitgliedschaft vereinbart werden. Grundlage ist dann ein Group Based Access, der über eine entsprechende Organisationsstruktur automatisch einen Zugriff etabliert.

Die Begrifflichkeit des ODI Spectrum und insbesondere die strikte Definition von Open, wie sie bei Open Data etabliert ist (siehe [↗https://opendefinition.org](https://opendefinition.org)), sollte auch bei API beibehalten werden. Mit einer Einschränkung bzgl. der Registrierung: Aus technischen Gründen sollte auch bei Open API eine Registrierung etabliert werden. Aber: Um öffentlich zugängliche APIs einerseits für den kostenlosen Zugang zu Daten zu nutzen und andererseits auch Bezahlmodelle zu ermöglichen, wird eine Unterscheidung in **Open API** (lizenzgebührenfrei zum Lesen von Echtzeitinformationen) und **Public API** (gegen Registrierung, dann auch Schreibzugriff u. U. gegen Bezahlung) empfohlen.

Einige Details zu dieser Sichtweise sind im [↗Kapitel 5.3.1 »Praktische Betrachtung des Referenzmodells«](#) dargestellt.

## Mythos 2: »API First« ist doch so 2002

*Baue einfach nur noch Schnittstellen, mache Dir keine Gedanken über die spätere Nutzung und Nutzbarkeit. Das wird sich in der Praxis schon von allein ergeben.*

Zu den Fakten: Mit dem Begriff »API First« wird eine Geschäftsstrategie bezeichnet, die insbesondere durch Amazon bekannt wurde. Jeff Bezos hatte 2002 diese Strategie eingeführt, um nicht die Technologie respektive Programmiersprache festzulegen, in der Services entwickelt wurden, sondern lediglich den Outcome von Systementwicklungen in einzelnen Abteilungen.

Folgende Punkte bilden dabei den Kern dieser Strategie:

- Alle Entwickler-Teams werden fortan ihre Daten und Funktionen über Serviceschnittstellen zugänglich machen
- Teams müssen über diese Schnittstellen miteinander kommunizieren
- Es wird keine andere Form der prozessübergreifenden Kommunikation geben: keine direkte Verknüpfung, kein direktes Lesen des Datenspeichers eines anderen Teams, kein Shared-Memory-Modell, keinerlei Hintertüren. Die einzige Kommunikation, die zulässig ist, erfolgt über Serviceschnittstellenaufrufe über das Netzwerk
- Es spielt keine Rolle, welche Technologie verwendet wird.
- Alle Serviceschnittstellen müssen ausnahmslos von Grund auf externalisierbar gestaltet sein. Das heißt, das Team muss planen und entwerfen, um die Schnittstelle für Entwickler in der Außenwelt verfügbar zu machen. Keine Ausnahmen.

Durch diese Vorgabe schuf Bezos ein Netzwerk von Abteilungen und Geschäftsbereichen innerhalb Amazon, die durch den Fluss von Daten und Informationen integriert und zusammengehalten wurden. Unter dem Gesichtspunkt der Softwarearchitektur wurden lose gekoppelte Systeme, Daten und Software für Apps und Abteilungen wiederverwendbar.

Dabei wird beim Entwurf und der Implementierung von Systemen zuerst die Schnittstelle festgelegt, die dann als alleinige Definition sozusagen einen »Vertrag« zur Nutzung der Funktionalität anbietet. Aus Sicht eines Architekten stellt dies ein attraktives Vorgehen dar, weil es technisch bedeutet, Systeme stark zu entkoppeln (sog. »design by contract«). Aus Geschäftsperspektive wird damit ein Produkt definiert, das ganzheitlich und langfristig gestaltet werden muss. Damit wird eine neue Herausforderung dergestalt geschaffen, als dass Schnittstellen aus der Technik-Welt »ans Licht der Öffentlichkeit« gelangen, (Third Party-) Entwickler die neue Kundengruppe werden und diese neuen Produkte vor dem Hintergrund der zunehmenden Bedeutung der Plattformökonomie mit Marketing und Lifecycle-Betrachtung als neues Marktsegment beworben werden müssen.

### Mythos 3: Um APIs kümmern sich eh nur Nerds

*Schnittstellen sind Technik-Kram und haben keinen Business Impact. Die Nerds spielen mit so einem Zeug, aber für geschäftliche Entscheidungen hat das keine Relevanz. Und wenn, dann nur für typische Internet-Firmen.*

Trotz aller Überlegungen und ggf. Notwendigkeiten zur Durchführung von Due Dilligence-Prüfungen im Kontext der Nutzung von Open APIs sollte dieses Thema nicht als technologisches Nischenthema abgetan werden – die Vorgehensweise von Jeff Bezos (siehe Mythos Nr. 2) zeigt deutlich welches Potential dieses einstige »Tech-Thema« bietet:

Durch die Einführung einer API-First-Kultur konnte Jeff Bezos innerhalb des Unternehmens unglaubliche Effizienzsteigerungen erzielen und sicherstellen, dass es eine universelle Sprache für die Kommunikation zwischen verschiedenen Teilen des Amazon-Systems gab. Einige dieser Teile waren so gut, dass sie als eigenständige Teile einer breiteren Öffentlichkeit zugänglich gemacht werden konnten – Basis der heutigen Service-Dienstleistung »Amazon Web Services (AWS)«, das den einstigen Buchhändler zum Global Player der Internet-Ökonomie gemacht hat.

Wie auch das nachfolgende Strategie-Kapitel zeigt, ist es notwendig hier vom Endanwender her zu denken – egal ob der nun Kunde, Antragsteller oder Bürger heißt.

## Mythos 4: Datenschutz verhindert Öffnung (Open Data und Open API)

*Alle reden von Datenschutz, jetzt soll ich die Daten öffnen – wie passt das zusammen? Verstoße ich da nicht gegen die DSGVO und andere Richtlinien?*

Der Umgang mit Daten erfordert immer Sorgfalt – ganz gleich, ob sie intern verwendet, verkauft oder frei zugänglich gemacht werden sollen. Die Datenschutzbestimmungen personenbezogener Daten sollen dafür sorgen, dass diese Daten nicht in falsche Hände gelangen und missbräuchlich genutzt werden können. Bevor Daten Dritten zugänglich gemacht werden, gehört also immer eine sorgfältige Prüfung dazu, ob es eine entsprechende Rechtsgrundlage dafür gibt und ob die Daten schützenswerte Inhalte aufweisen. Beim Einsatz entsprechender technisch-organisatorischer Maßnahmen wie z. B. nachgewiesene nachhaltige Anonymisierung können grundsätzlich auch personenbezogene Daten zu offenen Daten transformiert werden.

Dabei spielt es keine Rolle, in welcher Form letztlich Daten weitergegeben werden, also ob die Weitergabe als Open Data z. B. über Open API Services oder über einen USB-Stick oder über sonstige elektronische Datenträger erfolgt.

Für die Öffnung der Daten gilt also: Daten, die bisher problemlos an Dritte weitergegeben wurden, können auch als offene Daten über offene Schnittstellen zur Verfügung gestellt werden. Im Gegenteil: eine neue EU-Verordnung stellt seit Mai 2019 die rechtliche Grundlage für den freien Verkehr nicht-personenbezogener Daten innerhalb der EU her.

Die Definition von Open Data impliziert bereits die Berücksichtigung und den Schutz personenbezogener Daten. Insbesondere das Open-Data-Gesetz des Bundes (§ 12a Abs. 3 EGovG) greift diesen Schutz durch den Ausnahmetatbestand und Bezug zum Informationsfreiheitsgesetz (IFG) auf.

Näheres zum Thema Datenschutz ist in [Kapitel 5.2 »Potenziale für digitale Geschäftsmodelle mit Open API und Aspekte der Rechtslage«](#) zu finden.

## Mythos 5: Öffnung bringt nur Google & Co etwas, wir schaden uns dadurch

*In Deutschland gibt es viele wertvolle Daten, aber wenig Kompetenz diese wertbringend zu nutzen. Sobald dieser Datenschatz durch Öffnung allen sichtbar und nutzbar gemacht wird, werden sofort die »üblichen Verdächtigen« Google, Amazon, Facebook, Apple (manchmal erweitert durch Microsoft und/oder Netflix und häufig kurz als GAFA bezeichnet) mit ihren ausgeprägten Analysefähigkeiten und Rechnerkapazitäten diese Daten zu ihrem Nutzen auswerten und gleichzeitig den deutschen Datenbesitzer noch mehr ins Hintertreffen bringen.*

Hier kommt die Angst zum Ausdruck, dass ein »Datenschatz« vorhanden ist, aber eine Organisation nicht fähig ist, damit die Wertschöpfung in neuen Geschäftsmodellen auszureizen. Aufgrund der in den USA anderen Bedeutung von Datenschutz-Aspekten, der dort vorhandenen Rechnerkapazitäten und der fast wöchentlichen Meldungen über die Erfolge der US-IT-Industrie z. B. beim Einsatz von KI mit Daten, wird vermutet, dass Organisationen in Deutschland überhaupt nicht in der Lage seien, dieses »Rennen um Datennutzung« zu gewinnen. Schnell kommt dann die etwas verzweifelte Haltung auf, dass sich diesem Datenkarussell ganz verschlossen wird und damit zumindest dieses Rennen nicht noch mit eigenen Daten zum eigenen Nachteil befeuert wird.

Diese Einschätzung mag in einzelnen Fällen zutreffen und u. U. kann das Zurückhalten von Daten das eine gewisse Zeit verhindern. Auf Dauer **wird der Standort Deutschland** als Ganzes dadurch aber immer **unattraktiver**. Und damit setzt sich eine selbst verstärkende Negativspirale in Gang.

Klar ist, dass nationaler Datenprotektionismus keine Lösung darstellt<sup>9</sup>. Wir müssen uns vielmehr stärken und dann dem Wettbewerb stellen. Sinnvoll wäre also die vermuteten Hemmnisse und Nachteile zu beleuchten und zu prüfen, durch welche Maßnahmen eine »Waffengleichheit« erreicht werden kann. Das kann eine Cloud-Infrastruktur auf europäischer Ebene sein, oder die sehr konkrete lokale Kooperation mit einem führenden Startup. Das erste Beispiel zeigt eine Lösungs-Kategorie, die nur auf nationaler (oder gar EU-) Ebene gemeinschaftlich erreicht werden kann. Das zweite Beispiel dagegen skizziert einen sehr individuellen und auf spezielle Daten-Konstellationen zugeschnittenen Ansatz.

---

9 <https://www.sueddeutsche.de/digital/amazon-facebook-apple-google-microsoft-1.4304826>

# 5 Digitale Geschäftsstrategien mittels Open API implementieren

# 5 Digitale Geschäftsstrategien mittels Open API implementieren

## 5.1 Von der Geschäftsstrategie bis zur Open API

Getrieben durch die Digitale Transformation und den fortschreitenden globalisierten Wettbewerb verlagern immer mehr Organisationen (Unternehmen wie auch Behörden) Wertschöpfung zunehmend oder ganz in Richtung digitaler bzw. digital gestützter Angebote. So angebotene Services oder Daten liefern dabei einen wertvollen Beitrag zum Erhalt von Marktpositionen und deren Ausbau. Auf dem Weg der Entwicklung einer digitalen Geschäftsstrategie kommt jede Organisation zwangsläufig an den Punkt, ihr digitales Angebot an einer extern zugreifbaren und in der einen oder anderen Form offenen Schnittstelle anzubieten. So kann der angebotene Dienst von Konsumenten und auch anderen Organisationen genutzt werden (Vernetzung von Diensten) und letztlich einen Beitrag zum Geschäftserfolg leisten. Durch die Nutzung und Vernetzung von Diensten entstehen digitale Ökosysteme, die auf Basis von digitalen Plattformen Wertschöpfung und Wachstum ermöglichen – ortsunabhängig und zeitunabhängig.

Die Wertschöpfung, die eine Organisation durch ihre API generiert, ist dabei komplex und findet in multiplen Kontexten zwischen digitalen Komponenten einer Strategie und deren Umsetzung in Dienste und Stakeholdern statt. Prozessintegration und die Senkung von internen IT-Kosten sind im Kontext von Open API nicht die vorrangigen Ziele: Es geht vielmehr darum Wertschöpfungskomponenten einer Organisation internen und externen Partnern verlässlich und passgenau bereitzustellen. So können die eigene Strategie umgesetzt und die gesetzten Ziele, wie z. B. Erweiterung des Geschäftsmodells, Erhöhung von Transparenz in oder Beschleunigung von Verwaltungsverfahren, erreicht werden. Dabei ist eine Organisation in der Regel stets Open API-Anbieter und zugleich auch Open API-Nutzer – also Provider und Consumer von Open API.

Die zentralen Vorgaben für Design, Entwicklung und Betrieb von Open API leiten sich aus der Geschäftsstrategie einer Organisation ab. Die Digitalstrategie muss dabei in der Geschäftsstrategie eingebettet sein.

Planung und Entwicklung von Open API und der erforderlichen Infrastruktur einerseits und die operative Umsetzung von Open API andererseits müssen folglich in der für die Geschäftsstrategie verantwortlichen Ebene in der Organisation verankert werden und über die Enterprise-Architektur auch mit dieser Ebene verknüpft sein.

Der Prozess der Digital- und Open API-Strategie sowie die produktive Open API zur Bereitstellung der Dienste selbst liefern einer Organisation strategische Informationen und Kennwerte, wie z. B. Innovationen im Markt oder beim Wettbewerb, Vertriebsmöglichkeiten/Partner, Nutzerverhalten, Systemverhalten, Sicherheitsvorfälle. Diese können für die Weiterentwicklung der Geschäftsstrategie eingesetzt werden.

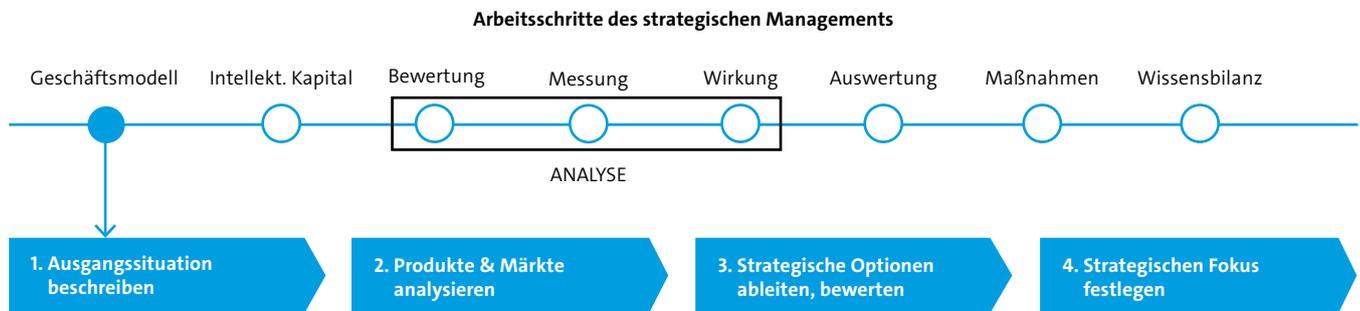


Abbildung 3: Arbeitsschritte des strategischen Managements (Quelle: Leitfaden »Strategische Ziele entwickeln«, Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK, Berlin, 2014)

In Abbildung 3 ist ein möglicher Prozess für das strategische Management und die Entwicklung einer fokussierten Geschäftsstrategie dargestellt. Solche Prozesse sind in der Lage, passgenau die für Design, Entwicklung und den Betrieb von Open API relevante Aspekte der Geschäftsstrategie bereitzustellen. Unternehmen, die Ihr Geschäftsmodell auf Open API aufbauen bzw. um Open API anreichern möchten, sollten daher einen zumindest pragmatisch orientierten Strategieprozess anstoßen und durchlaufen. Die Schritte in Abbildung 3 können dabei eine Leitlinie für ein solches Vorgehen darstellen.

Dabei erscheint eine Digitalstrategie insbesondere für KMU der deutschen Wirtschaft von besonderer Bedeutung: hierin liegt hohes Potenzial für Wachstum und langfristige Sicherstellung des Bestehens des jeweiligen Unternehmens. Unternehmen können dabei eine Reihe von möglichen digitalen Wachstumspfaden bei der Entwicklung einer Digitalstrategie und der Anwendung von Open API beschreiten, wie z. B.<sup>10</sup>

- die Integration digitaler Elemente, d. h. die Erweiterung bestehender analoger Produkte durch digitale Elemente wie z. B. Sensorik oder die Verbindung mit digitalen Services zur Aufwertung des Produkts bzw. des Leistungsspektrums des Produkts.
- Konnektivität, d. h. die Vernetzung von Objekten und Diensten, um eine Steigerung der Wertschöpfung zu erreichen und eine größere Bandbreite von verfügbaren Diensten um ein Produkt oder einen Dienst verfügbar zu machen.
- Produkt als Service (Servitization), d. h. statt des Verkaufs eines Investitionsguts einen Wechsel oder eine Ergänzung des Geschäftsmodells, dass ein Produkt auch als Service nur im Bedarfsfall genutzt oder remote gekauft werden kann, wie z. B. Fahrzeuge, Video Games, Online Marketplaces, individualisierte Produkte.

<sup>10</sup> zum Teil inspiriert von »Impulspapier: Wachstumspfade bei der Digitalisierung von Geschäftsmodellen in Industrieunternehmen«, Plattform Industrie 4.0, 27.02.2019

- Applikationen und Dienste, d. h. Ideen für neue Applikation und Dienste z. B. auf Basis von Daten und deren sekundärer Nutzung bieten Potenzial innerhalb von Geschäftsfeldern zu wachsen, Umsätze durch Diversifikation zu steigern und so das Unternehmen langfristig am Markt zu sichern.
- Plattformen: Plattformen haben oft Marketplace-Charakter und eröffnen vielen weiteren Unternehmen, ggfs. sogar Wettbewerbern, einen Zugang zu einem innovativen, zweiseitigen und durch Digitalisierung weltweiten erreichbaren Markt.

Darüber hinaus müssen Prozesse rund um Open API wie z. B. ein Partner Onboarding, ein Ökosystem-Management und auch eine Governance implementiert werden.

In den folgenden beiden Abschnitten werden zunächst Potenziale für digitale Geschäftsmodelle mit Open API, Aspekte der Rechtslage und darauf folgend ein konzeptioneller Ansatz zur Integration von Digitalstrategie und Open API durch Referenzmodelle für digitale Plattformen und Ökosysteme beschrieben.

## 5.2 Potenziale für digitale Geschäftsmodelle mit Open API und Aspekte der Rechtslage

Organisationen, die auf Basis von Open API Geschäftsmodelle ergänzen, kreieren und realisieren wollen, sollten in der Entwicklung grundlegende Aspekte des Geschäftsmodells, Potenziale für Wertschöpfung, relevante Datenquellen, Arten von Dienstleistungen sowie eine das Geschäftsmodell beschränkende oder fördernde Rechtslage mit in ihre Überlegungen einbeziehen.

Die folgende Sammlung von Fragen, Hinweisen und Aspekten dazu beansprucht keine Vollständigkeit, möchte aber Impulse und Anleitung für mögliche Denkrichtungen geben.

### Grundlegendes zum Geschäftsmodell

Die folgende Liste soll Impulse geben und Denkrichtungen zu grundsätzlichen Aspekten digitaler Geschäftsmodelle als Grundlage für Open API aufzeigen:

- Wie kann aus Daten mit Hilfe von Open API Wert generiert werden? Daten als Service, Services auf Basis von Daten, Pooling von Datenquellen als Datenmarktplatz?
- Welche wertschöpfenden Effekten in Markt und Gesellschaft können durch eine Open API unterstützt werden? Welche externen Effekte werden durch die Open API in verschiedenen Wertschöpfungsketten erreicht, wie z. B. die Erhöhung von Transparenz oder Zugänglichkeit durch die Entwicklung von Apps?

- Welchen Wertbeitrag liefert die Open API für die eigene Organisation? Ist direkt mit monetären Effekten zu rechnen? Soll zunächst auf Netzwerkeffekte (Community-Wachstum) gesetzt werden? Sollen auch interne Effekte, wie z. B. die Initiierung von Innovationsprozessen, berücksichtigt werden?
- Welche Möglichkeiten gibt es, das Angebot (Daten, Services) nutzbar zu machen und für wen?
- Gibt hierfür eine greifende Regulierung? Fördert diese das Geschäftsmodell oder behindert sie es eher?
- Wie können sich potenzielle Nutzer und Partner schnell an das Dienstportfolio anbinden, d. h. wie gut und wie schnell funktioniert beispielsweise das Onboarding oder Self-Onboarding für die API und damit der Eintritt in das Ökosystem?
- Wie kann eine sichere und verlässliche Bereitstellung des Dienstes garantiert werden? (Professionalisierung)

## Potenziale und Risiken für Wertschöpfung durch das Geschäftsmodell

Die folgende Liste von Fragen soll ergänzend zum Business Model Canvas Aufmerksamkeit auf deren frühe Betrachtung lenken:

- Ist das Geschäftsmodell tragfähig? Ab wann wird ein positiver Netzwerkeffekt eintreten und eine Monetarisierung stattfinden?
- Was genau ist das Kernangebot (Daten und Dienste) auf lange Sicht?
- Wie sind das Lizenzmodell / das Preismodell zu gestalten? Gibt es freie Angebote? Gibt es eine Staffelung? Gibt es Standard Angebote und Premium Angebote mit Veredelung von z. B. Daten oder besseren Angeboten für Service Levels Agreements?
- Wie können Bedarf und Angebot gezielt aufeinander abgestimmt und gegebenenfalls angepasst werden, ohne dabei grundlegende Änderungen am Geschäftsmodell und in der Konsequenz auch an der Open API zu benötigen?
- Welche Risiken, z. B. in Abhängigkeit vom Grad der Öffnung organisationsinterner Prozesse oder Datenquellen nach Außen, existieren hinsichtlich Sicherheit? Welche Regulierung steht einer Öffnung ggfs. entgegen und wie kann dieser Konflikt aufgelöst werden? Wie beeinflusst das ggfs. eine Open API Architektur?
- Welche Compliance-Regeln und Nutzungsbedingungen sind erforderlich um eine Open API sicher und rechtskonform betreiben zu können?

## Mögliche Datenquellen als Grundlage für Wertgenerierung

Die Möglichkeiten für Datenquellen für Open API und Open Data sind vielfältig. Besonders im Fall von Daten-basierten Dienste und Daten als Dienst selbst sollte die Frage nach den verfügbaren und benötigten Datenquellen möglichst frühzeitig gestellt, beantwortet und in der Folge möglichst stabil gehalten werden. Potenzielle Quellen – auch ist die Liste nicht als abschließend zu sehen – für Daten zur Verwendung in Services über Open API sind:

- Personenbezogene Daten nach Anonymisierung, z. B. Verkehrsdaten Individualverkehr (Standorte von Mobiltelefonen), Kontobewegungen und -umsätze, Gesundheitsparameter, Energie/Ressourcenverbrauch
- Maschinendaten, z. B. Verkehrsdaten (ÖP(N)V, Airlines), Fahrzeugdaten (OBD2), Produktionsdaten, Logistik- und Transportdaten
- Sonstige Daten, z. B. Geodaten, Wetterdaten, Parkplatzsituation in Städten

## Arten und Kategorien von Services

Die Ausrichtung von Services, die über Open API angeboten werden, kann grundsätzlich in drei Klassen gegliedert werden:

- Services für Menschen, z. B. Verkehrssituation, Gesundheitsdienste, Payment, Versicherungen, jeder denkbare Ansatz von Abo- über Freemium-/Premium-Modellen bis hin zu bezahlten Diensten, zweiseitige Marktplattformen, usw.
- Services für Unternehmen, z. B. Marktforschung auf personenbezogenen Daten, Mehrwertdienste für Fahrzeuge, ...
- Services für/mit Maschinen, z. B. M2M Communication, M2M Payment, Predictive Maintenance, usw.

## Rechtliche Aspekte zu Daten und Datenquellen

Neben der Identifikation von möglichen Quelldaten muss auch die relevante Rechtslage beachtet werden. Bei personenbezogenen Daten ist die DSGVO von hoher Relevanz, bietet aber auch Aspekte, die datenbasierte Geschäftsmodelle für Open Data und Open API unterstützen und fördern. Es wird beispielsweise auch geregelt, wie mit personenbezogenen Daten auf Basis einer nachweisbare sicheren und nachhaltigen Anonymisierung umgegangen werden darf: nach nicht mehr reversibler Anonymisierung von personenbezogenen Daten handelt es sich nicht mehr um personenbezogene Daten und die DSGVO hat keine Gültigkeit für diese Daten und deren Verarbeitung (vgl. DSGVO ErwGr 26). Somit wären solche Daten uneingeschränkt verfügbar für Open Data-Zwecke, was klar zeigt, dass Mythos 4 dieses Leitfadens tatsächlich ein Mythos ist. Es ist dabei sehr wichtig zu betonen, dass die Nutzung entsprechender Daten entweder durch

eine vorausgehende technische Maßnahme der Anonymisierung, die sicher nicht reversibel ist, geschehen kann oder es muss eine Rechtsgrundlage für eine sonstige Ausnahmeregelung geben. So können z.B. personenbezogene Daten in Open-API-Konzepten verarbeitet werden, wenn als Rechtsgrundlage eine Einwilligung der betroffenen Person besteht oder die Verarbeitung zur Erfüllung eines Vertrages mit der betroffenen Person erforderlich ist. Die Gesamtheit der möglichen Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten sind in der DSGVO (EU/2016/679) unter anderem in den Artikel 6, 8 und 9 zu finden. Weiterhin wird hier auch die Übertragbarkeit von personenbezogenen Daten (Art. 20) zwischen für die Verarbeitung Verantwortlichen rechtlich erlaubt, wenn eine entsprechende Rechtsgrundlage wie z. B. eine Einwilligung oder ein Vertrag mit der betroffenen Person vorliegt. Genau genommen verbietet Art. 20 sogar die Behinderung von Datenübertragung und erlaubt somit das Aufbrechen bestehender Datensilos im Hinblick auf personenbezogene Daten.

Zusätzlich besteht mit der Verordnung EU/2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (gültig seit Mai 2019) eine weitere Regelung für den freien Verkehr von Daten in der Europäischen Union. So wird die durch die DSGVO geregelte Datenübertragbarkeit personenbezogener Daten innerhalb der Europäischen Union um den freien Verkehr nicht-personenbezogener Daten wie z. B. elektronische Unternehmensdaten, Verkehrsdaten, Wetterdaten oder Daten von Behörden ergänzt. Genauso soll auch der Zugriff auf Daten in anderen Ländern z. B. durch Behörden nicht behindert werden. So entsteht gemeinsam mit der DSGVO die rechtliche Grundlage für einen freien Datenverkehr in der EU (»Data Schengen«), der mit der Digitalisierung und zunehmenden datenbasierten Services der Daten als Service selbst immer zentraler und kritischer für erfolgreiches wirtschaftliches und administratives Handeln wird.

Weitere mögliche relevante Aspekte ergeben sich aus dem Leistungsschutzrecht für Datenbankhersteller und dem Urheberrecht. Hier sind z. B. Inhalte, Daten und Dienste Dritter, die in eigene Dienste eingebunden werden, zu berücksichtigen und rechtlich (Lizenzbedingungen) sowie aus Sicht des Geschäftsmodells (Ressourcen, Kosten) zu bewerten. In Bezug auf Maschinendaten ist die Rechtslage noch weitgehend offen. Die Richtlinie zum Urheberrecht im digitalen Binnenmarkt (»Digital Single Market«) vom 19. April 2019 harmonisiert das Text- und Datamining und regelt das Verhältnis zur DSGVO. Hinsichtlich der oben genannten sonstigen Daten treffen Data Provider und Data Consumer bisher meist individuelle Regelungen.

Eine tiefere Analyse und Betrachtung relevanter rechtlicher Aspekte folgt in [Kapitel 8](#).

### 5.3 Referenzmodelle für Open API: digitale Ökosysteme und Open API Programme

Kern jedes digitalen Geschäftsmodells, welches sich in der Implementierung von Open API bedient, sind die Aspekte Business, Technology und Legal. Diese werden im Folgenden erläutert und mit Beispielen unterlegt.

»**Business**«: der Kern des digitalen Geschäftsmodells selbst, z. B. relevante Aspekte aus der Digitalstrategie und der Business Model Canvas, welche durch Open API realisiert werden sollen. Plattformen und digitale Ökosysteme formen oft zweiseitige Märkte und haben damit das Potenzial völlig neue Geschäftsfelder und Marktsegmente erst zu kreieren. Aber auch die Digitalisierung von Prozessen und Produkten mit dem Ziel Effizienz und Effektivität zu steigern sind mögliche und erfolgreiche Geschäftsmodelle, die als Basis für digitale Ökosysteme zu finden sind.

»**Technology**«: Der Technologie-Aspekt legt das Gewicht insbesondere auf das »Was« als Kern einer Umsetzung einer digitalen Geschäftsstrategie. Um neue innovative Geschäftsmodelle zu entwickeln, wird neben dem Zugriff auf externe Ökosysteme mit Hilfe von APIs, auch die einfache Nutzung von internen Daten & Funktionen wichtiger. Diese liegen aber in vielen Fällen unzugänglich und dezentral in verschiedenen Silos und können daher nicht für innovative Dienste herangezogen werden. Eine interne API-Zentrierte Architektur, welche sämtliche Schnittstellen, sowohl interne, als auch externe, in einem zentralen Katalog zusammenfasst, macht die Verwendung erst schnell und sinnvoll möglich. Dadurch können unerkannte und zu wenig genutzte Dienste eines Unternehmens ihren Wert besser ausschöpfen und helfen dem Unternehmen insgesamt schneller und innovativer am Markt zu agieren.

»**Legal**«: Rechtliche Aspekte, mögliche Compliance-Auflagen und Rahmenbedingungen für erfolgreiche Umsetzung von digitalen und datenbasierten Geschäftsmodellen. Einige Geschäftsmodelle werden einerseits durch gesetzliche Vorgaben beschränkt, andererseits aber auch durch dieselbe erst ermöglicht. Hier sind beispielsweise datenbasierte Dienste im Finanzwesen, die durch die Payment Service Directive 2 der EU in Form von Kontoinformationsdiensten und darauf aufbauenden Mehrwertdiensten ermöglicht werden oder durch das in der DSGVO verankerte Recht auf Datenübertragbarkeit – auch direkt von einem digitalen Dienst zu einem anderen, was auch die Aggregation verschiedenster Datenquellen und darauf aufbauende Analysen und Dienste ermöglicht, wenn Nutzer dies wünschen, wie es beispielsweise hinsichtlich der Aggregation von Daten vom neuen Dienst BitsaboutMe ([↗ https://bitsabout.me](https://bitsabout.me)) als persönlicher Datenmarktplatz angeboten wird.

In digitalen Geschäftsmodellen sind neben der gerade erwähnten Technologieebene auch die Ebene des Geschäftsmodells und rechtliche Aspekte von entscheidender Bedeutung: Business, Technologie und Recht bzw. Regulierung sind der Dreiklang, mit dem Digital Economy entsteht und betrieben wird.

Unabhängig davon, ob Plattform oder digitales Ökosystem: auf einer weiteren Ebene – der Ebene der Organisation – müssen weitere Themenbereiche wie Vision, Strategie, Engineering, Usage & Operation sowie Governance betrachtet werden. Diese werden später noch in einem Modell für Open API Programm weiter erläutert.

Die vorangehenden Aspekte eines digitalen Ökosystems bzw. einer Plattform sind im Fraunhofer Smart Ecosystems Reference Model des Fraunhofer IESE zusammengefasst, wie in Abbildung 4 dargestellt. Die Ebene zur Organisation wird im Folgenden näher beschrieben. Die Ebenen zu Partnern, Community, Wettbewerbern und anderen Marktteilnehmern werden kurz umrissen, da Kern und Organisation im Hinblick auf Ökosysteme im Fokus stehen sollen.

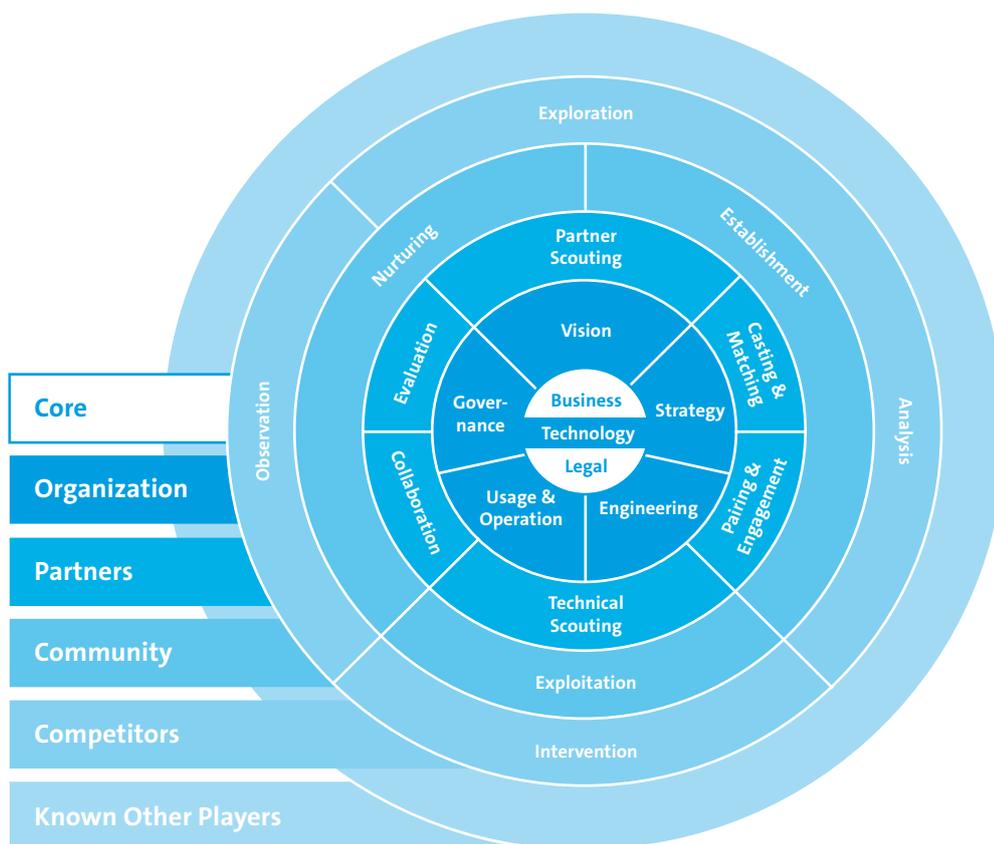


Abbildung 4: Fraunhofer Smart Ecosystems Reference Model. © Fraunhofer IESE

Vision und Strategie zielen dabei u. a. auf relevante Fähigkeiten für ein digitales Geschäftsmodell und Marktausrichtung ab. Engineering deckt den kompletten Bereich der Entwicklung der Plattform bzw. des Ökosystems ab, z. B. Gesamtarchitektur, Kommunikation, Sicherheit und Schnittstellen nach außen (API). Im Themenbereich Usage & Operation sind typische Themen des Betriebs der Plattform bzw. des Ökosystems verankert. Hierzu zählen Fragestellungen wie Cloud

Betrieb oder on-Premise Operation genauso wie Business Continuity Konzepte für Angebot und Services. Der Bereich Governance regelt Themen wie z. B. die Weiterentwicklung der Architektur nach innen genauso wie die Auflagen für Nutzer (Partner) des Ökosystems wie z. B. Daten- oder Dienst-Consumer oder -Provider. Hier werden Auflagen für eine Teilnahme am Ökosystem definiert sowie während und nach dem Onboarding überwacht, so dass hinsichtlich bestimmter Themen wie z. B. Compliance, Informationssicherheit, Datenschutz, API-Management, Qualität an und in den Schnittstellen ein definiertes Niveau gehalten werden kann – ein notwendiger Hygienefaktor und damit auch ein Erfolgsfaktor in jedem digitalen Ökosystem.

Auf weiteren Ebenen werden Partner, die Community um die Plattform bzw. das Ökosystem und insbesondere der Aufbau, die Nutzung und Pflege der Community zu der auch die Auswahl von internen und externen Kommunikationswegen und -partnern gehören, Wettbewerber (Competitors) und bekannte andere Marktteilnehmer (Known other Players), die z. B. Partner oder Wettbewerber sein oder werden können, betrachtet. Dabei sind die verschiedenen Aspekte immer als Leitplanke und Raum von Möglichkeiten zu sehen, nicht dagegen als strikte Vorgabe: Jedes Ökosystem hat eine eigene spezielle Ausrichtung, die stark vom Kern des Geschäftsmodells beeinflusst wird. Damit können einzelne Ebenen und Aspekte zu verschiedenen Zeitpunkten im Lebenszyklus eines Ökosystems relevant werden oder auch gar nicht. Anmerkung: Aus obigem Ökosystem Referenzmodell sollten immer nur diejenigen Aspekte, insbesondere für die Schichten Partners bis Known other Players, modelliert und in Betracht gezogen werden, die für den konkreten Fall tatsächlich relevant sind, d. h. ein pragmatischer Umgang mit dem Modell ist erforderlich um Over-Engineering zu vermeiden.

Auf der Ebene unterhalb des Modells für ein digitales Ökosystem befindet sich das API Programm. Das API Programm ergänzt dabei die Ebene Organisation im Ökosystem Modell und betrachtet als defacto API Management die Aspekte und Verbindung von

- Fachbereichen,
- Entwicklern für das Backend,
- Konsumenten/Nutzern und
- dem Betrieb einer Open API

für ein digitales Ökosystem in Form von Aufgaben.

Dabei sind insbesondere Aufgaben in den Themenfeldern

- Security und Authentifizierung von Benutzern,
- Kosten und Billing,
- Kontrolle,
- Anbindung der API an etwaige Bestandssysteme,
- die Messung von operativen KPI, die ein Feedback an Entwickler, Produktmanagement und Strategie (strategische Programm-Ebene) ermöglichen,
- das Onboarding von Entwicklern von Angeboten im Ökosystem,
- Versionsmanagement und Wartung sowie
- Dokumentation der Open API selbst sowie von Diensten, die die Open API nutzen

zu berücksichtigen.

Das Open API Programm ist in Abbildung 5 hinsichtlich der Aspekte und Aufgaben im Überblick dargestellt.

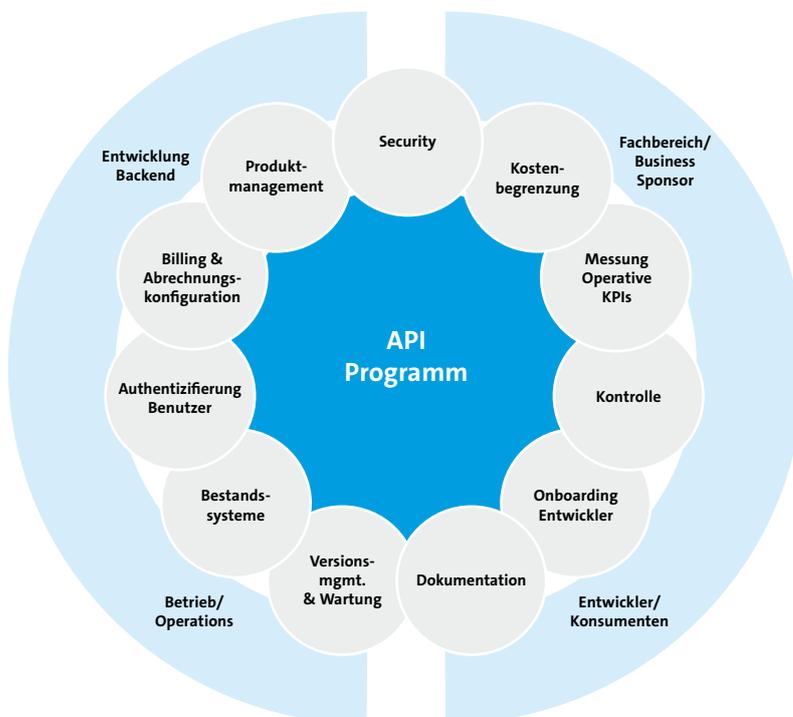


Abbildung 5: API Management – Aufgaben

Die Steuerung des Lebenszyklus eines digitalen Service ist in der Domäne des API Managements verankert. Dazu gehören unter anderem die Aufgaben

- Versionsmanagement,
- Zugriffspolicies und Zugriffskontrolle,
- Management der Konsumenten,
- Management möglichen externen Datenprovidern und
- Erfassen und Reporten von Nutzungs- und Performance-Daten.

API Management unterstützt dabei, die Parameter für das Management des Betriebs festzulegen und auszusteuern. Dies ist besonders relevant für Gebiete wie z. B.

- Abhängigkeitsmanagement,
- Flexibilität,
- Qualität,
- Geschwindigkeit und
- Kosten.

Im Rahmen eines auf die konsequente Verschränkung von Geschäftsstrategie für digitale Ökosysteme und Produkte sowie der API-Strategie und dem API Programm ausgerichteten Prozesses empfiehlt sich auch eine Übernahme entsprechender Strukturen in das übergreifende Enterprise Architektur Management der jeweiligen Organisation.

### 5.3.1 Praktische Betrachtung des Referenzmodells

Sobald das Ecosystem Referenzmodell in der Praxis angewendet werden soll, folgen daraus einige interessante Konsequenzen. Zunächst werden die sich ergebenden bzw. notwendigen Rollen und deren Interaktion und Kooperation betrachtet. Danach folgt die Instanziierung von Teilen des Referenzmodells in einer beispielhaften Systemstruktur, die das Zusammenspiel verschiedener Elemente aus dem Referenzmodell im überblicksartig zeigt.

### 5.3.2 Rollen im Open Ecosystem

Wo ein Open Ecosystem entsteht, dort etablieren sich einige Rollen:

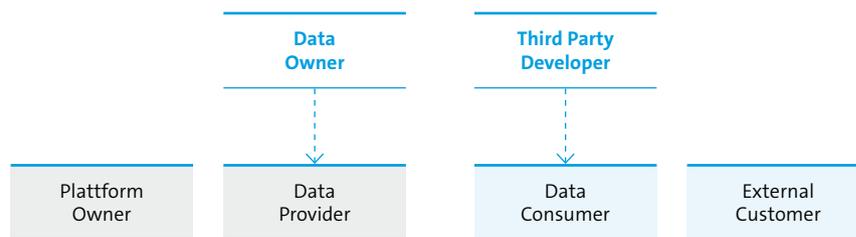


Abbildung 6: Rollen im Open Ecosystem

Die oberen Elemente (Data Owner und Third Party Developer) sind nicht direkt beteiligt. Die grauen Elemente sind interne Beteiligte: die Daten- oder Schnittstellen-Anbieter. Die hellblauen Elemente sind extern, die Daten-Abnehmer bzw. Schnittstellen-Nutzer.

Die Datenquelle bzw. der Datenbesitzer (der **Data Owner**) wird durch die Veröffentlichung zum Datenanbieter (im Leitfaden als **Data Provider** bezeichnet) und tritt erst damit in das Open Ecosystem ein. Dazu muss eine technische Plattform zur Veröffentlichung (die API und das zugehörige API-Management-System) existieren. Beide Teilsysteme werden vom **Plattform Owner** betrieben.

Beliebige Third-party Developer können durch Nutzung der angebotenen Daten in das Ecosystem einsteigen und werden damit zum Datennutzer (im Leitfaden als **Data Consumer** bezeichnet). Die Produkte und Dienstleistungen, die daraus entstehen, können wiederum von beliebigen Menschen z. B. über Apps oder Websites konsumiert werden. Diese **External Customer** können Bürger, Kunden, Reisende o.ä. sein. Der Data Provider hat keinerlei direkte Beziehung zu diesen Endkunden, obwohl sie ja letztlich »seine Daten« nutzen. Die Entwickler werden als Data Consumer quasi zum Zwischenhändler.

## Rollen im Überblick

- **Platform Owner:** Betreibt die technische Plattform, um API's zu veröffentlichen. Kann auch als Data Provider auftreten (siehe folgendes Kapitel zu Erklärung). *Synonym:* Plattform Betreiber.
- **Data Owner:** Der Datenbesitzer kümmert sich um die Datenbeschaffung,-Pflege und -klassische Nutzung von Daten und Systemen. Durch Veröffentlichung der Daten/Schnittstellen wird er zum Data Provider (siehe dort). *Synonym:* Datenbesitzer.
- **Data Provider:** Werden Daten/Schnittstellen öffentlich zur Verfügung gestellt, so ist es die Aufgabe des Data Provider, dieses »Datenprodukt« zu pflegen. Er muss dazu in enger Abstimmung mit dem Platform Owner (siehe dort) die Verfügbarkeit entsprechend der zugesicherten Eigenschaften gewährleisten. *Synonym:* Datenanbieter.
- **Data Consumer:** Beliebige Entwickler können die Daten/Schnittstellen gemäß der vereinbarten Bedingungen nutzen und werden dadurch zum Zwischenhändler, der neue Vertriebskanäle zum External Customer (siehe dort) eröffnet. *Synonym:* Datennutzer.
- **External Customer:** Im offenen Ecosystem entstehen neue Angebote (Apps, Website, Web-Services). Die Nutzer dieser Angebote sind als Endkunden nicht mehr direkt mit dem Data Provider verbunden oder dort bekannt. Hier können Skalierungseffekte auftreten und neue Märkte erschließen. *Synonym:* Endkunde (Bürger, Kunde)

Anmerkung: Customer und Consumer sollten nicht verwechselt werden. Zweitere benötigen technische Fähigkeiten, um die Datenangebote zu nutzen. Erstere sind typische Endkunden, die sich nicht für die Herkunft der Daten interessieren.

### 5.3.3 Systemelemente im Open Ecosystem

Im folgenden Prinzipbild wird ein Überblick über die entstehende Systemlandschaft gegeben (zur Orientierung sind die bereits genannten Rollen eingezeichnet):

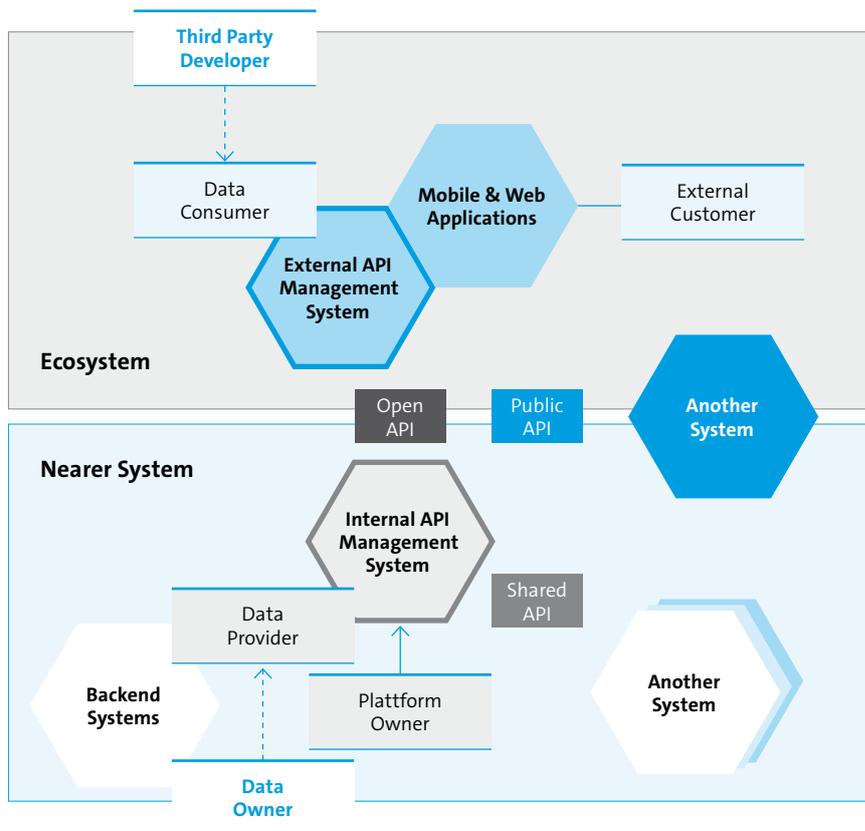


Abbildung 7: Systemelemente und Systemlandschaft im Open Ecosystem

Bei einem konsequenten API First-Ansatz (siehe auch entsprechender Mythos) werden nun alle Systeme über APIs miteinander verknüpft. Intern passiert dies über sogenannte Shared APIs, extern entweder kostenneutral über Open API oder mit Vertrag als Public API. Mit den beiden letztgenannten API-Varianten kann die Reichweite von Diensten deutlich erhöht werden, das so eine Sichtbarkeit und Verfügbarkeit in externen, weiter gefassten Ökosystemen gewährleistet ist. Mit einer Public API können zusätzliche Einnahmen generiert werden bis hin zur Schaffung neuer Geschäftsfelder für ein oder mehrere Unternehmen. Die Open API stimuliert externe Innovation (Open Innovation). In beiden Fällen entstehen letztlich neue Angebote. Werden diese nun von Endkunden genutzt, so nutzen diese indirekt auch die Daten bzw. Schnittstellen der Backend-Systeme.

Im Bild sind zwei denkbare API Management Plattformen (dick umrandet) zu sehen. Beides ist möglich, sogar in Kombination. Im ersten Fall wird der Data Owner zum Betreiber und somit Impulsgeber für das Ecosystem. Auch der Platform Owner selbst kann zum Data Provider werden. Ferner sind in dieser Variante auch leicht Shared Modelle mit ausgewählten Partnern denk- und umsetzbar.

Im zweiten Fall kann von an einem bereits existierenden Ecosystem partizipiert werden, indem eine bereits bestehende Plattform genutzt wird und die eigene Plattform an dieser Stelle sichtbar wird. Das reduziert den technischen Aufwand, was insbesondere beim Einstieg ins Thema eine Beschleunigung bedeuten kann: so entfällt der Auswahlprozess für eine Plattform-Technologie und der Skill-Aufbau für den Betrieb der Plattform.

In den beiden Abstufungen *Open* als auch *Shared* wird davon ausgegangen, dass frei bzw. leicht zugängliche Daten durch die Nachnutzung *mehr Wert* erzeugen können als durch einen klassischen Datenverkauf.

Anmerkung: Die Variante *Public* erzwingt aufgrund der expliziten Vertragsbeziehung besondere Maßnahmen, die den Datenhandel erst möglich machen. Z. B. ältere Versionen von Schnittstellen bzw. Schnittstellen-Änderungen müssen für eine vertraglich vereinbarte Zeit verfügbar sein bzw. entsprechend frühzeitig abgekündigt werden. Auch können verschiedene SLAs bzgl. Quality of Service festgelegt werden. Dies kann Genauigkeit der Daten, Häufigkeit des Zugriffs oder Umfang der verfügbaren Daten betreffen. D. h. eine »Public« Öffnung muss alle Qualitätsmerkmale von Datenhandel und digitalen Services berücksichtigen, denn hierbei müssen dem Vertragspartner zugesicherte Eigenschaften (nicht nur der Daten selbst, sondern auch der Plattform, z. B. Verfügbarkeit) dauerhaft garantiert werden. Viele Organisationen müssen hierzu die entsprechenden Fähigkeiten erst entwickeln.

In diesem Leitfaden liegt der Fokus auf *Open*, wobei die meisten Aussagen weitgehend auch auf *Shared* zutreffen.

# 6 Technisches API-Design

# 6 Technisches API-Design

## 6.1 Wechselwirkung Technik – Geschäftsstrategie

Die Entwicklung von Fähigkeiten der Umsetzung von Programmierschnittstellen beinhaltet

- Handlungsfelder und Organisationsform und Steuerung auf strategischer Programm-Ebene
- die Umsetzung der Steuerung und Kontrolle des Zugriffs
- die Service-Implementierung
- Anbindungsoptionen von Bestandssystemen und Datenquellen und
- die Umsetzung von Sicherheitsanforderungen

Bei allen oben genannten Themen sind die Rahmenbedingungen und Wechselwirkung auf die Umsetzung der Geschäftsstrategie zu berücksichtigen.

Sowohl für eine sinnvolle Nutzung der Daten als auch für ein mögliches Businessmodell sind die Aspekte des bereitgestellten Datenumfangs und der Datenaktualität essentiell.

Als einfaches, aber plakatives Beispiel sind Börsenkurse geeignet: Als Betreiber einer Börse ist eine Weitergabe von Realtime Kursen technisch sehr aufwändig einerseits, für verschiedene Nutzergruppen dafür unterschiedlich wertvoll. Es macht also unter Umständen Sinn, Daten mit verschiedenen Service Level Agreements bzgl. Datenaktualität anzubieten und zwischen freier und kostenbehafteter Nutzung zu unterscheiden. Das erlaubt bei einer hohen Zahl von Konsumenten – unter der Annahme einer Implementierung als RESTles API – einen Key-Value-Cache zwischen interner und externer Schnittstelle zu schalten. Dies reduziert die Last auf die internen Systeme und reduziert Anforderungen an Datenbanken etc. und eine Finanzierung der Aufwände für freie Benutzung andererseits.

## 6.2 Umsetzung der Steuerung und Kontrolle des Zugriffs auf die API/API-Management

Die Steuerung des Lebenszyklus eines Services gehört in die Domäne des API-Managements. Dazu gehören auch die folgenden Aspekte

- Versionsmanagement,
- Zugriffspolicies und Zugriffskontrolle,
- Management der Konsumenten,
- Management möglichen externen Datenprovidern und
- Erfassen und Reporten von Nutzungs- und Performance-Daten.

Architektonisch greifen dazu API-Management-Systeme zwischen einer internen und der nach außen dargestellten Schnittstelle ein.

API-Management hilft aber auch, die Parameter für das Management des Betriebs auszusteuern und festzulegen in den Gebieten wie

- Verfügbarkeit,
- Flexibilität,
- Qualität,
- Geschwindigkeit und
- Kosten.

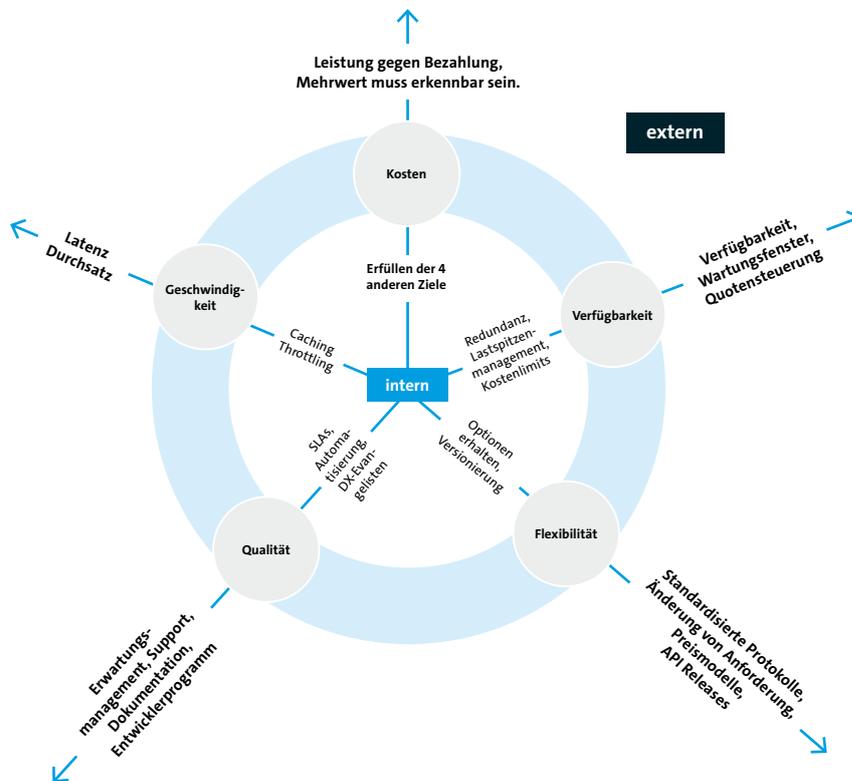


Abbildung 8: »Donut«: Interne/externe Sicht auf API Management

Aus architektonischer Sicht stellen sich die Komponenten einer API-Management Lösung schematisch wie folgt dar, wobei zwischen dem operativen Bereich (links) und dem Managementbereich (rechts) unterschieden werden kann.

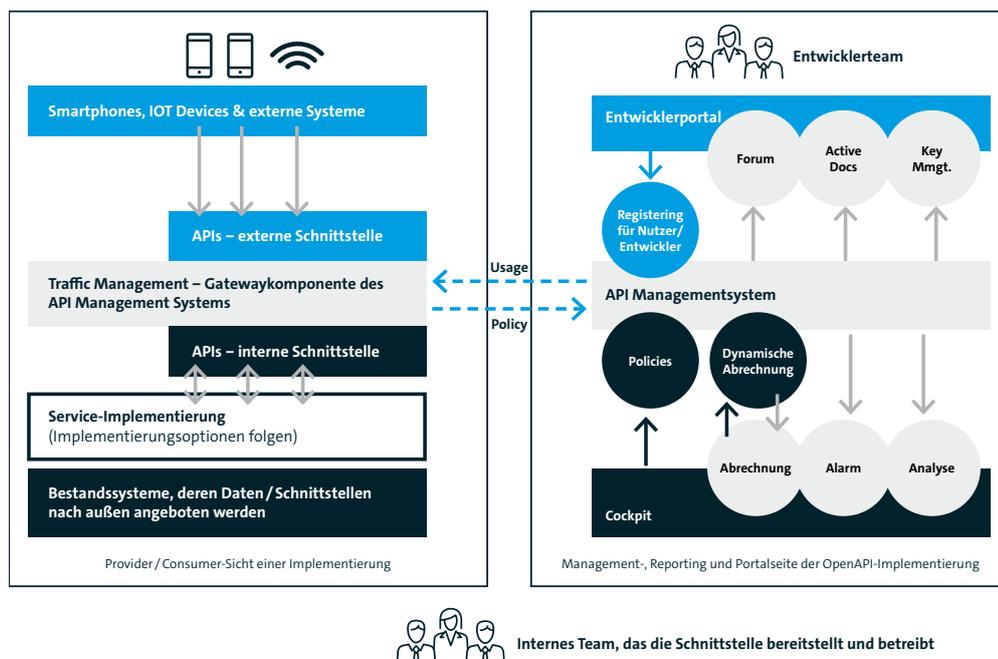


Abbildung 9: Systematische Übersicht der Komponenten einer API-Management-Lösung

Die Komponenten des API-Managements sind in Schwarz dargestellt. In Blau ist dargestellt, wie auf die API zugegriffen wird.

Die API-Management Lösung beinhaltet das Traffic-Gateway, das auf der operativen Seite zwischen den Konsumenten und der nach außen angebotenen Schnittstelle liegt. Das Gateway muss folgende Anforderungen erfüllen:

- Es sollte geringen Overhead, also Latenz und Last erzeugen.
- Die Kommunikation mit der Managementkomponente sollte den operativen Teil wenig beeinträchtigen (Last, Latenz, Durchsatz).
- Es sollte einfach und nahe bei dem Service deployed werden können, um mit diesem zu skalieren und geringen Overhead zu erzeugen.
- Aus obigem Punkt leitet sich ab, dass sich ein API-Management Gateway klassisch, aber auch bei verschiedenen Cloud Providern installieren lassen können und deployen lassen können muss.

API-Management überwacht auch das Einhalten von nicht-funktionalen Anforderungen und Service Level Agreements zu messen, steuern und missbräuchliche Zugriffen entgegenzusteuern.

## 6.3 Service-Implementierung und Anbindungsoptionen für verschiedene Datenquellen / Bestandssysteme und Szenarien

Bei allen Anbindungsoptionen sollten die bestehenden, internen Systeme von der nach außen dargebotenen API entkoppelt werden. Das betrifft sowohl die fachliche Integration, als auch die operative Umsetzung.

Eine API wird immer über einen Service implementiert. Der Service selbst benötigt eine Versorgung mit Daten und wird selbst nach außen beispielsweise als RESTless API dargestellt. Unten stehende Grafik zeigt die Komponenten einer exemplarischen Implementierung. Services, der die API nach außen anbietet, in hellgrau.

Der Übersichtlichkeit halber sind die Komponenten mit einem Farbcode hinterlegt:

- Die Implementierung des Services selbst ist in weiß dargestellt.
- Die Gatewaykomponente des API Managements, die das Traffic Management erzwingt ist in blau dargestellt.
- Bestandssysteme sind in schwarz dargestellt.

Diese Darstellung soll auch Augenmerk darauf legen dass neben einer fachlich korrekten Umsetzung auch die Optimierung bzgl. des »Fan-Out« berücksichtigt wird.

Fan-Out ist ein Begriff aus der Elektronik und ist dort eine Maßzahl wie viele Empfängerchips an ein signalgebendes Beinchen eines Chips angeschlossen werden können. Da wir mit geringen Betriebskosten eine u. U. immense Zahl an Zugriffen darstellen müssen, werden Strategien zur Optimierung des Fan-Out erläutert.

HINWEIS: Dieses Beispiel zeigt, wie wichtig es ist, früh eine umfassende Abstimmung mit den verschiedenen IT-Kompetenzträgern abzustimmen

Es ist grundsätzlich zu empfehlen diese Betriebsaspekte neben dem Softwaredesign sehr früh abzu prüfen und Fragen zur Zahl erwarteter Nutzer und Zugriffszahlen ernsthaft zu überdenken und ggf. Marketingmaßnahmen und Termine mit Betriebsverantwortlichen abzustimmen.

Schauen wir uns Implementierungsvarianten im Detail an und folgen der Darstellung von oben nach unten:

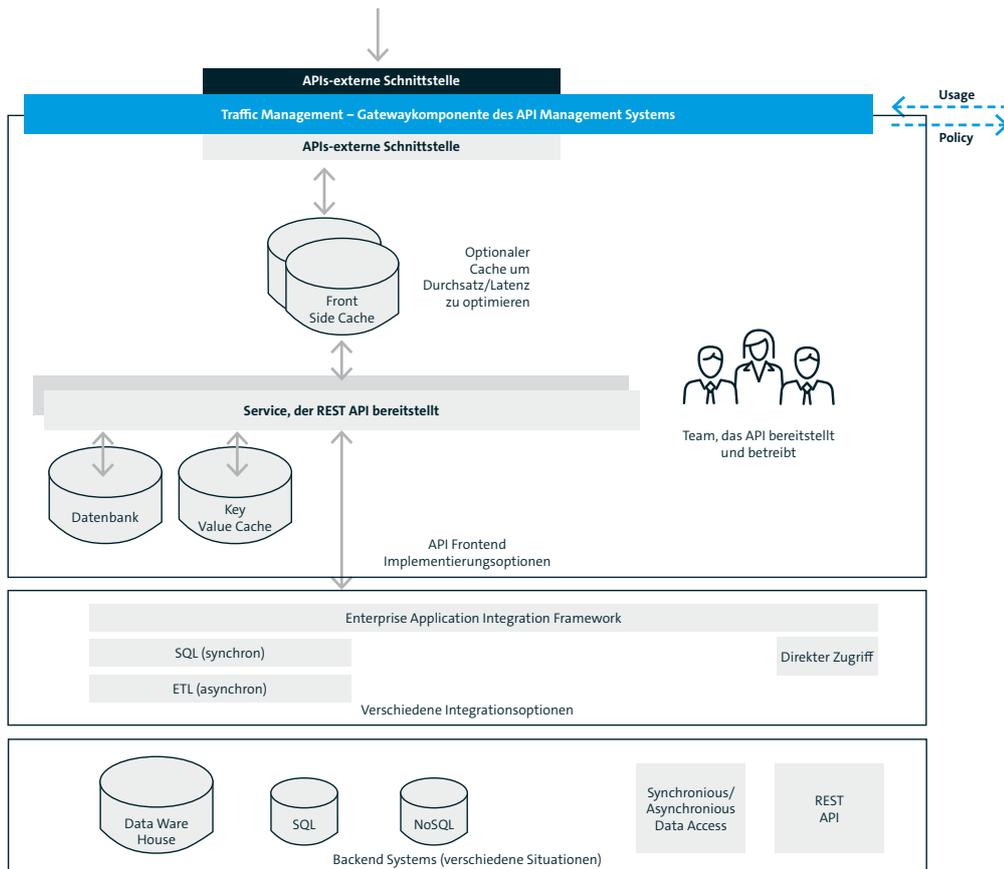


Abbildung 10: Übersicht verschiedener Implementierungsszenarien des Frontendservices

Um die Verfügbarkeit des Services, Zahl der Zugriffe, den Durchsatz und die Latenz, aber auch Betriebskosten zu optimieren, kann es sein dass es Sinn macht

- den Service mit mehreren Instanzen zu betreiben, idealerweise hinter einem Load Balancer. Dies erhöht auch die Verfügbarkeit des Services.
- dem Service einen Front Side Cache vorzuschalten (Einen Http-Reverse-Proxy wie z. B. Varnish) verbessert den Fan-Out erheblich. Front-Side Caches können sehr kostengünstig skaliert werden.
- bei der Auslieferung großer Binaries wie Bilder, Dokumenten, Plänen o.ä. zu prüfen ob es sinnvoll ist den Service in verschiedenen Rechenzentren oder bei Public Cloud Anbietern zu betreiben, mit dem Ziel, näher an der Backbone-Infrastruktur der verschiedenen Internetprovider platziert zu sein (wie es Content Delivery Netzwerkprovider machen). Dies reduziert Latenzen und Durchsatz, da solch ein Setup auf Seiten des Fan-Out optimiert ist.

Im unteren Bereich der Darstellung wird die Anbindung an potentielle Bestandstechnologien dargestellt. Über diese Anbindungen wird der Service mit Daten versorgt die dann nach außen angeboten werden.

Diese Daten können vom Service angefragt werden oder von den Bestandssystemen bereitgestellt werden. Der Service selbst benötigt dazu eine eigene Datenhaltung/Datenpersistenz, die je nach Situation über eine SQL-/NoSQL-Datenbank oder einen Key-Value-Store (Cache) umgesetzt werden kann.

## 6.4 Security-Aspekte im API-Management

Offene Schnittstellen stellen die Bereitsteller vor grundsätzliche Herausforderungen an Sicherheit. Ein frei im Internet verfügbares API, stellt ein mögliches Einfallstor für Hacker dar und lädt durch die freie Erreichbarkeit zum ertesten von Möglichkeiten zum Missbrauch dar. Das API ermöglicht Zugriff auf Daten und Systeme einer Organisation. Diese sind oft nicht auf den Zugriff durch den neuen Nutzerkreis vorbereitet und stellen nicht die erforderlichen Sicherheitsmechanismen bereit. Bei der Erstellung des API ist es deshalb erforderlich, die internen Ressourcen abzusichern.

Auch andere Sicherheitsaspekte sind relevant, wie die Möglichkeit zur Überlastung einer Schnittstelle durch viele Zugriffe bei hoher Nachfrage bis zur absichtlichen Überlastung durch einen sogenannten Distributed Denial of Service (DDOS) Angriff. Dieses Kapitel bietet einen Überblick über die Sicherheitsaspekte bei der Bereitstellung offener Schnittstellen.

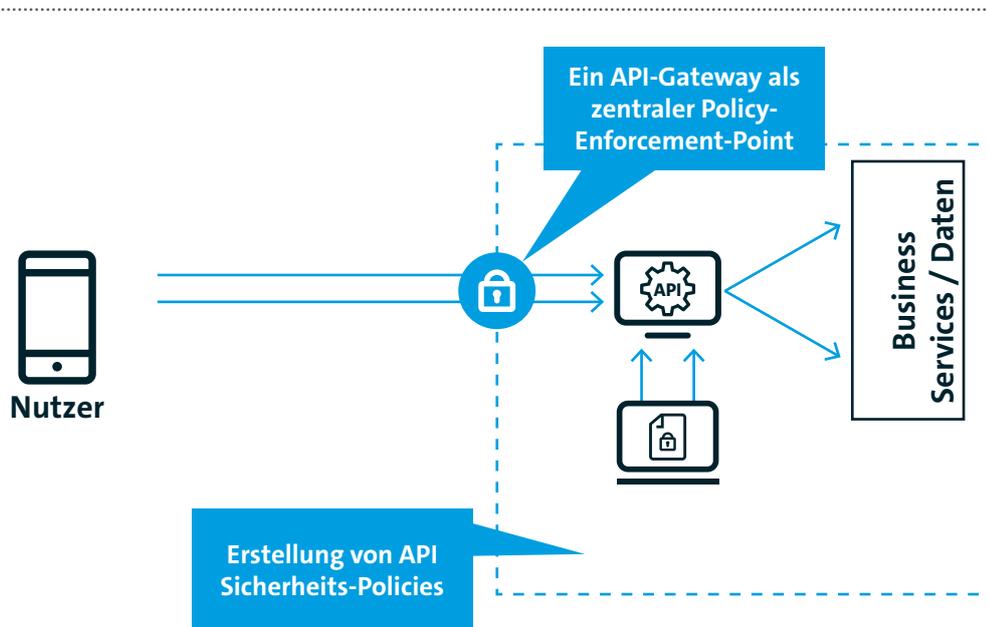


Abbildung 11: Absicherung offener APIs über ein Security Gateway

Die Sicherheitsanforderungen an offene APIs sind für alle APIs einer Organisation zu prüfen und zu konfigurieren. Mit einem API Gateway können Sicherheitsanforderungen für jede einzelne API umgesetzt werden.

Aspekte bei der Absicherung von APIs:

- Dokumentation
- Absicherung des Transports
- Authentifizierung und Autorisierung
- Zugriffsbegrenzung
- Prüfung von Inhalten
- Überwachung

## 6.4.1 Dokumentation

Ein sicheres Design beginnt mit einer genauen und aktuellen Dokumentation. Diese muss über den Lebenszyklus des API aktuell gehalten werden.

Dokumentation dient nicht nur dem Nutzer des API, sondern auch der Erstellung von Sicherheitstests, der Vorbereitung automatisierter Tests, sowie der Definition von Regeln zur Absicherung.

Die Dokumentation sollte in einem standardisierten Format, zum Beispiel OpenAPI, erstellt werden. Sie sollte alle Methoden und Kommunikationsmodelle umfassen die im Aufruf des API sowie den möglichen Antworten im Erfolgs- und Fehlerfall möglich sind.

Die Bereitstellung der Dokumentation für offene APIs sollte in einem Portal erfolgen, das Erstellung, Änderung und Einsicht ermöglicht. Für nicht-öffentliche APIs sollte die Dokumentation nur autorisierten Benutzern ermöglicht werden.

## 6.4.2 Authentifizierung und Autorisierungen

Für eine erfolgreiche Absicherung der Inhalte, muss für eine Schnittstelle bekannt sein, wer sie verwendet und ob der Zugriff erlaubt ist. Dafür ist die Verwaltung von Identitäten, Rollen und Rechten erforderlich.

Berechtigungen können generell Rollen- oder Transaktionsabhängig sein. Welche APIs welchen Berechtigungsmechanismen etc. unterliegen wird in Security Policies im API Management festgelegt.

Für rollenabhängiges Berechtigungsmanagement werden die drei Komponenten AAA (Authentifizierung, Autorisierung und Accounting – also Datenhaltung der Rollen/Rechte – Benutzer/Credentials) benötigt.

Im Kontext von OpenAPIs und offenen Standards bietet sich das OpenID Framework für eine Umsetzung an, das von den marktgängigen API-Management-Lösungen implementiert werden kann.

Transaktionsbasierte Autorisierung machen bei speziellen Use Cases Sinn. Bei unten stehendem Beispiel ist darauf hinzuweisen, dass das Verständnis, wann eine Schnittstelle eine OpenAPI ist, von Branchen-Vertical zu Vertical unterschiedlich ist.

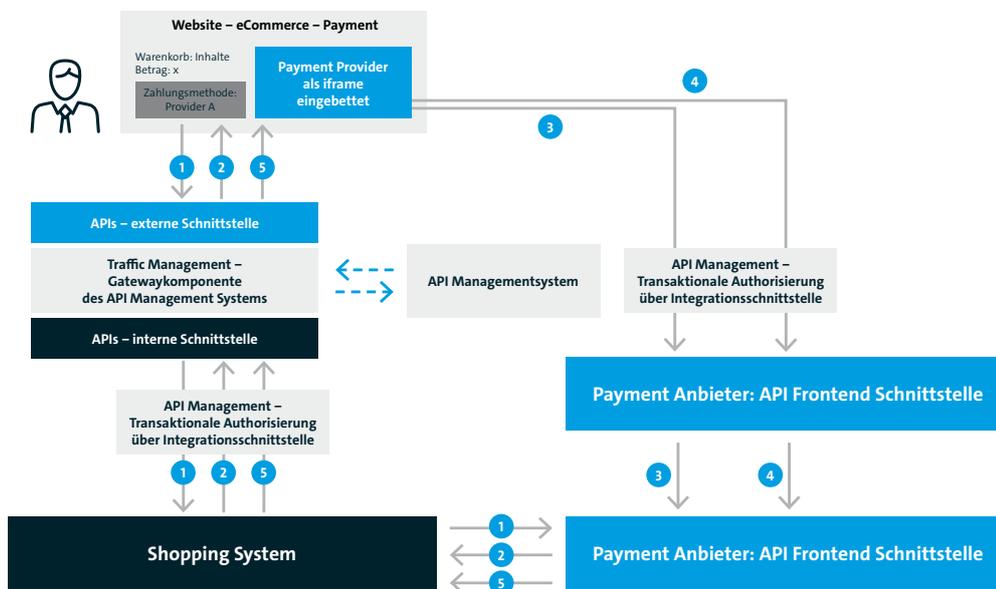


Abbildung 12: Transaktionsbasierte Autorisierung

Obiges Bild stellt ein plastisches Beispiel für einen Spezialfall dar, bei dem eine transaktionale Autorisierung über einen externen Partner erfolgt: Ein eCommerce-Anbieter hat die Bezahlmechanismen ausgelagert an einen Payment-Provider wie eine Bank oder einen speziellen Provider für Bezahldienste. Er betreibt im Beispiel eine Website und befindet sich dort auf der Seite wo der Warenkorb bezahlt werden soll. Betrag und Zahlmethode sind festgelegt, und damit auch der Dienstleister.

Der Reihe nach wird nun der Bezahlvorgang angestoßen (1) bei dem das eigene Backend beim Paymentprovider eine individuelle URL anfragt, die dann über (2) zurückgegeben wird. Daraufhin wird ein HTML-Schnipsel des Providers über ein `<iframe>` auf der Bezahlseite dargestellt. Hierüber werden Bezahl-details und Autorisierung der Zahlung vom Kunden an den Dienstleister gegeben (4). Ist dieser Bezahlprozess abgeschlossen, dann quittiert der Bezahl-dienstleister das mit einer Bestätigung im `<iframe>` und über eine Nachricht an das Backendsystem des Anbieters (5). Damit kann der Anbieter den Bestellvorgang abschließen und sendet eine Quittierung über die Website an den Kunden.

Die Autorisierungs-Aufrufe sollten selbst HTTP/REST basiert sein, denn dann sollten diese Autorisierungen wegen der Management- und Reportingsicht, der Konfigurierbarkeit der Security und Nutzungspolicies etc., der Integration ins bestehende Billing etc. über das API Management erfolgen.

**HINWEIS:** Für weitere Security-Aspekte ist eine sehr frühe Abstimmung mit den relevanten Kompetenzträgern in der IT zu veranlassen, insbesondere Enterprise-Architektur, Softwarearchitektur, Betriebs- und Netzwerkspezialisten, aber auch einem CISO (Chief Security Officer).

# 7 Fachliches API-Design: Metadaten für Datenkataloge

# 7 Fachliches API-Design: Metadaten für Datenkataloge

Eine spezialisierte Kategorie von Schnittstellen dient der Bereitstellung von Datenkatalogen. Ein Datenkatalog kann als Sammlung bzw. Liste von Datensätzen definiert werden, wobei ein Datensatz in den meisten Fällen ausschließlich Metadaten enthält. Auf die eigentlichen Daten bzw. Rohdaten wird referenziert, d. h. der Speicherort der Metadaten und der Daten ist different. Für die Beschreibung und Veröffentlichung solcher Datenkataloge und Metadaten haben sich vielfältige Standards und Spezifikationen entwickelt. Dabei spielt Interoperabilität eine entscheidende Rolle, da Datenkataloge häufig aggregiert, aufbereitet und exportiert werden. Insbesondere im Bereich der offenen Verwaltungs- und Geodaten, aber auch für Forschungs- und Bibliotheksdaten ist diese Praxis sehr verbreitet. Beispielsweise werden die offenen Daten der deutschen Bundesländer im nationalen Portal GovData und anschließend im Europäischen Datenportal zur Verfügung gestellt. Dieser Prozess, der Datenaggregation von einem Datenkatalog zu einem anderen, wird als Harvesting bezeichnet. Die Veröffentlichung von Datenkatalogen gewinnt auch zunehmend an Bedeutung für Industrieunternehmen, sowohl in der Form von offenen Daten, als auch zugriffsbeschränktes und/oder kostenpflichtiges Angebot. Im Folgenden werden relevante und verbreitete Standards zur Beschreibung von Schnittstellen für Datenkataloge beschrieben.

## DCAT

Das Data Catalog Vocabulary (DCAT) ist ein populäres Vokabular, um Datensätze aussagekräftig zu beschreiben. Übergeordnetes Ziel dabei ist die Interoperabilität zwischen Datenkatalogen zu erhöhen und Verbundsuchen zu ermöglichen. DCAT macht keine Annahmen über das Format der eigentlichen Daten. Der Standard besteht im Kern aus 3 Hauptklassen: Katalog (dcat:catalog), Datensatz (dcat:dataset) und Distribution (dcat:distribution), wobei ein Katalog aus mehreren Datensätzen besteht und ein Datensatz über mehrere Distributionen verfügen kann. Letzteres bezeichnet die eigentlichen Daten, also die Ressourcen. DCAT ist als sogenannte Linked Data Spezifikation veröffentlicht, ein Einsatz in anderen Serialisierungsformaten ist aber möglich und etabliert. Mehr Informationen: ↗ <https://www.w3.org/TR/vocab-dcat/>

Die Basis für DCAT stellt das Dublin Core Metadatenvokabular dar (↗ <http://dublincore.org/>).

Dublin Core ist ein genereller Standard zur Beschreibung digitaler Ressourcen. Die folgende Tabelle zeigt die Elemente des Metadatenstandards Dublin Core:

Element	Definition
<b>Contributor</b>	An entity responsible for making contributions the resource
<b>Coverage</b>	The spatial or temporal topic of the resource, the spatial applicability of the resource, or the jurisdiction under which the resource is relevant
<b>Creator</b>	An entity primarily responsible for making the resource
<b>Date</b>	A point or period of time associated with an event in the lifecycle of the resource
<b>Description</b>	An account of the resource
<b>Format</b>	The file format, physical medium or dimensions of the resource
<b>Identifier</b>	An unambiguous reference to the resource within a given context
<b>Language</b>	A language of the resource
<b>Publisher</b>	An entity responsible for making the resource available
<b>Relation</b>	A related resource
<b>Rights</b>	Information about rights held in and over the resource
<b>Source</b>	A related resource from which the described resource is derived
<b>Subject</b>	The topic of the resource
<b>Title</b>	A name given to the resource
<b>Type</b>	The nature or genre of the resource

Tabelle 2: Metadaten für DCAT nach Dublin Core Standard

## DCAT-AP

Das DCAT Application Profile for data portals in Europe (DCAT-AP) ist eine Erweiterung von DCAT zur Beschreibung von Datensätzen des öffentlichen Sektors. DCAT-AP wird u. a. von der Europäischen Kommission entwickelt und soll sich als Standard für die Bereitstellung von Open Data in ganz Europa etablieren. Dafür wurde DCAT um zahlreiche Metadatenfelder erweitert und konkrete Namensräume, z. B. für Kategorien oder Sprachen, eingeführt. Mehr Informationen: [↗ https://joinup.ec.europa.eu/release/dcat-ap-v11](https://joinup.ec.europa.eu/release/dcat-ap-v11). DCAT-AP findet zunehmend Verbreitung in ganz Europa. Dabei sind insbesondere länder-spezifische Erweiterungen entstanden. So hat der IT-Planungsrat im Juni 2018 DCAT-AP.de als formalen Austauschstandard für offene allgemeine Verwaltungsdaten festgelegt (siehe [↗ https://www.dcat-ap.de/](https://www.dcat-ap.de/)).

## GeoDCAT-AP

Wiederum eine Erweiterung von DCAT-AP für Datensätze und Dienste, die Geoinformationen beschreiben, ist GeoDCAT-AP. GeoDCAT-AP stellt keinen Ersatz für die INSPIRE Anforderungen basierend auf ISO 19115 bzw. 19119. Mit GeoDCAT-AP können raumbezogene Daten und Dienste über die (Dank INSPIRE erfassten) Metadaten auch auf (Open) Data Portalen suchbar gemacht werden (mehr Informationen siehe [↗ https://joinup.ec.europa.eu/release/geodcat-ap-v10](https://joinup.ec.europa.eu/release/geodcat-ap-v10))

## OAI-PMH

Das Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) ist ein freier Standard, der speziell für das Harvesting von Datenkatalogen entwickelt wurde. Es kann als Meta-Metadatenformat betrachtet werden, da es Informationen über Datenbereitsteller von Metadaten zur Verfügung stellt. Es basiert ebenfalls auf Dublin Core. Mehr Informationen:

[↗ https://www.openarchives.org/pmh](https://www.openarchives.org/pmh)

## CKAN

Die Open Source Lösung CKAN stellt eine Basissoftware zum Aufbau von Datenkatalogen, insbesondere für Open Data, dar. Es hat sich im Kontext des öffentlichen Sektors als de-facto Standard etabliert, wird aber auch zunehmend von Unternehmen eingesetzt. CKAN bietet zahlreiche Funktionalitäten zur Abbildung des gesamten Prozesses der Veröffentlichung von Datenkatalogen. Insbesondere hat sich ein umfangreiches Angebot von Erweiterungen entwickelt. Die CKAN API ist umfangreich dokumentiert und ermöglicht eine einfache maschinen-lesbare Möglichkeit die Metadaten des Datenkataloges abzurufen. Eine optionale Unterstützung für DCAT bzw. DCAT-AP ist ebenfalls gegeben. Mehr Informationen: [↗ https://ckan.org/](https://ckan.org/)

Metadaten für einen Datensatz helfen in Katalogen, Daten zu finden ähnlich wie es der Katalog in einer Bibliothek macht (Autor, Titel, ISBN-Nummer, Verlag, Erscheinungsjahr usw.). Bei Textdaten ist es denkbar, diese maschinell mit KI zu katalogisieren. Bei Bilddaten (wie Satellitenfotos) geht das nicht.

In Katalogverbänden werden heute nur die Metadaten repliziert nicht aber die Rohdaten/Ressourcen. Im Public Service in Europa sieht das dann so aus, dass z. B. Städte und Gemeinden Open-Data-Portale betreiben auf denen sie Rohdaten und Metadaten bereitstellen. Länder, der Bund ([↗ https://www.govdata.de](https://www.govdata.de)) und die EU holen sich dann (harvesten) die Metadaten von der jeweils unter ihnen liegenden Hierarchieebene. In der EU wird dafür der Metadatenstandard DCAT verwendet, der neben den Daten als Tabelle auch RDF-Triplets aus der Welt des semantischen Webs verwendet.

# 8 Rechtslage für Open API

## 8 Rechtslage für Open API

Bei den rechtlichen Aspekten zu Daten sind im Zusammenhang mit Open Data und Open API zwei grundsätzliche Richtungen zu unterscheiden: Der rechtliche Schutz von Daten und der freie Fluss von Daten.

Der rechtliche Schutz von Daten hat zwei unterschiedliche Zielrichtungen. Während das Datenschutzrecht, als Ausfluss des grundrechtlich geschützten »Rechts auf informationelle Selbstbestimmung« dem Schutz der Persönlichkeit dient, wird der urheberrechtliche Schutz von Datenbanken dem Hersteller einer Datenbank gewährt und ist eine Belohnung für den entsprechenden Investitionsaufwand. Das Datenschutzrecht findet daher nur auf personenbezogene Daten Anwendung, während urheberrechtlicher Schutz für alle Datensammlungen bestehen kann, also inhaltlich einen weiteren Kreis von Daten betrifft.

Für den Bereich der nicht-personenbezogenen Daten gilt seit dem 18. Juni 2019 das neue Rahmenwerk für den freien Fluss von nicht-personenbezogenen Daten innerhalb der Europäischen Union. Dazu werden Lokalisierungsaufgaben untersagt.

### 8.1 Schutz von personenbezogenen Daten

Seit dem 25. Mai 2018 ist die europäische Datenschutz-Grundverordnung (DSGVO) das zentrale Regelungsinstrument im Datenschutz. Sie regelt im Detail, welche Verarbeitungen von personenbezogenen Daten gesetzlich zulässig sind und welche rechtlichen Vorgaben dafür bestehen. Die Grundkonzeption ist dabei, dass jede Verarbeitung eines eigenen Erlaubnistatbestands bedarf. Dies kann entweder ein gesetzlich normierter Tatbestand sein oder aber die Einwilligung des Betroffenen. Die Einwilligung kann dabei nicht pauschal für beliebige Zwecke erteilt werden, sondern sie muss freiwillig für bestimmte Fälle, in informierter Weise und unmissverständlich erklärt werden. Zudem ist die Einwilligung gem. Art. 7 Abs. 3 DSGVO jederzeit widerrufbar. Eine Einwilligung ist aber nicht immer erforderlich. Gesetzliche Erlaubnistatbestände in Art. 6 DSGVO lassen die Verarbeitung auch ohne Einwilligung beispielsweise zur Erfüllung eines Vertrags (Art. 6 Abs. 1 S. 1 lit. b) DSGVO) oder zur Wahrung von berechtigten Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) des datenverarbeitenden Verantwortlichen zu. Obgleich insbesondere das berechtigte Interesse grundsätzlich einen weiten Anwendungsbereich für Datenverarbeitungen eröffnen kann, darf auch hier eine Verarbeitung nur dann erfolgen, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht die Interessen des Verantwortlichen überwiegen. Flankierend zum »ob« der Verarbeitung personenbezogener Daten enthält die DSGVO umfangreiche Regelungen zum »wie«, die dem praktischen Schutz der Betroffenen dienen und ihnen die Kontrolle der Verarbeitung ermöglichen sollen. Dies findet zum Beispiel in aktiven Informationspflichten bei der Erhebung (»Datenschutzerklärungen«), in Betroffenenrechten (bspw. Informations- und Löschanträge) und gewissen Anforderungen an die technische Sicherheit bei der Datenverarbeitung ihren Ausdruck.

Eine Verwendung personenbezogener Daten wird daher vielfach erst möglich sein, wenn diese anonymisiert wurden. Eine Anonymisierung liegt dann vor, wenn der Dateninhalt nicht mehr einer identifizierten oder identifizierbaren Person zugeordnet werden können. Gemäß Erwägungs-

grund 26 ist die DSGVO nicht auf die Verarbeitung anonymer Daten anwendbar. Allerdings sind anonymisierte Daten von lediglich pseudonymisierten Daten abzugrenzen. Letztere erlauben einen Rückschluss auf die betroffenen Personen durch die Hinzuziehung weiterer Informationen und unterfallen daher weiterhin der DSGVO. Solche Informationen können nicht nur in einem Schlüssel oder einer getrennten Datenbank mit Zuordnungsparametern bestehen, sondern auch in sonstigen technischen Mitteln, die eine Zuordnung ermöglichen. Es müssen hierbei alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden. Daher ist zu bedenken, ob Big Data-Analysen eine Zuordnung ermöglichen können, wenn verschiedene Parameter miteinander verknüpft werden und damit den Rückschluss auf eine konkrete Person zulassen. Dann sind die verarbeiteten Daten nur scheinbar anonym und unterfallen weiterhin dem Datenschutzrecht. Aufgrund der fortschreitenden technischen Möglichkeiten sind die Grenzen hier fließend.

## 8.2 Freier Fluss von nicht-personenbezogenen Daten in der EU

Die Digitalisierung der Wirtschaft beschleunigt sich zunehmend. Informations- und Kommunikationstechnologie stellen nicht länger einen besonderen Wirtschaftszweig dar. Sie bilden die Grundlage für modernes, innovatives wirtschaftliches Handeln und für eine moderne und innovative Gesellschaft. Digitale Daten nehmen eine zentrale Stellung ein und können eine große Wertschöpfung schaffen, wenn sie analysiert oder mit Dienstleistungen und Produkten kombiniert genutzt werden können. Gleichzeitig kommen mit der raschen Entwicklung der Datenwirtschaft und neuer Technologien, wie der künstlichen Intelligenz, Produkten und Diensten im Zusammenhang mit dem Internet der Dinge, autonomen Systemen und 5G neue rechtliche Fragen bezüglich des Zugangs zu und der Weiterverwendung von Daten, der Haftung, der Ethik und der Solidarität auf.<sup>11</sup>

Daten-Wertschöpfungsketten bestehen aus unterschiedlichen Datenaktivitäten: Datenerzeugung und Datenerhebung, Datenaggregation und Datenorganisation, Datenverarbeitung, Datenanalyse, Datenvermarktung und Datenverbreitung, Datennutzung und Datenweiterverwendung. Das wirksame und effiziente Funktionieren der Datenverarbeitung ist das tragende Glied jeder Daten-Wertschöpfungskette. Das wirksame und effiziente Funktionieren der Datenverarbeitung und die Entwicklung der Datenwirtschaft in der EU werden jedoch beeinträchtigt, insbesondere durch zwei Arten von Hindernissen für die Datenmobilität und für den Binnenmarkt: die von den Behörden der Mitgliedstaaten eingeführten Datenlokalisierungsaufgaben und das Modell der Anbieterabhängigkeit (Vendor-lock-in) im privaten Bereich.<sup>12</sup>

Daher werden im Rahmenwerk für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union die rechtlichen Grundlagen für eine Datenmobilität (quasi »Data Schengen«) und einen Daten-Binnenmarkt gelegt. So sollen Vendor-lock-ins abgebaut und Wettbewerb im Binnenmarkt gefördert werden.

<sup>11</sup> aus ErwGr 1 EU/2018/1807

<sup>12</sup> aus ErwGr 2 EU/2018/1807

Insbesondere werden für den freien Verkehr von nicht-personenbezogenen Daten in Artikel 4 grundsätzlich Datenlokalisierungsaufgaben, also Ortsbindungen von Daten, aufgehoben, es sei denn sie sind aus Gründen der öffentlichen Sicherheit (unter Achtung der Verhältnismäßigkeit) gerechtfertigt.

Ferner wird die Übertragung von Daten zum Zweck des Wechsel eines Diensteanbieters forciert und ein wirksamer Verhaltenskodex hierzu zwischen Anbietern von Diensten bis Mai 2020 gefordert (Artikel 6).

Insbesondere die in der Praxis voraussichtlich häufig vorkommenden Datensätze, die aus personenbezogenen und nicht-personenbezogenen Daten bestehen, sollen dabei Augenmerk über eine Bewertung der Entwicklungen der Märkte und technologischer Natur hinsichtlich neuer Möglichkeiten zur Entanonymisierung erhalten. Ferner werden Gründe für die Erhaltung von Datenlokalisierungsaufgaben aus Gründen der öffentlichen Sicherheit und die Verhaltensregeln von und für Wirtschaftsunternehmen zur Datenübertragung unter besonderer Beobachtung zum Zweck der Verbesserung stehen (Artikel 8).

Unter diesen Gesichtspunkten (insbes. Wegfall von Datenlokalisierungsaufgaben) sollen im Bedarfsfall Daten dennoch für zuständige Behörden verfügbar sein (Artikel 5), wobei eine Sanktionierung bei Verstoß gegen die Bereitstellungspflicht von Daten gegenüber Behörden stattfinden soll. Dazu werden auch Verfahren für die Zusammenarbeit zwischen Behörden über eine einheitliche Anlaufstelle, die Anfragen aus anderen EU Staaten für Behördendaten (nach Prüfung) an die relevante nationale Behörde weiter leitet und die Ausführung der Datenübermittlung überwacht (Artikel 7).

Weitere Details sind der Verordnung EU/2018/1807 selbst zu entnehmen. Der in diesem Absatz gegebene komprimierte Abriss der Verordnung beansprucht keine Vollständigkeit oder Klärung aller für den Leser relevanten Aspekte und Fragen zu der Verordnung.

## 8.3 Urheberrechtlicher Schutz von Datenbanken

Erheblicher praktischer Bedeutung kommt der urheberrechtliche Schutz von Datenbanken zu. Das Urheberrecht und urheberrechtliche Leistungsschutzrechte sind Verbotrechte, die dem Inhaber die Möglichkeit geben, alle anderen von der Nutzung seiner Datenbank auszuschließen oder eben auch vertraglich durch eine Lizenz zu gestatten.

### Datenbankwerke und das Datenbankherstellerrecht

Datenbanken sind gemäß § 4 Abs. 2 UrhG urheberrechtlich geschützt, wenn die Auswahl oder Anordnung ihrer Elemente eine persönliche geistige Schöpfung darstellt, d. h. ein Entscheidungsspielraum bei der Anordnung oder Auswahl der Daten genutzt wurde. Gedichtsammlungen und Lexika sind hierfür typische Beispiele. Jedoch können Datenbanken auch dann durch ein

urheberrechtliches Leistungsschutzrecht sein, wenn der Erstellung keine kreative Leistung zugrunde liegt.

### **Anforderungen an das Datenbankherstellerrecht**

Die EU-Datenbankrichtlinie von 1996 hat ein sui generis Leistungsschutzrecht für den Datenbankhersteller eingeführt, um dem Inhaber ein einfacheres Vorgehen gegen die unerlaubte Übernahme und Weiterverwendung von investitionsintensiven Datenbanken zu ermöglichen. Außerhalb dieses Schutzrechts kann eine Leistungsübernahme nur unterbunden werden, wenn sie unlauter ist und gegen Wettbewerbsrecht verstößt oder als Geschäftsgeheimnis geschützt ist. Gemäß § 87a Abs. 1 Satz 1 UrhG ist eine Datenbank eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind. Hinzu kommt das Erfordernis, dass deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Der Begriff beschränkt sich nicht auf elektronische Datenbanken, sondern erfasst auch Datensammlungen, die auf andere Weise – etwa in gedruckter Form – zusammengestellt sind.

Damit ergeben sich die folgenden fünf Tatbestandsmerkmale, die zu prüfen sind:

- Vorliegen einer »Sammlung«
- Gegenstand der Sammlung sind »Daten oder andere unabhängige Elemente«
- Die Daten müssen »systematisch oder methodisch angeordnet« sein
- Die Daten müssen »einzeln zugänglich« sein
- »Wesentliche Investition« (nach Art oder Umfang) für die Beschaffung, Überprüfung oder Darstellung der Daten

Eine systematische Anordnung der Daten liegt vor, wenn diese vordefinierten logischen oder sachlichen Kriterien folgt. Methodisch ist die Ordnung, wenn die planmäßige Strukturierung einem bestimmten Zweck dient. Typische Fälle sind die alphabetische oder chronologische Anordnung. Bloße »Rohdaten« oder »Datenhaufen« unterfallen nicht dem Schutz des Datenbankherstellerrechts. Dabei kommt es nicht darauf an, wie die Daten physikalisch vorliegen, sondern ob diese zielgerichtet abgefragt werden können.

Die Investition muss nicht finanzieller Art sein, sondern kann auch in Arbeit oder im Einsatz technischer Ressourcen bestehen (vgl. BGH GRUR 2011, 724, 725 – Zweite Zahnarztmeinung II). Allerdings muss sich die Investition auf die Beschaffung, Überprüfung oder Darstellung der Daten beziehen, während die Erstellung der Daten selbst außer Betracht bleibt. Dies bedeutet, dass nur die Investitionen zu berücksichtigen sind, die dazu dienen, um die generierten Daten zugänglich zu machen oder aufzubereiten (z. B. in ein XML-Format zu überführen). Folglich sind automatisch generierten Daten (z. B. Maschinendaten) nicht per se durch das Datenbankherstellerrecht geschützt, sondern nur dann, wenn außerhalb der Generierung für die

Beschaffung, Überprüfung oder Darstellung eine wesentliche Investition getätigt wurde (z. B. für die Programmierung zur Darstellung der Ergebnisse oder für den Erwerb der Daten).

Ob eine Investition wesentlich ist, muss im Einzelfall ermittelt werden. Die Gerichte waren bei der Beurteilung bislang recht großzügig und haben »keine ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen« als ausreichend erachtet.

Von außen lässt sich einer von Dritten erstellen Datenbank nicht ansehen, ob eine wesentliche Investition für die Beschaffung, Überprüfung oder Darstellung getätigt wurde. Daher muss im Zweifel davon ausgegangen werden, dass ein Datenbankherstellerrecht besteht und damit eine Lizenz zur Nutzung erforderlich ist, sofern nicht eines der vorgenannten Kriterien offensichtlich nicht gegeben ist.

### **Schutzumfang des Datenbankherstellerrecht**

Als erlaubnispflichtige Nutzungshandlung ist jede Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe eines nach Art oder Umfang wesentlichen Teils der Datenbank sowie die wiederholte und systematische Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank anzusehen (§ 87b UrhG). Somit ist durch das Datenbankherstellerrecht nicht das einzelne Datum einer Datenbank geschützt, sondern die gesamte Datenbank vor der Entnahme wesentlicher Bestandteile oder dem systematischen Zugriff von außen. Was als »wesentlich« anzusehen ist, hat der Gesetzgeber den Gerichten überlassen, die wiederum nach quantitativen und qualitativen Kriterien entscheiden. Es kommt damit nicht auf einen starren Prozentsatz an (der im Regelfall über 10% liegen dürfte, vgl. BGH GRUR 2011, 724), sondern auch darauf, ob der übernommene Teil für die schutzbegründende Investition relevant war. Die damit verbundenen Unsicherheiten haben dem Datenbankherstellerrecht auch einige Kritik eingebracht. Durch die geplante Novellierung der PSI-Richtlinie soll allerdings klargestellt werden, dass das Datenbankherstellerrecht grundsätzlich einer Weiterverwendung von Daten der öffentlichen Hand nicht entgegensteht. Diese Regelung und deren Ausnahmen werden bei der Verwendung von Daten im Bereich des Open Government von besonderer Relevanz sein.

### **Internationale Rechtslage**

International sind Datenbanken nur geschützt, wenn sie die Schöpfungshöhe eines Datenbankwerkes erreichen. Ein dem Datenbankherstellerrecht vergleichbares Leistungsschutzrecht existiert in den meisten Staaten nicht. In den USA besteht entsprechend nur Schutz durch vertragliche Regelungen oder ggf. als Betriebsgeheimnis. Auch können sich ausländische Datenbankhersteller nicht auf Schutz innerhalb der EU berufen, sofern sich nicht der Hauptsitz im Europäischen Wirtschaftsraum (EWR) befindet (§ 127a UrhG).

## 8.4 Open Data Lizenzierung

Wenn eine Datenbank durch das Datenbankherstellerecht, urheberrechtlich oder als Geschäftsgeheimnis geschützt ist, bedarf es einer Gestattung für eine Nachnutzung der Daten. Zu diesem Zweck haben sich Open Data Lizenzen etabliert, die auch die kommerzielle Nachnutzung gestatten. Bei der Beurteilung der Anforderungen an eine Open Data Lizenz wird überwiegend die »Open Definition« der Open Knowledge Foundation zugrunde gelegt ([↗ https://opendefinition.org/od/2.0/de/](https://opendefinition.org/od/2.0/de/)), wonach jedermann der freie Zugriff auf die Daten möglich sein muss und die Erlaubnis zur Nutzung, Weitergabe und Veränderung bzw. Aggregation der Daten erteilt wird.

Typische und anerkannte Open Data Lizenzen sind:

- Open Data Commons Open Database License (ODbL)
- Open Data Commons Attribution License (ODC-BY)
- Creative Commons Attribution 4.0 (CC-BY-4.0)
- Creative Commons Attribution Share-Alike 4.0 (CC-BY-SA-4.0)
- Datenlizenz Deutschland – Namensnennung – Version 2.0

Die beiden Lizenzen ODbL und CC-BY-SA-4.0 haben die Besonderheit, dass sie eine Lizenzklausel beinhalten, die verlangt, dass veränderte Datenbanken ebenfalls wieder unter der Ursprungslizenz lizenziert werden müsse, d. h. nur als Open Data genutzt werden dürfen. Diese Lizenzkonzept ist als »Copyleft« oder »ShareAlike« bereits aus der Open Source Welt bekannt. Die anderen genannten Lizenzen machen keine Vorgabe, wie eine eigene Datenbank zu lizenzieren ist, können aber sonstige Lizenzpflichten wie Herkunftshinweise oder die Angabe der Lizenz enthalten.

Für eine einfache Nachnutzung sind daher auch sog. »Public Domain«-Vermerke beliebt, durch die so weitgehend wie möglich auf Urheberrechte verzichtet wird und eine Nachnutzung frei von Lizenzpflichten möglich ist. Dazu gehören die folgenden Public Domain-Erklärungen:

- Commons CCZero (CC0)
- Open Data Commons Public Domain Dedication and Licence (PDDL)
- Datenlizenz Deutschland – Zero – Version 2.0

Bei der Nachnutzung von öffentlich zugänglichen Datenbanken ist folglich darauf zu achten, dass der Datenbankhersteller eine Open Data Lizenz oder sonstige Erlaubnis zur Nutzung erteilt hat. Aus dem Umstand eines unbeschränkten tatsächlichen Zugriffs kann hingegen nicht ohne weiteres auf das Recht zur Weiterverwendung und Übernahme der Daten in eine eigene Datenbank geschlossen werden.

# 9 Aspekte des Veränderungs- managements

## 9 Aspekte des Veränderungsmanagements

Neben den strategischen, organisatorischen und technischen Fragestellungen ist im Rahmen der Einführung und/oder Umstellung auf ein API-basiertes Geschäftsmodell ein wesentlicher Erfolgsfaktor das aktive Management des Veränderungsprozesses. Da hierbei sowohl auf kulturelle wie organisatorische Besonderheiten gleichermaßen eingegangen werden muss, sind die nachfolgenden Ausführungen für Unternehmen der Privatwirtschaft und die öffentliche Hand gleichermaßen relevant.

Wie die »Association of Change Management Professionals« es beschreibt, gilt es beim Management von Veränderungsprozessen einen »strukturierten Ansatz [zu nutzen], um eine Organisation unter Erreichung erwarteter Vorteile vom Ist-Zustand in einen Soll-Zustand zu überführen«. Dass Veränderungen unausweichlich sind und mittlerweile zum neuen Status Quo in der Unternehmensrealität geworden sind, hat auch das PMI (Project Management Institute) erkannt: »Unternehmen, die es (d. h. das Veränderungsmanagement) effizient managen, werden Ihren Wettbewerbern voraus sein«.

Eine aktive Kommunikation der Veränderung berücksichtigt dabei u. a. folgende Prämissen:

- Das »Warum« nach dem Sinn der Veränderung muss frühzeitig geklärt und diskutiert werden.
- Stakeholder (sowohl intern als auch extern) müssen identifiziert und zielgruppengerecht behandelt werden.
- »What's in for me?« – Für jeden Stakeholder sollte diese Frage persönlich, aber auch durch die Stakeholder selbst beantwortet werden.
- Die Unternehmensführung muss ein klares Alignment und damit auch eine klare Kommunikationsstrategie zum Veränderungsmanagement etablieren.
- Eine aktive Kommunikation betrifft auch das Projektteam: hier ist sowohl ein ausreichendes Staffing, die notwendige Management Attention und das Verlassen der Komfortzone essentiell. Aus dem Elfenbeinturm heraus lässt sich kein Paradigmen-Wechsel anstoßen!
- Ein Change Management Plan, der verschiedene Meilensteine beinhaltet, um die Betroffenen zu Beteiligten zu machen sollte aufgestellt werden. Im Falle von potentiellen Kunden stellt dieser Plan einen prädestinierter Ansatzpunkt für Marketing-Maßnahmen dar.

Durch das Anbieten und Nutzen von APIs wird ein neues Ökosystem geschaffen, welches Kunden und Partner gleichermaßen umfasst und über Schnittstellen verbindet. Diese »API-Ökonomie« schafft neue Möglichkeiten für organisationsübergreifende Services. Diese grundlegende Änderung des jeweiligen Geschäftsmodells und der Zusammenarbeit muss im Zentrum der Gestaltung des Veränderungsprozesses stehen und sollte dessen Ausgestaltung maßgeblich bestimmen.

Bei der Umsetzung eines Projekts zur Einführung von APIs müssen je nach Zielgruppe und Fortschritt des Einführungsprojekts unterschiedliche kommunikative Maßnahmen ergriffen werden. Von der initialen Ankündigung per Mail oder auf einer Website (z. B. Blog-Eintrag oder Newsletter), über Pressemitteilungen und aufwändigere Druckerzeugnisse sowie verschiedener Arten der direkten Kommunikation (town hall meetings, Kunden-Events etc.), kann aus einer Vielzahl an Maßnahmen gewählt werden.

# 10 Fazit/ Zusammenfassung/ Ausblick

# 10 Fazit / Zusammenfassung / Ausblick

Mit der Digitalisierung wird nicht nur die Bedeutung von Software in allen gesellschaftlichen Belangen immer grundlegender. Auch erzeugte und verwendete Daten werden immer wertvoller. Damit neue datenorientierte Software-Ecosystems entstehen können, sind entsprechende Möglichkeiten zum Datenaustausch notwendig. Um hier insbesondere Geschwindigkeit und Innovationsfähigkeit im Umgang mit offenen Daten zu ermöglichen, sollten APIs das Mittel der Wahl sein.

Wer sich mit digitalen Ökosystemen, Geschäftsmodellen und Open Data beschäftigt, wird schnell den Aufwand und den Nutzen realistisch einschätzen können. Mit etwas Praxis können hier die notwendigen Aktivitäten und der mögliche Nutzen ausbalanciert werden. Hierbei kann bereits dieser Open Data-Leitfaden helfen. Einmal erfolgreich in das Thema eingestiegen, wird bald die Notwendigkeit für Daten mit großer Aktualität ersichtlich. Dann wird es notwendig, sich mit offenen Schnittstellen zu beschäftigen, die gegenüber offenen statischen Daten sowohl eine höhere Komplexität in der Umsetzung (z. B. bei notwendigen Veränderungen in der Architektur von IT-Systemen) als auch größere Risiken bei fehlerhafter Absicherung der Produktivsysteme bedeuten. Dass dies aber gut handhabbar ist, so lange grundlegende Prinzipien beachtet und auf State-of-the-Art-Technik gesetzt wird, sollte mit diesem Leitfaden aufgezeigt werden.

Die Autor\*innen dieses Leitfadens sind davon überzeugt, dass Open API der nächste wichtige Schritt nach Open Data in der Digitalisierung der deutschen Verwaltung sondern generell in der deutschen Wirtschaft darstellt. Diese sind für zahlreiche zukünftige Entwicklungen essentielle Voraussetzung. Beispielsweise ist für den Einsatz von Künstlicher Intelligenz die Zugänglichkeit von Systemen zur schnellen Datenbeschaffung mittels offener Schnittstellen unabdingbar. Die Technologien dafür existieren bereits. Dieser Leitfaden möchte diese Möglichkeiten aufzeigen und ermuntern, diesen Weg zu gehen.

Da das Thema Open API von hoher Dynamik geprägt ist, kann dieser Leitfaden keine jahrelange Gültigkeit besitzen. Vielmehr möchten die Autor\*innen zum Dialog aufrufen, auf Grundlage dieses Leitfadens das Thema gemeinsam zu entwickeln. Die Autor\*innen freuen sich über Anregungen, um den Leitfaden bedarfsgerecht fortzuschreiben.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

**Bundesverband Informationswirtschaft,  
Telekommunikation und neue Medien e.V.**

Albrechtstraße 10  
10117 Berlin  
**T** 030 27576-0  
**F** 030 27576-400  
bitkom@bitkom.org  
[www.bitkom.org](http://www.bitkom.org)

**bitkom**