

Vorlage für die Sitzung des Senats am 15.07.2025

Zeichnung der Verwaltungsvereinbarung über ein Folgeprojekt für die Entwicklung eines Minimum Viable Products einer bundeseinheitlichen Justizcloud sowie die Einrichtung eines Aufbaustabs für eine Betriebseinrichtung von Bund und Ländern im Rahmen des Projekts e-justice

A. Problem

Auslöser und Grundlage des Projekts e-justice sind das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013 und das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 05.07.2017, mit denen u.a. der verpflichtende elektronische Rechtsverkehr und die gesetzliche Pflicht zur elektronischen Aktenführung in den Gerichten und den Staatsanwaltschaften ab dem 01.01.2026 als Motor der Digitalisierung der Justiz vorgegeben wurden.

Mit Senatsbeschluss vom 09.12.2014 und Beschluss des Haushalts- und Finanzausschusses vom 12.12.2014 wurde die Umsetzung und die Finanzierung des e-justice-Projekts erstmalig beschlossen. Gemäß dem Senatsbeschluss ist zu den jeweiligen Haushaltsaufstellungen zum Umsetzungsstand, zum konkretisierten Mittelbedarf sowie zu den Einspareffekten des e-justice-Projekts zu berichten. Im Zuge der Haushaltsaufstellung 2024/2025 ist über die aktualisierte Planung zum Projekt e-justice zuletzt umfassend zur Sitzung des Senats am 27.02.2024 (Top 5) berichtet worden.

Teil des Projektes ist die dringend nötige Ablösung der Altfachverfahren in der Justiz durch eine gemeinsame Neuentwicklung aller 16 Bundesländer mit dem Namen GeFa (Gemeinsames Fachverfahren). Die Herausforderungen des Betriebs der Neuentwicklung haben zu der in der Anlage 1 beigefügten Untersuchung der Machbarkeit einer Justizcloud geführt. Empfohlen wird darin eine Aufbauphase für einen ersten lauffähigen Teil einer Justizcloud auf der Grundlage einer Verwaltungsvereinbarung. Die in der Anlage 2 beigefügte Verwaltungsvereinbarung über ein Folgeprojekt für die Entwicklung eines „Minimum Viable Products“ einer bundeseinheitlichen Justizcloud sowie die Einrichtung eines Aufbaustabs für eine Betriebseinrichtung von Bund und Ländern soll nun gezeichnet werden.

B. Lösung

Die im Entwurf vorgelegte Verwaltungsvereinbarung wird von der Senatorin für Justiz gezeichnet.

Als Teil des Projektes E-Justice werden die bestehenden Altfachverfahren abgelöst. Voraussetzung für den (wirtschaftlichen) Betrieb ist der Aufbau einer „Minimum Viable Products“ einer souveränen Justizcloud und der länderübergreifend mandantenfähige Betrieb nach dem Einer-für-Alle-Prinzip. An der Justizcloud soll die Dataport AöR als IT-Dienstleister für den Norden beteiligt sein. Die Machbarkeit ist nach der Voruntersuchung gegeben, das Vorhaben soll Basis sein sowohl für GeFa, als auch für weitere gemeinsame Betriebskomponenten nach dem Software-as-a-Service-Prinzip im

Justizumfeld. Dabei werden im Gegensatz zur Deutschen Verwaltungswolke (DVC) auch die Anforderungen der Justiz an Unabhängigkeit und Eigenständigkeit erfüllt. Der erste Schritt zum Aufbau der Justizwolke ist auf der Grundlage einer Verwaltungsvereinbarung der Länder und des Bundes vorgesehen. Den Entwurf dazu hat in Erfüllung eines Auftrages der Justizministerinnen und Justizminister der E-Justice-Rat als Gremium der Justiz-Staatssekretärinnen und -Staatssekretäre in seiner Sitzung am 02.04.2025 zu Top 4 behandelt. Folgende Beschlüsse sind gefasst worden:

1. Der E-Justice-Rat nimmt den Bericht zur Kenntnis.
2. Der E-Justice-Rat beschließt, dass der Aufbaustab in Baden-Württemberg angesiedelt wird.
3. Der E-Justice-Rat beschließt, dass die als Anlage 2 beigefügte Verwaltungsvereinbarung über ein Folgeprojekt für die Entwicklung eines „Minimum Viable Products“ einer bundeseinheitlichen Justizwolke sowie die Einrichtung eines Aufbaustabs für eine Betriebseinrichtung von Bund und Ländern durch Bund und Länder gezeichnet werden soll. Baden-Württemberg wird gebeten, das Verfahren zur Zeichnung der Verwaltungsvereinbarung einzuleiten.
4. Der Aufbaustab wird gebeten, seine Arbeit unmittelbar aufzunehmen.
5. Das Bundesministerium der Justiz wird gebeten, die für eine Entsperrung der erforderlichen Haushaltsmittel aus der Digitalisierungsinitiative für die Justiz notwendigen Schritte vorzunehmen und nach erfolgter Mittelfreigabe das Folgeprojekt unmittelbar aufzunehmen.

Ab Produktivbetrieb der Justizwolke wird nach aktuellem Stand ein gesonderter Staatsvertrag die Grundlage der Zusammenarbeit bilden.

C. Alternativen

Einzige Alternative wäre die Ablehnung einer Beteiligung beim Aufbau der Justizwolke und der Entwicklung eines „Minimum Viable Products“. In dem Fall wäre die Voraussetzung zur Einführung des neuen Fachverfahrens GeFa nicht bzw. nur zu wesentlich höheren Kosten gegeben. Die Mehrkosten bei alleiniger Betriebsverantwortung werden auf mindestens 0,8 Mio. € jährlich geschätzt. Zudem wäre die aus sicherheitstechnischen Aspekten gebotene zeitnahe Ablösung der Altfachverfahren gefährdet und damit auch der Ruf einer funktionierenden und verlässlichen bremischen Justiz. Schließlich könnten weitere Synergieeffekte zum länderübergreifenden gemeinsamen Betrieb nicht gehoben werden.

D. Finanzielle / Personalwirtschaftliche Auswirkungen / Genderprüfung / Klimacheck

1. Finanzielle Auswirkungen

Vorgesehen ist die komplette Finanzierung des Vorhabens aus den Mitteln der Digitalisierungsinitiative durch das Bundesministerium für Justiz (BMJ) bis Ende 2026. Zudem bemüht sich das BMJV zusätzlich um eine weitere Anschubfinanzierung auch nach diesem Zeitpunkt. Als Ausfalloption mit geringer Eintrittswahrscheinlichkeit oder falls die Aufbauarbeiten Verzögerungen unterliegen, verpflichten sich in der Verwaltungsvereinbarung die Länder zu Kostentragung nach aktuellem Königsteiner Schlüssel. Die möglichen Kosten für die Justiz Bremen ab dem 01.01.2027 betragen ca. 0,053 Mio. €

Im Zuge der Aktualisierung der Planungen zum Projekt e-justice wurden im Rahmen der Haushaltsaufstellung 2020/2021 Verpflichtungsermächtigungen bis 2029 über 6,274 Mio € investiv und 29,923 Mio. € konsumtiv eingeplant, welche mit Zustimmung des Haushalts- und Finanzausschusses vom

03.07.2020 entsprechend erteilt worden sind. Etwaige Kosten ab dem 01.01.2027 bis zum Abschluss des Projekts könnten innerhalb der bestehenden Verpflichtungsermächtigungen abgebildet werden.

2. Personalwirtschaftliche Auswirkungen

Es handelt sich um betriebliche Rahmenbedingungen von IT-Fachverfahren. Deswegen hat das Vorhaben keine unmittelbaren personalwirtschaftlichen Auswirkungen.

3. Genderprüfung

In der Justiz werden überwiegend Frauen beschäftigt (ca. 60%), womit die Maßnahme zunächst überwiegend das Arbeitsumfeld dieser betrifft.

Mit der Einführung der vollelektronischen Akte und der Ablösung der Altfachverfahren werden in allen Bereichen Tätigkeiten im Homeoffice ermöglicht werden. Mit dieser Möglichkeit werden insbesondere auch entsprechende subjektive Bedürfnisse nach Veränderungen bei der Vereinbarkeit von Familie und Beruf befriedigt werden können. Welche objektiven gesellschaftlichen Auswirkungen eine steigende Homeofficequote (insbesondere bei Frauen) auf das Geschlechterverhältnis haben wird, erscheint gegenwärtig nicht valide prognostizierbar zu sein.

Die Justiz wird von Menschen jeden Geschlechtes in beruflichen und privaten Kontexten genutzt, so dass unmittelbar aus den Maßnahmen für die Nutzerinnen und Nutzer keine Genderrelevanz zu erwarten ist. Welche langfristigen strukturellen Veränderungen sich aus der Digitalisierung ansonsten in beruflichen Kontexten der Rechtspflege außerhalb der Justiz ergeben können, ist offen.

4. Klimacheck

Die Beschlüsse in der Senatsvorlage führen voraussichtlich zu einer Abnahme der Treibhausgasemissionen um bis zu 50 t CO² jährlich und haben daher positive Auswirkungen auf den Klimaschutz.

Hinweise zu positiven Auswirkungen auf den Klimaschutz:

Durch die gemeinsame Nutzung von Rechenzentrumsressourcen aller Bundesländer und des Bundes in der Justizcloud werden weniger Rechenzentren benötigt, die auch insgesamt weniger Energie verbrauchen.

E. Beteiligung / Abstimmung

Die Vorlage ist mit dem Senator für Finanzen und der Senatskanzlei abgestimmt.

F. Öffentlichkeitsarbeit/ Veröffentlichung nach dem Informationsfreiheitsgesetz

Eine Veröffentlichung der Senatsvorlage nach dem Informationsfreiheitsgesetz kann nach Beschlussfassung erfolgen. Anlage 1 ist bereits veröffentlicht auf der Webseite des BMJV. Anlage 2 kann erst nach Beteiligung der Länder und des Bundes veröffentlicht werden.

G. Beschluss

Der Senat ermächtigt die Senatorin für Justiz zur Zeichnung der Verwaltungsvereinbarung über ein Folgeprojekt für die Entwicklung eines „Minimum Viable Products“ einer bundeseinheitlichen Justizcloud sowie die Einrichtung eines Aufbaustabs für eine Betriebseinrichtung von Bund und Ländern.

Anlagen

1. Entwurf der Verwaltungsvereinbarung über ein Folgeprojekt für die Entwicklung eines „Minimum Viable Products“ einer bundeseinheitlichen Justizcloud sowie die Einrichtung eines Aufbaustabs für eine Betriebseinrichtung von Bund und Ländern nebst Begründung
2. Abschlussbericht Untersuchung der Machbarkeit einer bundeseinheitlichen Justizcloud

Abschlussbericht

Untersuchung der Machbarkeit
einer bundeseinheitlichen Justizcloud

Vorwort

Die Digitalisierung der Justiz in Bund und Ländern schreitet voran. Bedeutende Fortschritte wurden im elektronischen Rechtsverkehr, in der elektronischen Aktenführung, bei der Einführung moderner Fachverfahren sowie der Nutzung zukunftsweisender Technologien wie KI erzielt. Doch die Justiz sieht sich auch Herausforderungen gegenüber. Vor allem die fragmentierte, heterogene IT-Landschaft erschwert die Ausbringung gemeinsam entwickelter Verfahren und bindet sachliche und personelle Ressourcen in Zeiten knapper Haushalte und des Fachkräftemangels.

Ein Ansatz zur Bewältigung dieser Herausforderungen kann Cloud-Technologie sein. Der Auftrag des *Bund-Länder-Digitalgipfels* vom März 2023 war klar: „Ist eine bundeseinheitliche Justizcloud machbar?“

Ab Januar 2024 trieben die Länder und der Bund dieses Projekt mit großem Engagement gemeinsam voran. Über 200 Teilnehmende gaben tiefe Einblicke in die heutige Situation und waren fortan aktiv am Entwicklungsprozess beteiligt. Unsere Vision: „Gemeinsame Technologien für eine unabhängige und zukunftsfähige Justiz“.

Justizministerien, IT-Dienstleister und Entwicklungsverbünde teilten ihre Sorgen, aber auch Ideen. Durch interaktive

Zusammenarbeit wurden in Fachpanels und Cloud-Sprechstunden alle gehört und auf die „Reise in die Cloud“ mitgenommen.

Im monatlichen Sounding Board, bestehend aus den Ländern und dem Bund, wurden gemeinsame Lösungen im strategischen Dialog gefunden. Die ergebnisoffene Gestaltung des Prozesses ermöglichte es allen Beteiligten, ihre Perspektiven und Wünsche einzubringen, Herausforderungen zu benennen, Vorschläge kritisch zu hinterfragen und gleichzeitig Wissen und Vertrauen aufzubauen.

Das Ergebnis ist eindeutig: Die Justizcloud ist machbar und könnte passgenau von der Justiz für die Justiz im föderalen Gefüge errichtet werden. Sie würde auf vertrauter Infrastruktur aufbauen und böte einen souveränen Zugang zu innovativen Cloud-Technologien für eine moderne, nutzendenzentrierte Anwendungslandschaft.

Dieses Projekt ist ein eindrucksvolles Beispiel für die erfolgreiche Zusammenarbeit von Bund und Ländern, bei der der Austausch von Wissen und Kompetenzen nachhaltige Lösungen schafft. Unser besonderer Dank gilt allen Beteiligten für die inspirierende und konstruktive Zusammenarbeit auf unserem Weg in die Cloud.



Autoren und Mitwirkende

Die Untersuchung wurde erstellt durch die Accenture GmbH im Auftrag des Bundesministeriums der Justiz.

Wir danken allen Mitwirkenden für die Zusammenarbeit:

Bayerisches Landesamt für Steuern/ Rechenzentrum Nord
Bayerisches Staatsministerium der Justiz
Behörde für Justiz und Verbraucherschutz der Freien Hansestadt Hamburg
Bundesamt für die Sicherheit in der Informationstechnik
Bundesamt für Justiz
Bundesarbeitsgericht
Bundesfinanzhof
Bundesgerichtshof
Bundesministerium der Justiz
Bundesministerium des Innern und für Heimat
Bundesministerium für Arbeit und Soziales
Bundesnotarkammer
Bundespatentgericht
Bundesrechtsanwaltskammer
Bundessozialgericht
Bundesverfassungsgericht
Bundesverwaltungsgericht
Bund-Länder-Kommission für Informationstechnik in der Justiz inkl. AGs
Bund-Länder-Kommission Architekturbüro
Dataport
Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V)
Deutsche VerwaltungscLOUD
Die Senatorin für Justiz und Verfassung der Freien Hansestadt Bremen
DigitalService GmbH
Entwicklungsverbünde (GeFa, AuRegis, dabag, bk.text, e2T)
Föderale IT-Kooperation (FITKO)
govdigital eG
Hessische Zentrale für Datenverarbeitung (HZD)

Hessisches Ministerium für Justiz und für den Rechtsstaat
Information und Technik Nordrhein-Westfalen (IT.NRW)
IT-Dienstleistungszentrum Berlin (ITDZ Berlin)
IT-Servicezentrum der bayerischen Justiz (Jus-IT)
Justiz-IT Saarland
Landesbetrieb Daten und Information (LDI)
Landesoberbehörde IT Baden-Württemberg (BITBW)
Leitstelle für Informationstechnologie der sächsischen Justiz (LIT)
Ministerium der Justiz des Landes Brandenburg
Ministerium der Justiz des Landes Nordrhein-Westfalen
Ministerium der Justiz Rheinland-Pfalz
Ministerium der Justiz Saarland
Ministerium der Justiz und für Migration Baden-Württemberg
Ministerium für Justiz und Gesundheit des Landes Schleswig-Holstein
Ministerium für Justiz und Verbraucherschutz des Landes Sachsen-Anhalt
Ministerium für Justiz, Gleichstellung und Verbraucherschutz des Landes Mecklenburg-Vorpommern
Niedersächsisches Justizministerium
Sächsisches Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung
Senatsverwaltung für Justiz und Verbraucherschutz Berlin
Staatsbetrieb Sächsische Informatik Dienste (SID)
Thüringer Landesrechenzentrum (TLRZ)
Thüringer Ministerium für Migration, Justiz und Verbraucherschutz
Zentraler IT-Betrieb niedersächsische Justiz (ZIB)
Zentraler IT-Dienstleister der Justiz des Landes Brandenburg (ZenIT)
Zentraler IT-Dienstleister der Justiz des Landes NRW (ITD)

Inhaltsverzeichnis

Vorwort.....	2
Autoren und Mitwirkende.....	3
Management Zusammenfassung.....	13
1 Motivation und Vorgehen.....	15
1.1 Ausgangslage und Zielsetzung	15
1.1.1 Herausforderungen der Justizdigitalisierung	15
1.1.2 Cloud als Digitalisierungsbeschleuniger und Effizienztreiber	17
1.1.3 Politische Rahmenbedingungen und Projektauftrag	20
1.2 Projektvorgehen & Governance	21
1.2.1 Projektvorgehen und Rahmenwerk	21
1.2.2 Governance und Zusammenarbeit	23
2 Ist-Analyse.....	26
2.1 Zusammenfassende Erkenntnisse der Ist-Analyse	26
2.2 Detailergebnisse der Ist-Analyse.....	32
2.2.1 Anwendungslandschaft der Justiz	33
2.2.1.1 Analyse der Anwendungslandschaft der internen Domäne.....	38
2.2.1.2 Analyse der Anwendungslandschaft der externen Domäne.....	51
2.2.2 IT-Betrieb der Länder	57
2.2.3 Relevante Cloud-Initiativen	68
2.2.3.1 Bewertung relevanter Cloud-Initiativen	72
2.2.3.2 Internationale justiznahe Beispiele für Cloud-Nutzung.....	76
2.2.4 Zukunftsanforderungen der Justiz	78
2.2.4.1 Übersicht identifizierter Zukunftsanforderungen	80
2.2.4.2 Detailanalyse priorisierter Zukunftsanforderungen	81
2.2.4.3 Wesentliche Erkenntnisse zu Zukunftsanforderungen	85
3 Justizcloud-Zielbild	87
3.1 Prämissen und Strukturierung des Zielbilds.....	87
3.1.1 Prämissen und Bewertungsrahmen.....	87
3.1.2 Strukturierung des Zielbilds	89
3.2 Vision, Mission und strategische Ziele	91
3.3 Integriertes, machbares Justizcloud-Zielbild	96
3.3.1 Übergreifendes Justizcloud-Betriebsmodell	96
3.3.2 Fachliche und technische Ebene der Justizcloud-Plattform	98
3.3.3 Organisation zum Betrieb der Justizcloud-Plattform	102

3.3.4	Integration der Zielbildebene	104
3.4	Fachliche Zielbildebene	105
3.4.1	Abgrenzung Cloud-Nutzende	106
3.4.2	Justizcloud-Anwendungslandschaft	107
3.4.2.1	Anwendungslandschaft der internen Domäne	109
3.4.2.2	Anwendungslandschaft der externen Domäne	112
3.4.3	Mandantenkonzept für Anwendungen	117
3.4.4	Schnittstellenkonzept	120
3.4.4.1	Schnittstellenarten und -architekturen	121
3.4.4.2	Integrationswege und Architekturprinzipien	125
3.4.5	Datenkonzept	129
3.4.5.1	Datengovernance und Datenhaltung	129
3.4.5.2	Skalierbare Speicherkapazitäten	132
3.4.5.3	Datenaustauschkonzept	133
3.4.5.4	Justizcloud-Datendienste bzw. -Plattform	134
3.4.6	Identitäten-, Berechtigungs- und Administrationskonzept	136
3.4.6.1	Internes Identitäten- und Berechtigungsmanagement	136
3.4.6.2	Externes Kundenidentitäten- und Berechtigungsmanagement	141
3.4.7	Serviceportfoliostrategie und Servicekatalog	143
3.4.7.1	Serviceportfoliostrategie der Justizcloud	144
3.4.7.2	Entwurf Justizcloud Servicekatalog	145
3.5	Technische Zielbildebene	149
3.5.1	Auswahl des Bereitstellungsmodells	150
3.5.1.1	Bereitstellungsmodelle und Souveränität	150
3.5.1.2	Untersuchte Potenzialebenen	158
3.5.1.3	Bewertung möglicher Bereitstellungsmodelle	168
3.5.1.4	Auswahl des Bereitstellungsmodells	171
3.5.2	Netzkonzept	177
3.5.2.1	Virtuelles Netzwerk für die Justiz-Community-Cloud	177
3.5.2.2	Justiznetz in den Netzen des Bundes	180
3.5.2.3	Justizcloud Zertifikate-Provider	183
3.5.2.4	Justizcloud-Netzwerksegmentierung	183
3.5.3	Mandantenkonzept der Plattform	186
3.5.4	Justizcloud-Plattformdienste	188
3.5.4.1	Cloud-Management-Plattform	188
3.5.4.2	Container-Plattform	190

3.5.4.3	Integrationsplattform	192
3.5.5	Plattform-Administrationskonzept	196
3.5.5.1	Administration und Admin-IAM	196
3.5.5.2	Föderation von Administratoren	197
3.5.6	Justizcloud-Entwicklerarbeitsplatz	199
3.5.7	Justizcloud-Proof-of-Concept	204
3.6	Rechtlich-organisatorische Zielbildebene	207
3.6.1	Wertschöpfungstiefe der Justizcloud	207
3.6.2	Aufgaben, Anforderungen und Rahmenbedingungen	211
3.6.3	Organisationsmodell der Justizcloud	212
3.6.3.1	Strategische Organisationsebene	215
3.6.3.2	Operative Organisationsebene	217
3.6.4	Ausgestaltung der agilen Justizcloud-Einheit	221
3.6.5	Personalbedarf und -strategie	225
3.6.6	Rechtsform und Finanzierung	230
4	Wirtschaftlichkeitsbetrachtung	232
4.1	Szenarioentwicklung und Annahmen	233
4.1.1	Szenarioentwicklung	233
4.1.2	Annahmen zu Kostenblöcken	235
4.1.3	Annahmen zur Cloud-Plattform	238
4.1.4	Annahmen zur Cloud-Anwendungslandschaft	239
4.2	Datenerhebung und Schätzung	240
4.2.1	Schätzung Personal- und Sachkosten	241
4.2.2	Schätzung Betriebskosten	243
4.2.3	Schätzung Kosten für Weiterentwicklung und Pflege	246
4.2.4	Schätzung Investitionskosten	248
4.3	Ergebnisse und Bewertung	250
4.4	Zusatzmehrwerte einer Justizcloud	252
5	Strategisch-planerisches Konzept	254
5.1	Roadmap	255
5.1.1	Justizcloud-Fundament	258
5.1.1.1	Initiierungs- und Vorbereitungsphase	260
5.1.1.2	Aufbau und Pilotierung	261
5.1.1.3	Ausbau und Skalierung	262
5.1.2	Justizanwendungslandschaft	264

5.1.3	Strategisches Anforderungsmanagement inkl. Architekturboard	267
5.1.4	Strategische Steuerung und Agilisierung	269
5.2	Stakeholderkommunikation	270
5.2.1	Identifikation und Analyse der Stakeholder	270
5.2.2	Kommunikationsstrategie	272
6	Glossar	274
7	Anhang	283
7.1	Standardisierter Fragebogen Justizanwendungen	283
7.2	Standardisierter Fragebogen IT-Dienstleister	285

Hinweise:

Im Interesse einer besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Grün hinterlegter Text sind [Verlinkungen](#) zu externen Webseiten. Kapitel-, Tabellen- und Abbildungsreferenzen führen per Klick zum entsprechenden Textabschnitt.

Tabellenverzeichnis

Tabelle 1 Themenbereiche der Ist-Analyse	33
Tabelle 2 Wesentliche Funktionsblöcke und Beispielanwendungen der Justiz	38
Tabelle 3 Übersicht analysierter Anwendungen	47
Tabelle 4 Übersicht Postfächer und SAFE-public Instanzen	54
Tabelle 5 Übersicht aller durch die Justiz genutzten öffentlichen IT-Dienstleister	59
Tabelle 6 Besondere bundesweite Cloud-Initiativen	70
Tabelle 7 Übersicht wesentlicher Zukunftsanforderungen der Justiz	80
Tabelle 8 Übersicht Sach- und Personalkosten	241
Tabelle 9 Jährliche Kosten im laufenden Betrieb (Aggregierte Sicht)	243
Tabelle 10 Jährliche Kosten im laufenden Betrieb (Detailsicht)	245
Tabelle 11 Jährliche Kosten für Weiterentwicklung und Pflege	247
Tabelle 12 Investitionskosten für Szenario S1	249

Abbildungsverzeichnis

Abbildung 1 Überblick zu Ausgangslage und Herausforderungen der Justiz	16
Abbildung 2 Projektvorgehen in drei Phasen	21
Abbildung 3 Strategisches Cloud-Rahmenwerk (Fa. Accenture)	22
Abbildung 4 Projektgovernance in der Zielbildentwicklungsphase	24
Abbildung 5 Abgrenzung des Untersuchungsrahmens	30
Abbildung 6 Abhängigkeitsmatrix <i>bk.text</i>	44
Abbildung 7 Komplexität der Ausbringung von Justizanwendungen (illustrativ)	50
Abbildung 8 Übersicht Online-Services	51
Abbildung 9 Archetypen zur Kategorisierung von Online-Services	52
Abbildung 10 Nutzendengruppen analysierter Online-Services	53
Abbildung 11 Übersicht der IT-Dienstleister-Archetypen	60
Abbildung 12 Ausbringungskomplexität einheitlicher Software auf heterogene Umgebungen	65
Abbildung 13 Übersicht in Deutschland führender kommerzieller Cloud-Angebote	69
Abbildung 14 Internationale Beispiele für Cloud-Initiativen im Justizbereich	77
Abbildung 15 Übersicht Abhängigkeiten bzw. Synergiepotenziale zwischen Zukunftsthemen	86
Abbildung 16 Prämissen für die Zielbildentwicklung	88

Abbildung 17 Ebenen des integrierten Zielbilds	89
Abbildung 18 Strategische Ziele der bundeseinheitlichen Justizcloud	92
Abbildung 19 Gegenüberstellung Betriebsmodell mit und ohne Justizcloud.....	97
Abbildung 20 Zielbild Justizcloud-Plattform	98
Abbildung 21 Organisatorisches Zielbild Justizcloud-Einheit	103
Abbildung 22 Beispiele der integrierten Zielebenen	104
Abbildung 23 Abgrenzung Cloud-Nutzende	106
Abbildung 24 Justizcloud-Domänenmodell	108
Abbildung 25 Zielbild Anwendungslandschaft der internen Domäne	110
Abbildung 26 Zielbild Anwendungslandschaft der externen Domäne	116
Abbildung 27 Architekturmodelle für Mandantenfähigkeit	118
Abbildung 28 Multi-Tenant Betrieb vs. Mandantenfähiger Cloud-Betrieb.....	120
Abbildung 29 Typische Integrationsarchitekturen	121
Abbildung 30 Vergleich Client- vs. Server-Integration für eAkten-Rahmen.....	124
Abbildung 31 Überblick Integrationswege	126
Abbildung 32 Beispielhafte Schutzmaßnahmen nach Schutzbedarf.....	130
Abbildung 33 Modelle der Cloud-Datenhaltung	131
Abbildung 34 Übersicht Datenplattform-bezogener Cloud-Dienste.....	135
Abbildung 35 IAM und CIAM	136
Abbildung 36 IAM-Ausbringungsmodelle und Föderation	139
Abbildung 37 Delegation von Administrationsrechten	140
Abbildung 38 Cloud-nutzende Justizcloud-Plattformdienste	143
Abbildung 39 Illustrative Portfolioplanung der Justizcloud	145
Abbildung 40 Entwurf eines Justizcloud-Servicekatalogs	146
Abbildung 41 Logisches Cloud-Kontinuum.....	150
Abbildung 42 Auszug eines exemplarischen Cloud-Services-Katalogs	151
Abbildung 43 Cloud-Souveränitätskontinuum und -beispiele (Accenture)	154
Abbildung 44 Beispielhafte Private Cloud-Architektur (Accenture)	156
Abbildung 45 Cloud-Management-Software Kategorien und Markt (Gartner)	156
Abbildung 46 Potenzialebenen und Synergiepotenziale	158
Abbildung 47 Vor- und Nachteile einer Vereinheitlichung auf physischer Infrastrukturebene	159

Abbildung 48 Vor- und Nachteile einer Vereinheitlichung auf virtueller Infrastrukturebene	160
Abbildung 49 Vor- und Nachteile einer alleinigen Vereinheitlichung auf Plattformebene	161
Abbildung 50 Vor- und Nachteile einer alleinigen Vereinheitlichung auf Anwendungsebene	162
Abbildung 51 Präferiertes Bereitstellungsmodell	163
Abbildung 52 Denkbare Bereitstellungsmodelle auf physischer Infrastrukturebene	165
Abbildung 53 Denkbare Bereitstellungsmodelle auf virtueller Infrastrukturebene	167
Abbildung 54 Mögliche Evolutionsstufen präferierter Bereitstellungsmodelle	170
Abbildung 55 Funktionsweise eines virtuellen, Software Defined Netzwerks	178
Abbildung 56 Aufbau eines virtuellen, Software Defined Netzwerks	179
Abbildung 57 Mögliche Verantwortungsschnitte beim Netzbetrieb mit <i>BDBOS</i>	181
Abbildung 58 Souveränität der Justiz in den Netzen des Bundes steigt mit dem NdB Justiznetz	182
Abbildung 59 Netzwerkerweiterungen durch Hub-and-Spoke-Modell	184
Abbildung 60 Typische Netzwerksegmentierung für Hybrid-Cloud	185
Abbildung 61 Varianten der Mandantentrennung	186
Abbildung 62 Cloud-Service-Governance mit Cloud-Management-Plattform	189
Abbildung 63 Container-Plattform im Kontext einer Cloud-Architektur (Accenture)	190
Abbildung 64 Beispielhaftes Container-Cluster mit Service Mesh und Plattformdiensten	192
Abbildung 65 Funktionsumfang von Integrationsplattformen	193
Abbildung 66 Funktionsumfang eines API-Gateway	193
Abbildung 67 Integrationsherausforderungen im Länderkontext	194
Abbildung 68 Ablaufsequenz einer Anbindung von Länderumgebungen	195
Abbildung 69 Identitäten-Föderationsverfahren für Administratoren	198
Abbildung 70 Aufgabenschnitt bei Continuous Integration und Delivery	199
Abbildung 71 DevSecOps Zyklus entlang einer CI/CD-Prozesskette	200
Abbildung 72 CI/CD ohne (vorher) und mit Justizcloud (nachher)	201
Abbildung 73 Mehrwerte des „Shift-Left“-Ansatzes	202
Abbildung 74 Integration und Ausbringung im Status Quo vs. mit Justizcloud	202
Abbildung 75 Integrierte Engineering Intelligence Plattform	203
Abbildung 76 Justizcloud-PoC im Schichtenmodell	204
Abbildung 77 Wertschöpfungstiefe der Justizcloud	208
Abbildung 78 Einschätzung erforderlicher Eigenständigkeit der Justizcloud	213

Abbildung 79 Justizcloud-Organisationsmodell	215
Abbildung 80 Zielbild der agilen Justizcloud-Einheit inkl. Rollen	221
Abbildung 81 Kernteam der Justizcloud-Einheit	226
Abbildung 82 Strategien zur Personalbedarfsdeckung	228
Abbildung 83 Übergang von Aufbaustab zu eigenständiger Justizcloud-Einheit	231
Abbildung 84 Vorgehensmodell der Wirtschaftlichkeitsbetrachtung	232
Abbildung 85 Cloud-Anwendungsbetrieb mit und ohne bundeseinheitliche Justizcloud	233
Abbildung 86 Übersicht relevanter Kostenblöcke in den Szenarien	235
Abbildung 87 Software-Ausbringungsmodelle in den Szenarien S0 vs. S1	237
Abbildung 88 Komponenten der Cloud-Plattform in S0 und S1	239
Abbildung 89 Mittelfristig angenommenes Cloud-Anwendungsgefüge in S0 und S1	240
Abbildung 90 Gesamtsicht Einsparungen und Investitionen (in Jahren)	250
Abbildung 91 Barwertbetrachtung der Investition in Justizcloud (S1)	251
Abbildung 92 Kostenentwicklung für die Justizcloud-Plattform und -Anwendungslandschaft	252
Abbildung 93 Zusätzliche Mehrwertpotenziale einer Justizcloud	253
Abbildung 94 Übersicht vorgeschlagener Wertströme	257
Abbildung 95 Grobe Roadmap Justizcloud-Fundament	258
Abbildung 96 Indikative Roadmap für das Justizcloud-Fundament	259
Abbildung 97 Erfolgsfaktoren für den Aufbau des Justizcloud-Fundaments	263
Abbildung 98 Zielbild initialer Anwendungslandschaft in Justizcloud-Umgebung	264
Abbildung 99 Erfolgsfaktoren für die Justizcloud Anwendungslandschaft	266
Abbildung 100 Erfolgsfaktoren für das strategische Anforderungsmanagement und Architekturboard	268
Abbildung 101 Erfolgsfaktoren für die strategische Steuerung und Agilisierung	269
Abbildung 102 Übersicht der Stakeholdergruppen im engen und erweiterten Kontext	270
Abbildung 103 Übersicht Kernbotschaften für die Justizcloud-Kommunikation	272



Unsere Vision

**Gemeinsame Technologien für eine
unabhängige und zukunftsfähige Justiz**

Management Zusammenfassung

Cloud-Technologien sind Innovations- und Effizienztreiber. Ohne die Nutzung moderner Cloud-Plattformen kann die Justiz bspw. die **Vorteile moderner Fachverfahren** wie das länderübergreifende gemeinsame Registerfachverfahren (*AuRegis*) und das Gemeinsame Fachverfahren (*GeFa*) nicht voll ausschöpfen.

- Moderne Software wird heute auf Cloud-Plattformen und mit Cloud-Standards entwickelt und betrieben, um **signifikante Qualitäts-, Geschwindigkeits-, Skalierbarkeits- und Kostenvorteile** zu realisieren.
- Die Justiz entwickelt bereits alle neuen Fachverfahren **Cloud-nativ**, kann sie aber nicht überall ausbringen.
- Cloud-Plattformen bieten zudem viele **innovative Dienste**, die in traditionellen Rechenzentren kaum bereitgestellt werden können, weshalb einige Justiz-IT-Dienstleister lokale Cloud-Projekte verfolgen.

Die Justiz könnte **Investitionen in eine bundeseinheitliche Justizcloud bündeln**, um darauf die zukunftsfähige Justizanwendungslandschaft nicht nur einheitlich zu entwickeln, sondern auch einheitlich zu betreiben.

- Die vorliegende Untersuchung und ein Proof-of-Concept zeigen, dass eine bundeseinheitliche Justizcloud **fachlich, technisch und rechtlich-organisatorisch machbar** ist.
- Die Justizcloud **bindet dabei bestehende IT-Dienstleister** – deren Infrastrukturen und Cloud-Dienste – **aktiv ein**. Dafür werden Konzepte der **govdigital eG** und **Deutschen VerwaltungscLOUD-Strategie (DVS)** nachgenutzt.
- Eine gemeinsame Justizcloud-Einheit könnte das **Cloud-Know-how** bündeln und damit dem **Fachkräftemangel** gerade im IT-Bereich, **knappen Budgets** der Justizhaushalte sowie den nicht ausreichenden bzw. fehlenden Cloud-Kapazitäten begegnen.
- Der **gemeinsame Aufbau vermeidet** auch lokale **Risiken und Verzögerungen** beim Weg in die Cloud.

Die **Justiz** kann durch die Justizcloud und den dadurch ermöglichten **bundeseinheitlichen Betrieb von Plattform und Anwendungslandschaft Einsparungen** von **bis zu 337 Mio. EUR bis 2034** realisieren.

- Der Betrieb moderner Fachverfahren erfordert den **Aufbau neuer Cloud-Umgebungen** (z. B. Container-Plattformen), die **entweder jeweils separat pro Land oder einmal bundeseinheitlich** errichtet werden können.

- Der **Verfahrensbetrieb** wäre **pro Anwendung in der Justizcloud deutlich günstiger** im Vergleich zum eigenständigen Betrieb auf heterogenen Plattformen der Länder.
- Zudem gäbe es **signifikante Aufwands- und Zeitersparnisse** bei **Inbetriebnahme und Weiterentwicklung von Fachverfahren** durch einen **einheitlichen Entwicklerarbeitsplatz** in der Justizcloud.
- Für den **Aufbau der bundeseinheitlichen Justizcloud** wären in den kommenden sechs Jahren **einmalig 72-87 Mio. EUR** zu investieren. Der Bund möchte hierfür in den Jahren 2025 und 2026 eine **substanzielle Anschubfinanzierung** aus der Digitalisierungsinitiative für die Justiz bereitstellen. Die Höhe der verfügbaren Mittel ist aktuell in Prüfung.
- Beim **Betrieb** entstehen **ab 2027** sukzessive Kosten für die Plattform und den einheitlichen Anwendungsbetrieb. In der vollen Ausbaustufe fielen für die **Plattform** Kosten von **10-14 Mio. EUR** p.a. an. Für den **Anwendungsbetrieb** fielen zudem etwa **12-16 Mio. EUR** p.a. bei den Entwicklungs- bzw. Betriebsverbänden an.

Durch die Justizcloud entstünden **weitere Vorteile** gegenüber heterogenen Plattformen.

- Ein einheitlicher Entwicklerarbeitsplatz steigert Effizienz und Konsistenz der Entwicklungsverbünde und erlaubt es, **Anwendungen** früher miteinander zu **integrieren, automatisiert zu testen und auszubringen**.
- **Häufigere Softwareupdates** ohne Wartungsfenster ermöglichen schnelleres Feedback, kundenzentrierteres Arbeiten und **gleichzeitig hohe Entlastungen** der IT- und Fachbereiche durch **Testautomation**.
- Eine Justizcloud-Plattform ermöglicht trotz dezentraler Datenhaltung **gemeinsame Teilhabe an innovativen Diensten**, z. B. für Datenanalyse, Übersetzung sowie **KI**.
- Die Justizcloud bereitet das **Fundament für viele Zusatzpotenziale**, wie z. B. *Elektronische Gefangenenpersonalakte (eGPA)*, Beweismittelcloud, einen gemeinsamen Datenraum zum Teilen statt Versenden von Daten, gemeinsame KI-Nutzung uvm.
- Das Aufspannen eines **Justiznetzwerks für die Justizcloud** würde der Unabhängigkeit der dritten Gewalt entsprechen und die IT-Sicherheit verbessern.

In **2025 könnte die Vorbereitungsphase der Justizcloud starten**. Bei positivem Beschluss durch Bund und Länder in 2024 wäre **bis Anfang 2027** die Umsetzung der **ersten Justizcloud-Ausbaustufe machbar**.

1 Motivation und Vorgehen



1.1 Ausgangslage und Zielsetzung

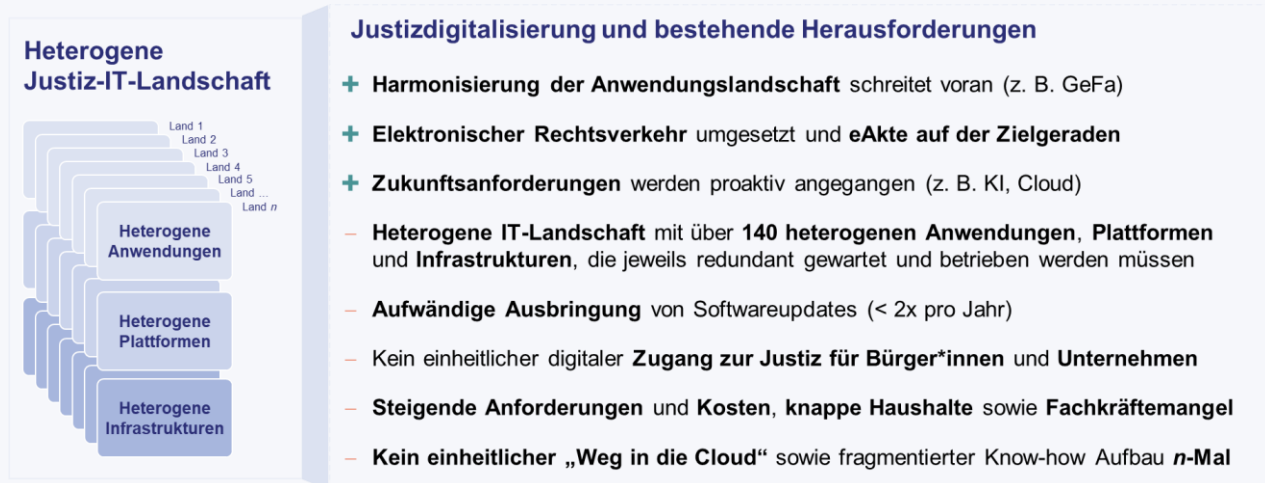
1.1.1 Herausforderungen der Justizdigitalisierung

Auf dem *Bund-Länder-Digitalgipfel* der Justizministerinnen und -minister (*BLDG*) im März 2023 wurde die Digitalisierung der Justiz als zentrales Zukunftsthema mit einem hohen Stellenwert für einen modernen Rechtsstaat hervorgehoben. Wichtige Ziele sind dabei u. a. Bürgernähe, barrierefreier Zugang zum Recht, Diskriminierungsfreiheit und Effizienz. Wichtiger Bestandteil der fortschreitenden Digitalisierung ist auch der Erhalt digitaler Souveränität und ein nachhaltiger Einsatz von Informationstechnik. Die Justiz hat als Dritte Gewalt besondere Anforderungen an ihre Unabhängigkeit. Gleichzeitig sollen digitale Lösungen dem neuesten Stand der Technik entsprechen und nicht hinter der freien Wirtschaft zurückbleiben. Daraus ergeben sich eine Vielzahl fachlicher, technischer und rechtlich-organisatorischer Anforderungen.

Die Justiz schreitet bei der Umsetzung ihrer Digitalisierungsziele zügig voran. Ein zentraler Eckpfeiler der Justizmodernisierung ist die laufende Umsetzung der *elektronischen Aktenführung* (*eAkte*). Mit dem *elektronischen Rechtsverkehr* (*ERV*) wurde ein digitaler Kanal zur Kommunikation der Justiz mit Bürgern und professionellen Nutzenden (Rechtsanwälte, Notare, Unternehmen) geschaffen und zugleich die justizinterne Kommunikation digitalisiert. Zudem wurde mit großen, bundeseinheitlichen Entwicklungsprojekten wie dem *Gemeinsamen Fachverfahren* (*GeFa*) sowie dem *länderübergreifenden gemeinsamen Registerfachverfahren* (*AuRegis*) ein erster Schritt zur Harmonisierung und Modernisierung der Anwendungslandschaft der Justiz gegangen. Die neuen Anwendungen sollen dabei sowohl moderne technische Standards erfüllen, benutzerfreundlich sein als auch durch eine gemeinsame Entwicklung aller Länder Effizienzgewinne und eine höhere Einheitlichkeit in der föderal organisierten Justiz schaffen. Darüber hinaus werden in einer Vielzahl von Initiativen Zukunftsanforderungen der Justiz adressiert, wie z. B. durch den Aufbau einer KI-Plattform. Mit der Entwicklung einer *Digitalen Rechtsantragstelle* (*RAST*) und dem *Zivilgerichtlichen Onlineverfahren* (*ZOV*) wird auch die Entwicklung moderner Online-Dienstleistungen für

Bürger und andere Nutzende, wie Rechtsanwälte, Notare und Steuerberater, aktiv vorange-
trieben.

Abbildung 1 | Überblick zu Ausgangslage und Herausforderungen der Justiz



Neben diesen Erfolgen bestehen in der Justiz fachliche, technische und rechtlich-organisatorische Herausforderungen, um eine gesamthafte, digitale Transformation umzusetzen. Aktuell ist die IT-Landschaft der Justiz geprägt von hoher Heterogenität der Anwendungslandschaft mit vielen Insellösungen, die in Bund und Ländern redundant betrieben werden. Die mehr als 140 Anwendungen sind meist in monolithischen Architekturen konzipiert, nutzen veraltete Technologien und sind durch hohe Abhängigkeiten wenig flexibel und teuer in Betrieb sowie in Weiterentwicklung. Auch die IT-Plattformen und -Infrastrukturen der Länder sind heterogen und es fehlen übergreifende Standards, die konsequent festgelegt und umgesetzt werden. Dies alles erschwert die Entwicklung und Ausbringung moderner Software und bremst somit die Justizdigitalisierung.

Gleichzeitig verändert der technische Fortschritt die Anforderungen und die Möglichkeiten im IT-Bereich rasant. Entwicklungszyklen haben sich deutlich beschleunigt und durch moderne Verfahren, wie z. B. Ende-zu-Ende Continuous Integration und Continuous Deployment-Strecken (sog. CI/CD-Pipelines), können Softwareanpassungen schnell und oft ohne Ausfallzeiten realisiert werden. Steigende Datenmengen oder neue Anforderungen an Rechenleistung (z. B. durch KI) erfordern hochverfügbare und idealerweise flexibel einsetzbare Daten- und Ressourcenkapazitäten. Zudem ermöglichen moderne Integrationsverfahren (z. B. Application Programming Interfaces (APIs)) über schnelle, flexible Vernetzung,

Datenstandards und Automatisierung die Schaffung komplexer digitaler Ökosysteme und Servicemodelle. Das verändert auch die Aufgaben der Justiz-IT und erfordert eine verbesserte Vernetzung sowohl justizintern als auch mit nationalen und internationalen Partnern sowie deren Systemen.

Um diese neuen Technologien für die Justiz zu erschließen, sind IT-Investitionen unerlässlich. Insbesondere Cloud-Technologie kann viele der genannten Herausforderungen adressieren, den Zugang zu Innovationen verbessern sowie Effizienz und Geschwindigkeit in der Digitalisierung erhöhen. Dazu investieren viele Länder bereits in Cloud und mit der gemeinsamen Entwicklung von *GeFa* und *AuRegis* werden bundeseinheitlich Cloud-native Anwendungen entwickelt. Eine gemeinsame Strategie oder Aufbau einer einheitlichen Cloud-Umgebung bestehen aber nicht. Dadurch entstehen justizweit auch im Bereich Cloud heterogene Strukturen und viele Mehrwerte von Cloud wie die Bündelung von Betriebsinfrastruktur können nicht realisiert werden. Angesichts knapper Haushalte und des Fachkräftemangels stellen die Aufwände zum Aufbau von Cloud sowie des erforderlichen Fachwissens eine erhebliche Herausforderung dar. Daher ist ein koordiniertes, justizweites Vorgehen entscheidend, um Cloud-Technologie erfolgreich und gewinnbringend zu erschließen.

1.1.2 Cloud als Digitalisierungsbeschleuniger und Effizienztreiber

Cloud-Technologie kann als Digitalisierungsbeschleuniger und Effizienztreiber ein entscheidender Lösungshebel für die digitale Transformation der Justiz sein.

Bei Cloud werden IT-Infrastrukturen wie Massenspeicher und Rechenkapazitäten virtualisiert. Auf dieser virtuellen Infrastruktur (IaaS: Infrastructure-as-a-Service) können Plattformen z. B. für Datenverarbeitung, KI-Nutzung, Dokumentenverwaltung und Anwendungsentwicklung (PaaS: Plattform-as-a-Service) sowie nachnutzbare Software (SaaS: Software-as-a-Service) einheitlich betrieben und bereitgestellt werden. Es ergeben sich drei entscheidende Mehrwertbereiche.

Innovationskraft und Agilität: Cloud-Anwendungen werden modular und damit flexibler entwickelt. Diese modularen Dienste kommunizieren über entkoppelte Schnittstellen (APIs) und sind somit einfacher zu warten und zu integrieren. Auch die Ausbringung ist durch moderne Integrations- und Testautomationswerkzeuge signifikant schneller. Dies steigert die Innovationskraft und bessere Nutzendenzentrierung. Zudem wird der Zugang zu innovativen Plattformen (z. B. No-Code- und KI-Werkzeuge) auch für Fachbereiche demokratisiert und damit die Transformation hin zu agilen, digitalen Organisationen unterstützt. Ein solch

moderner Arbeitsplatz sowie agile Zusammenarbeitsmodelle zwischen Fach und IT – befähigt durch Cloud – steigern zudem die Arbeitgeberattraktivität deutlich.

Kosteneffizienz und Skalierbarkeit: Bei Cloud werden IT-Ressourcen gebündelt und so besonders effizient verwaltet und provisioniert, um Skaleneffekte in IT- und Betriebstätigkeiten zu realisieren. Durch Virtualisierung kann Hardware bspw. deutlich effizienter genutzt werden. Auch Software – wie Plattformdienste – kann in der Cloud als Managed Service beschafft und betrieben werden. Dies bündelt die Aufbau- und Pflegeaufwände, ermöglicht eine einheitliche Bereitstellung, vermeidet Insellösungen, Heterogenität, redundante Betriebsmodelle und beugt so steigenden Kosten vor. Die Bündelung von Bedarfen erlaubt zudem eine effizientere Beschaffung und Fokussierung auf Qualität. Die hohe Skalierbarkeit von Cloud adressiert zudem nachhaltig die steigenden Anforderungen bspw. an Datenvolumina und Rechenlast (z. B. für KI). Besonders vorteilhaft ist auch die Möglichkeit, den Prozess der Software-Ausbringung und der Provisionierung benötigter Betriebsinfrastruktur über Infrastructure-as-Code (IaC) zu automatisieren. Dafür sind sog. Container-Umgebungen erforderlich. Damit können Cloud-native Anwendungen je nach Last skalieren und somit performanter ausgeführt werden. Gleichzeitig ist eine nutzungsbasierte Abrechnung (Pay-per-use) möglich. Bei knappen Haushalten schaffen diese effizienten Abrechnungsmodelle Entlastung und mehr Spielraum für Innovationen. Sie tragen auch zur Nachhaltigkeit bei, da durch die automatische Skalierung Ressourcen effizienter genutzt werden.

Prozessharmonisierung und IT-Sicherheit: Die Modularität von PaaS- und SaaS-Diensten ermöglicht deren einfache Nachnutzung und Vernetzung, um digitale Ende-zu-Ende-Prozesse zu entwickeln. Dies beschleunigt die Anwendungsentwicklung, -bereitstellung und -wiederherstellung erheblich. Daher stellen viele Hersteller ihre Anwendungen meist nur noch Cloud-nativ bereit. Cloud-Umgebungen erlauben zudem die einheitliche Absicherung von Daten und Nutzenden mit modernen IT-Sicherheitsstandards. Damit können finanzielle Ressourcen für die meist teureren Sicherheitswerkzeuge sowie Benutzer- und Berechtigungssysteme gebündelt werden. Diese sind auch Grundlage für das effiziente und sichere Teilen von Daten zwischen Teilnehmenden einer Cloud.

Cloud ist somit nicht nur ein IT-Thema, vielmehr ist es eine neue Art und Weise, IT zu nutzen, Software zu entwickeln und zu betreiben, die Zusammenarbeit zwischen Fachlichkeit und IT zu verbessern, Technologien zu demokratisieren und Innovation voranzutreiben, Dienste nachzunutzen, Kernkompetenzen zu bündeln, Mitarbeitende zu entlasten und dabei Sach- und Personalkosten zu reduzieren.

Es ist daher wenig überraschend, dass sich weltweit die Verlagerung von gesamten IT-Serviceportfolios hin zum Betrieb in Cloud-Umgebungen weiter beschleunigt. Cloud ist dabei ein Oberbegriff für eine Vielzahl möglicher Cloud-Bereitstellungsmodelle. Je nach Ausgangslage, Anforderungen und Zielsetzung kann eine andere Art von Cloud-Nutzung vorteilhaft sein. Mit dem Marktwachstum hat sich das Kontinuum an Bereitstellungsmodellen in den letzten zehn Jahren signifikant weiterentwickelt.

Neben bekannten **Public Cloud**-Angeboten der Hyperscaler (*Microsoft, Amazon, Google*) haben sich inter-/ national weitere Public Cloud-Anbieter etabliert (z. B. *OVH, Ionos, StackIT, Alibaba*). Zudem entstehen auch Public Cloud-Angebote für die besonderen Anforderungen regulierter Industrien (z. B. Finanzen) sowie für die souveräne Nutzung durch Behörden (sog. Government Clouds). Auch viele Softwarehersteller bieten ihre Produkte nur noch in oder für Public Cloud-Umgebungen an (z. B. *Oracle, IBM, SAP*).

Daneben haben sich auch zahlreiche **Private Cloud**-Varianten entwickelt. Hier reicht das Spektrum vom Private Cloud-Betrieb im eigenen Rechenzentrum mit spezieller Hardware und Virtualisierungssoftware, bis hin zur Managed Private Cloud bei Anbietern. Auch Mischformen wie Private Cloud Stack existieren, bei dem vorkonfigurierte Hardware eines Cloud-Anbieters im eigenen Rechenzentrum installiert und dort souverän genutzt wird.

Auch die Kombination von Cloud-Modellen ist möglich und aus Souveränitäts-, Effizienz- und Resilienzgründen zu empfehlen. Dadurch entstehen erweiterte Nutzungsszenarien, aber auch eine höhere Komplexität insbesondere beim Cloud-Management und Netzwerkdesign. Im **Multi Cloud**-Ansatz werden mehrere Public Clouds kombiniert, um bspw. die Vorteile verschiedener Clouds zu nutzen und die Abhängigkeit von einem Anbieter zu reduzieren (Vermeidung des sog. „Vendor Lock-in“). Der **Hybrid Cloud**-Ansatz verbindet die eigene Private Cloud mit Public Cloud-Angeboten, um bspw. je nach Anwendung ein passendes Betriebsmodell zu wählen und Abhängigkeiten zu minimieren. Dagegen verbindet eine **Community Cloud** die Rechenzentren mehrerer Parteien und spannt darüber eine gemeinsame Private Cloud. Darin werden für einen bestimmten Anwenderkreis gemeinsame Dienste aufgebaut sowie Anwendungen und Daten geteilt.

Behörden und Unternehmen in regulierten Industrien nutzen oft den Hybrid Cloud-Ansatz, bei dem die sensiblen Daten in der Private Cloud verbleiben, während Public Cloud für weniger sensible Daten und Prozesse genutzt wird. Mit zunehmendem Vertrauen in die eigenen Cloud-Fähigkeiten und Sicherheitsfunktionen der Cloud-Anbieter wird dieses Verhältnis teils sukzessive angepasst.

Unternehmen und Behörden sollten daher eine Cloud-Strategie entwickeln, um Cloud-Dienste für sich zu erschließen, effizient und sicher in die eigenen Prozesse einzubinden und die Cloud-Mehrwerte für sich zu nutzen. Die Bundesregierung verfolgt eine diversifizierte Cloud-Strategie, die alle o. g. Cloud-Modelle umfasst. Einerseits sollen Public Cloud-Angebote via sog. Cloud-Broker standardisiert nutzbar gemacht werden. Andererseits entstehen eigene Private Clouds (z. B. beim *ITZBund* und einigen Landes-IT-Dienstleistern) mit Standards der *Deutschen VerwaltungscLOUD-Strategie*. Weil Standardsoftware auf solchen privaten Plattformen meist nur aufwändig bzw. gar nicht portierbar ist, arbeitet man parallel an sog. **Third Party Private Clouds**. Dort stellen Hersteller wie z. B. *SAP* oder *Microsoft* ihre Produkte für Bundesbehörden auf souveräner Infrastruktur bereit.

Zwar ist der private Sektor Vorreiter in der Cloud-Nutzung, doch auf dem Weg zum digitalen Staat und zur Umsetzung von eGovernment-Diensten rückt Cloud immer mehr in den Fokus der öffentlichen Hand. Dies gilt auch für die Justiz weltweit, welche die Vorteile von Cloud für sich aktiv erschließt und sich damit auf einen modernen Innovations- und günstigeren Kostenpfad begibt.

1.1.3 Politische Rahmenbedingungen und Projektauftrag

Die Untersuchung der Machbarkeit einer bundeseinheitlichen Justizcloud wurde durch die gemeinsame Erklärung der Justizministerinnen und Justizminister von Bund und Ländern auf dem ersten [Bund-Länder-Digitalgipfel am 30. März 2023](#) angestoßen. Da in Bund und Ländern noch keine einheitliche Vorstellung über eine Justizcloud bestand, sollte zunächst grundsätzlich die „...Nutzbarmachung von sicheren, datenschutzkonformen Cloud-Technologien zur Erschließung wirtschaftlicher Skalierungsmöglichkeiten“ untersucht werden. Der *Bund-Länder-Digitalgipfel* hat daher das *Bundesministerium der Justiz (BMJ)* gebeten, die Untersuchung der Machbarkeit einer bundeseinheitlichen Justizcloud durchzuführen.

Ziel der Untersuchung ist die Konzeption möglicher Zielbilder für eine bundeseinheitliche Justizcloud und eine Bewertung der fachlichen, technischen und rechtlich-organisatorischen Machbarkeit. Dabei soll die Untersuchung laufende Initiativen mit Cloud-Bezug auf Bundes- und Landesebene (z. B. *DVS*, *govdigital eG*) sowie laufende Investitionen bei IT-Dienstleistern der Länderjustiz aufnehmen. Zudem sollen justizeigene Cloud-Bedarfe bspw. der Entwicklungsverbünde sowie durch Zukunftsanforderungen der Justiz aufgenommen werden. Um eine mögliche schrittweise Umsetzung vorzubereiten, soll zudem ein strategisch-planerisches Konzept entwickelt werden.

1.2 Projektvorgehen & Governance

1.2.1 Projektvorgehen und Rahmenwerk

Für die Untersuchung wurde ein strukturiertes Vorgehen entlang des Projektauftrags in den Phasen Ist-Analyse, Zielbildentwicklung sowie strategisch-planerisches Konzept gewählt. (vgl. **Abbildung 2**)

Abbildung 2 | Projektvorgehen in drei Phasen



In der **Ist-Analyse** erfolgte zunächst eine Initialisierung des Projekts gemeinsam mit der *Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) AG Zukunft*, die Festlegung der Bund-Länder-übergreifenden Governance und die Aufnahme eines PoC als Projektziel. Es wurden der Untersuchungsrahmen festgelegt und entlang von vier Themenfeldern eine fundierte Untersuchung der Ist-Situation in der Justiz vorgenommen. Erhoben wurden einerseits Anforderungen an Cloud durch eine Untersuchung der Justizanwendungslandschaft sowie durch Zukunftsanforderungen der Justiz. Andererseits wurden bestehende Cloud-Angebote der IT-Dienstleister der Justiz und laufende Initiativen mit Cloud-Bezug untersucht. Aus den Erkenntnissen der Ist-Analyse wurden umfassende Anforderungen und Herausforderungen der Justizdigitalisierung synthetisiert.

Bereits in der Ist-Analyse (bspw. zur Erhebung der Cloud-Fähigkeiten der IT-Dienstleister), aber insbesondere für die **Zielbildentwicklung**, wurde ein bewährtes Cloud-Rahmenwerk verwendet (vgl. **Abbildung 3**). Dieses stellt relevante Handlungsfelder und Aktivitäten für Planung, Aufbau und Betrieb von Cloud übersichtlich dar. Dabei werden die Aktivitäten je Handlungsfeld entlang vier typischer Phasen einer Cloud-Transition gegliedert. Die

vorliegende Untersuchung fokussierte sich auf die Phase „Strategie und Analyse“ und hat bereits einzelne Punkte aus der Phase „Design und Planung“ einbezogen.

Abbildung 3 | Strategisches Cloud-Rahmenwerk (Fa. Accenture)



Das Rahmenwerk unterstützte die Fachpanel bei der Identifikation relevanter Fragestellungen und Untersuchungsgegenstände (z. B. „DevOps und Automatisierungsstrategie“ im technischen Zielbild, „Serviceportfoliostrategie“ im fachlichen Zielbild oder „Organisatorische Blaupause“ im rechtlich-organisatorischen Zielbild). Das Rahmenwerk diente als Orientierung zur Themenauswahl der Cloud-Sprechstunden und half die Vollständigkeit bei der Zielbilderarbeitung sicherzustellen. Zur effizienten Bearbeitung wurden die Handlungsfelder in vier Zielbildebene gebündelt: die strategische, fachliche, technische und rechtlich-organisatorische Ebene.

Die **strategische Ebene** beschreibt die Vision, Mission und strategischen Ziele der Justizcloud sowie erwartete Mehrwerte. Sie entwickelt die Wirtschaftlichkeitsbetrachtung und die Umsetzungs- bzw. Transitions-Roadmap (vgl. **Kapitel 5**).

Die **fachliche Ebene** detailliert die wesentlichen Anforderungen der Cloud-Nutzenden sowie eine zukünftige Cloud-Anwendungslandschaft der internen und externen Domäne der Justiz. Dazu gehören u. a. ein Mandanten-, Identitäten- und Berechtigungs-, Schnittstellen- und Datenkonzept. Zudem wird ein Serviceportfolio auf Basis der Bedarfe zukünftiger Nutzer erstellt und ein Vorgehen zum schrittweisen Auf- und Ausbau des Portfolios definiert.

Die **technische Ebene** baut auf den Anforderungen der fachlichen Ebene auf, definiert mögliche technische Service- und Bereitstellungsmodelle wie Private, Public, Hybrid oder Community Cloud. Zudem wurde eine technische Zielarchitektur für die Justizcloud inklusive eines Netzwerkkonzepts entwickelt. Dabei wurde auch erarbeitet, wie die Rolle der Justizcloud im bestehenden Gefüge der IT-Dienstleister Hard- und Software nachnutzen kann. Darüber hinaus wurden technische Standards und Anforderungen für die Ausgestaltung der Justizcloud-Plattform definiert, wie z. B. Container- und Datenplattform. Schließlich wurde ein einheitlicher Entwicklerarbeitsplatz ausgestaltet, technische Detailkonzepte für einen Cloud-Betrieb ausgestaltet (z. B. die Föderation von Identitäten, Integration mit Legacy-Anwendungen) und passende Nachnutzungskonzepte und Synergien mit laufenden Cloud-Initiativen (z. B. DVC) in das Zielbild integriert.

Die **rechtlich-organisatorische Ebene** detailliert organisatorische und rechtliche Möglichkeiten zur Operationalisierung einer Justizcloud. Dazu wurden bspw. mögliche Organisationsformen wie der Aufbau einer dedizierten Betriebseinheit für die Justizcloud bewertet und erforderliche Rollen, Fähigkeiten und Prozesse beschrieben. Zudem wurden Möglichkeiten der organisatorischen Einbettung einer Justizcloud in die bestehenden föderalen Strukturen wie der *BLK* und den öffentlichen IT-Dienstleistern untersucht. Zentral war dabei auch die Erhebung möglicher Rechtsformen. Eine rechtliche Beratung hat nicht stattgefunden.

Im **strategisch-planerischen Konzept** wurden wichtige Fragestellungen der Wirtschaftlichkeit sowie planerische und kommunikative Voraussetzungen für eine mögliche Umsetzung des entwickelten Zielbilds geschaffen. Dazu wurden in einer Wirtschaftlichkeitsbetrachtung die ökonomischen Mehrwerte des Zielbilds den notwendigen Investitionen gegenübergestellt und so dem Auftrag des *BLDG* zur Erschließung wirtschaftlicher Skalierungsmöglichkeiten von Cloud-Technologie entsprochen. In einer Roadmap wurden zentrale Arbeitspakete und Meilensteine für den Aufbau des Zielbilds ausgeplant. Im Kommunikationskonzept wurden wesentliche Stakeholder identifiziert und Kommunikationsbotschaften abgestimmt.

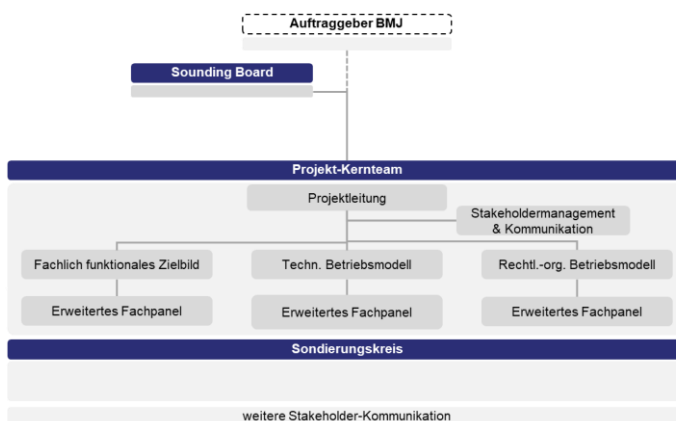
1.2.2 Governance und Zusammenarbeit

Für eine erfolgreiche justizweite Untersuchung der Machbarkeit war eine gemeinschaftliche Zusammenarbeit einer Vielzahl von Stakeholdern in Bund und Ländern von Beginn an vorgesehen. Dabei war darauf zu achten, u. a. die Justizministerien der Länder, die *BLK* sowie deren Arbeitsgruppen inkl. Architekturbüro sowie insb. auch die Entwicklungsverbünde und Vertreter der IT-Dienstleister als Wissensträger und Impulsgeber eng in die Untersuchung

einzubinden. Dazu wurde eine Governance aufgesetzt, die sowohl in der Projektsteuerung als auch auf Arbeitsebene eine Beteiligung aller Stakeholder sicherstellt.

Als Auftraggeber verantwortete das *BMJ* wesentliche Entscheidungen sowie die Steuerung des Projekts. Dabei arbeitete das *BMJ* eng mit einem Sounding Board zusammen, das mit Vertretern der *BLK AG Zukunft* zzgl. Hamburg, dem *BLK-Architekturbüro* sowie Vertretern für die Bundesgerichte besetzt war. Aufgabe des Sounding Boards war insb. die regelmäßige fachliche Bewertung und Ergänzung von Projektergebnissen und das Einbringen von Fach- und Kontextwissen.

Abbildung 4 | Projektgovernance in der Zielbildentwicklungsphase



Die laufende Bearbeitung der Projekthinhalte erfolgte in einem Kernteam des *BMJ*. Dabei wurden in jeder Projektphase Teams aus Projektmitgliedern sowie Vertretern von Bund und Ländern mit passendem Experten- und Fachwissen zusammengestellt. Die Zusammenstellung der Teams erfolgte dabei gemeinsam mit dem Sounding Board, über

das passende Ansprechpartner und Experten der Länder schnell identifiziert und für das Projekt gewonnen werden konnten.

In der Ist-Analyse wurden für Expertengespräche mehr als 50 Ansprechpartner aus Bund und Ländern mit Justiz- und IT-Fachwissen identifiziert, die ihr Wissen eingebracht haben und auch in den weiteren Phasen der Untersuchung als Experten zur Verfügung standen. Die Ansprechpersonen stammten überwiegend aus Justizministerien, Entwicklungsverbünden, öffentlichen IT-Dienstleistern sowie aus Projektteams der Länder (z. B. KI-Plattform).

Die Zielbildentwicklung erfolgte in sog. Fachpanels für jede Ebene des Zielbilds, d. h. fachlich, technisch und rechtlich-organisatorisch. Die Fachpanels waren jeweils mit zuständigen Ansprechpartnern aus Bund und Ländern besetzt. Die Fachpanels haben über acht Wochen das Zielbild der Justizcloud gemeinsam mit dem Projektteam erarbeitet und wichtiges Wissen aus dem operativen Betrieb eingebracht.

Zuletzt wurden im Rahmen des strategisch-planerischen Konzepts Teams für die Themen Wirtschaftlichkeitsbetrachtung, Roadmap und Kommunikationskonzept erstellt. Auch die

Teams im strategisch-planerischen Konzept haben in wöchentlichen Terminen eng zusammengearbeitet und die Untersuchungsinhalte entwickelt und abgestimmt.

Um möglichst breite Unterstützung und Einbindung sicherzustellen, wurde zudem ein Sondierungskreis mit verschiedenen Stakeholdergruppen gebildet. Diese wurden regelmäßig über den Projektfortschritt informiert und konnten wichtige relevante Impulse für das Projekt geben. Dabei waren z. B. einige Länder, die nicht über das Sounding Board eingebunden waren, Teil des Sondierungskreises. Eingebunden wurden zudem die *Bundesrechtsanwaltskammer (BRAK)*, die *Bundesnotarkammer (BNotK)*, das *Bundesamt für Sicherheitstechnik (BSI)*, Projektvertreter der *Deutschen Verwaltungscldoud (DVC)* sowie das *Programm P20*.

Im Rahmen des Projektes wurde darüber hinaus eine Cloud-Sprechstunde angeboten. Darin wurden in Regelterminen viele technische Konzepte rund um das Thema Cloud ausführlich dargestellt und es wurde Raum für Fragen und Diskussionen für die Teilnehmenden geschaffen. Damit wurde der nachhaltige Aufbau von Cloud-Wissen in der Justiz und bei den Projektbeteiligten unterstützt.



2 Ist-Analyse

2.1 Zusammenfassende Erkenntnisse der Ist-Analyse

Die Digitalisierung der Justiz wurde in den letzten Jahren durch viele Modernisierungsprojekte aktiv vorangetrieben. Die Justiz verfügt dazu über ein enges Netz an IT-Dienstleistern, Infrastrukturen und Partnern. Mit dem *elektronischen Rechtsverkehr (ERV)* und dem *Akten-einsichtsportal (AEP)* konnten erste Projekte bereits flächendeckend umgesetzt werden und weitere, wie die Einführung der *elektronischen Akte (eAkte)*, befinden sich auf der Zielgeraden. Hervorzuheben ist auch die Eigenentwicklung moderner, Cloud-fähiger Fachverfahren wie *GeFa*, *AuRegis* und dem *bundeseinheitlichen Datenbankgrundbuch (dabag)*, welche die Justiz bundeseinheitlich in Entwicklungsverbünden vorantreibt.

Die Steuerung der Justizdigitalisierung erfolgt dabei auf strategischer Ebene durch den *E-Justice-Rat (EJR)*, die *Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK)* und ihre Arbeitsgruppen (z. B. *AG IT-Standards*), die neue Anforderungen vorausschauend bewerten und deren Umsetzung zielgerichtet orchestrieren. Es bestehen jedoch noch signifikante Herausforderungen, den laufenden (IT-)Betrieb weiter zu modernisieren sowie zukünftige Anforderungen effektiv umzusetzen.

Die Untersuchung der Machbarkeit einer bundeseinheitlichen Justizcloud hat im Rahmen der Ist-Analyse das Ziel, Anforderungen der Justiz an eine Cloud zu erheben. Dafür wurden sowohl das bestehende Anwendungsgefüge der Justiz von Bund und Ländern als auch Zukunftsanforderungen analysiert. Zudem sollte das Cloud-Angebot erhoben werden. Dafür wurden die bestehenden IT-Dienstleister der Justiz und bundesweite Cloud-Initiativen (z. B. *Deutsche VerwaltungscLOUD-Strategie*, *Delos Cloud*, *GAIA-X*) analysiert.

Analyse Justizanwendungslandschaft: In der Justiz werden über 140 heterogene, teils veraltete Anwendungen in Bund bzw. Bundesgerichten und Ländern großteils redundant weiterentwickelt, gewartet und betrieben. Da diese Anwendungen vornehmlich an Justizmitarbeitende gerichtet sind, wird nachfolgend von der internen Anwendungsdomäne

gesprochen. Meist sind die Anwendungen nicht skalierbar und müssen daher in multiplen Instanzen ausgebracht werden – das ist komplex und teuer. Auch zwischen Ländern, die gleiche Software einsetzen, bestehen oft Versionsunterschiede, die zu Kompatibilitäts- und Schnittstellenproblemen führen. Medienbrüche sowie heterogene oder fehlende Schnittstellen behindern die Umsetzung digitaler Ende-zu-Ende-Prozesse. Dieser digitale Ballast bindet knappe Ressourcen, erfordert viel Koordination, ist teuer im Betrieb und fehleranfällig. Viele Anwendungen lassen sich zudem nur manuell und damit nur mit hohem Personalaufwand testen. Diese Gemengelage erschwert Neuerungen, weshalb Softwareupdates häufig nur ein bis zwei Mal pro Jahr je Anwendung erfolgen, soweit sie mangels Leistbarkeit nicht sogar gänzlich übersprungen werden.

In der Justiz besteht zudem die Besonderheit, dass die Anwendungen meist nicht alleinstehend funktionsfähig sind, sondern miteinander ein Anwendungsgefüge bilden und über Kommunikationsplattformen oder komplexe Punkt-zu-Punkt-Schnittstellen integriert sind. Viele Anwendungen werden zudem erst beim Nutzenden im Client verzahnt. Berücksichtigt man die Vielzahl heterogener Clients in der Justiz von Bund und Ländern, steigt die Komplexität und mit ihr der Test- und Ausbringungsaufwand exponentiell an. Zudem weist diese Form der direkten Integration am Client viele Nachteile auf. Sie erschwert agiles Ausbringen von Neuerungen, birgt Sicherheitsrisiken und führt oft zu signifikanten Performanceproblemen. Dieser Punkt wurde von Justizmitarbeitenden besonders häufig betont.

Neben den Anwendungen der internen Domäne bestehen zudem ca. 25 Applikationen, die an externe Parteien wie Rechtsanwälte, Notare, andere Behörden, Unternehmen sowie Bürger gerichtet sind. Nachfolgend wird in diesem Zusammenhang von der externen Domäne gesprochen. Diese Anwendungen bestehen meist nur einmal und werden meist bundeseinheitlich in einem Land betrieben. Dennoch bestehen auch in diesem Anwendungsumfeld wesentliche Herausforderungen. Bspw. sind sowohl Technologie- und Modernitätsstand als auch Entwicklungs- und Betriebsprozesse sehr heterogen. Zudem besteht kein einheitlicher Außenauftritt der Justiz ggü. externen Parteien bzw. wird parallel an vielen Stellen separat weiterentwickelt. Aber auch die Weiterentwicklung dieser nach außen exponierten Anwendungen bildet in punkto Sicherheitsstandards auf der Höhe der Zeit (z. B. Multifaktor-Authentisierung und API-Nutzung) eine große Herausforderung. Teilweise adressiert das *BMJ* dies bereits durch die Entwicklung neuer nutzendenzentrierter Anwendungen wie z. B. das *Zivilgerichtliche Online-Verfahren (ZOV)* und die *Digitale Rechtsantragstelle (RAST)*.

Cloud-Technologien können einen Baustein zum Adressieren dieser Herausforderungen bilden. Dafür müssen die Anwendungen aber auch entsprechend konsolidiert und modernisiert werden, um bspw. die Vorteile von Cloud-Skalierung nutzen zu können. Daher entwickelt die Justiz bereits gemeinsam neue, Cloud-native Fachverfahren (z. B. *GeFa* und *AuRegis*). Diese erfordern aber per Definition eine Container-Infrastruktur, auf der sie ausgebracht und betrieben werden können. Solche Infrastrukturen und v. a. das Know-how zu deren Betrieb bestehen aber derzeit noch nicht bzw. befinden sich erst im Aufbau.

Analyse der Zukunftsanforderungen: Die Justiz hat eine Vielzahl von Anforderungen in der nahen Zukunft zu adressieren, die sie zum Teil bereits in vielfältigen Initiativen vorantreibt. Dabei zeigt sich, dass viele Anforderungen wie der Aufbau einer KI-Plattform oder der Entwurf moderner Lösungen, z. B. für die automatisierte Aktenanalyse und zum digitalen Austausch von Beweismitteln zwischen Polizei und Justiz, ähnliche Anforderungen haben und von Cloud-Technologien profitieren könnten.

Auch die Möglichkeit, Daten innerhalb der Justiz miteinander zu teilen und einzusehen, anstelle sie über den *ERV* (redundant, d.h. als Kopie) zu verschicken, könnte durch einen gemeinsamen Cloud-basierten Datenraum und ein zentrales Berechtigungsmanagement erreicht werden. Zudem muss sich die Justiz mit skalierbaren Speicherlösungen beschäftigen und sich auf immer größere digitale Datenmengen vorbereiten, um diese auch für KI-Anwendungsfälle verfügbar zu machen. Eine bundeseinheitliche Justizcloud könnte daher für viele Zukunftsthemen als Katalysator wirken und eine flächendeckende und effektive Exploration, Entwicklung, Inbetriebnahme und insb. auch einfachere Nach- bzw. Mitnutzung der Lösungen für die Zukunftsthemen ermöglichen.

Analyse der Justiz-IT-Dienstleister: Die Justiz kann auf ein dichtes Netz an IT-Dienstleistern zurückgreifen. Sie hat aufgrund ihrer Anforderungen an Souveränität und Unabhängigkeit von der Verwaltung entweder eigene IT-Dienstleister bzw. IT-Stellen aufgebaut (z. B. alle Bundesgerichte, Niedersachsen, Nordrhein-Westfalen und Sachsen) oder betreibt bei gemeinsamen Dienstleistern mit der Verwaltung (z. B. Hessen und Bayern) ein eigenes, unabhängiges Anwendungsgefüge. Die meisten Länder sind dabei rechtlich an einen Dienstleister gebunden (Kontrahierungszwang). Insgesamt erfolgt der Betrieb des Justizanwendungsgefüges daher einmal pro Land. Eine Besonderheit stellt *Dataport AöR* dar, die als sog. Shared Service separate Umgebungen für vier Länder (Bremen, Hamburg, Schleswig-Holstein, Sachsen-Anhalt) betreiben.

In Summe wurden zwölf IT-Dienstleister sowie zwei Bundesgerichte untersucht, die in eine der o. g. Kategorien fallen. Grundsätzlich ist das Servicespektrum je IT-Dienstleister sehr unterschiedlich und reicht von Arbeitsplatz und Kommunikation, über reine Infrastruktur bis zum technischen und teils fachlichen Anwendungsbetrieb. Einige Dienstleister bieten auch Anwendungsentwicklung an, wie z. B. die *Hessische Zentrale für Datenverarbeitung (HZD)* oder die Bundesgerichte.

Die Kooperation der IT-Dienstleister ist aktuell noch gering und die Ausprägungen der Infrastrukturen, Technologien und Prozesse und damit auch Performanz und Sicherheitsstandards sehr heterogen. Das trifft auch auf das Cloud-Angebot zu. Bei vier der untersuchten Länder und allen Bundesgerichten besteht noch gar keine Cloud-Initiative. Zwei IT-Dienstleister haben bereits produktive Private Clouds, v. a. für Anwendungsfälle der Verwaltung, aufgebaut. Beim Rest befindet sich der Aufbau von Private Cloud-Umgebungen noch in der Entstehung und je nach Dienstleister mit verschiedenem Fortschritt.

Zur Ausbringung der neuen Justizfachverfahren müssten in jedem Land eigene Cloud-Infrastrukturen, -Plattformen und entsprechendes Know-how aufgebaut werden. Durch fehlende bundeseinheitliche Standards und geringe Kooperation entstehen aber derzeit länderspezifische, heterogene Container-Plattformen, die für die Anwendungsentwicklung, Ausbringung und den Betrieb der neuen Justizfachverfahren eine hohe Komplexität und Zusatzkosten bedeuten.

Analyse bundesweiter und internationaler Cloud-Initiativen: Viele Organisationen der öffentlichen Verwaltung haben die Relevanz von Cloud für die Digitalisierung bereits erkannt. Es gibt daher diverse zu betrachtende Cloud-Initiativen. Verwaltung und Justiz haben dabei besondere Anforderungen an Souveränität, Sicherheit und Kontrolle der Infrastruktur und Daten, weshalb sich am Markt verschiedene Nutzungsmuster und Angebote entwickelt haben. Die meisten Organisationen verfolgen langfristig eine Hybrid Cloud-Strategie, bei der für kritische Anwendungen und Daten der Aufbau von Private Cloud-Infrastruktur (z. B. beim *ITZBund*) vorgesehen ist. Kommerzielle Public Cloud-Angebote werden dabei für weniger kritische Daten und Prozesse genutzt. Zudem entstehen sog. Third Party Private Clouds, die eine souveräne Nutzung kommerzieller Angebote für die Verwaltung ermöglichen (z. B. *Delos Cloud*).

Auch die kommerziellen Public Cloud-Anbieter entwickeln sog. Government Cloud-Angebote, die für die besonderen Anforderungen der öffentlichen Verwaltung angepasst sind (z. B. Hyperscaler wie *Microsoft Azure*, *Google Cloud Plattform (GCP)*, *Amazon Web Services*

(AWS), Oracle Cloud (OCI), EU-Angebote wie OVHcloud und deutsche Anbieter wie IONOS, StackIT und Open Telekom Cloud (OTC)).

Für den komplexen Kontext der föderalen IT-Landschaft in Ländern und Kommunen haben sich in Deutschland auch Organisationen etabliert, die Kooperationen fördern (*Föderale IT-Koordination Anstalt öffentlichen Rechts (FITKO AöR)*, *govdigital eG*), Cloud-Standards entwickeln (z. B. *Deutsche VerwaltungscLOUD-Strategie (DVC/DVS)*) oder einheitliche Cloud-Dienste für verschiedene Nutzende bereitstellen und betreiben wollen (z. B. verteilter Kubernetes-Cluster und Cloud-Broker von *govdigital eG*, *DVC-Marktplatz*). Die Erfahrungen und Erkenntnisse dieser Initiativen sowie deren Lösungsansätze für das föderale Umfeld sind auch für die Justiz sehr wertvoll und teilweise nachnutzbar.

Auch international zeigt sich, dass die Justiz bereits sowohl Private als auch Public Cloud-Technologien einsetzt, um die Entwicklung innovativer Anwendungen und damit die Digitalisierung der Justiz zu beschleunigen. Dabei wird der Umstieg auf Cloud auch oftmals als Paradigmenwechsel genutzt, um die Anwendungslandschaft von Grund auf neu und damit flexibler, nutzendenzentrierter und kosteneffizienter zu gestalten (sog. „Greenfield“-Ansatz).

Exkurs zum Untersuchungsrahmen

In den ersten Gesprächen der Ist-Analyse, insb. zur Anwendungslandschaft und mit den IT-Dienstleistern, hat sich gezeigt, dass der Betrachtungsrahmen der Untersuchung klar definiert werden musste. Viele IT-Dienstleister stellen neben dem Verfahrensbetrieb auch die Arbeitsplatzanwendungen inkl. Betriebssystem (v. a. *Microsoft Windows*) und Produktivitätsanwendungen wie *Microsoft Office* und *Teams* für die Justiz bereit. Der Justizarbeitsplatz kann dabei als Schichtenmodell dargestellt werden (vgl. **Abbildung 5**).

Abbildung 5 | Abgrenzung des Untersuchungsrahmens



Die Basis für den Arbeitsplatz bildet die mobile oder stationäre Hardware, d. h. Endgeräte der Nutzenden. Darauf ist ein gehärteter Basis- bzw. virtueller Arbeitsplatz installiert, der vor allem das Betriebssystem und wichtige Basisanwendungen (z. B. Virenschutz, Netzlaufwerke etc.) enthält. In manchen Ländern wird ab der Ebene des Basis-Arbeitsplatzes bereits virtualisiert und sog. „virtuelle Desktops“ (z. B. via *Citrix Terminal Server*) bereitgestellt.

Auf dem Basis-Arbeitsplatz werden landes-, organisations-, oder rollenspezifische Anwendungsbündel installiert. Alle Mitarbeitenden erhalten bspw. Kollaborations-, Kommunikations- und Produktivitätsanwendungen (z. B. *Microsoft Office*) sowie Browser (sog. *Clients*, z. B. *Internet Explorer*, *Edge*, *Google Chrome*). Entwickler erhalten darüber hinaus bspw. Entwicklungs- und Datenbankwerkzeuge, Mitarbeitende der Justizverwaltungen z. B. Bestellsoftware und Verwaltungs-eAkten. Schließlich werden auf diesem Setup die Kernanwendungen der Justiz wie Verfahrens-eAkte, Fachverfahren und Textsystem installiert.

Derzeit stellen die Landes-IT-Dienstleister alle vier Ebenen des Arbeitsplatzmodells (z. B. „Hessen-PC“) oder haben Teile davon an Drittanbieter ausgelagert (z. B. Endgeräte und Basis-Arbeitsplatz). Bei IT-Dienstleistern, die sowohl für Justiz als auch Verwaltung arbeiten, unterscheidet sich die Ebene der Anwendungsbündel und insbes. der Justizkernanwendungen im direkten Vergleich zwischen Nutzenden der Verwaltung (z. B. Polizei, Steuer) und der Justiz. Aufgrund der hessischen Netzklage und grundsätzlichen logischen Trennung von justiznahen Anwendungen wird das Justizkernanwendungsgefüge individuell von den IT-Dienstleistern betreut und betrieben (vgl. **Kapitel 2.2.2**).

Außer der Hardware- bzw. Endgeräte-Ebene könnte Cloud grundsätzlich alle Software-nahen Ebenen des Arbeitsplatzes (z. B. sog. virtuelle Desktops) adressieren. Die Hardware-Ebene ist daher per Definition nicht Teil der Untersuchung. In der Ist-Analyse wurde schnell deutlich, dass derzeit eine Vielzahl heterogener, landesspezifischer Basis-Arbeitsplätze (virtuell und physisch) besteht und auch die Software-Beschaffung, -Lizensierung und -Distribution auf Ebene des Basis-Arbeitsplatzes und der Anwendungsbündel sehr landesspezifisch ausgestaltet ist. So finden sich z. B. auch erste Open Source-Anwendungsbündel für Produktivitätsanwendungen (z. B. [Phönix](#) bei *Dataport* oder [OpenDesk](#)). Diese Heterogenität kann und muss eine bundeseinheitliche Justizcloud nicht lösen.

Da die zukünftigen Cloud-Anwendungen der Justiz als skalierbare Web-Anwendungen konzipiert werden, könnten sie über Browser-Applikationen, die in allen Ländern auf dem Arbeitsplatz bereitgestellt werden, aufgerufen werden. Daher wurde der Betrachtungsrahmen für die Untersuchung gemeinsam mit dem Sounding Board auf die Justizkernanwendungen

beschränkt. Diese Abgrenzung galt über alle drei Projektphasen. Eine Ausnahme bildet der virtuelle Arbeitsplatz für Entwickler, der spezifische Anwendungen benötigt, um Justizanwendungen zu entwickeln, betreiben und auszubringen. Der Entwicklerarbeitsplatz wurde im Rahmen des technischen Zielbilds ausgestaltet.

2.2 Detailergebnisse der Ist-Analyse

Cloud-Infrastruktur bildet heute den Marktstandard zur Entwicklung und für den Betrieb von moderner, innovativer und nutzendenzentrierter Software und bietet einfachen Zugang zu einer breiten Palette an digitalen Technologien und Produkten. Cloud bietet so die Möglichkeit, nicht nur bestehende digitale Lösungen effizienter und performanter zu betreiben, sondern auch die Digitalisierung der Justiz durch Verfügbarkeit neuer Technologien und Services sowie deren Vernetzung zu beschleunigen.

Dabei steht die Justiz nicht am Anfang ihrer Digitalisierung, sondern hat bereits viele Fachprozesse durch den *ERV* und die *eAkte* digital umgesetzt. Auch ist das Thema Cloud für die Justiz kein Novum, denn sie arbeitet bereits an der Entwicklung Cloud-nativer Anwendungen (z.B. *GeFa*, *AuRegis*) und auch bei den Justiz-IT-Dienstleistern laufen bereits erste Projekte zum Aufbau von Cloud-Umgebungen.

Gleichzeitig steht die Justiz vor der Aufgabe, Zukunftsthemen und absehbare Anforderungen an ihre digitale Infrastruktur und den Ausbau ihres digitalen Serviceangebots aktiv voranzutreiben. Auch dafür laufen bereits zahlreiche Initiativen, in denen Innovationen wie bspw. Künstliche Intelligenz (KI) erschlossen und schrittweise nutzbar gemacht werden.

Für die Konzeption einer bundeseinheitlichen Justizcloud ist eine umfassende Analyse von Anforderungen und bestehenden bzw. im Aufbau befindlichen Cloud-Angeboten erforderlich. Anforderungen umfassen dabei sowohl solche aus **a)** bestehenden oder sich im Aufbau befindlichen Anwendungen als auch **b)** ergänzende aus Zukunftsthemen der Justiz. Cloud-Angebote umfassen **c)** Angebote bei den IT-Dienstleistern der Justiz sowie **d)** Angebote im bundesweiten Kontext. Alle vier Bereiche wurden in der Ist-Analyse behandelt und erforderten jeweils unterschiedliche Vorgehensweisen, Gesprächspartner und Fragestellungen. Großteils erfolgte die Analyse dabei durch Experteninterviews. Ergänzend wurden einige separate Themenbereiche über Onlinerecherche und Einzelgespräche analysiert.

Tabelle 1 stellt die Themenbereiche der Ist-Analyse sowie die betrachteten Anwendungen, Zukunftsanforderungen, IT-Dienstleister und Cloud-Initiativen dar. Zielsetzung, Vorgehen und Detailkenntnisse aus jedem Bereich werden nachfolgend umfassend beschrieben.

Tabelle 1 | Themenbereiche der Ist-Analyse

Cloud-Anforderungen		Cloud-Angebote	
a) Anwendungslandschaft der Justiz	b) Zukunftsanforderungen der Justiz	c) IT-Dienstleister der Justiz	d) Bundesweite Cloud-Initiativen
Interne Domäne • eAkten: eAS, e2A, eIP • Benutzer- und Berechtigungsmgmt: SAFE, SAmOA • Kommunikationsplattformen: E2P, eKP • Textsysteme: BK.text, e2T • Basiskomponenten (BKKB) und Basisdienste • Neue Fachverfahren: GeFa, AuRegis, dabag Externe Domäne • Elektronischer Rechtsverkehr: EGVP Enterprise, Intermediär, SAFE-public • Online-Services: RAST, ZOV	Priorisierte Themen • KI-Strategie/-Plattform • Akten/ Datenaustausch/einsichtsplattform • Analyse unstrukturierter Daten • e-CODEX-Anbindung • eGPA Depriorisierte Themen • Justizportal 2.0 • Veröffentlichung von Urteilen • Justiztoolbox (z. B. BL-Foren) • Basisdokumente (e-Akte neu) • eAkte Gerichtsverzeichnis • Beweismittelcloud	• BITBW (BW) • ITDZ Berlin (BE) • ZIB (NI) • ITD (NW) • IT.NRW (NW) • Dataport (HH, SH, HB, ST) • HZD (HE) • RZ Nord & Jus-IT (BY) • Bundesarbeitsgericht (BAG) • Bundesfinanzhof (BFH) • LDI (RP) • LIT (SN)	Behördliche Initiativen • Deutsche Verwaltungscld (DVC) • ITZBund • Beweismittelcloud • Gaia-X • Delos Cloud Kommerzielle Initiativen • Open Telekom Cloud • StackIT • OVHcloud • Cloud-Angebote amerikanischer Hyperscaler

2.2.1 Anwendungslandschaft der Justiz

Einordnung

Moderne Cloud-Technologien ermöglichen Innovationen in Entwicklung und Betrieb von Software durch Mehrwerte wie bspw. Skalierbarkeit, Ressourceneffizienz oder schnellere Ausbringung (sog. CI/CD). Die Mehrwerte materialisieren sich aber erst, wenn Anwendungen auf bzw. in der Cloud produktiv entwickelt und betrieben werden. Im Rahmen der Cloud-Konzeption sollten daher von Beginn an die technischen und organisatorischen Rahmenbedingungen geschaffen werden, um mit der Inbetriebnahme einer Cloud auch möglichst zeitgleich Anwendungen produktiv auf der Cloud zu entwickeln, auszubringen und dort zu betreiben.

Dazu muss einerseits die Cloud so konzipiert werden, dass sie die Anforderungen der Anwendungen und Verfahren bedient (z. B. Sicherheits-, Netzwerk-, Laufzeitumgebungs- und Datenbankanforderungen). Gleichzeitig müssen Anwendungen Cloud-nativ entwickelt werden, um von den Vorteilen einer Cloud-Umgebung und ihren Cloud-Diensten zu profitieren.

Zur Entwicklung eines auf die Bedarfe der Justiz angepassten, machbaren Cloud-Konzepts ist es daher aus vielen Gründen wesentlich, die für einen zukünftigen Cloud-Betrieb vorgesehenen Anwendungen bzw. Fachverfahren sowie insb. deren technische Anforderungen, architekturellen Eigenschaften, v. a. Cloud-Fähigkeit, und etwaige Abhängigkeiten bzw. Schnittstellen im Zusammenspiel der Anwendungen zu analysieren.

Für die Beurteilung, ob Verfahren bereits für den Cloud-Betrieb geeignet, d. h. Cloud-ready sind, sollten mindestens fünf wesentliche technische Konzepte umgesetzt sein: Containerisierung, Microservice-Architektur, Entkopplung, Webfähigkeit und Mandantenfähigkeit.

Containerisierung: Container sind isolierte Betriebsumgebungen, in der Anwendungen samt aller benötigten Abhängigkeiten verpackt werden, um sie unabhängig von der Betriebsinfrastruktur ausführen zu können. Dafür müssen Anwendungen containerisierbar entwickelt werden. Containerisierte Anwendungen sind z. B. unabhängig von spezifischer Hardware, zustandslos (stateless, d. h. einzelne Rechenprozesse sind unabhängig voneinander und der Container selbst speichert keine Daten) und können hoch-skalierbar betrieben werden. Die Pflege der Anwendungen wird vereinfacht, da sie sich bei Ausfällen selbst wiederhochfahren können. Zudem wird durch Standardisierung eine höhere Ausbringungsgeschwindigkeit ermöglicht.

Um viele verschiedene Container zu orchestrieren und so Anwendungen und Anwendungskomponenten mit unterschiedlichen technischen Konfigurationen und Architekturen (z. B. Laufzeitumgebungen) auf einheitlicher Infrastruktur zu betreiben, sind so genannte Container-Plattformen erforderlich (z. B. *Kubernetes*, *Ranger*, *Swarm*, *OpenShift*). Diese wiederum benötigen zugrundeliegende skalierbare, virtualisierte Infrastruktur.

Microservices-Architektur: Anwendungen, die eine sogenannte Microservice-Architektur nutzen, sind für den Cloud-Betrieb besonders geeignet. Dabei werden verschiedene funktionale Bestandteile einer Anwendung in kleine, flexibel anpassbare Microservices unterteilt, die über APIs oder Events miteinander kommunizieren. Dies ermöglicht z. B. bessere Wartbarkeit einzelner Services und damit der gesamten Anwendung, bessere Skalierbarkeit und Flexibilität in der Technologieauswahl je nach Anforderung der einzelnen Services sowie leichteres und automatisiertes Testen.

Entkopplung: Ein weiterer wesentlicher Aspekt sind moderne Schnittstellen- bzw. Integrationsarchitekturen, bei denen Anwendungen bzw. Services über Schnittstellen (sog. APIs) oder Events (sog. Event-getriebene Architekturen) miteinander kommunizieren. Statt individuell programmierten Punkt-zu-Punkt-Verbindungen, bieten Services ihre Funktionalitäten und Daten in Form von APIs oder Events an, die von anderen Anwendungen konsumiert werden können. Dies ermöglicht die Entkopplung von Anwendungen und vereinfacht so (Weiter-)Entwicklung, Testen und Ausbringung von Anwendungen innerhalb eines komplexen Anwendungsgefüges. Diverse Cloud-native Technologien wie API-Management Plattformen und Event Hubs unterstützen eine solche Integrationsarchitektur und bieten zahlreiche zusätzliche Vorteile (z. B. Sicherheitsmechanismen, Lastverteilung, Versionierung, Standard-Konnektoren, Monitoring/ Logging und integrierte Entwicklerportale).

Webfähigkeit: Unter Berücksichtigung der o. g. Konzepte ist auch die Konzeption der Anwendungen als Webservices wesentlich. Diese Anwendungen werden über den Browser (sog. Client) genutzt, ermöglichen den rein serverseitigen Betrieb der Anwendungsbestandteile und vermeiden hohe Pflege- und Integrationsaufwände am Client. So kann die Ausbringung, Skalierbarkeit und Performanz von Anwendungen deutlich gesteigert werden. Einfache Updates können vollständig ohne Wartungszeitfenster durchgeführt werden, was die Nutzerfreundlichkeit deutlich erhöht.

Mandantenfähigkeit: In einer Cloud können Anwendungen aus einer Betriebsumgebung und einer Instanz, d. h. einer Installation bzw. Ausbringung einer Anwendung, betrieben und administriert werden (sog. Software-as-a-Service (SaaS)). Dafür müssen Anwendungen jedoch u. a. in der Lage sein, anhand der Nutzenden verschiedene Mandanten zu unterscheiden sowie eine logische Trennung von Daten und Konfigurationen verschiedener Mandanten zu implementieren (vgl. **Kapitel 3.4.3**).

Zusätzlich zu diesen Eigenschaften ist für die Ausgestaltung und Vorausplanung benötigter Cloud-Infrastruktur auch der Technologie-Stack, d. h. die eingesetzten Frontend-, Backend, Datenbank-, Laufzeitumgebungs- sowie Ausbringungstechnologien je Anwendung zu berücksichtigen. Beispielsweise muss bei der Ausgestaltung der Cloud-Datenplattform beachtet werden, welche Datentechnologien wie Objektspeicher oder relationale Datenbanken durch Anwendungen genutzt werden. Weiterhin ist auch zu berücksichtigen, welche Berechtigungsmanagementsysteme (IAMs) Anwendungen nutzen oder inwiefern Anwendungen gesonderte Netzwerkanforderungen haben, wie z. B. Kommunikation mit dem Internet, erforderliche Bandbreiten oder spezifische Sicherheitsanforderungen.

Für die Planung der Inbetriebnahme bzw. Migration von Anwendungen auf eine Cloud-Umgebung muss zudem transparent sein, in welchem Entwicklungsstadium sich die Anwendungen befinden bzw. was getan werden muss, um diese Cloud-ready zu modernisieren. Für den Erfolg eines Cloud-Projektes ist idealerweise eine integrierte produktive Inbetriebnahme von Cloud-Plattform und Cloud-Anwendungen erforderlich. Es ist daher essenziell, diese Abhängigkeiten zu erkennen und die Planungen von Entwicklungsprojekten mit einer übergreifenden Cloud-Roadmap abzustimmen.

Vorgehen

Zur Analyse der genannten Fragestellungen wurde die Justizanwendungslandschaft im Rahmen der Untersuchung detailliert analysiert. Den Ausgangspunkt bildete dazu eine Übersicht des *BLK-Architekturbüros* aller bis dato bekannten Justizanwendungen.

Im Rahmen des Projekts wurden nicht alle Anwendungen detailliert betrachtet, sondern zunächst eine anwendungsübergreifende Analyse, Kategorisierung und Bewertung durchgeführt und anschließend 14 besonders (zukunfts-)relevante Anwendungen für eine Detailanalyse ausgewählt.

Zur Bewertung der Anwendungen wurde ein standardisierter Fragebogen (vgl. **Kapitel 7.1**) entwickelt, in dem die relevanten fachlichen, technischen und organisatorischen Informationen systematisch erhoben und dokumentiert wurden. Die Befüllung erfolgte in zwölf persönlichen Experteninterviews mit Anwendungs- und Verfahrensverantwortlichen der Justiz aus Entwicklungsverbünden, Justizministerien und IT-Dienstleistern.

Überblick Justizanwendungslandschaft

Viele Prozesse der Justiz werden bereits durch entsprechende Anwendungen elektronisch abgebildet. Durch das föderale Vorgehen hat sich bundesweit eine heterogene Landschaft von Einzel- und Inselanwendungen mit vielen Redundanzen herausgebildet. Die Justiz in Bund und Ländern betreibt und entwickelt aktuell mehr als 140 Anwendungen für unterschiedlichste fachliche Bedarfe.

Auswahl, Pflege und Betrieb der Anwendungen erfolgen immer je Land bzw. je Bundesgericht. Dadurch gibt es pro Land und Bundesgericht jeweils eine individuelle Anwendungslandschaft, die, auf jeweils individueller Infrastruktur, unabhängig voneinander weiterentwickelt und betrieben wird.

Um gemeinsame Standards zu schaffen und Aufwände zu bündeln, hat die Justiz im Jahr 2012 den *E-Justice-Rat (EJR)* errichtet. Unterstützt wird der *EJR* durch die *BLK* als seine

ständige Arbeitsgruppe. Der *BLK* gehören die Justizverwaltungen der Länder sowie die Bundesjustizverwaltung an. Die *BLK* hat wiederum eigene Arbeitsgruppen zu verschiedenen Themen gebildet, wie IT-Standards, IT-Sicherheit, elektronischer Rechtsverkehr uvm (vgl. **Kapitel 2.2.2**).

Um den hohen Aufwand zur (Weiter-)Entwicklung von Anwendungen effizient zu bündeln, gemeinsam Anforderungen zu erheben und Entwicklungsprojekte zu koordinieren, haben sich in der Justiz sog. Entwicklungsverbünde etabliert. Dabei schließen sich einige (z. B. *forumSTAR*, *JUDICA*) oder alle Länder (z. B. *GeFa*, *AuRegis*) zusammen und entwickeln Software gemeinsam, um sie anschließend im jeweiligen Land individuell auszubringen und zu betreiben. Regelmäßig werden die Entwicklungsverbünde durch eine Verwaltungsvereinbarung der beteiligten Länder eingesetzt, in denen vorrangig Fragen der Finanzierung, Projektsteuerung und Personalgestellung geregelt werden.

Durch die bisherige Zusammenarbeit konnte für manche Anwendungen bereits eine teilweise Konsolidierung in der Justizanwendungslandschaft erreicht werden, bspw. nutzt die Justiz in Deutschland einheitlich das Produkt *Elektronisches Gerichts- und Verwaltungspostfach (EGVP)* für den elektronischen Rechtsverkehr. Bei den eAkten existieren drei Verbünde und bei den Textsystemen werden zwei Anwendungen verfolgt. Trotz der Bestrebungen bleibt die Heterogenität der Anwendungslandschaft aber hoch, u. a. weil mangels bundeseinheitlicher Betriebsumgebungen im Anwendungsbetrieb keine Synergien gehoben werden können.

Trotz der Heterogenität in der Anwendungslandschaft ähneln sich die fachlichen und technischen Anforderungen der Justiz. Dementsprechend können die verschiedenen genutzten Anwendungen der Justiz nach Fachlichkeit und Funktionalität in Funktionsblöcke kategorisiert werden. Es wurden acht wesentliche Funktionsblöcke identifiziert.

Dabei unterscheidet man grundsätzlich zwischen Anwendungen der internen Domäne und externen Domäne. Die interne Domäne umfasst Anwendungen der Justiz, die insbesondere von Justizmitarbeitenden genutzt werden. Die externe Domäne umfasst Anwendungen, die vor allem an externe Parteien (z. B. Bürger, Rechtsanwälte) gerichtet sind und somit auch umfangreiche Kommunikationsverbindungen ins Internet aufbauen (z. B. *EGVP*, *Online-Services*).

Tabelle 2 | Wesentliche Funktionsblöcke und Beispielanwendungen der Justiz

Funktionsblock	Erläuterung	Beispielprodukte/-anwendungen	Ermitt. Anzahl Anwendungen
Fachverfahren	Fachspezifische Verfahren der Gerichtsbarkeiten, Staatsanwaltschaften und des Vollzugs zur digitalen Abbildung von Geschäftsprozessen	EUREKA, JUDICA, GeFa (in Entw.), AuRegis	40+ (exkl. Vollzug)
eAkten	Verfahren zur elektronischen Aktenführung, insb. Erstellung, Bearbeitung, Sichtung, Verwaltung und Versand von Akten	eAS, e2A, eIP, Go\$a, eGPA, eGov-Suite	13
Basiskomponenten	Anwendungen zur Umsetzung querschnittlicher Fachprozesse wie Erstellung von Texten, Kostenverfahren, Saalmanagement o. ä.	bk.text (in Entw.), BKKB, e2S	30+
Elektronischer Rechtsverkehr (ERV)	Anwendung zum rechtssicheren Austausch von Akten und Dokumenten zw. Gerichten und Nutzenden wie Behörden, Unternehmen, Rechtsanwälten oder Bürgern	EGVP, Intermediär, VAS	3
Kommunikationsplattformen	Technische Plattform zum Datenaustausch (z. B. Konvertierung, Weiterleitung etc.) zwischen Anwendungen und Diensten über nachrichtenbasierten Datenaustausch	eKP, e2P	2
Identitäten/Berechtigungsmanagement	Anwendungen zur Verwaltung von Identitäten und Berechtigungen, d. h. Verwaltung von Zugriffen auf Anwendungen der Justiz	AD, SAFE, SA-mOA (in Entw.)	3
Technische Basisdienste	Dienste (oft Standardprodukte) für technische Aufgaben wie Virenskan oder OCR zur Digitalisierung von Dokumenten	Malware-Scan, Optical Character Recognition (OCR)	5+
Anwendungen der externen Domäne	Services der Justiz gegenüber externer Nutzenden wie Rechtsanwälten, Notaren, Bürgern, Unternehmen etc.	Akteneinsichtportal, Registerportal, Online Mahnantrag	20+
Sonstige Anwendungen	Im Projekt nicht analysierte Anwendungen wie z. B. Vollzugsanwendungen	Basis-Web, IS-Vollzug, SoPart	30+
Gesamtanzahl bekannter Justizanwendungen			>140

Im Projekt wurde eine Access Datenbank mit allen bekannten Justizanwendungen inkl. Kategorisierung, nutzender Länder, Status im Lebenszyklus (Entwicklung, Betrieb, Abschaltung etc.) erstellt und dem *BLK-Architekturboard* zur weiteren Verwendung übergeben.

2.2.1.1 Analyse der Anwendungslandschaft der internen Domäne

Fachverfahren: In der Justiz bestehen eine Vielzahl individueller fachlicher Anforderungen in den verschiedenen Gerichtsbarkeiten, der Staatsanwaltschaft und dem Vollzug. Das heißt, dass bspw. innerhalb der ordentlichen Gerichtsbarkeit für die Zivil- und Strafgerichte entweder jeweils eigene Fachverfahren existieren oder zumindest eigene Fachaufsätze mit speziellen Funktionalitäten. Entsprechendes gilt für die Fachgerichte (Verwaltungs-, Sozial-, Finanz- und Arbeitsgerichte). Hinzu treten spezifische Verfahren für Register-, Mahn- und Grundbuchsachen. In der Vergangenheit wurden einige Fachanwendungen (z.B. *EUREKA*, *ForumSTAR*) bereits länderübergreifend entwickelt, wobei die Entwicklungsverbünde nicht

alle Länder umfassen. Erst seit einigen Jahren werden mit den Projekten *GeFa*, *AuRegis* und *dabag* Anwendungen in bundesweiten Entwicklungsverbünden entwickelt.

Fachliche Basiskomponenten: Fachliche Basiskomponenten bilden querschnittliche Fachanforderungen ab, die in verschiedenen Fachprozessen bzw. Anwendungen verwendet werden (z. B. Personenverwaltung, Protokollierung). Als besondere fachliche Basiskomponenten wurden die Textsysteme (*bk.text* und *e2T*), Kostenverfahren (z. B. *BKKB*) und das Saalmanagement (z. B. *e2S*) hinzugezählt. *Bk.text* und *BKKB* wurden dabei im Rahmen von *GeFa* und *AuRegis* bundeseinheitlich mitentwickelt. Die Gesamtliste der Basiskomponenten wird im Rahmen der Zielbildentwicklung (vgl. **Kapitel 3**) erörtert.

Elektronische Aktenführung: Aufgrund des Gesetzes zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 (BGBl. I 2017, S. 2208) sind Gerichte und Staatsanwaltschaften verpflichtet, bis zum 1. Januar 2026 alle Verfahrensakten elektronisch zu führen. Zu diesem Zweck entwickelt die Justiz eigene Anwendungen, die alle Funktionalitäten zur Erstellung, Verwaltung und zum Versand von Verfahrensakten bereitstellen. Aktuell gibt es in der Justiz keine einheitliche Lösung, sondern drei eAkten-Verbünde mit eigenen eAkten-Lösungen (*e2A*, *eIP*, *eAS*). Einige Bundesgerichte nutzen zudem das Produkt *GO§A*. Die Einführung der eAkten-Systeme befindet sich aktuell in vollem Gange.

Davon unabhängig gibt es für die Gerichtsverwaltungen weitere eAkten-Systeme, vornehmlich die Produkte der Justizverwaltungen, die von der Landesverwaltung vorgegeben werden. Auch bei diesen Verwaltungs-eAkten stellt sich das Gesamtbild sehr heterogen dar.

Elektronischer Rechtsverkehr: Der *elektronische Rechtsverkehr* ermöglicht den rechtssicheren Austausch von Dokumenten (insb. Akten) zwischen Parteien, sowohl innerhalb der Justiz (z. B. zwischen Gerichten) als auch mit externen Parteien (z. B. Rechtsanwälte, Notare oder Bürger). Dafür nutzt die Justiz bundeseinheitlich das *Elektronische Gerichts- und Verwaltungspostfach (EGVP)*, welches für die Bedürfnisse der Justiz angepasst ist. Der Zugriff durch externe Nutzende erfolgt dabei durch individuelle Postfächer wie z. B. das *Mein Justizpostfach (MJP)* oder das *Besondere elektronische Anwaltspostfach (beA)* (vgl. **Kapitel 2.2.1.2**). Intern besitzt jedes Gericht ein Postfach, das auf ein eAkten-System oder eine andere postfachfähige Anwendung verweist, sodass Schriftverkehr in und aus den jeweiligen Verfahren ermöglicht wird. *EGVP* ist dabei z. B. für die Ver-/ Entschlüsselung der Nachrichten verantwortlich und interagiert dazu mit *SAFE-public*. Eingehende Nachrichten

werden dabei zunächst auf einem (technischen) Intermediär gesammelt, von dem sich z. T. verschiedene *EGVP*-Instanzen im Land Nachrichten je nach Postfach abholen können.

Kommunikationsplattformen: Wie viele Organisationen nutzt auch die Justiz eine klassische Kommunikationsplattform (engl. Enterprise Service Bus) zur Integration von Anwendungen (Enterprise Service Integration (EAI)). Die Kommunikationsplattform ist eine sog. Middleware und fungiert dabei vornehmlich im technischen Hintergrund. Sie erfüllt mehrere Aufgaben, wie z. B. die Konvertierung von Nachrichtenformaten, stellt die Kompatibilität von Protokollen sicher oder leitet Nachrichten zwischen Anwendungen weiter bzw. stellt die Übermittlung sicher. In der Justiz gibt es zwei Entwicklungsverbünde für den Aufbau der Kommunikationsplattformen (*eKP*, *e2P*).

Identitäten- und Berechtigungsmanagement: Das Identitäten- und Berechtigungsmanagement dient der Anlage und Verwaltung von Identitäten (z. B. Anlage eines neuen Mitarbeitenden oder einer externen Partei) sowie dem Zugriffsberechtigungsmanagement (z. B. Anlage neuer Berechtigungsrollen und deren sichere Verteilung an Identitäten), um Zugriffe auf Anwendungen der Justiz sicher zu verwalten. Zudem übernimmt das Identitäts- und Berechtigungsmanagement die sichere Zugriffssteuerung im Produktivbetrieb wie Authentisierung („Wer bin ich?“) und Autorisierung („Was darf ich?“) von Nutzenden (User-to-application (U2A)) und Maschinen bzw. Anwendungen (Application-to-application (A2A)). Diese Aufgaben werden idealerweise (best practice) in einem System (sog. authorisation server oder IAM) abgebildet, welches durch verschiedene Anwendungen als zentrales Berechtigungssystem genutzt werden kann. Die Justiz nutzt derzeit kein einheitliches Identitäten- und Berechtigungsmanagement, sondern betreibt verschiedene Anwendungen (*Active Directory*, *SAFE* bzw. in Zukunft *SAmOA* (*SAFE mit OAuth* auf Basis *KeyCloak*)).

Technische Basisdienste: Wie in jeder IT-Landschaft, werden auch in der Justiz viele Dienste eingesetzt, die technische Aufgaben im Hintergrund, z. B. im Kontext des Datenverkehrs, wahrnehmen. Dazu gehören bspw. Malware-Scanner und Software zur Digitalisierung und Konvertierung von Dokumenten (z. B. Optical Character Recognition (OCR)).

Anwendungen der Externen Domäne: In der externen Domäne, d. h. dem Netzwerksegment mit Verbindungen zu externen Nutzenden, wie Rechtsanwälten, Notaren, Bürgern, Unternehmen etc., finden sich viele der Funktionsblöcke ebenfalls. Statt Fachanwendungen werden dort Online-Services betrieben, die ebenfalls über eine Kommunikationsplattform verfügen, z. B. für den Versand von *EGVP*-Nachrichten, eigene Basisdienste oder ein eigenes Benutzer- und Berechtigungsmanagement (*SAFE-public*).

Gemeinsamkeiten der justizweiten Anwendungslandschaft

Aufgrund der hohen Heterogenität der genutzten Anwendungen innerhalb der Funktionsblöcke ergibt sich die Herausforderung, allgemeingültige Erkenntnisse über den Status Quo der Justizanwendungslandschaft herauszuarbeiten. Zum Startpunkt der Untersuchung bestand dazu noch keine einheitliche, für Bund und Länder stimmige, Gesamtsicht auf die Anwendungslandschaft. Daher wurde im Verlauf der Ist-Analyse zunächst ein übergreifendes Bild der Justizanwendungslandschaft entlang der Funktionsblöcke entworfen und dieses anschließend sukzessive im Rahmen der Interviews erweitert und ergänzt. Ziel war es dabei, die wesentlichen Funktionsblöcke und Anwendungen zusammenhängend zu verstehen, Abhängigkeiten und Kommunikationsverbindungen transparent darzustellen und so systematisch justizweite Merkmale der Justizanwendungslandschaft und wesentlicher Herausforderungen herauszuarbeiten.

Die Analyse hat dabei gezeigt, dass in allen Ländern die beschriebenen funktionalen Anwendungsblöcke sowie weitreichend vergleichbare Vorgehensweisen, Technologien, Verfahren und Herausforderungen bestehen. Diese werden nachfolgend beschrieben.

Erkenntnisse im Anwendungs- bzw. Schnittstellengefüge

Die Justizanwendungslandschaft bildet viele Fachprozesse der Justiz bereits digital ab und ermöglicht den Austausch von Daten auch zwischen Anwendungen. Die verschiedenen Einzelanwendungen der Justiz sind dazu vielfältig miteinander integriert. Vereinzelt sind auch technische Systeme wie bspw. Scanner in das Anwendungsgefüge eingebunden, die über technische Basisdienste und Kommunikationsplattformen integriert werden.

Der Zugriff auf die Justizanwendungen der internen Domäne erfolgt dabei in der Regel über sog. Fat Client Anwendungen auf den physischen oder virtuellen (z.B. *Citrix*) PC-Arbeitsplätzen der Nutzenden. Nutzende sind dabei insbesondere Richter, Staatsanwälte, Rechtspfleger, Urkundsbeamte, usw. Im Client wird eine Rahmenanwendung gestartet, aus der heraus sich dann eine oder verschiedenen Fachverfahren, Textsysteme und eAkten starten lassen und die damit eine unmittelbare, integrierte Arbeitserfahrung über die verschiedenen Anwendungen hinweg ermöglichen.

Die wichtigsten Anwendungen für Justizmitarbeitende sind dabei die Fachverfahren, eAkten und Textsysteme, die den Mittelpunkt der täglichen Arbeit bilden. Nutzende können sowohl das Fachverfahren, die eAkte oder direkt bspw. das Textsystem ansprechen. Daher bestehen auch Kommunikationswege zwischen allen drei Anwendungstypen.

Die Kommunikation der Anwendungen erfolgt dabei meist Client-seitig innerhalb der Rahmenanwendung und wird direkt über Integrationslogik in den Anwendungen verbaut (enge Kopplung). Der moderne browserbasierte Zugriff auf Webanwendungen, die serverseitig kommunizieren, ist in der Justiz noch nicht etabliert. Dies trägt zur Komplexität (z. B. Kompatibilitätsprobleme, Testaufwand) bei und erschwert Wart- und Modernisierbarkeit.

Die wichtigsten Kommunikationsverbindungen bestehen zwischen dem Fachverfahren und der eAkte (bspw. Aufruf von Akten aus einem laufenden Verfahren), zwischen Fachverfahren und Basiskomponenten (z. B. zur Kostenbearbeitung oder Saalbuchung) sowie zwischen eAkte und Textsystemen (z. B. zur Erstellung und Veraktung von Schriftstücken). Viele Verfahren kommunizieren dabei über die Kommunikationsplattform – je nach Land *eKP* oder *e2P*. Diese Plattform dient dabei der Entkopplung und Integration von Anwendungen und übernimmt z. B. die Konvertierung von Formaten zwischen Anwendungen oder übersetzt zwischen verschiedenen Protokollen.

Die Integrationen können sich dabei je Anwendung unterscheiden und sind zumindest für die Bestandsverfahren der Justiz nicht standardisiert. Auch in den Kommunikationsplattformen sind viele proprietäre Integrationsmuster verbaut, die z. T. fachliche Geschäftslogik enthalten und dadurch bei Weiterentwicklung und Pflege von Anwendungen stets berücksichtigt und nachgetestet werden müssen. Im Gegensatz zu modernen Kommunikationsmustern, müssen so Sender und Empfänger stets auch das Team der Kommunikationsplattform einbinden, was die o. g. Komplexitätsfaktoren weiter negativ beeinflusst.

Zwar hat die Justiz in den letzten Jahren über die Einführung des sog. *XJustiz*-Standards bereits eine stärkere Standardisierung von Nachrichtenformaten erreicht. Dennoch erzeugen die oft großen Nachrichtenpakete hohen Traffic und können Performanz und damit Nutzendenerfahrung beeinträchtigen, weil die sog. *XJustiz*-Standards sowohl die Metadaten der Nachricht als auch die Objekte wie Anhänge in einer Nachricht verpacken. Moderne Integrationsplattformen wie API-Management Gateways und Event Hubs, die solche Aufwände reduzieren können, existieren in der Justiz noch nicht. Stattdessen dominieren SOAP-Schnittstellen (SOAP: Simple Object Access Protocol) und nachrichtenbasierte Kommunikation über klassische Kommunikationsplattformen.

Während Anwendungen innerhalb eines Landes direkt über die beschriebenen Integrationswege miteinander kommunizieren, nutzt die Justiz für den Austausch von Daten zwischen den Ländern die Anwendung *EGVP-Enterprise*. Darüber können vor allem Dokumente, wie z. B. eine Klageschrift von einem Rechtsanwalt an ein Gericht, aber auch Akten von einem

Gericht an ein anderes, verschickt werden. So wird bspw. beim Versand einer eAkte von der eAkten-Anwendung eine *XJustiz*-Nachricht des sendenden Gerichts über die Kommunikationsplattform an *EGVP* gesendet. Dieses sucht das Postfach des empfangenden Gerichts in *SAFE-public*, verschlüsselt die Nachricht und übermittelt an den Intermediär des empfangenden Gerichts. Dabei werden stets Kopien der Akten verschickt, die im Zeitverlauf inkonsistent werden können. Der direkte Datenaustausch durch API-Zugriff auf Datenbestände anderer Länder ist aktuell nicht möglich.

Um die heterogenen, nachrichtenbasierten Integrationsverfahren in der Justiz weiterzuentwickeln, wurde im Jahr 2020 eine Integrationsstrategie durch das *BLK-Architekturbüro* entwickelt. Diese Strategie sieht grundsätzlich die Umsetzung einer nachhaltigen, serviceorientierten Anwendungsarchitektur vor. Ziel ist es dabei, Services so zu bauen, dass die spezifischen Aufgaben mit eigener Datenhaltung und Logik erfüllt und skalierbar über standardisierte APIs durch andere Services genutzt werden können. Dies fördert die Entkopplung und klare Trennung von Funktionalitäten sowie eine Modularisierung der Service-Landschaft und erhöht damit Skalierbarkeit, Wiederverwendbarkeit, Flexibilität und Wartbarkeit des Anwendungsgefüges. Dafür wurde auch die Verwendung moderner API-Gateways sowie Event-basierter Kommunikation empfohlen (vgl. **Kapitel 3.4.4**).

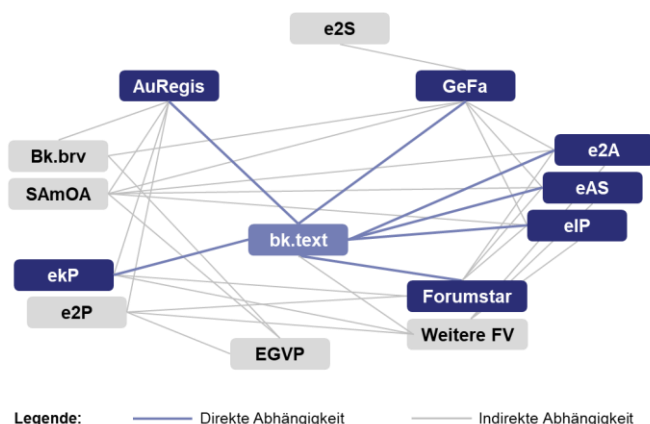
Die in der Integrationsstrategie empfohlenen Standards werden aktuell für die neuen Anwendungen der Justiz bereits teilweise umgesetzt. Bspw. werden parallel zu *GeFa* sogenannte fachliche Basiskomponenten entwickelt, die serviceorientierte, einheitliche Funktionalität für verschiedene Fachverfahren bieten (z. B. Personenverwaltung).

Durch die komplexe Integration zwischen den Bestandsanwendungen verstetigen sich viele Herausforderungen auch beim Aufsatz neuer Anwendungen (sog. „Henne-Ei-Problem“). Bspw. müssen die neuen Webanwendungen wie *GeFa* auch mit bestehenden eAkten über die Rahmenanwendung im Fat Client kommunizieren. Zudem müssen eigene Integrationslogiken (Adapter) entwickelt werden. Auch existiert in der Justiz noch kein API-Management Gateway, wodurch neue Anwendungen unvorteilhaft direkt miteinander kommunizieren müssen, anstelle dies über ein Gateway zu entkoppeln. Die nach wie vor bestehende Vielfalt an Textsystemen, Kommunikationsplattformen und eAkten führt zu einer komplexen Abhängigkeits- und Kompatibilitätsmatrix, die bei der Weiterentwicklung und Pflege stets berücksichtigt werden muss und die Testaufwände signifikant erhöht.

Eine Herausforderung dabei ist bspw., dass Änderungen von Anwendungen oder neue Features oftmals Anpassungserfordernisse in verbundenen Systemen erzeugen. Viele

Fachverfahren haben dabei nicht nur enge Schnittstellen zu einer eAkte und einem Textsystem, sondern müssen für verschiedene Länder und deren Umsysteme individuell angepasst und konfiguriert werden. So entstehen sehr komplexe Abhängigkeiten zwischen Anwendungen, deren Pflege sowohl technisch als auch organisatorisch herausfordernd ist.

Abbildung 6 | Abhängigkeitsmatrix *bk.text*



Ein Beispiel dafür ist die Anwendung *bk.text*, die aktuell pilotiert und noch weiterentwickelt wird. Mit der Zielsetzung, als modernes Textsystem zukünftig alle eAkten sowie neue als auch alte Fachverfahren bedienen zu können, muss das Entwicklungsteam Schnittstellen zu mindestens sieben Anwendungen mit jeweils vielen Besonderheiten entwickeln und pflegen.

Da sich die Anwendungen bzw. deren Versionen und Konfigurationen je nach Land unterscheiden, steigen Zeit- und Ressourcenaufwände exponentiell an. Damit fließt ein Großteil der Projektbudgets in die Pflege und Ausbringung von Anwendungen, anstatt in die Entwicklung nutzendenzentrierter moderner Funktionalität. Auch andere (Text-) Anwendungen haben komplexe Abhängigkeiten. Bspw. *e2T* fokussiert sich zwar auf *e2A* statt auf drei eAkten, muss aber die anderen in **Abbildung 6** dargestellten Schnittstellenrichtungen (z. B. zu *e2P* statt *ekP*, *EUREKA* statt *ForumSTAR*, *GeFa* und *AuRegis*) ebenfalls bedienen.

Erkenntnisse im Identitäten- und Berechtigungsmanagement

Wie der Betrieb von Anwendungen ist auch das Identitäten- und Berechtigungsmanagement (engl. Identity and Access Management (IAM)) in der Justiz in Hoheit der jeweiligen Länder bzw. des Bundes. Die Pflege der Identitäten erfolgt dabei typischerweise pro Land bzw. pro Bundesgericht in Verzeichnisdiensten wie z. B. *Microsoft Active Directory*.

Die Authentisierung, d. h. Identitätsprüfung, des Nutzers erfolgt dabei in der Regel über die Anmeldung am PC-Arbeitsplatz klassisch über Nutzernamen und Passwort. Multifaktor-Authentisierung wie bspw. über RSA-Token oder Handy sind nicht einheitlich bzw. durchgehend umgesetzt.

Zur Autorisierung, d. h. Zugriffssteuerung, werden je nach Anwendung unterschiedliche Logiken genutzt. Einige Anwendungen verfügen über ein eigenes Berechtigungsmanagement.

Dies ist herausfordernd und komplex, da die Vergabe von Berechtigungen in verschiedenen Anwendungen erfolgen muss. Bei Anpassungen, z. B. Entzug bestimmter Berechtigungen, muss dies in allen Anwendungen manuell nachgehalten werden. Teilweise können auch Berechtigungen von einem Verfahren, z. B. dem Fachverfahren, in anderen Anwendungen genutzt werden. So besitzen z. B. einige eAkte kein eigenes Berechtigungsmanagement, sondern übernehmen die Berechtigungen aus dem Fachverfahren.

Zur Modernisierung des Berechtigungsmanagements im Rahmen der Entwicklung der neuen Fachverfahren wurde in der Justiz die Anwendung *SAFE* als einheitliches Berechtigungsmanagementsystem entwickelt, das basierend auf dem SAML-Standard die Authentisierung und Pflege von Berechtigungen übernehmen soll. Es bietet dabei sichere Authentisierung und Single Sign-On (SSO). *SAFE* befindet sich aktuell noch in der Pilotierung. Weil *SAFE* noch keine Authentisierungsstandards wie OIDC und OAuth 2.0 (Token-basierte Zugriffskontrolle) unterstützt, diese aber für moderne Webanwendungen wie *GeFa* benötigt werden, wird es derzeit zu *SAmOA* weiterentwickelt. Dieses soll künftig die Authentisierung und Token-Erstellung übernehmen. Für die grob-granulare (sog. coarse-grained) Zugriffssteuerung bzw. Autorisierung auf Justiz-Webanwendungen wurde im Kontext von *GeFa* zudem eine Basiskomponente Berechtigungsverwaltung entwickelt. Fein-granulare (sog. fine-grained) Zugriffe sollen weiterhin in der jeweiligen Anwendung erfolgen. Für die länderübergreifende Authentisierung sowie für Online-Services der externen Domäne ggü. externen Nutzenden bestehen eigene Berechtigungssysteme bzw. *SAFE*-Instanzen (*SAFE-public*) (vgl. **Kapitel 2.2.1.2**).

Damit verfügt die Justiz in Zukunft über ein modernes Berechtigungssystemgefüge, das allerdings als eigenentwickelte Anwendung viele mögliche Zukunftsanforderungen, die auch in einem Cloud-Kontext relevant wären, noch nicht bedient. Dazu gehören bspw. adaptive Multifaktor-Authentisierung, Delegation von Berechtigungsverwaltung oder moderne Föderationsverfahren für Identitäten (mit sog. Identity Providern (IDP)). Für die interne Domäne wäre in einer gemeinsamen, bundeseinheitlichen Cloud voraussichtlich eine Weiterentwicklung von *SAmOA* oder ein neues zentrales IAM-System notwendig. (vgl. **Kapitel 3.4.6**)

Erkenntnisse zur Anwendungsarchitektur und Technologie-Stack

Die meisten Bestandsanwendungen der Justiz, die in der Ist-Analyse betrachtet wurden, verwenden klassische, monolithische Schichtenarchitekturen. Modernere Microservice-Architekturen finden sich nur bei den neuen Anwendungen *GeFa* und *AuRegis*. Modernste Serverless-Architekturen gibt es mangels Cloud-Einsatz noch gar nicht.

In einer Schichtenarchitektur bestehen Anwendungen aus einem Frontend (z. B. JSF) sowie einem monolithischen Backend mit der Geschäftslogik (z. B. JBoss, JEE), die auf sog. Application Servern betrieben werden. Das Backend nutzt in der Regel ein klassisches, serverbasiertes relationales Datenbanksystem wie *MS SQL* oder *Oracle*.

Zum Teil begründet durch die Heterogenität der historisch gewachsenen Anwendungslandschaft, weist auch die Technologielandschaft (sog. Technologie-Stack) eine hohe Heterogenität auf. Ein anderer Grund liegt darin, dass die Justizverwaltungen individuelle Rahmenverträge mit Technologie-Providern bzw. Herstellern schließen und somit im jeweiligen Land z. B. nur bestimmte Datenbanktechnologien bzw. -produkte verfügbar sind. Viele Justizanwendungen müssen daher zum Teil mehrere Datenbanksysteme unterstützen, je nachdem in welchem Land sie betrieben werden. Dies wiederum beeinflusst die Entwicklungs- und Ausbringungskomplexität sowie -geschwindigkeit negativ.

Wie eingangs erläutert sollten Anwendungen, die für einen zukünftigen Cloud-Betrieb in Frage kommen, containerisiert, mandantenfähig und mit Desktop-unabhängigen Frontends (Webfähigkeit) ausgestattet sein. Abgesehen von den Neuentwicklungen *GeFa* und *AuRegis* ist keine der analysierten Anwendungen der Justiz aktuell in diesem Sinne Cloud-ready. Einige Anwendungen (z. B. *e2T*, *e2A* oder *bk.text*) planen zwar eine Modernisierung, aber durch die Abhängigkeiten von bestehenden Betriebskontexten (z. B. zur Rahmenanwendung im Client) ist der Umbau zu leichtgewichtigen, Cloud-nativen Webanwendungen aufwändig. Für einen Cloud-Betrieb von Verfahren müsste dies architekturell langfristig vorgeplant und parallel zum Aufbau einer Cloud umgesetzt werden (vgl. **Kapitel 3.4.2** und **5.1**).

Eine weitere Erkenntnis ist die fehlende oder eingeschränkte Mandantenfähigkeit vieler Anwendungen. Im derzeitigen landesspezifischen Betrieb bezieht sich Mandantenfähigkeit auf die Abbildung verschiedener Gerichte innerhalb einer Anwendungsinstanz. Mangels ausreichender Skalierbarkeit werden viele Fachverfahren und eAkten mehrfach pro Land, d. h. multi-istanziiert betrieben. Dabei sind bspw. nur ausgewählte Gerichte einer Anwendungsinstanz zugewiesen. Dies treibt die Komplexität und Aufwände für Ausbringung, Wartung und Pflege enorm, weil dementsprechend auch die Kommunikationsplattformen und der *ERV* dieses Setup berücksichtigen müssen.

Einige Anwendungen (z. B. *e2T*) können aus einer Instanz für ein Land betrieben werden. Mandantenfähig im Sinne eines Betriebs einer Anwendungsinstanz für mehrere Länder ist bisher aber noch keine Anwendung der Justiz. Aufgrund fehlender einheitlicher Betriebsumgebungen war diese Form der Mandantenfähigkeit bisher nicht gefordert. Um für einen

zukünftigen Betrieb in einer bundeseinheitlichen Justizcloud größtmögliche Synergien zu erreichen, sollte diese Möglichkeit in der künftigen Anwendungsentwicklung aber berücksichtigt werden (vgl. **Kapitel 3.4.3**).

Tabelle 3 | Übersicht analysierter Anwendungen

Anwendung	Lebenszyklus	Containerisiert	Webfähigkeit	Mandantenfähigkeit
GeFa	Entwicklung	Ja	Ja	Für Landesbetrieb*
AuRegis	Pilotierung	Ja	Ja	Für Landesbetrieb
dabag	Entwicklung	Nein	k. A.	Für Landesbetrieb
eAkten	Ausbringung lfd.	Nein	Nein	Nein
EGVP	Produktiv	Nein	Nein	Für Landesbetrieb
SAFE	Pilotierung	Nein	Nein	Für Landesbetrieb
SAmOA	Entwicklung	Ja	Ja	Für Landesbetrieb
eKP	Produktiv	Nein	Nein	Nein
e2P	Produktiv	Nein	Nein	Nein
e2T	Produktiv	Nein	Nein	Für Landesbetrieb
bk.text	Pilotierung	Nein	Nein	1x Instanz je FV und Land

* Mandantenfähigkeit im Landesbetrieb bedeutet, Installation einer Instanz pro Land, die alle Mandanten, d. h. Gerichte, bedienen kann. Keine der genannten Anwendungen ist aktuell auch für einen landes-übergreifenden Betrieb mandantenfähig.

Erkenntnisse zu Anwendungsentwicklung, -ausbringung und -betrieb:

Wie beschrieben erfolgt die Entwicklung von Anwendungen in der Justiz weitgehend in sog. Entwicklungsverbünden. Im Rahmen der Planung, Anforderungserhebung, Konzeption und Entwicklung muss dabei jeder Entwicklungsverbund auch auf die landesspezifischen, heterogenen Anwendungslandschaften und Betriebsumgebungen bzw. -infrastrukturen eingehen. Anwendungen müssen bspw. verschiedene Umsysteme mit ähnlicher Funktionalität aber unterschiedlichen Schnittstellen anbinden (z. B. zwei Textsysteme und drei eAkten). Darüber hinaus unterscheiden sich die Betriebsinfrastrukturen, z. B. in Bezug auf verfügbare Datenbanktechnologien und Laufzeit- bzw. Container-Umgebungen. Daher fließen in der Entwicklung viele Ressourcen in das Bedienen der komplexen heterogenen Umfeldes anstatt in die Entwicklung nutzendenzentrierter Funktionalitäten oder Features.

Eine weitere Herausforderung ist das Fehlen eines justizweiten Anforderungs- und Releasemanagements. Zwar wurde mit der *Servicestelle Anforderungsmanagement (SAM)* dafür eine Einheit geschaffen. Diese ist allerdings noch nicht im Wirkbetrieb etabliert. Entwicklungsverbünde müssen sich daher, z. B. bei der Schnittstellendefinition und der Lieferung

von Features, selbst koordinieren, obwohl sie Änderungen am Gesamtanwendungsgefüge vornehmen. Auch diesbezüglich fließen viele Ressourcen in Koordination und Abstimmung statt in die eigentliche Entwicklung.

Die Entwicklung innerhalb des Entwicklungsverbunds selbst erfolgt in der Regel durch externe Dienstleister. Einheitliche Vorgaben zu Entwicklungs- und Ausbringungstools, Entwicklungs- und Testumgebungen, einzusetzenden Technologien sowie zu Vorgehensmodellen bestehen nicht. Die Vorgehensweisen in der Anwendungsentwicklung können sich daher über verschiedene Entwicklungsverbünde stark unterscheiden. Ein einheitlicher Entwicklerarbeitsplatz, der beispielsweise auch den übergreifenden Einsatz von Entwicklern auf verschiedenen Entwicklungsprojekten der Justiz ermöglichen würden, besteht nicht.

Die Heterogenität und Komplexität in der Anwendungsentwicklung wirkt sich auch unmittelbar auf die Anwendungsausbringung in höheren Teststufen bzw. den Betrieb aus. In den meisten Fällen ist es Ziel der Entwicklungsverbünde, neue Features und Updates zwei Mal pro Jahr und pro Land zu ermöglichen. Durch die Entwicklungsverbünde wird dabei oft ein fertiges Softwarepaket inklusive Installations-Tools zur Ausbringung (sog. Release Kits) bereitgestellt. Anschließend treffen sich Fachvertreter des Entwicklungsverbundes und testen die Anwendung umfassend auf Referenzumgebungen (vgl. **Abbildung 7**). Häufig werden Tests dabei noch manuell ausgeführt. Es bestehen zwar in den Entwicklungsverbünden standardisierte Testprotokolle und Testfälle, moderne Automation von technischen und funktionalen Tests ist aber sehr selten (z. B. hat *GeFa* bereits eine CI/CD-Pipeline in einer Test-/Referenzumgebung inkl. Testautomatisierung). (vgl. **Kapitel 3.5.6**)

Wenn die Anwendungen sowohl durch den Entwickler im Entwicklungsverbund als auch durch die Fachvertreter auf der Referenzumgebung erfolgreich getestet wurden, müssen die Anwendungen im letzten Schritt auch bei dem jeweiligen IT-Dienstleister-Land bzw. bei den Bundesgerichten final getestet und produktiv ausgebracht werden. Hier fallen in vielen Fällen noch Fehler und landes- bzw. bundesgerichtsspezifische Probleme auf, die wiederum zu Anpassungen und erneuten Test- und Ausbringungszyklen führen.

Diesbezüglich wurde auch die Softwarequalität in vielen Expertengesprächen bemängelt. Dies liegt insbesondere daran, dass die Entwicklungsverbünde die bundesweit heterogenen Betriebsumgebungen und jeweiligen Umsystem-Konstellationen nicht bzw. nur bedingt nachstellen können. Die Software kann daher nur bis zu einem gewissen Grad während der Entwicklung integriert und mit Umsystemen getestet (sog. Integrationstests) werden. In den Testzyklen vor der Ausbringung ergeben sich daher häufig Probleme, welche Nacharbeiten

und Anpassungen durch die Hersteller erfordern. Dies treibt sowohl die Dauer von Ausbringungszyklen als auch die Kosten.

Eine besondere Komplexität bei der Ausbringung entsteht dadurch, dass nicht nur unterschiedliche Umsysteme, sondern auch oft unterschiedliche Versionen der Umsysteme laufen. Dies kann z. B. der Fall sein, wenn ein Land einen Release überspringt, was durch fehlende Ressourcen oder technische Probleme immer wieder vorkommt.

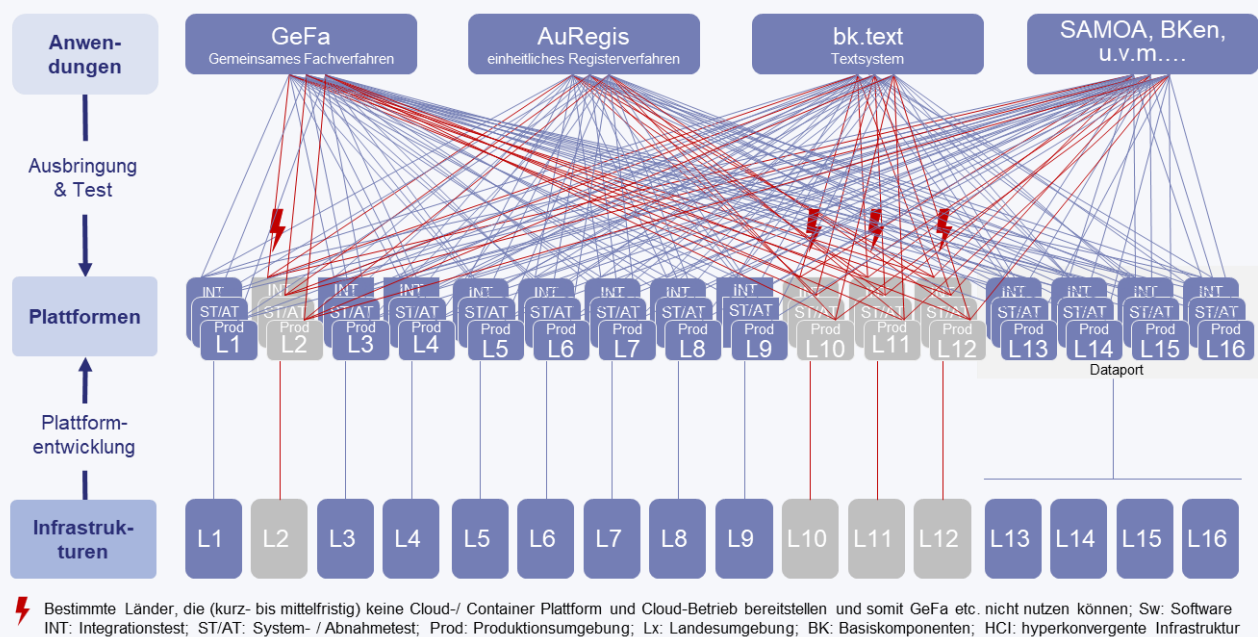
Aufgrund der genannten Probleme sind auch die geplanten zwei Releases pro Jahr in der Justiz nicht immer machbar. Im Vergleich zum Marktstandard moderner Cloud-nativer Webapplikationen, die häufig mehrmals pro Tag (z. B. neue Features) aktualisiert werden können, hat die Justiz hier Nachholbedarf. Dies einerseits, um Fehler früher zu entdecken und ein iterativeres Entwickeln zu ermöglichen. Aber vor allem, um nutzendenzentrierte Anwendungen zu entwickeln, bei denen es darauf ankommt, dass Entwickler zeitnahes Feedback zu neuen Features bzw. zur Betriebsstabilität ihrer Anwendungen von Nutzenden erhalten. Bei ein bis zwei Ausbringungen pro Jahr (und Land) erhalten Entwicklungsverbünde nur stark verspätetes, sequenzielles Feedback, welches sich oftmals auf Anwendungsteile bezieht, die der Entwicklungsverbund vor Monaten bearbeitet hat.

Eine drastische Beschleunigung der Ausbringung könnte durch einen einheitlichen Entwicklerarbeitsplatz und den Aufbau von CI/CD-Pipelines erreicht werden. Diese ermöglichen kontinuierliche, automatisierte Ausbringungen entlang der Teststufen bis in die Produktion. Dieses Konzept ist in der Regel jedoch nur sinnvoll, wenn die Entwicklung konsequent auf betriebsnahen Umgebungen und damit aktuell pro Land bzw. Bundesgericht stattfinden würde. Einzelne Länder oder Entwicklungsprojekte investieren bereits in CI/CD, aber umfassende, moderne Automation und damit Beschleunigung der Ausbringung ist aufgrund der Trennung von Entwicklung bei Herstellern und Betrieb bei IT-Dienstleistern aktuell nicht effizient umsetzbar. Dazu wäre entweder eine hohe Standardisierung der IT-Betriebe oder der Aufbau einer gemeinsamen Cloud-Umgebung notwendig, auf der zukünftig naturgemäß standardisiert entwickelt, getestet und betrieben wird.

Bei der Ausbringung von Cloud-nativer Software (wie *GeFa* und *AuRegis*) ergeben sich durch die heterogenen Betriebsumgebungen noch weitere Herausforderungen. Um solche Cloud-nativen Anwendungen betreiben zu können, sind umfassende Investitionen in (private) Betriebsumgebungen mit modernen Container-(Orchestrierungs-)Plattformen notwendig. Diese müssen auf bestehender virtualisierter Infrastruktur aufgebaut und dazu neue Netzwerksegmente (sog. Mikrosegmentierung) sowie entsprechende Monitoring-,

Logging- und Sicherheitsmechanismen für den Cloud-Betrieb geschaffen werden. Zudem muss das entsprechende Know-how zum Aufbau und laufenden Betrieb aufgebaut werden. Ohne eine einheitliche Betriebsumgebung müssen für den Betrieb der neuen Cloud-nativen Anwendungen diese Aufwände für den Aufbau, den Betrieb und die Pflege der entsprechenden Cloud-Infrastruktur jeweils pro Land bzw. Bundesgericht aufgebracht werden. Einige Länder haben dabei mit dem Aufbau begonnen, während andere noch gar keine Vorkehrungen getroffen haben (vgl. **Kapitel 2.2.2**). Für die Ausbringung der neuen Fachverfahren bedeutet dies, dass einige Länder die Anwendungen noch gar nicht bzw. auf absehbare Zeit nicht einsetzen könnten. **Abbildung 7** zeigt die hohe Komplexität und resultierende Herausforderungen bei der Ausbringung neuer Anwendungen auf.

Abbildung 7 | Komplexität der Ausbringung von Justizanwendungen (illustrativ)



Aus Sicht der Entwicklungsverbünde entsteht im föderalen Aufbau von Cloud-Infrastruktur aktuell wiederum eine heterogene Landschaft. Denn je IT-Dienstleister bzw. Land kommen unterschiedliche Container-Plattformen zum Einsatz. Ein weiterer Nachteil des derzeitigen Verfahrens ist, dass der laufende Anwendungsbetrieb pro Land organisiert ist. Für weitgehend identische Anwendungen, die gemeinsam konzipiert und entwickelt wurden, muss daher in jedem Land neues Personal aufgebaut bzw. geschult werden, das die Wartung und Überwachung der Anwendungen im Regelbetrieb sicherstellt.

Eine gemeinsame Cloud-Umgebung könnte den beschriebenen Entwicklungs-, Test- und Betriebsprozess signifikant vereinheitlichen, die erforderlichen Investitionen in Cloud bündeln und somit erhebliche Kosten- und Komplexitätsreduktion ermöglichen (vgl. **Kapitel 3**).

2.2.1.2 Analyse der Anwendungslandschaft der externen Domäne

Neben der internen Anwendungslandschaft für die Gerichte, Staatsanwaltschaften und den Vollzug stellt die Justiz Online-Services für externe Nutzende bereit. Die wichtigsten externen Nutzendengruppen sind Bürger, Rechtsanwälte, Notare, Unternehmen bzw. Organisationen sowie nationale Behörden (z. B. Polizei) und internationale Behörden (z. B. EU-Justiz). Insgesamt konnten im Rahmen der Ist-Analyse 23 bestehende und in Entwicklung befindliche Online-Services der externen Domäne identifiziert werden (vgl. **Abbildung 8**).

Abbildung 8 | Übersicht Online-Services

1. Registerportal (z.B. Handels- und Genossenschaftsregister)	9. Zwangsversteigerungstermine	17. Mein Justizpostfach
2. Insolvenzportal für zentralen Zugriff auf Insolvenzverfahren	10. Restrukturierungsbekanntmachungen	18. Online-Terminbuchung
3. Akteneinsichtsportal	11. Orts- und Gerichtsverzeichnis	19. Elektronische Kostenmarke
4. Online Mahnantrag zur Beantragung Mahnbescheiden	12. Grundbuchportal	20. Führungszeugnis
5. Schutzschriftenregister für Antrag/Abfrage Schutzschriften	13. Justiz-Auktion	21. E-Erbschein
6. Digitale Rechtsantragstelle (RAST)	14. Rechtsdienstleistungsregister	22. Dolmetscher- und Übersetzerdatenbank
7. Zivilgerichtliches Online-Verfahren (ZOV)	15. Transparenzregister	23. Vollstreckungsportal
8. Justizportal <i>justiz.de</i>	16. Negativbescheinigung Insolvenzgericht	

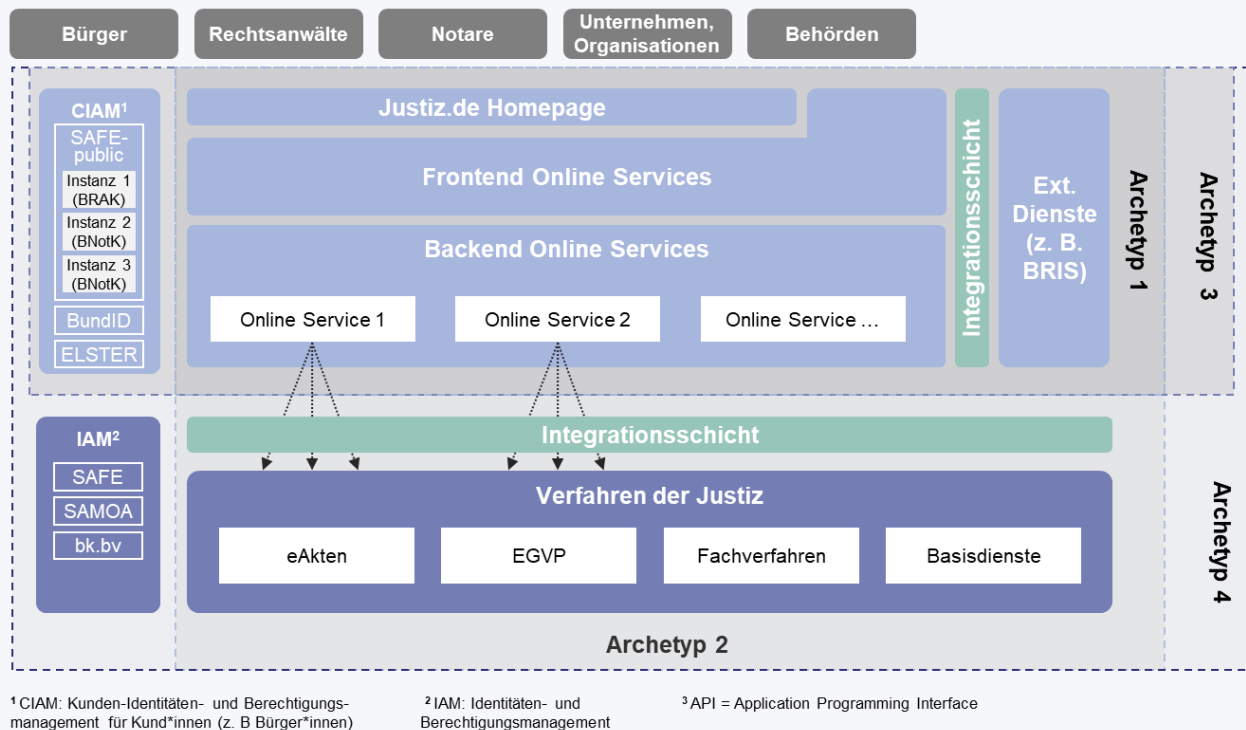
Nach der Bestandsaufnahme wurde eine Auswahl sechs wesentlicher Online-Services getroffen, um diese in einem gemeinsamen Workshop mit den Serviceverantwortlichen detaillierter zu untersuchen. Im Fokus der fachlichen, technischen und rechtlich-organisatorischen Betrachtung standen dabei die Online-Services: *Registerportal*, *Insolvenzportal*, *Akteneinsichtsportal (AEP)*, *Online Mahnantrag*, *Schutzschriftenregister* sowie die noch im Auftrag des *BMJ* in Entwicklung befindliche *Digitale Rechtsantragstelle (RAST)*.

Wesentliche Erkenntnisse zu Online-Services

Online-Services der Justiz werden typischerweise durch ein Land federführend entwickelt und dort für die deutsche Justiz betrieben. Viele Online-Services betreibt dabei das Land

Nordrhein-Westfalen, bei dem auch das gemeinsame Justizportal *www.justiz.de* betrieben wird. Das Portal stellt dabei Verlinkungen zu Online-Services für Nutzende bereit, d. h. die Anwendungen und/ oder Dokumentsammlungen selbst sind über eigene Webseiten aufrufbar, die bundesweit verteilt sind. Grundsätzlich können in der Justiz vier verschiedene Archetypen von Online-Services unterschieden werden (vgl. **Abbildung 9**).

Abbildung 9 | Archetypen zur Kategorisierung von Online-Services



Archetyp 1 sind frei zugängliche Online-Services ohne dedizierte Nutzendenberechtigung und Backend-Integration, z. B. Dienste mit einfachen CMS-Systemen (z. B. Justizportal). **Archetyp 2** sind Online-Services mit Integration zur internen Domäne, aber ohne Nutzendenberechtigung für externe Nutzende (z. B. Registerportal). **Archetyp 3** sind personalisierte Online-Services mit eigener Nutzendenberechtigung, aber ohne Integration zur internen Domäne (z. B. Online Mahnantrag). **Archetyp 4** sind komplexe Online-Services mit Integration zur internen Domäne und eigener Nutzendenberechtigung für externe und interne Nutzende (z. B. Akteneinsichtsportal).

Bei der Analyse von Online-Services sind vier Bereiche besonders relevant: Benutzer- und Berechtigungsmanagement, Interaktionsmanagement, Schnittstellenmanagement und Integration sowie fachliche und technische Services bzw. deren Umsetzung (vgl. auch Cloud-

Readiness insb. Containerisierung und Microservice-Architektur). Mandantenfähigkeit im Sinne der Cloud-Readiness spielt bei Online-Services eine untergeordnete Rolle, da sich die Services an externe Nutzendengruppen richten.

Erkenntnisse im Benutzer- und Berechtigungsmanagement

Die Analyse zeigt, dass nicht alle Online-Services eine eigene Benutzer- und Berechtigungsverwaltungen benötigen (siehe Archetyp 1 und 2). Die dort bereitgestellten Informationen sind öffentlich verfügbar und können z. B. durch Aufruf der Webseite eingesehen werden. Beispiele dafür sind das *Insolvenzportal* oder das *Registerportal* (z. B. Handelsregister).

Abbildung 10 | Nutzendengruppen analysierter Online-Services

		Bürger	Rechtsanwälte	Notare	Unternehm., Organisat.	Behörden
Archetyp / Service		MJP inkl. BundID	beA	beN	eBO	beBPo
1	Insolvenzportal	Keine Authentisierung für <i>Auskunftsportal</i> notwendig				
2	Registerportal	Keine Authentisierung zur Nutzung notwendig				
3	Online Mahnantrag (auch e-ID mögl.)	x	x		x	
4	Schutzschriften- register		x		x	
	Akteneinsichtsportal	x	x	x	x	x
	Digitale Rechts- antragstelle	In Konzeption			In Konzeption	
	Zivilgerichtl. Online- Verfahren					

Legende: x = Authentifizierung notwendig

Für Online-Services der Archetypen 3 und 4 (z. B. *Online Mahnantrag* oder *Schutzschriftenregister*) besteht mit *SAFE-public* ein eigenes Benutzerverwaltungssystem (sog. Authentisierungsdienst), dass die Zugriffe auf Online-Services der Justiz ermöglicht. Die Trennung von User Pools nach interner (sog. B2E) und externer (sog. B2B/ B2C) Domäne ist Markt- und Sicherheitsstandard. Diese kann logisch in einem gemeinsamen IAM-System oder – wie in der Justiz – physisch in getrennten Systemen erfolgen.

SAFE-public ist ein Verzeichnisdienst, der vor allem auch im Kontext des Austausches von *EGVP*-Nachrichten zwischen Gerichten und Strafverfolgungsbehörden sowie zwischen Justiz und externen Parteien wie Bürgern und Rechtsanwälten genutzt wird. In *SAFE-public*

werden die Adressen der *EGVP*-Postfächer sowie Nutzenden-spezifische Verschlüsselungszertifikate gehalten und können so durch die Sende-und-Empfangskomponenten der Nutzenden für den Versand von Nachrichten gefunden und adressiert werden.

Für die verschiedenen Nutzendengruppen der Justiz bestehen jeweils unterschiedliche Postfächer. Bei Bürgern und Rechtsanwälten entspricht die *SAFE-ID* quasi auch der Identität der Nutzenden, bei Gerichten, Behörden und Unternehmen hält *SAFE* eine funktionale Adresse und keine Identitäten. Um die User Pools und Anlageprozesse zu unterscheiden, besteht je Nutzendengruppe eine eigene *SAFE-public* Instanz, die jeweils von unterschiedlichen Betreibern gehostet wird und die unterschiedlichen Onboarding-Prozesse unterstützt.

Tabelle 4 | Übersicht Postfächer und *SAFE-public* Instanzen

Kommunikationspartner	Unterstützte Postfächer	Betreiber <i>SAFE-public</i> Instanz
Gericht <> Gericht	Klassisches elektronisches Gerichts- und Verwaltungspostfach (EGVP)	Instanz 1: Bundesnotarkammer
Behörden <> Gerichte	Besonderes elektronisches Behördenpostfach (beBPo)	
Notare <> Justiz	Besonderes elektronisches Notarpostfach (beN)	
Unternehmen <> Justiz	Elektronisches Bürger- und Organisationenpostfach (eBO)	
Bürger <> Justiz	Mein Justizpostfach (MJP)	Instanz 2: Bundesnotarkammer
Rechtsanwälte <> Justiz	Besonderes elektronisches Anwaltspostfach (beA)	Instanz 3: Bundesrechtsanwaltskammer
Steuerberater <> Justiz	Besonderes elektronisches Steuerberaterpostfach (beSt)	Instanz 4: Bundessteuerberaterkammer

Da die Nutzendenkonten in verschiedenen *SAFE-public* Instanzen gepflegt werden, sind Featureupdates im Kontext des Benutzer- und Berechtigungsmanagements an verschiedenen Stellen notwendig. Da *SAFE-public* nur ein Authentisierungs- und kein Autorisierungsdienst ist, sind zudem weiterhin Berechtigungsverwaltungen in den eigentlichen Anwendungen erforderlich.

Die meisten Online-Services lassen sich heute per (Hyper-)Link auf dem *Justizportal* (justiz.de) ansteuern und bieten teilweise eine individuelle Authentisierung (Archetyp 3 und 4) mit dem jeweiligen *SAFE-public* Dienst an (z. B. Mahnantrag für Rechtsanwälte). Aufgrund

der unterschiedlichen Verteilung und Umsetzung der Dienste ist aber ein modernes „once-only“ Single-Sign-on (SSO) für externe Nutzende nicht möglich. Zudem gibt es kein übergreifendes Portal, das SSO initial übernimmt und darüber hinaus z. B. die Selbstpflege von Identitäten-Stammdaten und Passwortrücksetzung der Nutzenden (Self-Service) ermöglicht und je nach Kundengruppe den vorauthentisierten Zugriff auf verschiedene Online-Services je nach Berechtigung ermöglicht. Ein modernes IAM für externe Nutzende (sog. CIAM = Customer Identity and Access Management) sollte daher im Rahmen des Zielbilds für die externe Domäne aufgenommen werden (vgl. **Kapitel 3.4.6**).

Erkenntnisse im Interaktionsmanagement

Zur Interaktion von Nutzenden mit der Justiz besteht zwar ein gemeinsames Portal (vgl. *justiz.de*), aber die einzelnen Services sind hinsichtlich der Nutzendenerfahrung, Benutzeroberflächen (UI/UX), Funktionalitäten und Zugangswege uneinheitlich. Dabei wachsen die Anforderungen an eine Einheitlichkeit des Onlineauftritts seit vielen Jahren stetig. Nutzende haben zunehmend Erfahrung mit einheitlichen Kundenplattformen und erwarten ähnliche Qualität und Nutzendenerfahrung auch von der Justiz und Verwaltung. Zudem bestehen auch zunehmend gesetzliche Vorgaben an die Einheitlichkeit und Qualität von Webauftritten wie z. B. durch das Onlinezugangsgesetz (OZG).

Die Kommunikation erfolgt derzeit hauptsächlich über Postfächer. Möglichkeiten wie Self-Services, direkter Service-Support, einheitliche Dokumentenverwaltung oder einfache Upload- und Download-Möglichkeiten mit Statusangaben zur Sache sowie Nutzerprofile bzw. Stammdatenpflege oder personalisierte Dienste in einer Plattform sind aktuell nicht möglich. Unabhängig davon erfolgt zudem keine systematische, serviceübergreifende Aufnahme und Auswertung von Nutzendenfeedback, z. B. zur iterativen Weiterentwicklung, Verbesserung und Standardisierung der Online-Service-Landschaft.

Abschließend sind die Justiz-Online-Services primär Browser-basierte Anwendungen, d. h. für die PC-Nutzung ausgelegt. Dedizierte Mobile Apps oder Justiz-APIs zur Entwicklung von „Justiz-Apps“ oder Einbindung in externe Anwendungen durch Dritte (z. B. für Rechtsanwälte, Notare) bestehen noch nicht.

Erkenntnisse zu Schnittstellenmanagement und Integration

Auch im Bereich der Online-Services ist die Schnittstellen- und Integrationslandschaft heterogen und komplex. Einige Online-Services (des Archetyps 2 und 4) müssen vielfältige

teilweise zu Gerichten, verschiedenen Fachverfahren sowie in manchen Fällen auch zu EU-Verfahren bedienen bzw. konsumieren.

Da viele Anwendungen der internen Domäne noch keine REST-APIs anbieten, ist die Integration von Daten aus diesen Verfahren in die Online-Services (z. B. bei Handelsregistereinträgen) komplex. Oftmals werden Daten nachrichtenbasiert und damit redundant und teilweise langsam übertragen. Teilweise werden die Daten auch nicht automatisiert erhoben, sondern von verschiedenen Ländern durch manuelle Eingabe zugeliefert (z. B. Insolvenzportal). Dabei bestehen signifikante Synergien mit der Modernisierung der Fachverfahren (z. B. *GeFa*, *AuRegis*). Aufgrund des API-First Ansatzes bei modernen Cloud-nativen Webanwendungen, nutzen nämlich die Frontend-Client-Applikation eine API, um mit den Backend-APIs zu kommunizieren. Das beschleunigt nicht nur die parallelisierte Entwicklung von Frontend und Backend, sondern erlaubt es auch, dass Backend-Services untereinander über die APIs kommunizieren (sog. Maschine-Maschine-Kommunikation). Dabei können Teile der APIs eben auch über ein API-Gateway anderen internen oder eben auch externen Maschinen entkoppelt, sicher und performant zugänglich gemacht werden.

Auch für Externe bietet die Justiz nur in Einzelfällen APIs zum Exponieren von Online-Services an (z. B. API des [Handelsregister](#)). Sofern Justiz-APIs bestehen, werden diese weder internen (Fachverfahrens-)Entwicklern der internen Domäne noch externen Entwicklern in einem modernen API-Developer Portal angeboten, d. h. dokumentiert, publiziert, test- und beantragbar gemacht.

Für den Aufbau eines API-Serviceportfolios, das im Rahmen des sich entwickelnden API-Ökosystems in einer digitalisierten Wirtschaft sowohl externe Services konsumiert als auch interne Services exponiert, sollte die Justiz die Online-Service-Landschaft weiterentwickeln, modernisieren, vereinheitlichen und flexibilisieren.

Erkenntnisse zur technischen Architektur

Ebenso wie bei Anwendungen der internen Domäne sind auch die Architekturen und Technologien im Bereich der Online-Services uneinheitlich. In der Analyse wurde eine Heterogenität genutzter Entwicklungsumgebungen, Programmiersprachen, Frontend- und Schnittstellentechnologien etc. festgestellt. Zudem sind die meisten Online-Services noch nicht Cloud-ready, d. h. nicht containerisiert oder Microservice-basiert.

Für alle Herausforderungen der Online-Service Landschaft, die u. a. durch die Komplexität der Bestandssysteme und Heterogenität von Anwendungen und Infrastrukturen im Mehr-

Länder-Betrieb resultieren, könnte eine einheitliche Justizcloud Synergiepotenziale bieten. Hier sind bspw. der Betrieb eines modernen Justizportals, querschnittliche Services wie ein CIAM und Kommunikationsdienste, einheitliche Frontend- und Backend-Technologien sowie moderne Integrationswege über ein API-Gateway zu nennen. Eine ausführliche Darstellung der Synergien durch eine Justizcloud findet sich in **Kapitel 3.4.2.2.**

2.2.2 IT-Betrieb der Länder

Einordnung

Die Entwicklung einer bundeseinheitlichen Justizcloud hat das Potenzial, die Art und Weise, wie Software in der Justiz entwickelt, integriert und betrieben wird, deutlich zu transformieren. Insbesondere der Anwendungsbetrieb erfolgt derzeit durch dedizierte Landes-IT-Dienstleister. Diese haben ggf. bereits in Cloud-Technologie und/ oder -kompetenzen investiert bzw. planen es, was in der Untersuchung berücksichtigt wurde. Eine bundeseinheitliche Betriebsumgebung würde sich auch auf die Beauftragung der IT-Dienstleister durch die Länder bzw. Bundesgerichte auswirken. Wie genau diese Auswirkungen aussehen, hängt sowohl vom Justizcloud-Zielbild als auch von der Ausgangssituation und Cloud-Strategie der IT-Dienstleister ab. Daher ist es zentral, zu verstehen, wie genau die Justiz heute Software entwickelt, integriert und betreibt und welche Rolle dabei die öffentlichen IT-Dienstleister und deren (ggf. noch im Aufbau befindlichen) Cloud-Angebote spielen.

Die Ist-Analyse zielt daher auf drei Aspekte ab: Erstens, die Erhebung der aktuellen Rahmenbedingungen, wie bspw. gesetzliche Anforderungen, die auch von einer bundeseinheitlichen Justizcloud erfüllt werden müssten. Zweitens, die Analyse von Stärken bestehender Cloud-Angebote der IT-Dienstleister, wie bspw. Infrastruktur oder Kompetenzen, welche die Justizcloud ggf. nachnutzen kann. Und drittens, die Identifikation von Herausforderungen, da diese im Rahmen der Konzeption der Justizcloud adressiert werden müssen. Dabei sind rechtlich-organisatorische, fachliche und technische Themen zu bewerten.

Rechtlich-organisatorisch sind neben den gesetzlichen Rahmenbedingungen bspw. die bestehende Organisation und „Kundenbetreuung“ der Justiz bei IT-Dienstleistern sowie etwaige Kontrahierungszwänge relevant. Zudem hat die Justiz als dritte Gewalt besondere Anforderungen an ihre Unabhängigkeit, die auch im IT-Bereich und damit für die Ausgestaltung einer Justizcloud berücksichtigt werden müssen (z. B. etwaig bestehende IT-Kontrollkommissionen). Abschließend ist auch relevant, ob der IT-Dienstleister unter der Dienstaufsicht der Justiz oder der Verwaltung steht.

Fachliche Aspekte, wie u. a. die jeweilige Wertschöpfungstiefe der IT-Dienstleister, sind relevant, da hierdurch bspw. abgeleitet werden kann, ob moderne Formen der Zusammenarbeit bzw. Verfahren der Softwareentwicklung (z. B. DevOps, CI/CD) bereits etabliert oder möglich sind. Auch die Rolle externer kommerzieller IT-Dienstleister und der Bedarf, diese im Cloud-Konzept zu berücksichtigen, kann hier analysiert werden.

Technisch ist zum einen die aktuell genutzte technische Basis, wie bspw. Rechenzentren, Netze aber auch Cloud-Plattformen und -Produkte, interessant, sofern bereits entsprechende Cloud-Umgebungen vorhanden sind. Zum anderen sind die existierenden Cloud-Strategien, -Kompetenzen und -Services von Interesse. So kann abgeleitet werden, welche Cloud-Erfahrungen und -Fähigkeiten bereits etabliert sind. Sollten bspw. bereits sehr gereifte Services oder Standards existieren, können diese so identifiziert und ggf. nachgenutzt bzw. durch die Justizcloud bundeseinheitlich bereitgestellt werden.

Vorgehen

Für die Erhebung der Informationen wurde ein standardisierter Fragebogen entwickelt, der detaillierte Informationen zu den rechtlich-organisatorischen, fachlichen und technischen Bereichen abfragt (vgl. **Kapitel 7.2**). Der Fragebogen war in die drei Abschnitte (1) Justiz als Kunde, (2) Cloud-Strategie sowie (3) organisatorischer Rahmen eingeteilt.

Die Erhebung der Informationen erfolgte im Rahmen von Experten mit Vertretern der jeweiligen IT-Dienstleister. Im Fokus standen dabei 13 IT-Dienstleister, welche die Justizvertreter servizieren und auch im Sounding Board vertreten waren. Darüber hinaus wurden die IT-Stellen von zwei Bundesgerichten (*BAG*, *BFH*) und dem *BVerfG* befragt. Einige Gespräche wurden dabei in mehreren Iterationen geführt. Die ausgefüllten Fragebögen wurden den Gesprächspartner anschließend zur Prüfung vorgelegt. Zur Vertiefung der technischen Aspekte rund um virtuelle Infrastruktur und Cloud-/ Container-Cluster sowie Netze, wurde zudem eine zusätzliche schriftliche Abfrage der IT-Dienstleister durchgeführt. Zusätzlich wurden die bestehenden NdB-Netzanschlüsse (Verbindungsnetz) und Bandbreiten der jeweiligen IT-Dienstleister zusammen mit dem *BMI* und der *BDBOS* erhoben.

E-Justice-Struktur und Übersicht der IT-Dienstleister der Justiz

In der Justiz sind Strukturen für die Governance der Justiz-IT etabliert. Der *E-Justice-Rat* (*EJR*) ist in diesem Kontext das oberste Gremium. Er trifft grundlegende Entscheidungen bspw. zu IT-Projekten oder übergreifenden Fragen der Informationstechnik, legt Standards fest und befasst sich mit Zukunftsthemen (z. B. Entwicklung der modernen Fachverfahren *GeFa* und *AuRegis*, *Justizcloud*). Zum anderen stellt der *E-Justice-Rat* auch die Mitwirkung

der Justiz im *IT-Planungsrat* sicher und ist dadurch auch an der verwaltungsübergreifenden IT-Governance beteiligt. Mitglieder sind alle Länder und der Bund, die durch die Amtschefinnen und Amtschefs bzw. die Staatssekretärinnen und Staatssekretäre vertreten werden.

Zur Unterstützung des *E-Justice-Rats* sowie der Vorbereitung und Umsetzung seiner Entscheidungen wurde die *Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK)* als ständige Arbeitsgruppe eingerichtet. Ihr gehören die Justizverwaltungen von Bund und Ländern an. Zur Wahrnehmung ihrer Aufgaben organisiert sich die *BLK* in Arbeitsgruppen und Themenkreisen. Die Umsetzung der erarbeiteten gemeinsamen Positionen und Lösungen obliegt anschließend den Justizverwaltungen und ihren jeweiligen IT-Dienstleistern. Darüber hinaus befasst sich auf übergeordneter Ebene auch die *BLK* in verschiedenen Arbeitsgruppen sowie dem *BLK-Architekturbüro* mit Innovationen, Zukunftsthemen und abgeleiteten Weiterentwicklungsbedarfen für die Justiz-IT und ihren Betrieb.

Die Ist-Analyse hat ergeben, dass der Betrieb der Justiz-IT von über 20 IT-Dienstleistern, Unterdienstleistern oder eigenen Justizabteilungen wahrgenommen wird (vgl. **Tabelle 5**).

Tabelle 5 | Übersicht aller durch die Justiz genutzten öffentlichen IT-Dienstleister

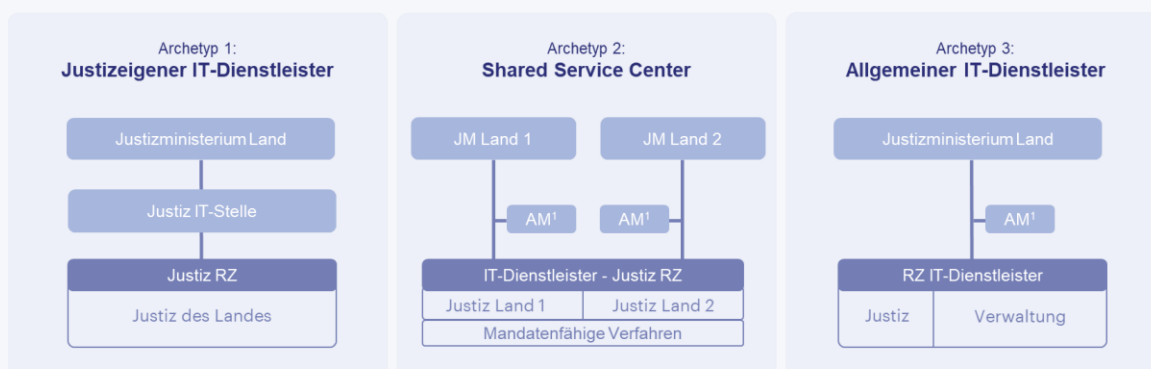
Land	IT-Dienstleister	Archetyp
Baden-Württemberg (BW)	BITBW, IuK Fachzentrum am OLG Stuttgart	3
Bayern (BY)	Jus-IT beim Justizministerium, RZ Nord, IT-DLZ, Arbeitsplatz bei kommerziellem Anbieter	3
Berlin (BE)	ITDZ Berlin	3
Brandenburg (BB)	ZenIT	1
Bremen (HB)	Dataport	2
Hamburg (HH)	Dataport	2
Hessen (HE)	HZD	3
Mecklenburg-Vorpommern (MV)	DVZ M-V	3
Niedersachsen (NI)	ZIB im Justizministerium, Netz bei IT.N	1
Nordrhein-Westfalen (NW)	ITD beim Justizministerium, IT.NRW	1 bzw. 3
Rheinland-Pfalz (RP)	LDI, IT-Stelle im Justizministerium	3
Saarland (SL)	IT-Referat im Justizministerium	1
Sachsen (SN)	LIT, Netz bei SID	1
Sachsen-Anhalt (ST)	Dataport	2
Schleswig-Holstein (SH)	Dataport	2
Thüringen (TH)	TLRZ	3
Bundesarbeitsgericht (BAG)	Eigene interne IT-Einheit	1
Bundesfinanzhof (BFH)	Eigene interne IT-Einheit	1
Bundesgerichtshof (BGH)	Eigene interne IT-Einheit	1

Land	IT-Dienstleister	Archetyp
Bundespatentgericht	Eigene interne IT-Einheit	1
Bundessozialgericht	Eigene interne IT-Einheit	1
Bundesverfassungsgericht	Eigene interne IT-Einheit	1
Bundesverwaltungsgericht	Eigene interne IT-Einheit	1

Basierend auf ihrem organisatorischen Zusammenspiel mit der Justiz lassen sich die IT-Dienstleister in drei Archetypen unterteilen (vgl.).

- **Archetyp 1** sind **justizeigene IT-Dienstleister**, die der jeweiligen Justiz direkt zugeordnet sind und über die Justizverwaltungen oder Justiz-IT-Stellen von der Justiz beauftragt und gesteuert werden, d. h. unter Dienstaufsicht der Justiz stehen. Diese Dienstleister bzw. Stellen bedienen ausschließlich die Justiz.
- **Archetyp 2** wird als **Shared Service Center** bezeichnet. Dabei bedient ein IT-Dienstleister unabhängig voneinander die Justizressorts mehrerer Länder und bietet getrennt davon auch Dienstleistungen für weitere Teile der Verwaltung an. Die Beauftragung, Steuerung und Kontrolle erfolgt durch ein Auslagerungsmanagement der IT-Stellen in den Justizministerien bzw. die IT-Kontrollkommissionen der Länder.
- **Archetyp 3** sind **allgemeine IT-Dienstleister** der Verwaltung. Diese bedienen parallel alle bzw. mehrere Ressorts der Verwaltung und der Justiz eines Landes ohne eine wesentliche Spezialisierung. Ebenso wie beim Archetyp 2 erfolgt die Beauftragung, Steuerung und Kontrolle durch das Auftrags- bzw. Auslagerungsmanagement der IT-Stellen der Justizministerien bzw. die IT-Kontrollkommission des jeweiligen Landes.

Abbildung 11 | Übersicht der IT-Dienstleister-Archetypen



¹AM = Auslagerungsmanagement und Kontrollfunktion

Von den über 20 öffentlichen IT-Dienstleistern der Justiz fokussieren sich 14 in ihrer Tätigkeit auf ihr jeweiliges Land bzw. Bundesgericht. Der Großteil der Justiz greift somit nur auf Leistungen eines IT-Dienstleisters zurück. Ausnahmen hiervon stellen bspw. Nordrhein-Westfalen und Bayern dar, deren Justiz-IT von mehreren IT-Dienstleistern betrieben wird. Eine weitere Ausnahme stellt *Dataport AöR* dar, da dieser als einziger IT-Dienstleister des Archetyps 2 die Justizressorts von vier Ländern individuell versorgt. Justizeigene IT-Dienstleister (Archetyp 1) gibt es in insgesamt fünf Ländern und bei allen Bundesgerichten.

Am häufigsten finden sich allgemeine IT-Dienstleister des Archetyps 3. Insgesamt acht Länder lassen sich diesem Archetyp zuordnen. Diese IT-Dienstleister richten ihr Angebot an alle Ressorts. Dies kann dazu führen, dass die Justiz Entscheidungen des IT-Dienstleisters mitträgt und ggf. querfinanzieren muss, die von anderen Ressorts getrieben wurden, ihre Anforderungen aber ggf. weniger passgenau erfüllen.

Die rechtlich-organisatorische Ausgestaltung bzw. Grundlage der IT-Dienstleister ist sehr unterschiedlich. Dies zeigt sich zum einen in der gewählten Rechtsform. Diese reichen von der Anstalt öffentlichen Rechts bis zu Landesbetrieben nach der jeweiligen Landeshausordnung. Entsprechend variiert die rechtliche Grundlage, auf deren Basis die IT-Dienstleister gegründet wurden und die den Auftrag und die Struktur vorgeben. Sie reichen von Errichtungs- oder Runderlässen über förmliche Gesetze bis hin zu Staatsverträgen. Weitere Rahmenbedingungen folgen aus den E-Government-Gesetzen der Länder sowie teilweise bestehenden Justiz-IT-Gesetzen.

Die Ist-Analyse hat hier insb. zwei wesentliche Besonderheiten für die Justiz identifiziert, die für eine bundeseinheitliche Justizcloud relevant sind:

- **Kontrahierungszwänge** sind (unter-)gesetzliche Regelungen, welche die Landesjustiz dazu verpflichten, Leistungen des jeweiligen IT-Dienstleisters abzunehmen bzw. diesen für den Betrieb von Anwendungen zu beauftragen. Vom Kontrahierungszwang sind in einigen Ländern jeweils Ausnahmen vorgesehen. Zum einen, wenn der IT-Dienstleister die benötigte Leistung nicht anbieten bzw. beschaffen kann und zum anderen, wenn ein alternativer Leistungsbezug bspw. durch ein gemeinsames bundeseinheitliches Vorgehen deutliche Effizienzvorteile aufweist. Im Rahmen der Ist-Analyse konnten Kontrahierungszwänge in knapp einem Drittel der Länder identifiziert werden. Inwiefern eine bundeseinheitliche Justizcloud mit einem bestehenden Kontrahierungszwang konfliktieren würde bzw. ob in diesem Fall ein Ausnahmetatbestand erfüllt oder sogar Änderungsbedarf an den (unter-)gesetzlichen Bestimmungen

besteht, muss von den jeweiligen Ländern selbst rechtlich bewertet und entschieden werden.

- **IT-Kontrollkommissionen** vertreten die Interessen der Judikative gegenüber den IT-Dienstleistern und stellen sicher, dass die besonderen Belange der Justiz (insbesondere die richterliche Unabhängigkeit) berücksichtigt und geschützt werden. Dies erfolgt regelmäßig vor allem im Wege einer geteilten Fachaufsicht des Justizministers bzw. der -ministerin und des für den IT-Dienstleister federführenden Ressorts für die in richterlicher, rechtspflegerischer oder staatsanwaltlicher Tätigkeit erstellten Dokumente. Ihnen werden dabei zum Teil umfassende Auskunfts-, Prüfungs- und Zugangsrechte bezüglich des Betriebs der Justiz-IT eingeräumt. Im Rahmen der Ist-Analyse konnten etablierte IT-Kontrollkommissionen in insgesamt zehn Ländern identifiziert werden. Die Einbindung der bestehenden IT-Kontrollkommissionen ist dabei auch für die Konzeption einer Justizcloud relevant und muss im Rahmen der Zielbildentwicklung berücksichtigt werden (vgl. **Kapitel 3.6**).

Trotz der Landesgrenzen ist hervorzuheben, dass verschiedene Austausch- und Zusammenarbeitsformate der öffentlichen IT-Dienstleister existieren. Neben den Entwicklungsverbünden (vgl. **Kapitel 2.2.1**), in denen einige IT-Dienstleister gemeinsam an der Entwicklung von Justizanwendungen mitwirken, sind hier insbesondere die Initiative *Deutsche VerwaltungscLOUD (DVC)* im Kontext der *FITKO* sowie die Genossenschaft *govdigital eG* zu nennen. Im Rahmen der *DVC* existiert dabei eine umfangreiche Kollaboration der IT-Dienstleister mit dem Ziel, gemeinsame Bund-Länder-übergreifende Standards (z. B. Container- oder Netzstandards) und Synergien für Cloud-Lösungen (z. B. Cloud-Services Marktplatz) zu schaffen. Das Thema Cloud steht auch bei der *govdigital eG* im Fokus. Als Mitglieder der *govdigital eG* tauschen sich die IT-Dienstleister über Potenziale von Technologien (z. B. Security, KI und Cloud) für die öffentliche Verwaltung aus und erarbeiten gemeinsame bundesweite technische und organisatorische Lösungen wie bspw. ein gespanntes Kubernetes-Cluster oder Strukturen zur standardisierten Beschaffung von kommerziellen Cloud-Diensten (sog. Cloud-Broker). Darüber hinaus existieren bspw. mit Mitgliederversammlungen, Betriebsleitertreffen, Leitertagungen der Rechenzentren oder Fachanwendungsarbeitskreisen weitere formelle und informelle Austausche, sowohl auf Leitungs- als auch auf Arbeitsebene.

Wesentliche Erkenntnisse zum Leistungsspektrum der IT-Dienstleister

Typischerweise reicht das Leistungsspektrum eines IT-Dienstleisters von der initialen Beratung und Anforderungsanalyse über die Anwendungsentwicklung und -integration sowie

dem Infrastruktur- und Plattformbetrieb bis hin zum technischen und fachlichen Anwendungsbetrieb sowie der kontinuierlichen Weiterentwicklung und Optimierung der IT-Umgebung. In der Justiz liegt der Fokus der IT-Dienstleister vor allem auf dem Betrieb, auch wenn sich das Leistungsspektrum der IT-Dienstleister im Einzelnen unterscheidet.

Für die Anforderungsaufnahme und Beratung der Justiz existieren bei nahezu allen IT-Dienstleistern entsprechende Strukturen. Justizfokussierte Teams, Servicebündel, (Key) Account Managements uvm. sind etabliert oder befinden sich im Aufbau.

Entwicklungsleistungen für Justizsoftware werden hingegen nur in einzelnen Fällen, bspw. im e2-Verbund oder zum Teil von justizeigenen IT-Dienstleistern, erbracht. Der Großteil der Justizanwendungen wird im Rahmen der Entwicklungsverbünde, also dem Zusammenschluss mehrerer Länder zum Zwecke der gemeinsamen Anforderungserhebung und Entwicklung von Justizsoftware, durchgeführt (vgl. **Kapitel 2.2.1**). Die Entwicklung der Software erfolgt dabei meist durch vom Entwicklungsverbund beauftragte externe kommerzielle und auf Justizsoftware spezialisierte Dienstleister.

Der Fokus der IT-Dienstleister liegt auf dem Betrieb dieser zentral erstellten Software auf eigener Infrastruktur. Im Infrastrukturbetrieb steht die Bereitstellung, Verwaltung und Wartung der physischen und virtuellen IT-Infrastruktur, wie bspw. Server, Netzwerke oder Speicherlösungen, im Fokus. Im Plattformbetrieb stellen IT-Dienstleister bspw. Arbeitsplatz, Kommunikations-, Datenbank-, Virtualisierungs- oder Container-Plattformen bereit. Auf Anwendungsebene übernehmen die IT-Dienstleister zudem den technischen Betrieb der Komponenten der Justizanwendungslandschaft und sorgen dafür, dass die jeweiligen Anwendungen eingeführt sowie störungsfrei, stabil und performant betrieben und gepflegt werden können. Dies erfolgt jedoch nicht in allen Ländern für alle Anwendungen, da teilweise bestimmte Betriebsleistungen auch an unterbeauftragte IT-Dienstleister ausgelagert werden.

Der fachliche Anwendungsbetrieb, also die Sicherstellung der korrekten fachlichen Nutzung der Anwendungen (bspw. durch Anwender-Support oder Schulungen), die (Vor-)Analyse und Priorisierung von Problemen sowie die Identifikation von Änderungsbedarfen wird größtenteils nicht durch die IT-Dienstleister wahrgenommen. Diese Aufgaben werden vor allem von der Fachseite in den Justizministerien oder Gerichten, den IT-Stellen oder Fachpflegestellen übernommen und bei Bedarf mit den Entwicklungsverbünden abgestimmt.

Wesentliche Erkenntnisse zu Entwicklung und Betrieb

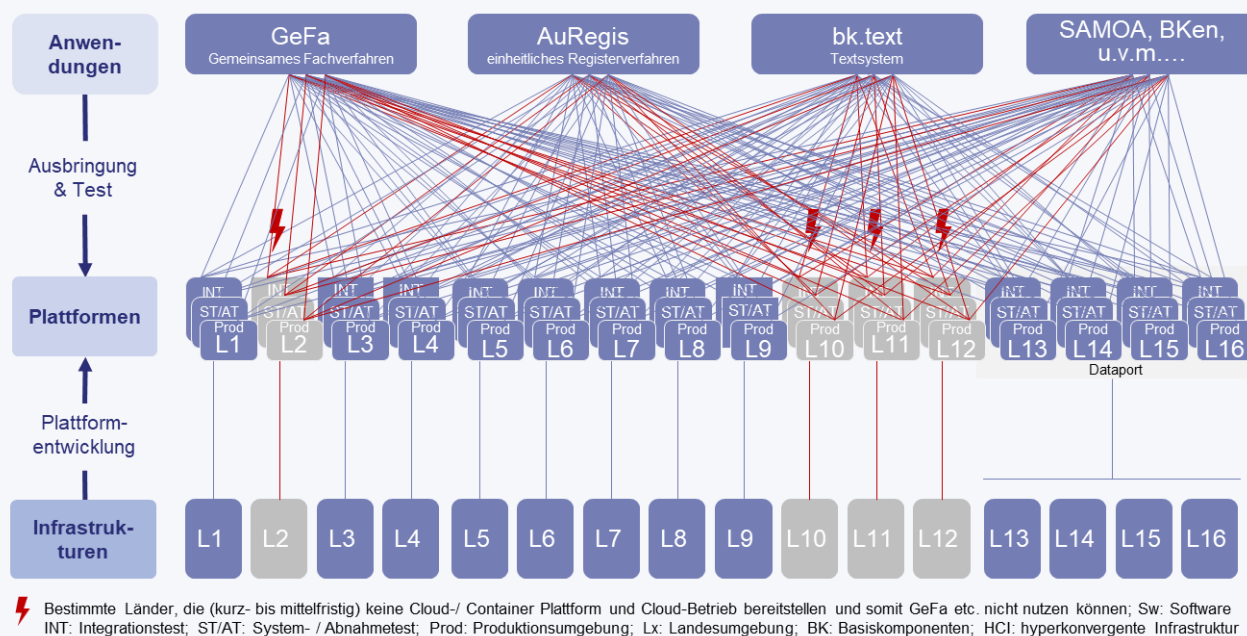
Das Leistungsspektrum der meisten IT-Dienstleister umfasst keine Anwendungsentwicklungsleistungen. Lediglich sechs IT-Dienstleister (davon zwei Bundesgerichte) gaben an,

Anwendungen der Justiz zum Teil auch selbst zu entwickeln. Die meisten Anwendungen der Justiz werden in sog. Entwicklungsverbünden entwickelt. Die Distanz zwischen einheitlicher Entwicklung und länderspezifischem Betrieb erschwert per Definition den Informationsaustausch und ist insbesondere für Einführung und Betrieb dieser Anwendungen sehr komplex. Für IT-Dienstleister sind oftmals die Anforderungen an den Betrieb von neuen Anwendungen lange unklar, was auch zu Verzögerungen bei der Integration der Anwendungen bzw. neuer Versionen davon sowie deren Aufnahme in den Betrieb führen kann.

Es verwundert daher nicht, dass viele IT-Dienstleister als Herausforderung die mangelnde Qualität zugelieferter Software benannt haben, welche die Bedarfe des IT-Betriebs wenig berücksichtigt. Dies führt immer wieder zu Problemen in den Teststufen vor der Ausbringung, aber auch im laufenden produktiven Betrieb (bspw. durch Stabilitäts- und Performanzprobleme) und zieht zum Teil umfassende Nacharbeiten bzw. Anpassungen an der Software nach sich. Hierdurch verzögert sich die Ausbringung neuer Anwendungen oder mehrere Versionen der Anwendung müssen vorgehalten werden, was zu höheren Kosten für Entwicklung und IT-Betrieb führt.

Problematisch sind vor allem die heterogenen Betriebsorganisationen, Infrastrukturen (z. B. Netze) und Plattformen (z. B. landesspezifische Datenbanktechnologien und Container-Plattformen) der IT-Dienstleister. Die Entwicklungsverbünde können die Heterogenität der Betriebsumgebungen nicht vollumfassend, z. B. mit Referenzumgebungen, nachbilden. Die Software kann daher im Rahmen der Entwicklung oftmals nicht ausreichend integriert und getestet werden, was in der Konsequenz zu vielen der genannten Qualitätsproblemen führt. Zudem ist grundsätzlich die Ausbringung von einheitlich entwickelten Anwendungen in bis zu 16 heterogene IT-Dienstleisterumgebungen und jeweils mindestens drei Umgebungen (vgl. **Abbildung 12**) eine komplexe Herausforderung, ressourcenaufwändig sowie fehleranfällig und teuer (vgl. **Kapitel 2.2.1.1**). Aufgrund der langen Ausbringungszeiten und Integrationsaufwände setzten viele Länder/ IT-Dienstleister regelmäßig Software-Releases aus. Zudem erhalten in diesem Konstrukt die Entwicklungsverbünde nur stark verzögert technisches und fachliches Feedback zu ihren Anwendungen. Zum Teil erfolgt das Feedback erst nach Monaten, obwohl die Entwickler bereits seit vielen Zyklen an anderen Weiterentwicklungen arbeiten. Damit müssen verschiedene Versionen vorgehalten werden und ein nutzendenzentriertes Arbeiten ist kaum möglich.

Abbildung 12 | Ausbringungskomplexität einheitlicher Software auf heterogene Umgebungen



Wesentliche Erkenntnisse zu Cloud-Fähigkeiten der IT-Dienstleister

Auch wenn Cloud für die IT-Dienstleister der Justiz kein neues Thema ist, unterscheiden sich die Cloud-Erfahrung und -Fähigkeiten der IT-Dienstleister deutlich. Ein Teil der IT-Dienstleister richtet sich bereits nach bestehenden Cloud-Strategien aus und plant oder investiert in den Aufbau von dedizierten Cloud-Einheiten sowie Cloud-Umgebungen, während einige wenige IT-Dienstleister noch ganz am Anfang ihres Weges in die Cloud stehen oder noch nicht damit begonnen haben.

Sechs Länder bzw. IT-Dienstleister verfügen bereits über schriftliche Cloud-Strategien, während drei weitere diese gerade erarbeiten. Teilweise handelt es sich dabei um Konzepte, die eine landesweite Geltung haben, da sie v. a. durch die allgemeinen IT-Dienstleister (Archetyp 3) der jeweiligen Länder ausgearbeitet wurden. Sie nehmen somit nicht spezifisch die Cloud-Bedarfe der Justiz in den Fokus, sondern versuchen, alle Teile der Verwaltung zu bedienen. Lediglich in zwei Fällen bestehen justizspezifische Cloud-Strategien, die durch das Justizministerium bzw. den justizeigenen IT-Dienstleister (Archetyp 1) erstellt wurden.

Bei der inhaltlichen Ausgestaltung der Cloud-Strategien werden ebenfalls unterschiedliche Wege gegangen. In drei Strategien wird eine Hybrid Cloud-Strategie und in weiteren drei eine Multi Cloud-Strategie unter expliziter Einbindung von Public Cloud-Angeboten wie *IONOS*, *Microsoft Azure* oder *Oracle* verfolgt. Ein IT-Dienstleister rückt seine Private Cloud-Angebote mit *DVC*-Standards zur Nachnutzung von Diensten dritter öffentlicher

Dienstleister in den Fokus. Ein weiterer IT-Dienstleister möchte sich selbst als Cloud-Broker positionieren und damit verschiedene private und kommerzielle (Public) Cloud-Angebote vermitteln, anstatt diese selbst aufzubauen.

Insgesamt fünf IT-Dienstleister gaben an, bereits spezifische Cloud-Einheiten bzw. Kompetenzzentren etabliert zu haben. Weitere zwei verweisen auf entsprechende Aufbauaktivitäten bzw. Planungen. Dabei weichen Aufbau und Aufgaben bzw. der Fokus dieser Einheiten z. T. stark voneinander ab. Cloud-Einheiten werden bspw. als Arbeitsgemeinschaften, in Programmorganisationen, als Stabstellen oder innerhalb von Abteilungsstrukturen ausgeübt. Einige schienen noch eher temporären Charakter zu haben und sind z. B. mit der Umsetzung der Cloud-Transformation beim IT-Dienstleister betraut. Andere sind bereits als dauerhafter Bestandteil der Organisation im Organigramm zu finden, um alle Cloud-Themen zu bündeln bzw. zu verantworten. Die im Aufbau befindlichen Einheiten wurden demgegenüber in den Gesprächen oft zunächst als Cloud-Kompetenzzentren charakterisiert, um zunächst das entsprechende Know-how zu bündeln bzw. aufzubauen.

Als wesentliche Herausforderungen für den Aufbau von Cloud-Know-how wurde neben der oft angespannten Haushaltslage vor allem der (IT-)Fachkräftemangel benannt sowie qualifiziertes Personal zu finden und anwerben zu können. Viele IT-Dienstleister setzen daher verstärkt auf Schulung und Weiterbildung ihres Bestandspersonals, um auf diesem Weg intern Experten zu entwickeln. Dabei beeinflussen diese Faktoren die Geschwindigkeit des Aufbaus und der Etablierung entsprechender Einheiten maßgeblich.

Für die notwendigen Veränderungen, die sich bei einer Entwicklung hin zu Cloud bspw. durch neue Formen der Zusammenarbeit (DevOps), einen veränderten Verantwortungsschnitt beim Betrieb von Cloud-Plattformen und Cloud-nativen Anwendungen oder die Nutzung neuer Werkzeuge ergeben, sind Akzeptanz und Entwicklungsbereitschaft der Beschäftigten essenziell. Dies betrifft insb. die Beschäftigten, die nicht Teil der Cloud-Einheiten sind. Neue Prozesse, Fähigkeiten und Ansprüche können jedoch auch zu Vorbehalten führen. Einige IT-Dienstleister sehen neben den technischen und fachlichen Herausforderungen zum Teil auch organisatorische bzw. kulturelle Widerstände auf dem Weg in die Cloud.

Bei den konkreten Cloud-Angeboten und -Initiativen zeigt sich ein ähnlich heterogenes Bild. Sieben IT-Dienstleister gaben an, der Justiz in gewissem Rahmen bereits Cloud-Angebote zur Verfügung zu stellen bzw. bereitstellen zu wollen, sobald die Nachfrage entsteht. Eine wesentliche Erkenntnis ist nämlich, dass bislang Cloud-Anforderungen vor allem vom Rest der Verwaltung bekannt sind (z. B. Polizei), aber die Justiz noch wenig Bedarf gezeigt hat.

Eine Cloud-Strategie der deutschen Justiz gibt es bis dato noch nicht und die Cloud-nativen Anwendungen der Justiz (z. B. *GeFa* und *AuRegis*) befinden sich noch in der Entwicklung bzw. in erster Pilotierung, d. h. sind noch nicht im bundesweiten Wirkbetrieb angekommen.

Die Cloud-Angebote von zwei IT-Dienstleistern befinden sich aktuell noch im Aufbau. Das konkrete Angebot unterscheidet sich jedoch zwischen den Organisationen erheblich. Fünf der sieben Cloud-Angebote beziehen sich jeweils nur auf eine Cloud-Ebene und umfassen entweder nur IaaS-, PaaS- oder die Nachnutzung von SaaS-Diensten. Ein IT-Dienstleister gibt an, nur IaaS- und PaaS-Services zur Verfügung zu stellen und nur ein IT-Dienstleister bietet Services auf allen drei Ebenen an. Alle IT-Dienstleister mit Cloud-Angeboten befinden sich aber aktuell in der Entwicklung, ihre Angebote auszuweiten. Ein kleiner Teil der IT-Dienstleister gab an, aktuell Bestell- bzw. Cloud-Serviceportale aufzubauen, die auch eine automatisierte Bestellung ermöglichen, wie man es von kommerziellen Cloud-Anbietern kennt. Durch die Vernetzung der meisten IT-Dienstleister im Kontext der *DVC* sowie der *govdigital eG* entstehen dabei bereits erste nachnutzbare, wenn auch nicht justizspezifische bzw. für die Justiz passgenaue Cloud-Service-Angebote wie bspw. Terminfinder oder gespannter Kubernetes-Cluster für Kommunen (vgl. **Kapitel 2.2.3**).

Der Bedarf für Zusammenarbeit ist groß, denn um Cloud-Anwendungen betreiben zu können, müssen IT-Dienstleister in eigene (Private) oder souveräne kommerzielle Cloud-Umgebungen, mit modernen Container-, Daten- und Integrationsplattformen investieren und diese betreiben. Dafür müssen zum Teil noch physische Infrastruktur virtualisiert (als Grundlage für IaaS), neue Netzwerksegmente geschaffen (sog. Microsegmentierung etabliert), die Monitoring- und Sicherheitsinfrastruktur ausgebaut sowie entsprechende Plattformen und Plattformteams aufgebaut werden. Dies ist vor allem vor dem Hintergrund des geschilderten (IT-)Fachkräftemangels sowie durch die hohen Investitionskosten eine immense Herausforderung für viele IT-Dienstleister.

Durch die wenig standardisierten und orchestrierten Anforderungen der föderalen Verwaltung und Justiz sowie durch die föderale Beschaffungspolitik ist ähnlich wie bei den klassischen IT-Umgebungen auch bei der Ausgestaltung der neuen Cloud-Umgebungen ein Aufwuchs heterogener Landschaften und Plattformen zu beobachten.

Beginnend bei den unterschiedlichen Cloud-Strategien und den unterschiedlich ausgeprägten Cloud-Einheiten, sind auch die Cloud-Angebote, -Umgebungen und -Produkte entsprechend heterogen. Eine Vielzahl unterschiedlicher Virtualisierungs- und Container-Plattform- (CaaS) sowie Cloud-Management-Produkten wird eingesetzt. Auf

diese Weise entstehen unterschiedliche Clouds mit unterschiedlicher Ausrichtung, unterschiedlicher Organisation und wenig Synergien. Gemeinsam entwickelte Software muss so jeweils an die lokalen Cloud-Gegebenheiten angepasst werden, was zu steigender Komplexität, hohen Testaufwänden sowie Kosten für die Justiz führt. Ein gemeinsamer Betrieb der gemeinsam entwickelten Anwendungen und damit das Heben eines der wesentlichen Effizienzpotenziale für die Justiz ist auf diese Weise nicht möglich.

Um die Vorteile von Cloud umfassend nutzen zu können und Effizienzgewinne, Kosteneinsparungen sowie einen einheitlichen Zugang zu Cloud zu schaffen, wären Festlegungen zur Standardisierung der eingesetzten Technologien und Produkte sowie zur Vernetzung der individuellen Cloud-Umgebungen in einer gemeinsamen Cloud-Strategie für die Justiz ideal. Dabei hat eine Analyse des *BMI* mit der *BDBOS* gezeigt, dass auch auf Ebene der Landesnetze (insb. eingesetzter Layer 3 Gateways und Firewalls) sowie der physischen Netze und Carrier eine hohe Heterogenität herrscht. Auch beim *Verbindungsnetz* (VN), das nach dem *IT-NetzG* zur länderübergreifenden Kommunikation genutzt wird (z. B. für Video- und E-Mail-Kommunikation), besteht ein sehr heterogenes, historisch gewachsenes Bild. Denn die Netzanschlüsse sind stark unterdimensioniert.

Die bundeseinheitliche Justizcloud könnte einen wesentlichen Beitrag zur Harmonisierung der Cloud-Landschaft für die Justiz und deren Entwicklungsverbünde leisten. Aber auch die Netzanschlüsse der Länder zu einer bundeseinheitlichen Justizcloud wären demnach zu adressieren.

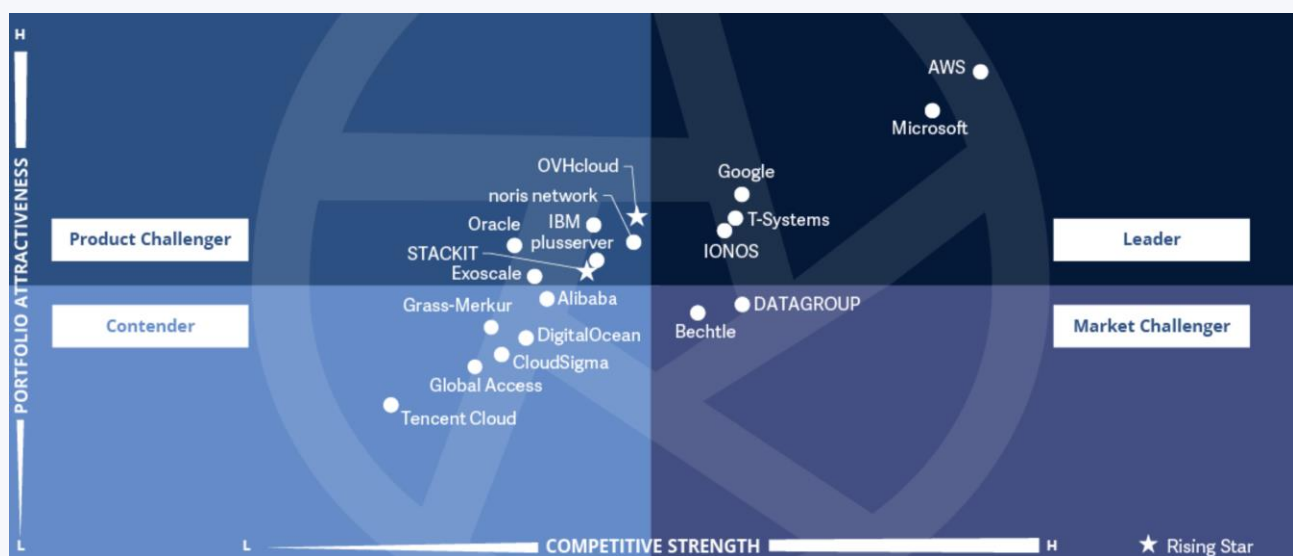
2.2.3 Relevante Cloud-Initiativen

Wie die Justiz, prüfen auch andere Organisationen der öffentlichen Verwaltung (z. B. Polizei, Steuerverwaltung, Bildung) seit einigen Jahren die Nutzung von Cloud. Einige haben bereits Strategien zur Cloud-Nutzung entwickelt oder befinden sich schon in der Umsetzung. Der öffentliche Sektor hat dabei besondere fachliche, technische und rechtlich-organisatorische Anforderungen. Besonders wichtig ist die Sicherstellung digitaler Souveränität bspw. durch die Wahrung der Unabhängigkeit gegenüber privaten Anbietern bzw. einer Wechselfähigkeit sowie die Sicherstellung der Kontrolle über die IT-Infrastruktur und insb. der verarbeiteten Daten. Daneben bestehen besondere technische Herausforderungen, wie z. B. die Nutzung besonders abgesicherter Netze, Integration eigener Zertifikats- und Netzstrukturen, aber auch die Zugänglichkeit durch multiple, heterogene Länderbetriebe und deren Umgebungen sowie organisatorische Besonderheiten wie bspw. bestehende Kontrahierungszwänge.

Für die besonderen Bedarfe der Verwaltung hat sich dabei ein breites Spektrum an Cloud-Lösungen herausgebildet. Einerseits arbeiten viele öffentliche IT-Dienstleister bereits am Aufbau spezieller behördlicher, d. h. privater Cloud-Angebote, wie z. B. das *ITZBund* oder diverse Landes-IT-Dienstleister.

Aber auch viele kommerzielle Anbieter, allen voran die sog. Hyperscaler wie *Azure*, *AWS*, *Google Cloud* und *Oracle* sowie nationale Anbieter wie *Telekom*, *Ionos*, *StackIT* oder *OVHcloud* haben spezielle Cloud-Modelle entwickelt, die für die besonderen Souveränitätsanforderungen des öffentlichen Sektors angepasst sind.

Abbildung 13 | Übersicht in Deutschland führender kommerzieller Cloud-Angebote



Quelle: [ISG Provider Lens 2023](#)

Hinzu kommen Initiativen und Projekte, die Konzepte für den öffentlichen Sektor entwickeln und die Kollaboration und Kooperation zwischen Behörden fördern, um die Cloud-Nutzung und die damit verbundenen Vorteile systematisch zu erschließen. Diesbezüglich seien insbesondere die *Deutsche Verwaltungscld-Strategie (DVS)* im Kontext der *FITKO* als auch die *govdigital eG* genannt. Auf EU-Ebene gilt z. B. die *Gaia-X-Initiative* als solcher Standard-setzer. Viele dieser Angebote adressieren die besonderen Anforderungen der öffentlichen Verwaltung und somit auch der Justiz. Deshalb ist es wichtig und notwendig, diese Angebote zu prüfen und für die Phase der Zielbildentwicklung bzgl. ihres Nachnutzungspotenzials für die Justiz und die Justizcloud einzuwerten. Dabei gilt es zu beachten, dass die Justiz eigene

Anforderungen hat, die eine „einfache“ Nachnutzung von Angeboten der Verwaltung einschränken.

Tabelle 6 | Besondere bundesweite Cloud-Initiativen

Typ	Cloud-Initiative bzw. Angebot	Grobe Beschreibung
Koordinierungs-initiativen	Deutsche Verwaltungscloud-Strategie (DVS, DVC)	Koordination und Schaffung bund-länder-übergreifender Standards (z. B. für Container und Identity Broker) und Schnittstellen für Cloud-Lösungen (z. B. Cloud-Marktplatz) sowie die Förderung einer Multi Cloud-Infrastruktur von IT-Dienstleistern für IT-Dienstleister aus Bund und Ländern. Die DVC ist bzw. durch die DVC entsteht keine Cloud im eigentlichen Sinne, sondern das Ziel ist, dass multiple Clouds bei den IT-Dienstleistern entstehen, die durch Standards interoperabel sein sollen.
	govdigital eG	Bundesweit ausgerichtete Genossenschaft öffentlicher IT-Dienstleister, um sichere und zuverlässige digitale Infrastrukturen und Dienste insbes. auch mit Fokus auf Cloud für die Anforderungen der Verwaltung und Kommunen bereitzustellen und deren Nachnutzung zu erleichtern. Dafür bietet die govdigital eG sowohl eigene Dienste, als auch projektbegleitende Unterstützung, sie fördert den Austausch zwischen IT-Dienstleistern und bietet ihnen flexible vertragliche Konstrukte und Rahmenverträge, um (Cloud-)Projekte gemeinsam und damit synergetisch anzugehen. Sämtliche Landesbehörden können Dienstleistungen von der govdigital eG als Kunden beziehen. Dienstleister sind dabei die Mitglieder der govdigital eG sowie ausgewählte externe Dienstleister.
Private Cloud-Angebote	Bundescloud des ITZBund	Umsetzung der Hybrid Cloud-Strategie des Bundesfinanzministeriums, durch den Aufbau einer Private Cloud im ITZBund (Fokus IaaS) mit einem Cloud-Management-System, welches auch angeschlossene kommerzielle Public Cloud-Angebote für Bundesbehörden zugänglich macht.
	Delos GmbH	Aufbau einer sog. Third Party Private Cloud, also einer im Auftrag der öffentlichen Verwaltung von SAP (Delos als Tochter von SAP) betriebenen souveränen Cloud auf nationaler Infrastruktur, um vor allem das Microsoft Office M365 Angebot weiterhin der öffentlichen Verwaltung zugänglich zu machen, da sich dieses künftig nur noch als Cloud-Dienst aus der Microsoft-Cloud (Azure) beziehen ließe.
	Dataport Data Center Justiz (DCJ)	Dataport ist der einzige IT-Dienstleister, der gemeinsam von Bundesländern und Kommunen getragen wird. Träger im Dataport-Verbund sind die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt, Schleswig-Holstein sowie der kommunale „IT-Verbund Schleswig-Holstein“. Basis dafür ist der Dataport-Staatvertrag. Dataport ist Anstalt öffentlichen Rechts. Damit unterscheidet sich Dataport als Archetyp 2 „Shared Service“ IT-Dienstleister von den meisten anderen Dienstleistern, da sie proaktiv auch für andere Länderbehörden Dienste anbieten will. Für die Justiz wurde die Infrastruktur auf logischer Ebene von der Verwaltung getrennt (konform mit hessischer Netzklage) und damit jeweils individuelle logische Netze für die Justizen der vier Trägerländer geschaffen. Innerhalb dieser Netze werden die jeweiligen Anwendungen der Justiz betrieben. Es gibt zwar einige für die vier Länder querschnittlich genutzte Dienste, die Umgebungen unterscheiden sich aufgrund der Länder aber wesentlich, bspw. weil drei eAkten-Systeme genutzt werden. Die Dataport baut derzeit sowohl die eigene Private Cloud als auch Zugang zu Public Cloud-Angeboten aus, weshalb das Data Center Justiz zu einem der modernen IT-Dienstleister-Angebote gehört.

Typ	Cloud-Initiative bzw. Angebot	Grobe Beschreibung
Souveräne Public Cloud- Angebote	Open Telekom Cloud (OTC)	Deutsches kommerzielles Public Cloud-Angebot der Telekom/ T-Systems auf Basis von Produkten verschiedener Hersteller für Institutionen und Geschäftskunden mit hohen Souveränitätsanforderungen. Die OTC wird bereits von der Justiz für die Softwareentwicklung von GeFa, nicht aber für den Anwendungsbetrieb genutzt. Telekom bietet auch alternative Cloud-Umgebungen an, in denen sie bspw. – wie die Delos GmbH – Google Cloud-Umgebungen auf deutscher Telekom-Infrastruktur betreibt. Analoge Public Cloud-Betriebsmodelle bietet bspw. die OVHcloud aus Frankreich. Alternative souveräne Cloud-Angebote entstehen auf nationaler Ebene z. B. bei Ionos (Tochter von 1&1) oder der StackIT (Tochter der Schwarz-Gruppe) sowie auch direkt bei den Hyperscalern als sog. Government Cloud-Angebote von Azure, AWS und Google sowie Oracle (B-Cloud).
Cloud- Initiativen	Gaia-X	Standardisierungsorganisation ohne eigenen Cloud-Betrieb zur Entwicklung von Richtlinien und Standards mit dem Ziel ein Datenökosystems für Organisationen und Industrien in Europa zu schaffen. Dabei arbeitet die Gaia-X Organisation mit Sitz in Brüssel aktiv mit Regierungen und kommerziellen Technologiepartnern zusammen. Erste Standards finden bereits Verwendung, z. B. beim Mobility Data Space des BMWK sowie bei Catena-X, der deutschen Automobilwirtschaft. Auch die International Data Space Association (IDSA) sowie das Fraunhofer ISST in Darmstadt nutzen und fördern Gaia-X Standard. Gaia-X ist somit kein Cloud-Angebot, sondern unterstützt die Entwicklung von Standards für den souveränen Datenaustausch mit/ und ohne Cloud. Die Initiative zählt damit auf die EU-Datenstrategie ein, die die Entwicklung von industriespezifischen Datenräumen und den einfachen Austausch von kritischen Datenelementen sowie den einfachen Zugang zu öffentlichen Daten (Open Data) forciert.
	Beweis- mittelcloud	Initiative von Polizei- sowie Justizbehörden aus Bund und Ländern zur Entwicklung einer Plattform für ressortübergreifende Verwaltung und Zugriffe auf digitale Beweismittel. Dabei auch besondere Berücksichtigung von Revisionssicherheit, Versionierung sowie Authentizität der digitalen Beweismittel. Aufgrund der enormen Datenmengen bei Berücksichtigung von Schmutz- (z. B. Bilder und Videos, Festplatten- bzw. Handyinhalte), sind skalierbare Cloud-Speicherlösungen prädestiniert, um somit auch das Datenteilen anstatt des heutigen Kopierens von Daten zwischen Polizei und Justiz bzw. des Versendens von Datenträgern zu befähigen.

Auch international hat die Justiz damit begonnen, Cloud-Technologie für sich zu erschließen. Es bestehen vergleichbare Herausforderungen und Anforderungen wie in der deutschen Justiz beispielsweise an Datenschutz und Souveränität (vgl. **Kapitel 2.2.3.2**).

Für die Zielbildentwicklung sollen diese bestehenden Angebote, Initiativen sowie internationale Beispiele bzgl. Relevanz und Nutzbarkeit für die Justiz geprüft werden. Im Rahmen der Ist-Analyse wurden daher die o. g. nationalen sowie internationalen Cloud-Angebote und -Initiativen detaillierter betrachtet.

2.2.3.1 Bewertung relevanter Cloud-Initiativen

Deutsche VerwaltungscLOUD-Strategie (DVS): Eine der wichtigsten Initiativen, um Cloud für die deutsche Verwaltung nutzbar zu machen, ist die vom *IT-Planungsrat* initiierte *Deutsche VerwaltungscLOUD-Strategie (DVS)*. Diese wird gemeinsam durch Bund und Länder vorangetrieben und soll als Multi Cloud-Strategie die verschiedenen Cloud-Lösungen bzw. -Umgebungen von Bund, Ländern und Kommunen standardisieren und damit interoperabel machen. Die *DVS* zielt daher vor allem darauf ab, gemeinsame Standards und offene Schnittstellen für Cloud-Lösungen (z. B. SaaS-Dienste) zu schaffen.

Über einen durch die *DVS* bereitgestellten Cloud-Dienste-Marktplatz sollen standardisierte Cloud-Dienste und -Anwendungen (SaaS) zur Nachnutzung bereitgestellt werden. Die dafür notwendigen Interoperabilitätsstandards, dabei insb. die Aspekte der Beschaffung und Abrechnung, Netzarchitektur und Netze des Bundes, Föderation von Identitäten und Berechtigungen, Schnittstellen- sowie Container-Standards, werden durch die *DVS*-Arbeitsgruppen erstellt.

Eine bundeseinheitliche, zentrale Cloud-Plattform zum gemeinsamen Betrieb von Cloud-Anwendungen für die Verwaltung wird durch die *DVS* nicht geschaffen. Vielmehr sollen die vielfältigen, teilweise noch in Entstehung befindlichen Cloud-Umgebungen der kommunalen, Landes- bzw. Bundes-IT-Dienstleister standardisierter und damit interoperabler werden. Durch die Standardisierung wird auch eine teilweise Nachnutzbarkeit durch Behörden ohne eigene Cloud-Infrastruktur angestrebt.

Im Umkehrschluss bietet die *DVS* daher keine bundeseinheitliche Cloud-Umgebung, in welche die Justiz „einziehen“ könnte. Zwar wäre mit *DVS*-Prinzipien ein Betrieb von einzelnen Justizanwendungen durch ein Land für alle Länder denkbar. Dem gegenüber stehen aber Anforderungen an die Unabhängigkeit und Eigenständigkeit der Justiz sowie rechtliche (bspw. Kontrahierungszwang) als auch technische Hürden (insbes. Latenz und Möglichkeit lokal zu speichern). Letztere vor allem aufgrund dessen, dass die Anwendungslandschaft der Justiz ein Anwendungsgefüge bildet, welches nicht wahllos trennbar und auf Länder verteilbar ist (vgl. **Kapitel 2.1**).

Dennoch sind diverse Konzepte des *DVC*-Architekturboards für den Aufbau einer bundeseinheitlichen Justizcloud interessant. Insbesondere die Netz- und Containerstandards sowie die behördenübergreifende Föderation von Identitäten, als auch das IT-Dienstleister-Reifegradmodell wurden in den Regelterminen zwischen *DVC*-Architekturboard und Justiz (-cloud) als wesentliche Synergien identifiziert. Für die Zielbildentwicklung wurden diese

Konzepte daher einbezogen und ein regelmäßiger Austausch dazu etabliert. Letzterer insbesondere, weil sich die Standards weiterentwickeln und die Justizcloud als erster Feldversuch zur Anwendung der *DVC*-Standards gelten kann.

govdigital eG: Die *govdigital eG* ist eine bundesweit ausgerichtete Genossenschaft öffentlicher IT-Dienstleister von Ländern und Kommunen, mit dem Ziel, die Digitalisierung der Verwaltung durch vereinfachte Kollaboration der IT-Dienstleister untereinander sowie durch niedrigschwellige kommerzielle Angebote zu fördern und zu skalieren. Dies auch insbesondere beim Cloud-Aufbau sowie der Cloud-Nutzung. *Govdigital eG* unterstützt dabei die *DVS*-Multi Cloud-Strategie von Bund und Ländern.

Govdigital eG bietet im Wesentlichen drei Services. Erstens einen [Cloud-Broker-Vertrag](#), über den Kommunen und andere Behörden der öffentlichen Verwaltung Zugang zu kommerziellen Cloud-Angeboten erhalten. Über die *govdigital eG* können Organisationen somit vertraglichen Zugang zu den eigenen Cloud-Umgebungen von fünf Anbietern (*Ionos*, *StackIT*, *AWS*, *Google*, *Azure*) erhalten. Es gilt zu beachten, dass über den Cloud-Broker allein die Beschaffung und Abrechnung mit dem kommerziellen Anbieter geregelt ist. Die technische und fachliche Anbindung (insbes. Netzverbindung und Landing Zone), Absicherung (insbes. IAM und Cloud-Access-Security) und Ausgestaltung (insbes. Anwendungsauswahl und -umbau) der Cloud-Umgebung obliegt dem jeweiligen Nutzenden.

Zweitens unterstützt *govdigital eG* öffentliche Organisationen auch mit einem dedizierten Angebot von Beratungs- sowie Projektunterstützungsleistungen für strategische und operative Initiativen, z. B. im Umfeld von Cloud oder auch bei Anwendungsentwicklung (z. B. Portalen wie dem EfA-Marktplatz). Dabei ist hervorzuheben, dass durch die *govdigital eG* Leistungen von Mitgliedern für Mitglieder als sog. Inhouse-Geschäfte gelten und daher zum einen von der Ausschreibungspflicht sowie von der Mehrwertsteuer befreit sind und damit einen wesentlichen Beitrag zu Geschwindigkeit und Konkurrenzfähigkeit beitragen. Bemerkenswert ist zum anderen, dass alle in **Kapitel 2.2.2** genannten IT-Dienstleister der Justiz bereits un-/ mittelbare Mitglieder der *govdigital eG* sind und damit Inhouse-fähig wären.

Drittens entwickelt *govdigital eG* gemeinsam mit allen oder ausgewählten Mitgliedern („flexibility-by-design“) auch gemeinsame Dienstleistungen, bspw. ein gemeinsames verteiltes, d. h. auf multiplen Knoten der beteiligten IT-Dienstleister gespanntes, Kubernetes-Cluster. Dies ist eine Container-Betriebsplattform auf der Kommunen Cloud-fähige, containerisierte Anwendungen betreiben können, ohne eigene Container-Plattformen aufbauen zu müssen. Andere gemeinsame Dienste finden sich im Bereich Cyber-Sicherheit und KI.

Insbesondere das gespannte, einheitliche Kubernetes-Cluster ist für die Justiz ein höchst interessantes Konzept. Aufgrund der *govdigital* eG Mitgliederstruktur, der Ausrichtung und Ausgestaltung des Kubernetes-Dienstes ist das *govdigital* eG Produkt „gespannter Kubernetes-Cluster“ jedoch für die Justiz nicht unmittelbar nachnutzbar. Dies insbesondere weil das Produkt die Unabhängigkeit der Justiz einschränkt, es nur ein Element der Justizcloud darstellt und nicht das gesamthafte Zielbild adressiert, die mitgliederorientierte Entscheidungsstrukturen die Gestaltungsfreiheit einschränken sowie die Kapazität der (noch) „kleinen“ Clusters für einen bundeseinheitlichen Betrieb der Justiz insgesamt nicht ausreichen.

Unabhängig davon besteht großes Potenzial zur Nachnutzung des Konzepts einer „gespannten Kubernetes-Plattform“ für die Justiz. Zudem ist die Inhouse-Fähigkeit zu allen IT-Dienstleistungen der Justiz von besonderem Interesse, weshalb die *govdigital* eG proaktiv bei der Zielbildentwicklung (insb. rechtlich-organisatorisches Zielbild) unterstützt hat. Auch die projekthafte Unterstützung bzw. Einbindung der *govdigital* eG beim Aufbau der Justizcloud wäre interessant sowie die Nachnutzung des Cloud-Broker-Rahmenvertrags, um kommerzielle Cloud-Umgebungen für die Justiz(-cloud) zu beschaffen.

Bundescloud des ITZBund: Wie viele andere IT-Dienstleister hat auch das *ITZBund* eine Cloud-Strategie und verfolgt dabei einen hybriden Multi Cloud-Ansatz. Dabei entsteht innerhalb der Infrastruktur des *ITZBund* eine eigene Private Cloud, die sog. *Bundescloud*. Dabei nutzt das *ITZBund* ein kommerzielles [Cloud-Angebot der Firma Ionos](#), das innerhalb der *ITZBund*-Rechenzentren als „Private Enterprise Cloud“ von *Ionos*, mit *Ionos* Software auf *ITZBund*-Hardware (sog. „air-gapped“) betrieben werden soll. Im Kontext der Multi Cloud-Strategie sollen weitere kommerzielle Cloud-Angebote sukzessive hinzukommen.

Insbesondere für die Länder ist die Nutzung der *ITZBund*-Infrastruktur des Bundes nicht ohne weiteres möglich. Das *ITZBund* gehört zum Geschäftsbereich des *BMF* und bietet damit in erster Linie Dienstleistungen für die Bundesverwaltung, z. B. im Zuge der *IT-Betriebskonsolidierung Bund*. Jedoch ist die Cloud-Strategie, das Vorgehen sowie der Aufbau einer Private Cloud durch kommerzielle Anbieter auf souveräner eigener Infrastruktur als Blaupause für ein mögliches Justizcloud-Zielbild von grundsätzlichem Interesse.

Delos GmbH: *Delos* ist ein Projekt des *BMF* zur Sicherstellung der nachhaltigen und souveränen Nutzbarkeit von *Microsoft*-Produkten für die öffentliche Verwaltung. Hintergrund ist, dass *Microsoft* die in der öffentlichen Verwaltung und Privatwirtschaft weit verbreitete *Office*-Software – wie viele andere Dienstleister (vgl. **Kapitel 1.1.2**) – sukzessive nur noch aus deren kommerzieller Public Cloud verfügbar macht. Die *Delos GmbH* ist eine

Tochtergesellschaft der *SAP AG* und handelt im Auftrag des Bundes/ des *BMF*. Sie verfolgt dabei ein sog. Treuhändermodell bei dem *Microsoft* Cloud-Software durch *SAP* bzw. *Delos* auf souveräner Infrastruktur des Bundes betrieben werden (sog. [Third Party Clouds](#)). Damit könnte die nachhaltige Teilhabe von Bundesbehörden am *Microsoft*-Produktportfolio sichergestellt werden, sofern keine alternativen Produkte wie bspw. [OpenDesk](#) oder [OpenOffice](#) sukzessive Einzug finden. Nebenbei sollen auch andere *Azure*-Cloud-Dienste in 2025 pilotiert und verfügbar werden. Darüber hinaus soll die Plattform sukzessive auch für Drittanbieter geöffnet werden, um so deren BSI-konforme Bereitstellung zu ermöglichen.

Analog der Argumentation bei der Bundescloud des *ITZBund*, ist auch die *Delos Cloud* aufgrund der Trägerschaftsstruktur sowie der Nutzung von Bundesinfrastruktur für die Justiz keine Option, um darauf den Kern der Justiz, d. h. Fachverfahren und eAkten-Systeme zu betreiben. Das *Delos* Angebot könnte aber ggf. künftig bei der Nutzung von Third Party Standardsoftware-as-a-Service (z. B. von *Microsoft*, *SAP*, uvm.) interessant sein. Das Justizcloud-Zielbild sollte daher eine sichere Anbindung an kommerzielle Umgebungen wie das *Delos*-Angebot vorsehen.

Open Telekom Cloud (OTC): Die *Open Telekom Cloud* ist ein Cloud-Angebot der *Deutschen Telekom* und bietet ein breites Angebot von Cloud-Diensten wie IaaS, PaaS und SaaS. Die *OTC* betreibt ihre Services dabei in eigenen Rechenzentren in Deutschland. Das Angebot richtet sich vornehmlich an Behörden, Institutionen und Geschäftskunden mit hohen Souveränitätsanforderungen in Deutschland. Zwar wird das Angebot sukzessive erweitert, aber im Vergleich mit den Services amerikanischer Hyperscaler wie *MS Azure*, *AWS* und *Google Cloud* ist das Angebot der *OTC* noch beschränkt. Daher bietet die Telekom auch alternative Cloud-Umgebungen an, in denen sie bspw. wie die *Delos GmbH* oder die *OVHcloud*, *Google* Cloud-Software auf deutscher *Telekom*-Infrastruktur betreibt.

Alternative souveräne kommerzielle Cloud-Angebote entstehen auf nationaler Ebene z. B. bei *Ionos* (Tochter von *1&1*) oder der *StackIT* (Tochter der *Schwarz-Gruppe*). Zudem bieten die Hyperscaler (*Azure*, *AWS* und *Google* sowie *Oracle (B-Cloud)*) sog. Government Cloud-Angebote und versuchen über Gründung von nationalen Betriebsgesellschaften und Rechenzentren Souveränitätsaspekte ihrer Cloud-Angebote zu verbessern.

Im Rahmen von *GeFa* wird bereits die *OTC* zur Entwicklung des Fachverfahrens genutzt. Für einen (bundeseinheitlichen) Betrieb von *GeFa* ist die *OTC* als souveräne Public Cloud-Lösung jedoch noch nicht betrachtet worden. Dies insbesondere, weil es noch keine bundeseinheitliche Untersuchung und demnach kein Zielbild sowie keine Anbieterauswahl für

die Cloud-Nutzung der Justiz aller Länder und des Bundes gab. Unabhängig davon ist die Nutzung von souveränen Public Cloud-Angeboten wie dem der OTC von großem Interesse für die Justiz und die Nutzung von externen kommerziellen Cloud-Umgebungen für bestimmte Anwendungsfälle ist auch für das Justizcloud-Zielbild zu betrachten.

Gaia-X: *Gaia-X* ist eine europäische Initiative mit Sitz in Brüssel mit dem Ziel der Schaffung eines digitalen Datenökosystems in der EU, in dem Daten verfügbar, zusammenführbar und konform mit europäischen Datenschutzstandards teilbar sind. *Gaia-X* ist dabei keine eigene Cloud-Infrastruktur, sondern die *Gaia-X* Governance entwickelt Standards, die dabei helfen, aus bestehenden Infrastrukturen ein gemeinsames „digitales Ökosystem“ zu schaffen. Da *Gaia-X* keine Cloud per se ist, wurde die Initiative in der Untersuchung nicht weiter betrachtet. Jedoch sind die *Gaia-X* Standards z. B. zur Interoperabilität von Daten und [Datenräumen](#) auch bspw. für den justizinternen Datenaustausch relevant. Die *Gaia-X* Standards, Blaupausen und bestehende Anwendungsbeispiele (z. B. [Catena-X](#) in der Automobilwirtschaft oder der vom [BMWK](#) geförderte *Mobility Data Space*) können in zukünftigen Ausbaustufen der Justizcloud zur Schaffung eines Justizdatenraums und bspw. zum souveränen Teilen von Justizdaten, z. B. mit dem polizeilichen Datenraum, berücksichtigt werden.

Beweismittelcloud: Das Teilen von Daten steht auch bei der gemeinsamen Beweismittelcloud-Initiative von Justiz und Polizei im Fokus. Dabei sollen digitale bzw. digitalisierte Beweismittel einfach und sicher über eine gemeinsame Plattform zwischen Polizei und Justiz erfasst, analysiert, geteilt und revisionssicher (insbes. Datenauthentizität) in beiden Kontexten verwendet werden können. Die Beweismittelcloud soll somit den wachsenden fachlichen und technischen Anforderungen zur Verwaltung, Speicherung und Analyse großer Datenmengen (sog. Massendaten) gerecht werden. Aufgrund der enormen Datenmengen ist die Beweismittelcloud-Plattform prädestiniert für Cloud-Infrastruktur.

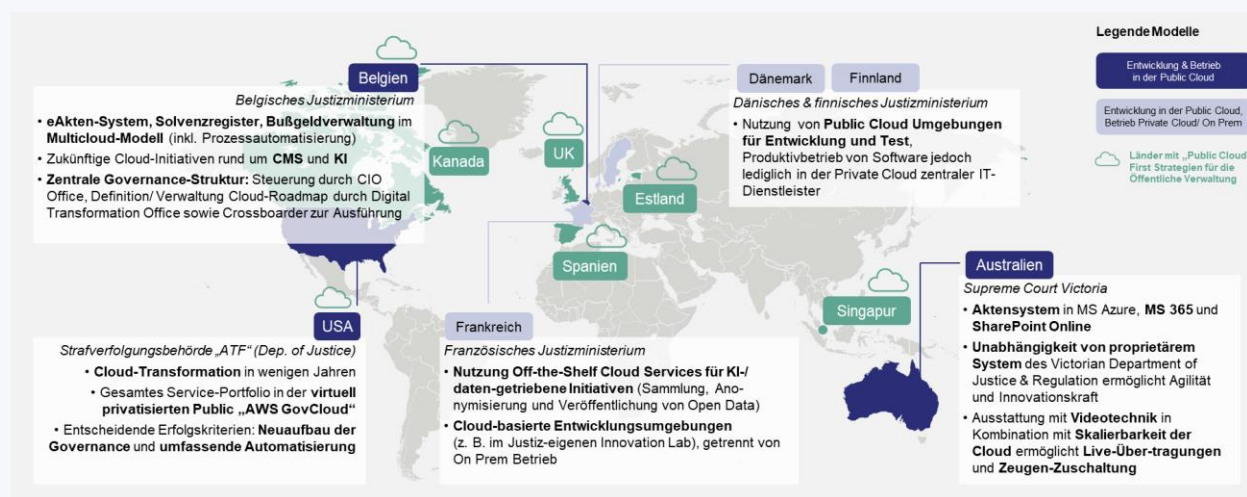
Damit wäre die Beweismittelcloud eine gemeinsam von Polizei und Justiz nutzbare Plattform bzw. Anwendung auf möglicherweise gemeinsamer Cloud-Infrastruktur. Daher wurde die Beweismittelcloud in der vorliegenden Untersuchung nicht als Cloud-Umgebung bzw. dediziertes Cloud-Angebot, sondern als Zukunftsanforderungen der Justiz analysiert.

2.2.3.2 Internationale justiznahe Beispiele für Cloud-Nutzung

Auch international nutzt die Justiz bereits Cloud. Im Rahmen der Untersuchung konnte mit Vertretern der Justiz weltweit gesprochen und Anwendungsfälle identifiziert werden, die den Mehrwert von Cloud sowie Best Practices bei der schrittweisen, datenschutzkonformen Exploration und Einführung von Cloud aufzeigen.

Dabei konnten verschiedene Nutzungsformen von Private bis Public Cloud festgestellt werden. Einige Länder wie Dänemark, Finnland und Frankreich nutzen bereits Public Cloud-Angebote, um moderne Anwendungsentwicklung (analog o. g. *GeFa-OTC*-Beispiel) zu ermöglichen. Der Betrieb der Anwendungen findet aber noch on-premises in der Private Cloud statt. In Dänemark wird diese bspw. durch einen zentralen IT-Dienstleister bereitgestellt. Die Justiz kann somit von den Möglichkeiten schneller und flexibler Anwendungsentwicklung und der Verfügbarkeit moderner Technologien und Cloud-Services in der Public Cloud profitieren, um Innovationen zu testen, voranzutreiben und die Geschwindigkeit der Anwendungsentwicklung zu steigern. In Ländern mit nationalen Public Cloud-First Strategien wie Singapur und Estland fällt der Einsatz von Cloud auch im Justizbetrieb dabei umso leichter.

Abbildung 14 | Internationale Beispiele für Cloud-Initiativen im Justizbereich



Die Analyse hat auch gezeigt, dass in einigen Ländern Cloud nicht nur für die Entwicklung von Anwendungen eingesetzt wird. Cloud ermöglicht auch, insb. Innovationen wie KI oder Low Code/ No Code-Plattformen zur Prozessautomation einzubinden. Diese Public Cloud-Plattformen werden daher bspw. in den USA oder Belgien dabei als Treiber für Digitalisierung und Effizienz eingesetzt (vgl. **Kapitel 1.1.2**).

Ein gutes Beispiel ist dabei die [Transformation der US-Strafverfolgungsbehörde ATF](#). Die Behörde hatte über Jahrzehnte ein komplexes Gefüge von Legacy-Anwendungen und Betrieb in über 500 lokalen, teilweise kommunalen Rechenzentren aufgebaut. Im Zuge einer umfassenden Cloud-Transformation konnte durch einen „Greenfield“-Ansatz systematisch das Anwendungsgefüge vereinfacht, standardisiert und unter Nutzung souveräner Cloud-Angebote neu aufgebaut werden. Dabei wurden auch viele Altanwendungen durch

Prozessautomation oder Re-design von Prozessen komplett abgelöst. Durch Cloud konnten somit nicht nur Effizienzen in IT-Entwicklung und Betrieb gehoben, sondern auch Fachprozesse modernisiert und digitalisiert werden.

Bemerkenswert ist, dass eine erste Iteration der geplanten Cloud-Migration gescheitert war. Dabei war das Ziel zunächst war, so viele der Altanwendungen wie möglich aus den lokalen Rechenzentren in die Cloud zu heben. Für eine reine IT-Konsolidierung ist der Cloud-Business Case zu gering und die Komplexität von Altanwendungen zu hoch. Denn Legacy-Anwendungen nutzen die Fähigkeiten von Cloud, bspw. Elastizität und damit Pay-per-use, nicht, weshalb Altanwendungen kontinuierlich viele Ressourcen verbrauchen und damit nach gewisser Zeit in der Cloud mehr kosten als im lokalen Betrieb. Zudem nutzen Altanwendungen oft Altkomponenten und Technologien, die in Cloud-Umgebungen kaum angeboten werden, weshalb ein Umbau bzw. Modernisierung der Anwendungen nötig war, was wiederum Kosten und Komplexität signifikant steigerte. Diese Erfahrungen sind auch für die deutsche Justiz von besonderer Relevanz, weshalb der „Greenfield“-Ansatz im Zielbild näher untersucht wird.

Insgesamt wurden die positiven internationalen Beispiele zur Cloud-Nutzung in der Justiz für die Zielbildentwicklung einbezogen. Aufgrund der Heterogenität der Ausgangslagen, Herausforderungen und Unterschiedlichkeit der Justiz in den jeweiligen Ländern, kann aber kein Land als Blaupause für eine bundeseinheitliche Justizcloud im deutschen Föderalismus herangezogen werden.

2.2.4 Zukunftsanforderungen der Justiz

Einordnung

Die Justiz betreibt bereits mit dem elektronischen Rechtsverkehr und den eAkten eine grundlegende digitale Infrastruktur und treibt ihre Digitalisierung mit den neuen Cloud-fähigen bundeseinheitlichen Fachverfahren wie *GeFa* und *AuRegis* sowie der Online-Service-Landschaft (z. B. *RAST*, *ZOV*) voran (vgl. **Kapitel 2.2.1.1**). Das Tempo der Digitalisierung hat sich in den letzten Jahren weiter beschleunigt und auch die Justiz muss sich in einem dynamischen, stetig wandelnden Umfeld zukunftsicher ausrichten.

Der Bedarf zur Digitalisierung ist groß und wird vor allem getrieben durch stetig steigende Anforderungen an die Justiz, z. B. durch neue gesetzliche Anforderungen, steigende Datenmengen, der weiteren Digitalisierung von Verfahren und Prozessen sowie allgemein höheren Anforderungen an einen modernen Zugang zur Justiz. Damit einher gehen auch

signifikante Investitionen in die digitale Infrastruktur sowie Gewinnung von IT-Fachkräften. Andererseits kann eine moderne, digitale Infrastruktur auch ein Lösungshebel sein. Denn auch der demographische Wandel treibt den Digitalisierungsbedarf. In den nächsten Jahren verrenten viele Justizbeschäftigte, während gleichzeitig die [Arbeitsbelastung in der Justiz](#) zunimmt und die Justiz im Wettbewerb um immer knapper werdende Fachkräfte steht.

Das Erschließen und Ausschöpfen neuer Technologien, wie z. B. Künstlicher Intelligenz (KI), Robotic Process Automation (RPA) und Cloud kann dabei unterstützen, Prozesse neu zu gestalten und die Effizienz in der Justiz zu steigern. KI kann bei sich wiederholenden Tätigkeiten unterstützen und hierdurch Ressourcen freisetzen, damit sich Justizmitarbeitende auf ihre Kerntätigkeiten konzentrieren können. Viele Technologien erschließt die Justiz in laufenden Vorhaben. Cloud-Technologie spielt dabei eine zentrale Rolle und kann für die Justiz eine wichtige Basistechnologie sein, um ihre Zukunftsthemen voranzutreiben.

In **Kapitel 2.2.1** wurden bereits bestehende Modernisierungsbedarfe und Verbesserungspotenziale durch eine bundeseinheitliche Justizcloud herausgearbeitet. Dabei handelt es sich um eine Momentaufnahme des Status Quo. Um ein ganzheitliches Bild der Anforderungslage für die Justiz zu erhalten, ist es daher essenziell auch die Zukunftsthemen der Justiz in den Blick zu nehmen. Dadurch können auch künftige Anforderungen frühzeitig berücksichtigt und auf ihr Cloud-Potenzial hin untersucht werden.

Um zu bewerten, inwieweit die Umsetzung von Zukunftsthemen der Justiz von einer bundeseinheitlichen Justizcloud profitieren kann, müssen die wichtigsten Zukunftsthemen zunächst identifiziert und detailliert werden. Dadurch können spezifische Anforderungen und Abhängigkeiten sowie mögliche Synergiepotenziale zur Justizcloud oder zu anderen Initiativen herausgearbeitet werden, um schließlich in die Zielbildentwicklung einzufließen.

Vorgehen

Im ersten Schritt wurde im Rahmen der Auftaktgespräche zur Ist-Analyse der Anwendungslandschaft mit Vertretern von Bundes- und Landesjustiz eine Longlist relevanter Zukunftsanforderungen, d. h. künftigen oder laufenden Initiativen erstellt, die sich auf die bestehende Anwendungslandschaft auswirken. Als nächstes wurde diese Themenliste gemeinsam mit dem Sounding Board nach fachlicher Relevanz und zeitlicher Kritikalität priorisiert und damit bestimmte Themen für die Detailanalyse ausgewählt (vgl. **Tabelle 7**).

Die priorisierten Themen wurden zunächst im Rahmen einer Online-Recherche als standardisierter Steckbrief aufbereitet und die gewonnen Erkenntnisse in zusätzlichen

Expertengesprächen mit den federführenden Länder- bzw. Bundesvertretern validiert, diskutiert und ergänzt. Dabei standen u. a. die genaue Zielsetzung der Vorhaben, ein umfassendes fachliches und technisches Verständnis zur Identifikation von Cloud-Ansatzpunkten und deren Cloud-Affinität sowie bestehende Verantwortlichkeiten, deren Umsetzungsstand und Zeithorizont zur Umsetzung im Fokus. Darüber hinaus wurden Gemeinsamkeiten und Abhängigkeiten sowie Synergiepotenziale mit einer bundeseinheitlichen Justizcloud vertieft.

2.2.4.1 Übersicht identifizierter Zukunftsanforderungen

In den Auftaktgesprächen mit den Vertretern der Bundes- und Landesjustiz konnten insgesamt elf wesentliche Zukunftsanforderungen identifiziert werden. Die Zukunftsanforderungen bilden dabei ein breites Spektrum an Themen ab, von sehr konkreten Fachanforderungen, wie zur automatisierten Übersetzung von Dokumenten, über sehr breite und weitreichende Themen, wie der Digitalisierung im Vollzug durch die *elektronische Gefangenenpersonalakte (eGPA)*, bis zur Erschließung von Grundlagentechnologien wie KI.

Tabelle 7 | Übersicht wesentlicher Zukunftsanforderungen der Justiz

Nr.	Federf.	Zukunftsanforderung	Erläuterung
1	BW	KI-Strategie und -Plattform	Entwicklung einer bundesweiten KI-Strategie sowie einer einheitlichen KI-Plattform für die Entwicklung und Nachnutzung von KI-Tools für die Justiz federführend für alle Länder und den Bund durch BW.
2	BE	Akten-/ Datenaustausch	Digitaler und effizienter Austausch von Akten und Daten ohne Datenduplikationen insbesondere innerhalb der Justiz im länderübergreifenden Kontext
3	Versch. Länder	KI-Unterstützung in justizieller Arbeit	Zum Beispiel Strukturierung von Verfahrensdaten (inbs. Akten), maschinelle Übersetzung, Nutzung von Sprachmodellen
4	NW	Elektronische Gefangenenpersonalakte (eGPA)	Digitalisierung der Gefangenenpersonalakte im Vollzug zur digitalen Verwaltung und Austausch von Gefangenendaten
5	NW	e-CODEX-Anbindung	Digitale Schnittstelle für den Austausch von Daten der Justiz mit EU-Behörden und anderen Justizorganisationen in der EU
6	Bund	Justizportal 2.0	Bundeseinheitliches modernes Online-Portal für den Zugang zu Informationen und digitalen Dienstleistungen der Justiz an die externe Domäne und als Nachfolger des derzeitigen Portals justiz.de gedacht
7	Bund	Zentrale Veröffentlichung von Urteilen	Bundeseinheitliche Bereitstellung gerichtlicher Entscheidungen für in- und externe Parteien über eine zentrale Plattform
8	(Bund)	Justiztoolbox (z. B. Foren)	Bundeseinheitliche Bereitstellung querschnittlicher Werkzeuge (z. B. Übersetzung) sowie Hilfsmittel und Kollaborationstools (z. B. Richter-Forum), um sich justizintern auszutauschen

Nr.	Federf.	Zukunftsanforderung	Erläuterung
9	BE	eAkte „neu“	Weiterentwicklung der elektronischer Aktenführung sowie der gemeinsamen modernen datengetriebenen Zusammenarbeit an Dokumenten, z. B. im Zivilprozess
10	NW	eAkten-Ablage Gerichtsvollzieher	Plattform für die Speicherung elektronischer Akten der Gerichtsvollzieher
11	Bund	Beweismittelcloud	Cloud-Lösung zur Speicherung, Analyse, Bereitstellung und Verwaltung sowie Teilen digitaler Beweismittel zw. Polizei und Justiz

Die ersten fünf Zukunftsanforderungen wurden für die Detailanalyse vom Sounding Board priorisiert.

In seiner dritten Sitzung hat das Justizcloud Sounding Board fünf Themen als besonders fachlich relevant und zeitlich kritisch bewertet. Diese werden im Folgenden detaillierter betrachtet.

2.2.4.2 Detailanalyse priorisierter Zukunftsanforderungen

(1) KI-Strategie und -Plattform: Um den Einsatz von KI zu ermöglichen und das Potenzial für die Justiz nutzbar zu machen, erarbeiten Bund und Länder derzeit eine bundesweite KI-Strategie für die Justiz. Dabei werden sowohl organisatorische, rechtliche als auch ethische Fragestellungen adressiert und bewertet. Gleichzeitig baut die Justiz im Zuge der Digitalisierungsinitiative für die Justiz unter Federführung des Landes Baden-Württemberg auch eine KI-Plattform für die gesamte Justiz.

Die KI-Plattform ist systematisch eine bereits antizipierte Maßnahme der KI-Strategie. Sie ist zentraler Bestandteil des dort beschriebenen KI-Ökosystems der Justiz und die technische Umsetzung der Strategie. Das macht sie zur Grundlage für eine nachhaltige Integration von modernen Assistenzanwendungen in die Geschäftsprozesse in den Justizdienststellen. Die KI-Plattform erleichtert erheblich Nach- und Mitnutzbarkeit von KI-Systemen (Nachnutzbarkeit: Anwendungen können in die Betriebsumgebungen der anderen Länder migriert werden. Mitnutzbarkeit: Länder können auf Anwendungen zugreifen, die in einer fremden Umgebung betrieben werden). Des Weiteren bildet die KI-Plattform den Anwenderinnen und Anwendern eine standardisierte Oberfläche für das Aufrufen von KI-Anwendungen. Durch die Standardisierung der Schnittstelle wird es zudem möglich sein, sich gegenüber initiativen Anbietern, insb. Start-Ups und KMUs, zu öffnen. Dies kann insb. dadurch geschehen, dass eine Testinstanz der Schnittstelle mit Testdaten öffentlich zur Verfügung gestellt wird.

Das Cloud-Potenzial der KI-Plattform wurde als „mittel“ eingestuft, da ein Betrieb der Plattform mit den drei o. g. Anwendungsfällen grds. auch ohne Cloud möglich wäre.

(2) Akten-/ Datenaustausch: Die Möglichkeit zum Akten-/ Datenaustausch umfasst fachlich sowohl die Akteneinsicht, also die Möglichkeit des lesenden Aktenzugriffs für justizexterne Parteien wie Rechtsanwälte, als auch den Austausch von Akten/ Daten zum Versand oder zur gemeinsamen Bearbeitung. Der Austausch bzw. das Teilen von Daten kann dabei entweder zwischen Mitarbeitenden der Justiz (landesintern oder -übergreifend) oder zwischen Justiz und externen Parteien wie Rechtsanwälten, Bürgern oder der Polizei erfolgen.

Weil die Justiz die Funktion der Akteneinsicht mit der [Einführung des AEP](#) bereits adressiert hat, hat die Untersuchung den Fokus der Analyse insbesondere auf den Akten-/ Datenaustausch gelegt. Insbesondere der justizinterne Datenaustausch hat eine hohe Relevanz für die Justizmitarbeitenden. Er könnte die bestehende, teilweise überlastete *EGVP*-Lösung signifikant entlasten und dabei die Aktualität, Authentizität und Integrität der geteilten Akten bewahren. Denn derzeit findet der in- und externe Datenaustausch hauptsächlich durch Versand von Aktenkopien über *EGVP* statt. Entsprechend entstehen Datenredundanzen und die Möglichkeiten der Zusammenarbeit an Daten ist nicht gegeben. Änderungen in Daten führen zu erneutem Versand, Aktualisierungen sind dem Empfänger nicht transparent und führen zu manuellen Prozessen.

Ein System zur Freigabe (Pull-Ansatz) anstatt der Übermittlung von Daten (Push-Ansatz) könnte diesen Herausforderungen und insb. der Duplikation von Daten effektiv begegnen. Für dessen Ausgestaltung bestehen verschiedene Lösungsoptionen.

Option 1 Modell „Dropbox“ beinhaltet die Schaffung eines gemeinsamen Ablageorts auf einer gemeinsamen Infrastruktur. In diesem würden Daten zentral gehalten und für einzelne Nutzende freigegeben werden. Die Daten müssten zwischen lokalen (z. B. den eAkten-Systemen) und der zentralen Umgebung synchronisiert werden und eine zentrale Benutzer- und Berechtigungsverwaltung würden für den Freigabeprozess genutzt.

Option 2 Modell „Datenraum“ ermöglicht es Daten weiter dezentral bei den Dateneignern zu halten (z. B. eAkten-System je Land) und diese über den technischen Ansatz der Datenvirtualisierung sowie ein gemeinsames Berechtigungsmanagement (lesend und/ oder schreibend) zugreifbar zu machen. So könnten Daten bzw. Akten von Nutzenden über einen zentralen Datenkatalog gesucht und Lese- bzw. Schreibrechte beim Eigner angefordert werden. Alternativ könnte der Dateneigner proaktiv seine eigenen Daten an bestimmte Nutzende im eigenen Land oder Behörden anderer Länder per Link freigeben.

Da es sich beim so definierten Datenaustausch um die Entwicklung einer komplett neuen Fähigkeit in der Justiz handelt, gibt es noch keine konkrete Zeitplanung für das Thema. Der

breite Bedarf innerhalb der Justiz und auch im Kontext Beweismittelcloud spricht für eine zeitnahe Umsetzung. Das Cloud-Potenzial wurde insgesamt als „hoch“ eingestuft, da die Cloud eine wesentliche Voraussetzung zur Umsetzung der o. g. Optionen wäre.

(3) KI-Unterstützung justizieller Arbeit: Die Justiz sieht sich seit mehreren Jahren dem Phänomen der Massenverfahren (z.B. Fluggastrechte-Verfahren, Diesel-Verfahren) gegenüber. Befördert wird dieses Phänomen durch Legal-Tech-Anbieter, die (teil-) automatisierte Anspruchsprüfung und -durchsetzung in für die Nutzenden leicht zugänglichen Verfahren anbieten. Hinzu tritt der Umstand, dass Künstliche Intelligenz für die schnelle Erstellung umfangreicher Schriftsätze eingesetzt werden kann. In der Folge sieht sich die Justiz einerseits mit einer Masse an gleichgelagerten, aber auch umfangreichen Verfahren konfrontiert.

Um diesem Problem zu begegnen, arbeitet die Justiz bereits an neuen fachlichen Lösungen, große Datenmengen schneller zu durchdringen, auszuwerten und zu verarbeiten. Dafür entstehen aktuell viele Ideen und Produkte, z. B. KI-basierte Aktenanalysen, Werkzeuge zur intelligenten Datenextraktion aus Dokumenten, Übersetzungs-Werkzeuge sowie verschiedene Anwendungen zur konkreten Unterstützung in Massenverfahren (z. B. Entwicklung des Oberlandesgerichtsassistent *OLGA* am *OLG Stuttgart* oder die *Massenverfahrens-Assistenz mithilfe von KI (MAKI)* durch das Niedersächsische Justizministerium). Aber auch außerhalb von Massenverfahren bietet KI Möglichkeiten, die Justiz bei repetitiven Aufgaben und beim Umgang mit großen Datenmengen zu unterstützen und damit mehr Zeit für die Kernaufgaben der justiziellen Arbeit zu schaffen.

Mit dem steigenden Datenaufkommen und den vielen Lösungsideen der Justiz, diese Daten schneller analysieren und bearbeiten zu können, steigt auch der Bedarf an entsprechender technischer Infrastruktur. Die derzeitigen Speicher- und eAkten-Lösungen der Justiz kommen teilweise schon heute an Ihre Grenzen, wenn bspw. großen Akten in mehrere *EGVP*-Nachrichten aufgeteilt werden müssen. Die Zurverfügungstellung von großen Datenmengen ist für KI-Anwendungen jedoch zentral. Zudem sind KI-Anwendungen selbst sehr rechenintensiv, sodass bei einem klassischen on-premises-Betrieb die Nutzung nur mit Einschränkungen möglich ist.

Das Cloud-Potenzial wurde insgesamt als „hoch“ eingestuft, da die Cloud eine wesentliche Säule zur einheitlichen Speicherung, Verarbeitung und Bereitstellung großer Datenmengen und Plattform zur Umsetzung von datengetriebenen innovativen Lösungen wäre.

(4) Elektronische Gefangenepersonalakte (eGPA): Die *analoge Gefangenepersonalakte (GPA)* enthält alle relevanten Informationen zur Betreuung und Überwachung von Inhaftierten im Justizvollzug. Dazu gehören die Strafakte, Vollzugsplan oder deren Gesundheitsstatus. Derzeit wird die *GPA* primär in Papierform geführt, wobei ihre Gestaltung zwischen den Ländern stark variiert. Ein digitales Teilen von Gefangenendaten mit anderen Vollzugsanstalten oder gar Ländern ist nicht möglich. Bei einer Verlegung von Gefangenen müssen digitale Informationen de facto ausgedruckt und die physische Akte gemeinsam mit dem Gefangenen transportiert werden.

Dies soll sich durch die Einführung einer bundeseinheitlichen *elektronischen Gefangenepersonalakte (eGPA)* ändern. Damit könnten auch die Fachprozesse vereinheitlicht, der Zugriff auf strukturierte Daten verbessert und der Austausch von Akten mit anderen Behörden (z. B. bei Verlegungen) erleichtert werden. Im Kontext der *eGPA* bietet es sich an, auch das Umfeld heterogener Fachverfahren in den Ländern von Grund auf neu zu denken und eine datenzentrierte eAkte und digitale Ende-zu-Ende-Prozesse im Vollzug zu entwickeln. Dabei ließe sich auch ein moderner, Cloud-nativer Funktionsschnitt zwischen Fachverfahren und Akte explorieren sowie die Möglichkeit, die *eGPA* als mandantenfähige Plattform bundesweit einheitlich bereitzustellen.

Die *eGPA* steht dabei jedoch vor großen technischen als auch fachlichen Herausforderungen. Die Akte muss revisionssicher sein, hohe Datenschutz- und Sicherheitsstandards erfüllen und die Vorgehensweisen verschiedener länderspezifischer Vollzugsanstalten bundesweit erhoben und standardisiert werden. Zudem nutzt der Vollzug aktuell noch nicht den *XJustiz*-Standard und weist vergleichbar hohe Heterogenität in Bestandsverfahren, Umsystemen und Infrastruktur auf, die eine bundeseinheitliche Neuentwicklung und vor allem eine bundesweite Ausbringung einer neuen Gefangenenaakte aufwändig machen.

Da sich die Anforderungserhebung zur *eGPA* noch mindestens bis 2025 hinzieht, bestünden interessante zeitliche Synergien zwischen dem Aufbau der Justizcloud und einer *eGPA*. Das Cloud-Potenzial wurde insgesamt als „hoch“ eingestuft, da die Cloud eine Grundlage zur gemeinsamen Entwicklung und zum einheitlichen Betrieb einer modernen, bundeseinheitlichen *eGPA*-Plattform darstellen könnte.

(5) e-CODEX-Anbindung: In einer immer enger zusammenwachsenden Europäischen Union ist auch die Notwendigkeit der grenzüberschreitenden justiziellen Zusammenarbeit stark gestiegen, und zwar sowohl im Bereich des Zivilrechts, einschließlich Handels- und Familienrecht, als auch im Bereich des Strafrechts.

Für diese Aufgabe stellt das europäische *e-CODEX*-System die technische Infrastruktur für die staatenübergreifende elektronische Kommunikation zwischen Gerichten, Behörden und EU-Institutionen innerhalb der Europäischen Union bereit. Dabei werden strukturierte Daten über standardisierte Protokolle bilateral zwischen den Systemen der Justiz der EU-Staaten ausgetauscht. Der Datenaustausch erfolgt dabei zwischen nationalen Konnektoren, die die Verbindung zwischen dem *e-CODEX*-System und den nationalen Infrastrukturen herstellen.

Bislang stand es den EU-Mitgliedstaaten frei, an *e-CODEX* teilzunehmen und einen nationalen Konnektor aufzubauen und zu betreiben. Doch mit der Verabschiedung der Europäischen Digitalisierungsverordnung wird die Abwicklung von 24 Verfahrensarten über *e-CODEX* sukzessive ab 2026 verpflichtend eingeführt.

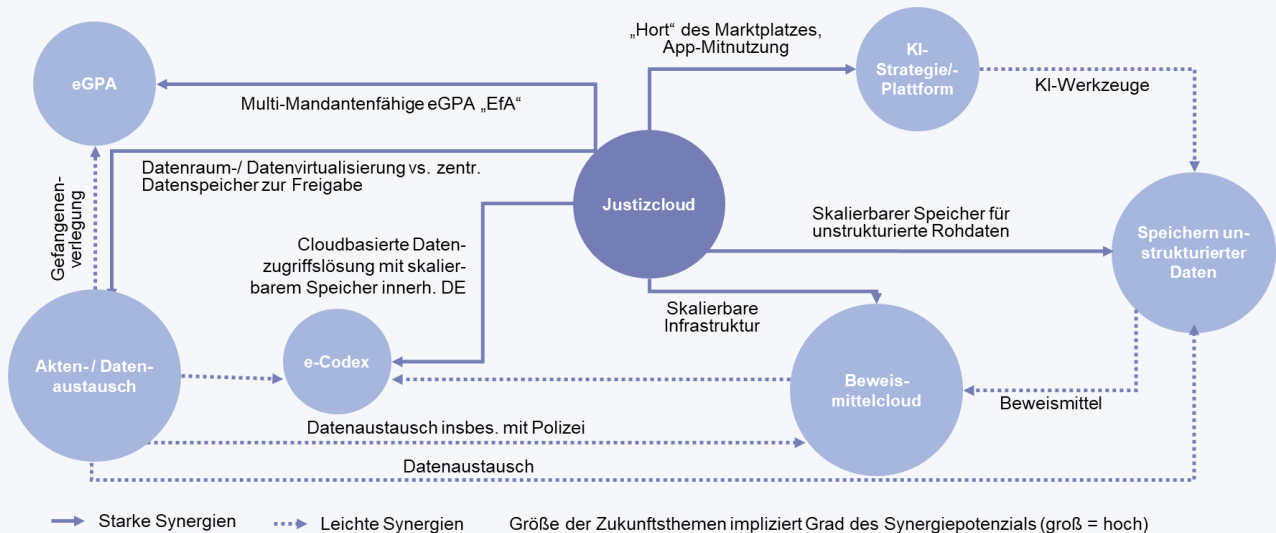
Obwohl der Fokus von *e-CODEX* klar auf der zwischenstaatlichen Kommunikation von Systemen der E-Justiz liegt, wird auch der Bedarf einer effizienten Datenaustauschlösung (Akten-/ Datenaustausch) innerhalb der deutschen Justiz steigen. Die komplette Eingliederung der europäischen Verfahren in die deutsche Anwendungslandschaft der Justiz wird voraussichtlich aber erst zu einem viel späteren Zeitpunkt erfolgen. Bis dahin wird zwangsläufig die von der Europäischen Kommission bereitgestellte Browseranwendung zum Einsatz kommen, deren Betrieb – einschließlich der Serverkomponenten – die deutsche Justiz selbst gewährleisten muss. Diese Aufgabe kann eine bundeseinheitliche Justizcloud vereinfachen. Daher ist das Cloud-Potenzial von *e-CODEX* insgesamt als „mittel“ einzustufen.

2.2.4.3 Wesentliche Erkenntnisse zu Zukunftsanforderungen

Die Analyse zeigt, dass in den nächsten Jahren neben den bereits laufenden Modernisierungsinitiativen wie z. B. *GeFa* oder den Online-Services wie *RAST* und *ZOV*, eine Vielzahl neuer Zukunftsanforderungen zu berücksichtigen sind. Die Analyse hat auch gezeigt, dass vielfältige Synergiepotenziale sowie einige Abhängigkeiten zwischen den Zukunftsthemen bestehen (vgl. **Abbildung 15**).

Schon unabhängig von einer Justizcloud weisen die Themen viele Synergiepotenziale auf. Insbesondere die Möglichkeit eines modernen und sicheren Akten-/ Datenaustauschs kann sowohl das Teilen von Daten im Kontext von *e-CODEX*, der Beweismittelcloud mit der Polizei, der Freigabe von Datenzugriffen bei Gefangenenerverlegungen als auch beim Teilen von großen Dateien fördern bzw. standardisieren und bestehende Infrastruktur (z. B. *EGVP*) entlasten.

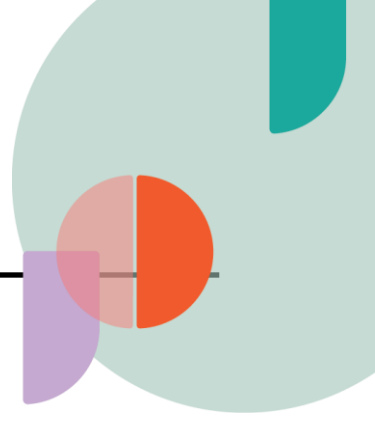
Abbildung 15 | Übersicht Abhängigkeiten bzw. Synergiepotenziale zwischen Zukunftsthemen



Bei allen betrachteten Zukunftsthemen zeigt sich, dass alle Themen grds. von Cloud profitieren und damit eine bundeseinheitliche Justizcloud viele Synergie- und Beschleunigungspotenziale bieten würde. Eine Justizcloud könnte grundsätzlich den Explorationsprozess unterstützen und beschleunigen, in dem für die Zukunftsthemen prototypische Umsetzungen erfolgen und ggf. auch schnell wieder verworfen werden. Die Justizcloud könnte die notwendigen Komponenten zum Aufspannen eines gemeinsamen virtuellen Datenraums bereitstellen, der das länderübergreifende Teilen von Daten ermöglicht. Auch könnte die Justizcloud benötigten Speicher für den Dropbox-Ansatz beim Datenaustausch bieten. Da die Justizcloud ohnehin ein gemeinsames IAM benötigen würde, könnte dieses auch die Grundlage für viele der Datenaustausch-Anwendungsfälle innerhalb der Justiz oder auch zur Polizei bilden.

Zudem könnte eine Justizcloud gleichermaßen für alle Länder einen skalierbaren Speicher für die rasant steigenden Datenmengen, etwa für digitale Beweismittel und kuratierte Trainingsdaten für KI-Modelle, bieten. Die Justizcloud könnte auch die Betriebsumgebung von bundeseinheitlichen KI-Anwendungen oder der KI-Plattform sein. Auch die bundeseinheitliche eGPA-Plattform könnte auf einer gemeinsamen, von allen Ländern gleichermaßen zugänglichen Cloud-Infrastruktur betrieben werden, anstelle eine eGPA auf die heterogenen, lokalen Betriebsumgebungen anzupassen. Im Bereich der europäischen Zusammenarbeit im e-CODEX könnte eine Justizcloud aufgrund der externen Standards eine geringere Rolle spielen, aber ggf. die Umsetzungskomplexität für den nationalen Konnektor reduzieren.

3 Justizcloud-Zielbild



3.1 Prämissen und Strukturierung des Zielbilds

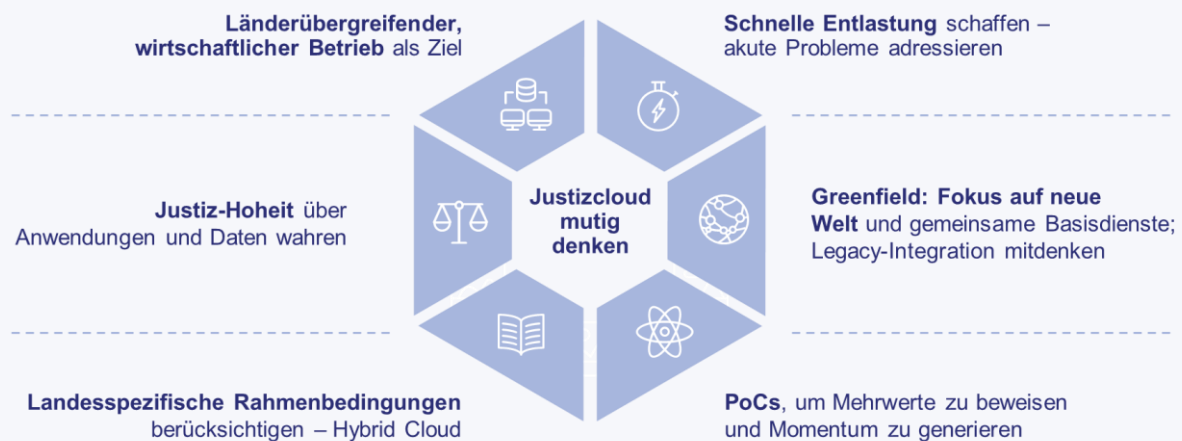
3.1.1 Prämissen und Bewertungsrahmen

Basierend auf den Erkenntnissen der Ist-Analyse konnten viele Bedarfe für ein bundeseinheitliches Vorgehen beim Erschließen einer gemeinsamen Cloud-Umgebung identifiziert werden. Insb. die akuten Anforderungen aus der Justizanwendungslandschaft (vgl. **Kapitel 2.2.1**) sowie die heterogene Umsetzung von Cloud in den jeweiligen IT-Umgebungen der Länder (vgl. **Kapitel 2.2.2**) können durch eine bundeseinheitliche Justizcloud adressiert werden. Durch diese könnten Entwicklung, Ausbringung und Betrieb der neu entwickelten Cloud-nativen Anwendungen wie *GeFa* und *AuRegis* von Beginn an Cloud-ready gedacht und umgesetzt werden. Aber auch die neuen Anwendungen der externen Domäne sowie die schrittweise Modernisierung der Online-Services würden signifikant von einer bundeseinheitlichen Cloud-Plattform profitieren.

Auch bei den Zukunftsthemen (vgl. **Kapitel 2.2.4**) haben sich vielfältige Synergiepotenziale durch eine Cloud-Lösung ergeben und vielfach ist Cloud als Basistechnologie für deren Umsetzung (z. B. Beweismittelcloud) eine Voraussetzung. Parallel dazu entstehen in Deutschland diverse Cloud-Angebote und -Initiativen (vgl. **Kapitel 2.2.3.1**) und es gibt zahlreiche internationale Beispiele (vgl. **Kapitel 2.2.3.2**) für die Cloud-Nutzung in der Justiz.

Insgesamt hat die Ist-Analyse also grundsätzlich großes Potenzial für Cloud in der Justiz ergeben. Die Ausgestaltung eines Zielbilds sowie die Bewertung der Machbarkeit erfolgte jedoch ergebnisoffen in einem strukturierten Vorgehen gemeinsam mit Vertretern der Justiz und IT-Dienstleistern aus Bund und Ländern. Dazu wurden sog. Fachpanels aus dem Projektteam und Vertretern der Länder und Bundesgerichte etabliert, die in Regelterminen das Zielbild in drei Ebenen entwickelt, validiert und abgestimmt haben. Um dabei zielgerichtet vorzugehen, wurden zunächst gemeinsame Prämissen definiert, die für den Zielbildentwicklungsprozess und als Leitplanken zur Orientierung dienen. In die Prämissen sind die wichtigsten Erkenntnisse zu Anforderungen und Herausforderungen der Justizanwendungslandschaft und der IT-Dienstleister eingeflossen.

Abbildung 16 | Prämissen für die Zielbildentwicklung



Eine zentrale Prämisse für das Zielbild ist, die Justizcloud nicht nur als mögliche Entwicklungsumgebung für Anwendungen zu verstehen, sondern auch einen länderübergreifenden, wirtschaftlichen und gemeinsamen Anwendungsbetrieb zu ermöglichen.

Gleichzeitig war den beteiligten Stakeholdern auch wichtig, ein Zielbild zu entwickeln, das schnell Entlastungen in der Justiz-IT schaffen kann und dabei vor allem die Ausbringungsprobleme bei neuen Fachverfahren wie *GeFa* und *AuRegis* sowie akute Zukunftsanforderungen der Justiz (z. B. Betriebsumgebung für neue Online-Services) adressiert.

Zudem wurde entschieden, dem Best-Practice-Ansatz vergleichbarer Cloud-Transformationen zu folgen und die Justizcloud im „Greenfield“-Ansatz aufzubauen. Das heißt, den Fokus auf die Entwicklung und den Betrieb bereits Cloud-fähiger Fachverfahren sowie den Aufbau eines neuen Anwendungsgefüges mit einheitlichen Architekturstandards und Technologien zu legen. Die Integration mit Legacy-Anwendungen in den bestehenden Betriebsumgebungen (insb. eAkten) sollte dabei mitgedacht und Lösungen für einen übergangsweisen Parallelbetrieb von Cloud- und Legacy-Umgebungen entwickelt werden. Diese Prämisse ist auch relevant, weil die Justiz derzeit noch wenige Cloud-fähige Anwendungen hat, bspw. sind die eAkten-Systeme noch nicht Cloud-ready.

Um das Zielbild nicht nur konzeptionell zu erstellen, sondern zeitnah auch auf seine Machbarkeit hin zu testen, wurde beschlossen, einen sog. Proof-of-Concept (PoC) im Rahmen der Untersuchung durchzuführen. Dieser soll nicht nur technische Erkenntnisse liefern, sondern auch das länderübergreifende Arbeiten von Justiz und IT-Dienstleistern an und mit der Cloud erproben und damit auch ein initiales Momentum aufbauen.

Bei der Zielbildentwicklung war es zudem elementar, landesspezifische Rahmenbedingungen, wie z. B. bestehende (Cloud-)Fähigkeiten von lokalen IT-Dienstleistern, rechtliche Einschränkungen sowie bereits getätigte Investitionen (z. B. Modernisierung des Rechenzentrums, lokaler Rollout der eAkte bis 2026 oder Anschaffung von Basistechnologien wie Container-Plattformen) soweit möglich in das bundeseinheitliche Zielbild zu integrieren.

Als abschließende Prämisse soll die Hoheit der Justiz über ihre Anwendungen und Daten bei der Cloud-Nutzung sichergestellt werden. Dazu zählen einerseits Aspekte der Unabhängigkeit der Justiz als Dritte Gewalt und damit die Einschränkung der Nachnutzbarkeit von Cloud-Services der Verwaltung. Zudem zählt dazu die Möglichkeit, landesspezifische Daten auch auf landesspezifischer Infrastruktur zu halten. Aber auch die Einschränkung des Nutzendekreises für die Justizcloud und das zugrundeliegende Justiznetz zählen zu dieser Prämisse. Alle Aspekte wurden bei der Bewertung machbarer Optionen in den jeweiligen Ebenen des integrierten Zielbilds der Justizcloud in den Fachpanels berücksichtigt.

3.1.2 Strukturierung des Zielbilds

Das integrierte Zielbild der Justizcloud besteht aus vier Ebenen, die unter Berücksichtigung der Prämissen ausgestaltet wurden. Die **Justizcloud-Vision** bildet die übergeordnete **strategische Ebene** und formuliert die grundsätzlichen Ziele („Warum?“). Die Ziele treiben die Ausgestaltung der **fachlichen Ebene** („Was?“), welche vor allem die Anwendungsfälle für die Justizcloud beschreibt. Um diese Anwendungsfälle zu realisieren, benötigt man die **technische Ebene** („Wie?“). Je nach Ausgestaltung der technischen Ebene sind verschiedene Festlegungen auf der **rechtlich-organisatorischen Ebene** („Wer?“) möglich.

Abbildung 17 | Ebenen des integrierten Zielbilds



Auf der obersten strategischen Ebene wurden für die bundeseinheitliche Justizcloud eine **Vision** und eine **Mission** erarbeitet. Zudem wurden acht konkrete **strategische Ziele** abgeleitet, die detaillieren, welche Mehrwerte der Aufbau einer bundeseinheitlichen Justizcloud für die Justiz generieren soll und welche Rahmenbedingungen dabei berücksichtigt werden müssen. Das strategische Zielbild wurde dabei in enger Zusammenarbeit mit dem Sounding Board von Bund und Ländern iterativ entwickelt und abgestimmt.

Aus der strategischen Ebene leitet sich das integrierte Zielbild der Justizcloud ab, das aus drei Teil-Zielbildern – dem fachlichen, technischen und rechtlich-organisatorischen Zielbild – besteht. Die drei Ebenen sind dabei eng verzahnt. Das **fachliche Zielbild** leitet die Anforderungen an die Justizcloud direkt aus den strategischen Zielen sowie den Bedarfen der Anwendungslandschaft und Zukunftsanforderungen der Justiz ab. Es beschreibt das zukünftige Zielbild der Anwendungslandschaft, die dafür benötigten Services und Dienste sowie die Nutzendengruppen der Cloud (vgl. Cloud-Nutzende in **Kapitel 3.4.1**).

Aus dem strategischen und fachlichen Zielbild leitet sich das **technische Zielbild** ab. Dieses beschreibt, in welchem Bereitstellungsmodell (z. B. Private, Public oder Hybrid Cloud) die benötigten Dienste bereitgestellt werden können und konkretisiert technische Aspekte wie das Berechtigungs-, Sicherheits- und Netzwerkkonzept damit Bund und Länder gleichermaßen auf die bundeseinheitliche Justizcloud zugreifen können.

Dies wiederum beeinflusst die Ausgestaltungsoptionen im **rechtlich-organisatorischen Zielbild**. Es beschreibt, wer die fachlichen und technischen Konzepte organisatorisch entwickelt und betreibt sowie welche Rollen und Fähigkeiten dafür erforderlich sind. Außerdem spielen dabei die Ausgestaltung des Finanzierungsmodells und der Rechtsform für die Justizcloud eine wesentliche Rolle.

Während das strategische Zielbild mit dem Sounding Board entwickelt wurde, sind das fachliche, technische und rechtlich-organisatorische Zielbild jeweils mit Vertretern der Justiz aus Bund und Ländern sowie von IT-Dienstleistern in sog. Fachpanels iterativ erarbeitet, Optionen diskutiert und die Zielbilder miteinander integriert worden. Abschließend wurden die Zielbildvorschläge turnusmäßig mit dem Sounding Board validiert.

Zu Beginn der Untersuchung lagen noch keine konkreten Vorgaben oder Zielbilder zu den jeweiligen Ebenen vor. Die Entwicklung des integrierten Zielbilds war also ein iterativer Prozess, der verschiedene Ausgestaltungsoptionen je Ebene in den Blick nahm und die Abhängigkeiten und Auswirkungen zwischen den Ebenen beleuchtete. Zu Beginn wurde bspw. eine eher generische strategische Vision mit Fokus auf Innovation in der Cloud genutzt, um

den Einstieg in die Ebenen zu erleichtern. Nachdem aber die Ist-Analyse der Anwendungslandschaft konkrete Schmerzpunkte identifiziert hat und auf der fachlichen Ebene der „Greenfield“-Ansatz als Prämisse festgelegt wurde sowie auf der technischen Ebene erste Lösungsansätze diskutiert waren, konnte die strategische Ebene passgenauer formuliert werden.

3.2 Vision, Mission und strategische Ziele

Die **Vision** gibt das langfristige übergeordnete Ziel eines Vorhabens wieder. Um die in der Ist-Analyse identifizierten Herausforderungen und Anforderungen zu adressieren, soll die Schaffung einer gemeinsamen technologischen Infrastruktur sowohl Effizienz, Innovation und Digitalisierung für die Justiz verbessern bzw. beschleunigen und Bund und Länder gleichermaßen von Cloud profitieren lassen. Gemeinsam mit dem Sounding Board wurde folgende Vision für die Justizcloud entwickelt:

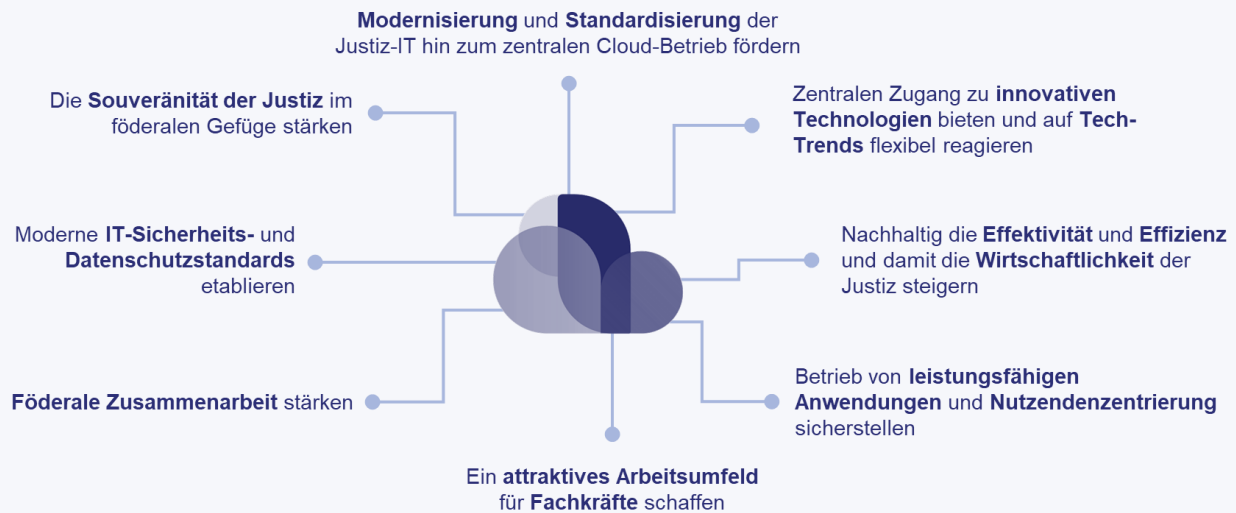
**Gemeinsame Technologien für eine
unabhängige und zukunftsfähige Justiz**

Die Vision unterstreicht die Stärkung der Unabhängigkeit der Justiz durch eine eigene, in Justizhoheit stehende Cloud-Umgebung und betont gleichermaßen indirekt die Dringlichkeit des Projekts, um die Zukunftsfähigkeit der Justiz im digitalen Zeitalter sicherzustellen. Aus der Vision leitet sich die **Mission** ab und konkretisiert wesentliche Ziele und Mehrwerte für alle Beteiligten.

Die Justizcloud bietet für die Justiz einen souveränen Zugang zu innovativen Cloud-Technologien und damit eine gemeinsame Plattform, um eine moderne und nutzendenzentrierte Anwendungslandschaft zu entwickeln und zu betreiben.

Die Justizcloud-Mission beschreibt damit das wichtigste strategische Ziel, nämlich den Aufbau einer gemeinsamen Plattform für die Entwicklung und den Betrieb der modernen (vgl. „Greenfield“-Ansatz) Anwendungslandschaft der Justiz. Um die Mission in konkrete Handlungsfelder zu übersetzen, wurden **strategische Ziele** entwickelt, die durch den Aufbau einer gemeinsamen, bundeseinheitlichen Justizcloud erreicht werden sollen:

Abbildung 18 | Strategische Ziele der bundeseinheitlichen Justizcloud



Die strategischen Ziele reflektieren auf den ersten Blick typische Ziele im Kontext von Cloud-Initiativen. Bei genauerem Hinsehen wird klar, dass die im Sounding Board von Bund und Ländern entwickelten Ziele die derzeitigen Herausforderungen, sowie die Vision und Mission aufgreifen und passgenau für die Justiz formulieren. Bspw. wird der gemeinsame Betrieb von Anwendungen betont, da die Justiz zwar gemeinsam Anwendungen entwickelt, aber noch nicht betreibt. Gleichzeitig wird eine Stärkung der Souveränität der Justiz angestrebt, weil die Justiz bei Landes-IT-Dienstleistern teilweise an Infrastrukturen, Technologien und Entscheidungen der Verwaltungen gebunden ist, obwohl diese ggf. nicht passgenau für die Justiz sind. Zudem soll die Justizcloud zur konsequenten Modernisierung und Standardisierung der Justiz-IT beitragen und damit zur Reduktion der bestehenden Heterogenität und Komplexität. Besonders wichtig ist auch die Betonung der Stärkung der föderalen Zusammenarbeit, die auch als Leitlinie für die vorliegende Untersuchung zur Justizcloud galt und die Zusammenarbeit zwischen Justiz, IT-Dienstleistern und Entwicklungsverbünden förderte. Jedes strategische Ziel wird im Folgenden detailliert.

Souveränität der Justiz im föderalen Gefüge stärken: Souveränität umfasst hierbei zum einen die verfassungsgemäße Unabhängigkeit der Justiz als „Dritte Gewalt“ (d. h. die Sicherstellung der Gewaltenteilung und der richterlichen Unabhängigkeit), zum anderen die Sicherstellung digitaler Souveränität. Dies erfordert u. a. die Sicherstellung organisatorischer Unabhängigkeit (z. B. von IT-Dienstleistern unter Aufsicht anderer Ressorts), die Unabhängigkeit von privaten Anbietern (z. B. private Unternehmen wie Hyperscaler), die Sicherstellung technischer Interoperabilität (z. B. Nutzung offener Standards und Open

Source Technologien), Datensouveränität (z. B. durch prozessuale und technische Maßnahmen) und Wissenssouveränität (z. B. durch Bündelung und Sicherstellung der Verfügbarkeit bzw. Zugänglichkeit zu Cloud-spezifischem Wissen und Know-how).

Modernisierung und Standardisierung der Justiz-IT hin zum zentralen Cloud-Betrieb fördern: Die Justizcloud soll die Entwicklungs-, Ausbringungs- und Betriebsprozesse der Justiz-IT verbessern. Die Anwendungsentwicklung profitiert durch einheitliche Plattformkomponenten und einheitliche Ausbringungsprozesse. Die Ausbringung wird beschleunigt, indem Software auf und gegen eine einheitliche standardisierte Infrastruktur getestet und mit einheitlichen Werkzeugen ausgebracht werden kann. Dies ist Grundlage, um einen einheitlichen Betrieb von Anwendungen zu ermöglichen sowie eine höhere Stabilität, Performanz und Verfügbarkeit von Cloud-Anwendungen zu gewährleisten. Der Fokus liegt dabei auf neuen, Cloud-fähigen Justizanwendungen. Auf mittlere Sicht ist daher ein Hybridbetrieb aus bestehenden Systemen (z. B. eAkten) in den Ländern und neuen Anwendungen in der Justizcloud (z. B. *GeFa* und *AuRegis*) erforderlich. Die Anwendungslandschaft kann dabei sukzessive modernisiert und die Verortung von Anwendungen in der Justizcloud kontinuierlich angepasst werden. Es handelt sich um eine langfristig angelegte Transition hin zur Cloud.

Zentralen Zugang zu innovativen Technologien bieten und auf Tech-Trends flexibel reagieren: Im dynamischen Technologieumfeld werden stetig neue Arbeitsweisen und Technologien entwickelt, die für die Justiz hohe Mehrwerte liefern könnten. Während der Zugriff zu solchen Technologien aufwändig und teuer sein kann, bietet die Justizcloud einen Explorationsraum („Sandbox“) für neue Dienste und Verfahren (z. B. Low-Code-Plattformen oder moderne Speicherlösungen). Zudem ermöglicht Cloud-Technologie sowohl neue Arbeitsweisen zwischen Fach und IT als auch zwischen Anwendungsentwicklungs- und -betriebsteams (z. B. *DevSecOps*). Die Justizcloud bietet so einen einheitlichen, gleichberechtigten Zugang zu neuen Technologien und Arbeitsweisen und damit eine Möglichkeit, auf Tech-Trends flexibler und zeitnaher zu reagieren, diese zu erproben und in den Wirkbetrieb zu überführen.

Nachhaltig Effektivität und Effizienz und damit die Wirtschaftlichkeit der Justiz steigern: Durch die Justizcloud als Betriebsumgebung (s. o.) und die sukzessive Modernisierung und Standardisierung der Anwendungslandschaft (s. o.) könnte die Komplexität signifikant reduziert, länderübergreifende Synergien in Anwendungsentwicklung und -betrieb ermöglicht, Kompetenzen gebündelt und die Entwicklung von Justizanwendungen durch

kürzere Ausbringungszyklen beschleunigt werden. Zusätzlich könnten neue, agilere Arbeitsweisen zwischen Fach und IT ermöglicht werden. Außerdem könnte die Wirtschaftlichkeit durch den bundeseinheitlichen Betrieb (s. o.) von Anwendungen maßgeblich verbessert werden. Zudem würde die Justizcloud neuartige Nutzungs- bzw. Abrechnungsmodelle (z. B. „Pay-per-use“ und Software-as-a-Service (SaaS)) und damit weitere Effizienzpotenziale erlauben. Gleichzeitig könnte die gesteigerte Effizienz indirekt auch zur Erreichung ökologischer Nachhaltigkeitsziele beitragen, wenn z. B. nur eine Container-Plattform für die Justiz betrieben werden muss.

Betrieb von leistungsfähigen Anwendungen und Nutzendenzentrierung sicherstellen:

Nutzende sind dabei insb. interne Mitarbeitende der Justiz sowie externe Nutzende wie Bürger, Rechtsanwälte, Notare und Unternehmen. Nutzendenzentrierung meint sowohl innovativere, ergonomischere und intuitivere Anwendungen zu erstellen als auch die Performanz, Stabilität, Sicherheit und Verfügbarkeit der Anwendungen zu verbessern. Wirkliche Nutzendenzentrierung kann nur erreicht werden, wenn man kontinuierlich Anwendungen an Kundenbedarfe anpassen bzw. Neuerungen schnell Kunden bereitstellen kann, zeitnahes Feedback aus Test und Produktion erhält und dieses wiederum zur Verbesserung der Anwendung, ihrer Funktionen oder der Performanz nutzen kann. Eine skalierbare Cloud-Infrastruktur und elastische, selbstheilende Cloud-native Anwendungen sind wichtige Grundlagen zur Steigerung von Performanz und Verfügbarkeit moderner Justizanwendungen.

Ein attraktives Arbeitsumfeld für Fachkräfte schaffen: Cloud-Technologie ist eine wesentliche Grundlagentechnologie und ermöglicht die Entwicklung und den Betrieb moderner, innovativer und performanter Anwendungen. Viele Entwickler und IT-Fachkräfte sind diese Technologien (z. B. aus dem Studium) gewohnt, wollen diese vertiefen und suchen daher vornehmlich nach innovativen Arbeitgebern, die diese Technologien einsetzen. Aber auch bestehende Fachkräfte wollen gefördert und graduell an neuen Technologien geschult werden. Vor dem Hintergrund des stetig steigenden Fachkräftemangels muss auch die Justiz entsprechende Perspektiven bieten. Dabei muss auch festgestellt werden, dass der Aufbau von Cloud-Kompetenzzentren und -Entwicklungsteams nur für die Justiz in allen Ländern nicht wirtschaftlich und ggf. auch nicht machbar ist. Von daher ist eine Bündelung der Aufwände, Gewinnung von Talenten und gezielte Anwerbung in eine bundeseinheitliche Justizcloud sowohl quantitativ (insb. Ressourcenbedarf) und qualitativ (insb. Qualifikation) für die Justiz vielversprechender.

Gleichzeitig verbessert Cloud-Technologie auch die Gestaltung moderner Arbeitsumgebungen für die gesamte Justiz, z. B. durch Bereitstellung moderner, intuitiver Kollaborationstools (z. B. *Confluence/ Jira*), modernen Möglichkeiten des Datenaustauschs sowie durch die Gewährleistung sicherer, ortsunabhängiger Zugriffe auf wichtige Ressourcen und Anwendungen. Die Justizcloud trägt so auch zu flexibleren Arbeitsmodellen, mehr Heim-/ Remote-Arbeit und damit auch zu einem modernen Arbeitsumfeld für Endnutzende bei.

Föderale Zusammenarbeit stärken: Für strategische Fragestellungen soll die Justizcloud in die bewährten Entscheidungsstrukturen der Justiz (z. B. *EJR* und *BLK*) eingebettet werden. Die Justizcloud würde die Weiterentwicklung föderaler Entscheidungsstrukturen und übergreifender Fähigkeiten (z. B. Architekturboard und strategisches Anforderungsmanagement) unterstützen. Sie kann auch den Aufbau und die Bündelung von Cloud- und Entwicklungskompetenzen für die Justiz insgesamt fördern. Dabei würde die Justizcloud die Umsetzung landesspezifischer Vorhaben nicht einschränken. Im Gegenteil würde sie auch Platz für länderspezifische Umgebungen bieten (sog. Mandanten/ Tenants).

Moderne IT-Sicherheits- und Datenschutzstandards etablieren: Cloud erfordert zur Nutzung die Etablierung moderner Sicherheitsmaßnahmen (z. B. Verschlüsselung und IAM), ermöglicht aber gleichzeitig auch eine bundeseinheitliche Standardisierung und Härtung der IT-Sicherheit der Cloud-Umgebung auf Höhe der Zeit (z. B. Hardware Security Module (HSM), Multi-Factor-Authentisierung (MFA), Cloud Firewalls/ Proxies und Microsegmentierung), von der alle Länder gleichermaßen profitieren.

Der aktuelle Betrieb multipler, heterogener Infrastrukturen und damit IT-Sicherheitsbetriebe vergrößert die potenzielle Angriffsfläche vor dem Hintergrund der allgemein steigenden Cyber-Bedrohungslage insb. bei nach außen exponierten Online-Services. Gleichzeitig ist die Sicherstellung von Cloud-Sicherheit und Cloud-nativer Anwendungssicherheit (z. B. DevSecOps, API-Sicherheit, Datensicherheit, Container-Härtung) komplex und teuer. In einer bundeseinheitlichen Justizcloud kann dieses spezifische Wissen gebündelt sowie Sicherheitsmaßnahmen effektiv und einmal für alle umgesetzt werden. Dazu dient u. a. die Implementierung durchgängiger Sicherheitsprotokolle, umfassender Verschlüsselungs-Mechanismen mit länderspezifischen Zertifikaten, tiefgreifender technischer Maßnahmen zur Absicherung der Infrastruktur bereits ab Ebene des Justiznetzwerks sowie einer einheitlichen, systematischen Zugriffsberechtigung und -kontrolle auf Anwendungen und verarbeitete Daten, wobei die Identitäten der Nutzenden aus den Länder-Providern sicher gefördert werden können.

Auf Grundlage von Vision, Mission und strategischen Zielen wird im Folgenden zunächst das gemeinsam formulierte, integrierte und machbare Zielbild für die bundeseinheitliche Justizcloud beschrieben. Danach werden die jeweils untersuchten Optionen und Empfehlungen auf der fachlichen (vgl. **Kapitel 3.4**), technischen (vgl. **Kapitel 3.5**) und rechtlich-organisatorischen (vgl. **Kapitel 3.6**) Zielbildebene in dedizierten Kapiteln erörtert.

3.3 Integriertes, machbares Justizcloud-Zielbild

Im Ergebnis der fachlichen, technischen und rechtlich-organisatorischen Fachpanel-Arbeit wurde ein integriertes, machbares Zielbild für die bundeseinheitliche Justizcloud entwickelt. Das Zielbild erlaubt die Etablierung eines neuartigen, Cloud-nativen Betriebsmodells entlang des Cloud-Servicespektrums der Infrastruktur (IaaS), Plattformen (PaaS) und Anwendungen (SaaS). Dieses wird im Folgenden beschrieben. Anschließend werden die fachliche, technische sowie rechtlich-organisatorische Ebene erläutert.

3.3.1 Übergreifendes Justizcloud-Betriebsmodell

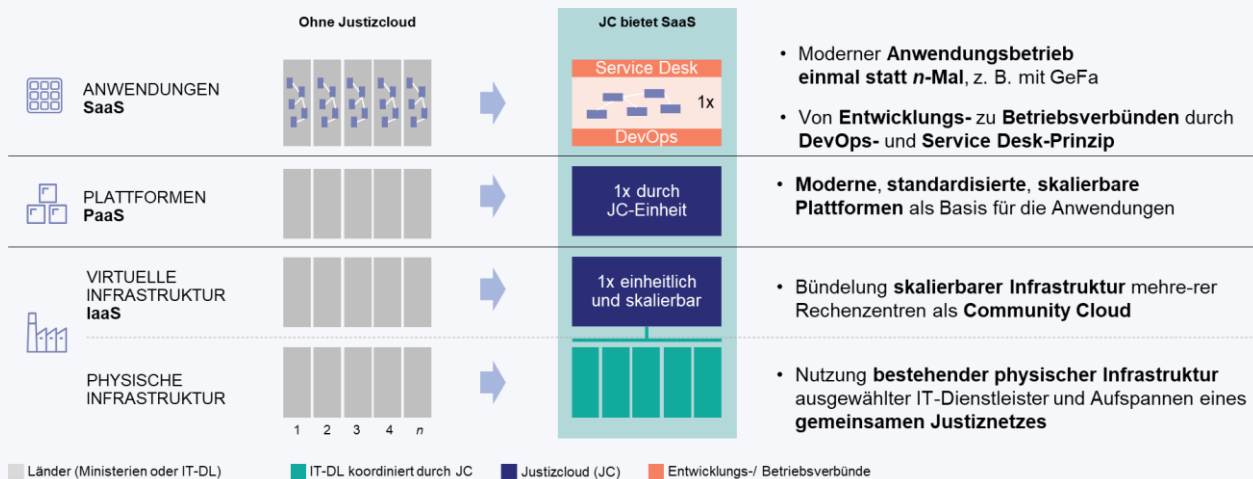
Im Grundsatz besteht jede Cloud aus vier Schichten. Auf physischer Infrastruktur eines oder mehrerer Rechenzentren wird virtuelle Infrastruktur definiert (sog. Virtualisierung). Auf der virtuellen Infrastruktur (IaaS, z. B. Speicher, Datenbanken, Netzwerk) werden Plattformdienste (PaaS, z. B. Container-, Daten-, Monitoring- und API-Plattformen) ausgebracht. Mit den Plattformdiensten können Anwendungen (SaaS) entwickelt und betrieben werden.

In einer Cloud sind die IaaS-, PaaS- und SaaS-Schichten zwar miteinander verzahnt bzw. vertikal integriert, aber per API entkoppelt. Damit profitieren nachgelagerte Schichten von Verbesserungen in vorgelagerten Schichten. Gleichmaßen kaskadieren Ressourcenbedarfe von den Anwendungen über die Plattformen auf die Infrastruktur. Eine Cloud-Plattform kann so als Ganzes elastisch skalieren – natürlich nur innerhalb der physischen Grenzen des Rechenzentrums. Selbst Hyperscaler stoßen in bestimmten Regionen, in denen der Bedarf hoch, aber die Rechenkapazitäten gering sind, an physische Grenzen.

Abgeleitet aus der Mission und den strategischen Zielen soll die bundeseinheitliche Justizcloud ermöglichen, dass die Justiz die modernen Justizanwendungen (z. B. *GeFa*, *AuRegis*) nicht nur bundeseinheitlich entwickeln, sondern auch bundeseinheitlich, d. h. für alle Länder, betreiben kann (sog. SaaS). Dafür ist es notwendig, dass die zukünftigen Entwicklungsverbünde befähigt werden, ihre Anwendungen mit dem DevOps-Ansatz kontinuierlich auf einer einheitlichen Plattform auszubringen. Durch den bundeseinheitlichen technischen Betrieb auf einer einheitlichen Plattform wird zudem ein weiteres Synergiepotenzial im

fachlichen Anwendungsbetrieb ermöglicht. Der fachliche Betrieb könnte in einem virtuellen länderübergreifenden Service Desk gebündelt werden. Aus Entwicklungsverbünden können somit durch die Justizcloud-Plattform Betriebsverbünde werden.

Abbildung 19 | Gegenüberstellung Betriebsmodell mit und ohne Justizcloud



Die bundeseinheitliche Plattform-Schicht (PaaS) bildet dabei das Kernelement der Justizcloud und basiert selbst auf einem Pool standardisierter und skalierbarer virtueller Infrastruktur (IaaS). Die virtuelle Infrastruktur wird im Justizcloud-Ansatz von ausgewählten bestehenden IT-Dienstleistern der Justiz (sog. Knoten-Providern) bezogen, die über ein gemeinsames Justiznetz miteinander verbunden sind (vgl. **Abbildung 19**).

Statt wie bisher Infrastruktur, Plattformen und das Anwendungsgefüge der Justiz in jedem Land individuell zu betreiben, orchestriert, vereinheitlicht und vernetzt die bundeseinheitliche Justizcloud die virtuelle Infrastrukturschicht (IaaS). Darauf etabliert, bündelt und betreibt sie die bundeseinheitliche Cloud-Plattformschicht (PaaS) sowie das dafür notwendige Know-how, was wiederum den bundeseinheitlichen Betrieb des modernen Anwendungsgefüges (SaaS) durch die Betriebsverbünde der Justiz ermöglicht.

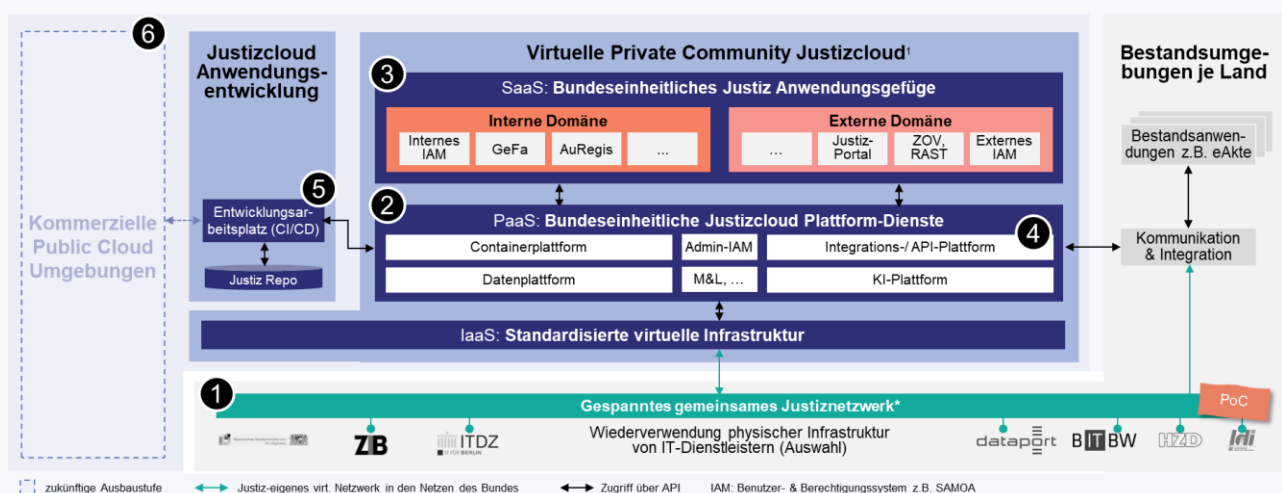
Unter Berücksichtigung der Prämissen (vgl. **Kapitel 3.1**) und strategischen Ziele (vgl. **Kapitel 3.2**) wurde der Aufbau einer Private Community Cloud als die fachlich, technisch und rechtlich-organisatorisch machbarste Alternative bestimmt. Diese nutzt bestehende physische Infrastruktur der Justiz-IT-Dienstleister und verbindet diese mit einem justizeigenen, privaten Netz in den *Netzen des Bundes (NdB)*. Dieser Ansatz hat erhebliche Vorteile, da auf bestehende Investitionen zurückgegriffen und die Souveränität und Datenhoheit

gleichermaßen bewahrt werden kann. Dabei ist der Ansatz modular und erlaubt die flexible Einbindung aller IT-Dienstleister und so auch die Teilhabe aller Länder sowie die native Konnektivität und Integration von Cloud-Anwendungen und lokalen Legacy-Umgebungen. Das Justizcloud-Modell ist somit auch konform mit den Konzepten der *Deutschen Verwaltungscloud-Strategie (DVS)* bzw. wendet sie für die Justiz an und denkt sie weiter.

3.3.2 Fachliche und technische Ebene der Justizcloud-Plattform

Die Justizcloud ist eine über IT-Dienstleister gespannte private Cloud-Plattform und bietet bundeseinheitliche Platfordmdienste für Entwicklung und Betrieb der modernen Anwendungslandschaft der in- und externen Domäne. Sechs Elemente sind dabei besonders entscheidend (vgl. **Abbildung 20**).

Abbildung 20 | Zielbild Justizcloud-Plattform



1. Gemeinsames Justiznetz: Auf der untersten Ebene etabliert die Justizcloud ein sog. **virtuelles privates Netzwerk**, das die IT-Dienstleister der Justiz miteinander verbindet. Das ist nachhaltig, sicher und erlaubt die konsequente Netzttrennung der Justiz. Dies stärkt die Unabhängigkeit der dritten Gewalt. Dieses Konzept wird bspw. bereits bei Verfassungsschutzbehörden analog genutzt.

Das gemeinsame Justiznetz erlaubt es, die Infrastrukturen der Justiz-IT-Dienstleister sicher, resilient und performant miteinander zu verbinden. Aus Justizcloud-Sicht entsteht dadurch ein bundesweites virtuelles Rechenzentrum mit ausreichend Speicher- und Rechenkapazität für die Zukunft. Zudem erlaubt das Netzwerk, lokale Anwendungen, z. B. eAkten, aus der

Justizcloud heraus anzusprechen. Auch ist es Grundlage zur Schaffung eines bundesweiten Justizdatenraums, in dem in Zukunft Daten sicher geteilt anstatt als redundante Kopien versendet werden können (vgl. **Kapitel 3.4.5**).

2. Standardisierte Plattform-Dienste: Auf dem homogenen Netzwerk und der standardisierten Infrastruktur können nun bundeseinheitliche Plattform-Dienste für die Justiz entstehen. Neben der Container-Plattform zum Betrieb der modernen Cloud-Anwendungen, können so z. B. auch eine gemeinsame Daten- sowie KI-Plattform aufgebaut werden, an denen alle Länder partizipieren können. Die Container-Plattform spannt eine homogene Betriebsumgebung über die im Justiznetzwerk verfügbare föderale Infrastruktur und ist damit skalierbarer und resilienter. Die Justiz kann dabei souverän passgenaue Plattformprodukte auswählen und sowohl in deren Beschaffung als auch im Betrieb signifikante Einsparungen realisieren (vgl. **Kapitel 3.4.7**).

3. Bundeseinheitliches Cloud-Anwendungsgefüge: Auf den standardisierten Plattformdiensten soll in der Justizcloud ein bundeseinheitliches Cloud-Anwendungsgefüge der justizinternen und -externen Domäne entstehen und einheitlich betrieben werden. In der internen Domäne könnten sich insb. alle neuen Fachverfahren und Basiskomponenten sowie zukünftig modernisierte Textsysteme befinden.

Wesentlicher Teil der Justizcloud ist auch ein einheitliches, internes Benutzer- und Berechtigungssystem (IAM). Dieses wird über die Integrationsplattform mit allen Länder-IAMs föderiert, d. h. die Identitäten und deren Verwaltung verbleiben im jeweiligen Land. Das Justizcloud-IAM ist auch Voraussetzung für den modernen SaaS-Ansatz und später zur Schaffung des bundesweiten Datenraums.

Für die externe Domäne kann die Justizcloud eine einheitliche Plattform für den Betrieb der Online-Services der Justiz bereitstellen. Über standardisierte Integrationswege (vgl. 4. Integrationsplattform) böte sich die Möglichkeit, Online-Services einfacher miteinander zu vernetzen und sichere Zugriffsmöglichkeiten für externe Nutzende und Anwendungen (sog. Maschine-zu-Maschine-Kommunikation) über APIs anzubieten. Zudem können auf der Justizcloud viele Synergien rund um die Standardisierung von Online-Services hinsichtlich der eingesetzten Front- und Backend-Technologien sowie Design-Systeme (z. B. barrierefreie UI-Komponenten) gehoben werden.

Eine der größten Synergien wäre auch ein einheitliches externes Benutzer- und Berechtigungssystem (CIAM) auf der Justizcloud. Darin könnte die Justiz die Identitäten und Berechtigungen aller externen Parteien sicher verwalten, moderne Registrierungs- und

Authentisierungsprozesse abbilden sowie durch Self-Services (z. B. Profilpflege und Berechtigungsanfragen) und Föderation (z. B. mit IAMs justizexterner Behörden) signifikant zur Effizienz, Kundenzufriedenheit und Sicherheit beitragen.

Eine detaillierte Betrachtung der Zielanwendungslandschaft für die interne und externe Domäne findet sich in **Kapitel 3.4.2**.

4. Integrationsplattform: Die Integrationsplattform als weiterer Plattformdienst ist ein essenzieller Bestandteil moderner Anwendungslandschaften. Sie unterscheidet sich wesentlich von klassischen Kommunikationsplattformen (vgl. **Kapitel 2.2.1.1**) vor allem durch API- und Event-basierter, anstelle von Nachrichten-basierter Kommunikation. Eine Integrationsplattform bietet nicht nur einen sicheren, nachhaltigen Kanal zur Anbindung lokaler Bestandsanwendungen, sondern ist auch Dreh- und Angelpunkt für die entkoppelte (sog. asynchrone) Kommunikation der Justizanwendungen und Basiskomponenten untereinander.

Die Integrationsplattform ist auch essenziell, um die derzeitige Client-seitige Integration von Anwendungen abzulösen. Sie bietet dabei nicht nur moderne API-Verwaltungs- und Sicherheitsverfahren, sondern enthält auch das sog. API Developer Portal. Damit könnte die Justiz sukzessive interne und externe Justiz-APIs publizieren. Zudem können interne und externe Entwickelnde berechtigt und befähigt werden, digitale Prozesse durch Maschine-zu-Maschine-Kommunikation umzusetzen sowie auf Daten effizient zuzugreifen.

5. Einheitlicher Anwendungsentwicklerarbeitsplatz: Eine zentrale Komponente, um nahtlose Entwicklungs-, Ausbringungs- und Betriebsprozesse (DevOps) für die modernen Justizanwendungen auf der Justizcloud zu ermöglichen, ist die Bereitstellung eines einheitlichen Entwicklerarbeitsplatzes für die Justiz. Durch die Verzahnung von Container-Plattform und Entwicklerarbeitsplatz über eine standardisierte CI/CD-Pipeline werden Entwicklungsverbünde befähigt, Justizanwendungen effizienter, automatisierter und damit signifikant häufiger auszubringen. Entwicklungsverbünde können so schnelleres Feedback zu ihren Anwendungen erhalten und in Zukunft viel kundenzentrierter entwickeln.

Darüber hinaus befähigen der gemeinsame, standardisierte Entwicklerarbeitsplatz und das gemeinsame Justiz-Code-Repository alle Entwicklungsverbünde (inkl. bedarfsweise externe Entwickler) schon während der Entwicklung, Code-Elemente wiederzuverwenden und gemeinsame Schnittstellen früher zu testen. Fehler können so viel früher identifiziert (sog. Shift-left) und deren Behebung so vereinfacht und beschleunigt werden. Zudem können durch Testautomation die Testaufwände im technischen und fachlichen Anwendungsbetrieb

gesenkt werden. Testfälle können als Code hinterlegt und wiederverwendet werden. Dadurch werden v. a. Fachnutzende im Regressionstest entlastet.

Die Automation von Pipeline und Tests sowie die Normierung der Container-Plattform erlaubt auch die effiziente Ausbringung der Justizanwendungen bis in die Produktion. Durch diesen Cloud-nativen Ansatz müssen keine länderspezifischen Anwendungsbetriebe für neue Cloud-Anwendungen aufgebaut werden. Die Entwicklungsverbünde werden befähigt, als Betriebsverbünde zu agieren, um die von ihnen entwickelten Anwendungen auf der Justizcloud einheitlich für alle Länder als SaaS zu betreiben.

Anwendungen können zudem standardisiert entwickelt werden und nutzen normierte Technologien, gemeinsam entwickelte Komponenten (z. B. Basiskomponenten oder Designsysteme) sowie eine gemeinsame Code-Basis, welche im Justiz-Code-Repository läge. Durch den Austausch von Code und Know-how wird auch die Effizienz in der Entwicklung gefördert. Der Einsatz justizspezifischer KI-Copiloten in der Anwendungsentwicklung wäre greifbar und ein erhebliches Effizienzpotenzial. Dabei steigt auch die Sicherheit, weil für jede Anwendung in der Justizcloud-CI/CD-Pipeline umfangreiche Security-Tests fortlaufend mitgeprüft (sog. DevSecOps) sowie in der Entwicklung sanitisierte Bibliotheken und Images genutzt würden. Code-Basis und das Berechtigungssystem für die Entwicklung (sog. Admin-IAM) lägen künftig in Hoheit der Justiz, wodurch auch das Onboarding von Entwicklern effizienter und sicherer wäre.

Dieses technisch-prozessuale Fundament unterstützt damit auch das durch die Länder angestoßene und vom *E-Justice-Rat* im Rahmen der Digitalisierungsinitiative für die Justiz priorisierte Konzept eines perspektivischen Justiz-Softwarehauses (aktuell in Erarbeitung).

6. Kommerzielle Cloud-Umgebung: Im ersten Schritt ist die bundeseinheitliche Justizcloud eine sog. Private Cloud, in der die Kernanwendungen des justiziellen Anwendungsgefüges der Justiz sicher betrieben werden können und in der das Justiznetz eine besondere Vertrauens- und damit Sicherheitsstellung zu den lokalen Legacy-Umgebungen hat. Es ist aber bereits heute absehbar, dass die Justiz für bestimmte Anwendungsfälle auch kommerzielle Cloud-Umgebungen in Ergänzung in Betracht ziehen sollte und mit dem Justizcloud-Konzept auch kann (z. B. Auslagerung großer anonymisierter Trainingsdaten für KI-Modelle oder Verfügbarmachung kommerzieller SaaS-Dienste für alle Länder). Aber auch der Betrieb unkritischer Anwendungen mit geringem Schutzbedarf ist in einer kommerziellen Umgebung denkbar.

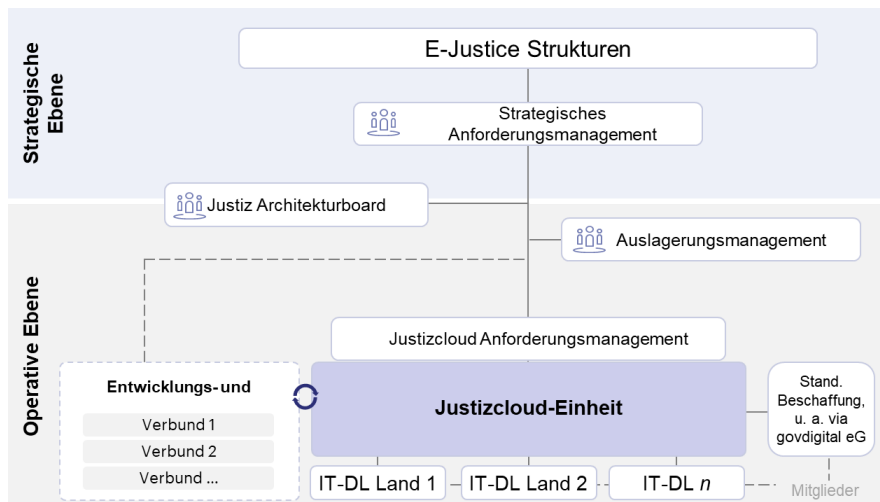
An dieser Stelle ist das Justizcloud-Zielbild bereits nachhaltig aufgestellt, denn das Justiznetz kann perspektivisch per Site-to-Site VPN auch auf einen kommerziellen Cloud-Anbieter ausgeweitet werden. Die Justizcloud könnte dabei sowohl die technischen, fachlichen, als auch rechtlich-organisatorischen und vertraglichen Aspekte einer kommerziellen Public Cloud-Anbindung bündeln und damit die kommerzielle Umgebung für alle Länder gleichermaßen erschließen.

3.3.3 Organisation zum Betrieb der Justizcloud-Plattform

Im Zielbild wird also das moderne Justizanwendungsgefüge von den Entwicklungs- bzw. Betriebsverbünden als SaaS auf der bundeseinheitlichen Justizcloud betrieben, während die physische Infrastruktur, deren Virtualisierung und die lokalen Bestandsanwendungen von den bestehenden IT-Dienstleistern betrieben werden.

Um die bundeseinheitlichen Plattformelemente der Justizcloud aufzubauen und zu betreiben, ist der Aufbau einer eigenständigen **Justizcloud-Einheit** zu empfehlen. Damit die Justizcloud-Einheit effektiv Verantwortung übernehmen kann, muss sie rechtlich-organisatorisch mit eigenem Personal ausgestattet sowie geschäftsfähig sein. Ihr Aufgabenspektrum würde dabei zum einen den Betrieb der Plattformdienste und zum anderen das Vertragsmanagement mit den IT-Dienstleistern (z. B. zum Bezug der virtuellen Infrastruktur) und Produktherstellern umfassen. Zudem würde sie den Aufbau und Betrieb des privaten Justiznetzes zusammen mit der *BDBOS* verantworten. Aufgrund der hoheitlichen Aufgaben dürfte es angezeigt sein, die Gründung einer juristischen Person des öffentlichen Rechts durch die Länder und den Bund näher zu prüfen. Als Rechtsform käme bspw. eine rechtsfähige *Anstalt öffentlichen Rechts* (AöR) in Betracht. Eine Rechtsprüfung hat im Zuge der Untersuchung nicht stattgefunden.

Abbildung 21 | Organisatorisches Zielbild Justizcloud-Einheit



Die Justizcloud-Einheit selbst besteht aus Leitungs-, Architektur- und übergreifenden Funktionen, aber vor allem aus dedizierten Teams, welche die Plattformdienste betreiben und weiterentwickeln. Damit wird das relevante Cloud-Know-how für die Justiz gezielt

an einer Stelle gebündelt. Zudem sollte es dedizierte Brückenköpfe in die Entwicklungs- und Betriebsverbünde geben. Unter Berücksichtigung aller erforderlichen Rollen dürfte die Justizcloud-Einheit ca. 50-60 Mitarbeitende umfassen. (vgl. **Abbildung 21** und **Kapitel 3.6.4**)

Um der Justizcloud-Einheit den Abschluss von Verträgen mit den Infrastruktur-gebenden IT-Dienstleistern zu vereinfachen, könnte auf die bewährten Strukturen und Verfahren der *govdigital eG* zurückgegriffen werden. Damit könnte sie sog. Inhouse-Geschäfte mit den IT-Dienstleistern schließen. Die meisten Justiz-IT-Dienstleister sind bereits Mitglieder der *govdigital eG* und somit direkt beauftragbar. Es wäre damit auch möglich, weitere Dienstleistungen, über die Infrastruktur hinaus, von IT-Dienstleistern zu beziehen. IT-Dienstleister könnten also perspektivisch eigene Dienste je nach Reifegrad in der bundeseinheitliche Justizcloud einbringen – die Justizcloud ist damit inhärent DVS-konform.

Die Justizcloud-Einheit sollte in die bewährten strategischen Strukturen aus *E-Justice-Rat* und der *BLK* eingebettet werden. Um aber in Zukunft rund um die neue, einheitliche Entwicklungs- und Betriebsplattform die Zusammenarbeit zwischen Justizcloud, Entwicklungsverbünden und IT-Dienstleistern zu orchestrieren, wird empfohlen, zwei neue strategische Funktionen außerhalb der Justizcloud vorzusehen.

Ein **strategisches Anforderungsmanagement** bewertet Zukunftsthemen und verteilt gezielt Anforderungen und Umsetzungsbeschlüsse an die relevanten Parteien, wie z. B. Entwicklungsverbünde, das *EGVP-Projektbüro* oder die Justizcloud-Einheit. Unterstützt wird es dabei durch ein Architekturboard, das mit den Lösungs-/ Anwendungsarchitekten der Entwicklungsverbünde und der Justizcloud besetzt ist und das ganzheitliche Zielbild der Justizanwendungslandschaft verantwortet, die dafür notwendige Technologieharmonisierung

und ggf. Transition zur Justizcloud konsequent vorantreibt sowie das Zusammenspiel der Anwendungen der in- und externen Domäne als sog. Enterprise Architektur betreut.

Da die Justiz hoheitliche Aufgaben an die Justizcloud-Einheit übertragen würde, soll die Justizcloud-Einheit darüber hinaus durch ein länderbesetztes Auslagerungsmanagement unterstützt werden.

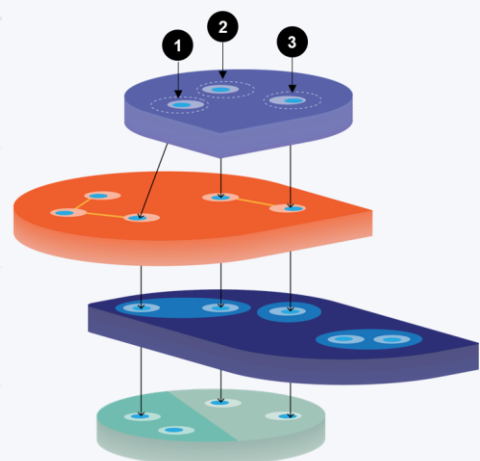
Das beschriebene Zielbild wurde als das fachlich, technisch und rechtlich-organisatorisch machbarste Zielbild ausgewählt und ist passgenau auf die strategische Zielsetzung zugeschnitten. Im Verlauf der Untersuchung wurden dabei in den einzelnen Zielbildebene – fachlich, technisch und rechtlich-organisatorisch – alle zentralen Komponenten und verschiedene Lösungsoptionen detailliert diskutiert und dabei jeweils die machbarste und strategisch wünschenswerteste Option herausgearbeitet. Alle Überlegungen sowie die Ergebnisse in allen relevanten Zielbildebene und -komponenten werden im Folgenden beschrieben.

3.3.4 Integration der Zielbildebene

Gemeinsam ergeben das strategische, fachliche, technische und rechtlich-organisatorische Zielbild ein integriertes Zielbild für die Justizcloud. Die Fachpanels haben an verschiedenen Aspekten der Verzahnung der Zielbildebene gemeinsam gearbeitet. **Abbildung 22** illustriert einige wesentliche Beispiele der Integration der Zielbildebene.

Abbildung 22 | Beispiele der integrierten Zielebene

	Beispiel 1	Beispiel 2	Beispiel 3
Strategische Dimension <i>Warum?</i>	Souveränität stärken	Modernisierung und Standardisierung vorantreiben	Föderale Zusammenarbeit stärken
Fachliche Dimension <i>Was?</i>	Passgenaues, nachhaltiges Cloud-Serviceportfolio nur für die Justiz	Zielbild für eine Green-field-Anwendungslandschaft mit APIs und Microservices	Identity Federation und Access Management Delegation sowie Schaffung eines Datenraums
Technologische Dimension <i>Wie?</i>	Justizeigene Hybride Cloud Plattform auf eigenem virtuellen Netzwerk (SD-WAN*)	Standardisierte IaaS-PaaS-Dienste auf einer einheitlichen Container Plattform	Private Community Cloud auf föderaler Infrastruktur
Rechtl.-org. Dimension <i>Wer?</i>	Justizeigene Cloud-Einheit und -Personalgewinnung	Schaffung strategisches Anforderungsmanagement und Architekturboard empfohlen	Service Desk- und DevOps-Prinzip für Anwendungsbetrieb durch Entwicklungsverbünde



Beispiel 1 zeigt dies eindrücklich am strategischen Ziel zur Stärkung der Souveränität der Justiz. Auf fachlicher Ebene wurde ein passgenaues Cloud-Serviceportfolio für die Justiz definiert. Das heißt, die Justiz kann souverän entscheiden, welche Services die Anwendungslandschaft der Justiz benötigt und muss nicht auf die Entscheidungen Dritter warten. Auch auf technologischer Ebene bilden das justizeigene Netzwerk und die justizeigenen Cloud-Plattformen (insb. Container-Plattform) eine wesentliche Säule der technologischen Souveränität und Unabhängigkeit von Anbietern zur Unterstützung des fachlichen Zielbilds. Abschließend bildet die justizspezifische Personalgewinnung und Bündelung des Cloud-Know-hows in der Justizcloud-Einheit einen wesentlichen Souveränitätsfaktor.

3.4 Fachliche Zielbildebene

Das fachliche Zielbild wurde durch das fachliche Panel entwickelt. Grundlage dafür war das in der Ist-Analyse erarbeitete Verständnis der bestehenden Anwendungslandschaft der internen und externen Domäne (vgl. **Kapitel 2.2.1**). Dabei waren insb. die grundsätzliche Cloud-Readiness, technischen Anforderungen, Abhängigkeiten und Schnittstellen sowie die wesentlichen Herausforderungen (z. B. Ausbringung) der Anwendungen relevant. Dabei sind auch Anforderungen externer Parteien (z. B. *BRAC* und *BNotK*) bspw. an Maschine-zu-Maschine-Kommunikation eingeflossen.

Auch die Arbeitsteilung zwischen Entwicklungsverbünden und IT-Dienstleistern (vgl. **Kapitel 2.2.2**) wurde berücksichtigt sowie Anforderungen aus Zukunftsthemen der Justiz (vgl. **Kapitel 2.2.4**). Wesentliche Leitplanken zur Ausgestaltung des Zielbilds waren die Vision, Mission und strategischen Ziele der Justizcloud (vgl. **Kapitel 3.1**).

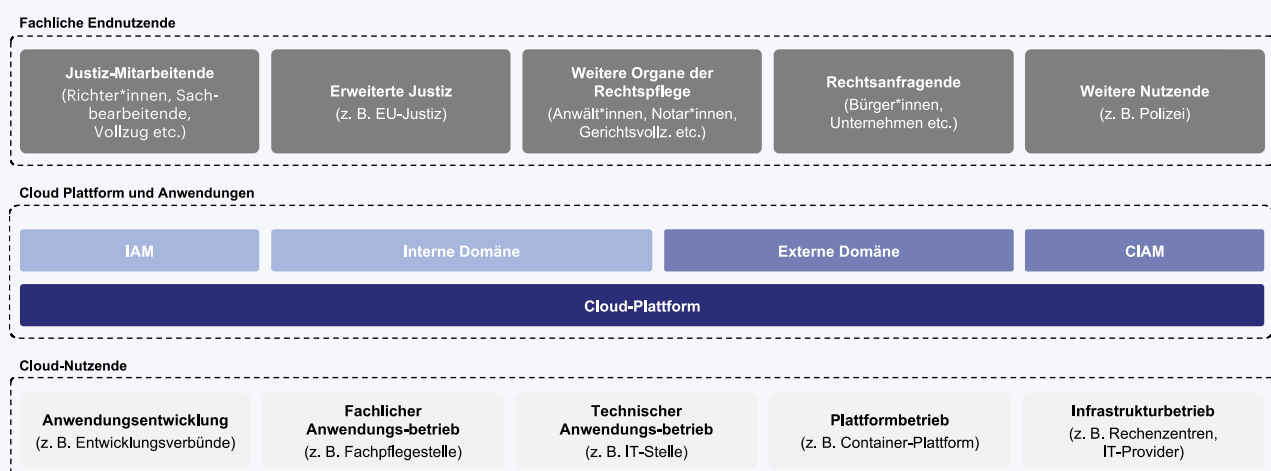
Das fachliche Justizcloud-Zielbild besteht aus verschiedenen Elementen. Zunächst wird eingeordnet, wer die eigentlichen Cloud-Nutzenden sind, welche die fachlichen Anwendungen auf der bundeseinheitlichen Justizcloud betreiben (vgl. **Kapitel 3.4.1**). Kernstück des Zielbilds bildet dann die Justizcloud-Anwendungslandschaft, in der sowohl ein Zielbild für die interne (vgl. **Kapitel 3.4.2.1**) als auch die externe Domäne (vgl. **Kapitel 3.4.2.2**) sowie deren Integration entwickelt wurde. Um das fachliche Zielbild zu befähigen, werden danach wichtige Cloud-Handlungsfelder für die Anwendungen und die Ausgestaltung der Justizcloud-Anwendungsebene vertieft, insb. das Mandantenkonzept (vgl. **Kapitel 3.4.3**), das Schnittstellenkonzept (vgl. **Kapitel 3.4.4**), das Datenkonzept (vgl. **Kapitel 3.4.5**) sowie das Identitäten-, Berechtigungs- und Administrationskonzept (vgl. **Kapitel 3.4.6**). Abschließend wird auf Basis des Zielbilds und der Anforderungen der Anwendungslandschaft eine Serviceportfoliostrategie und ein erster Servicekatalog für die Justizcloud entwickelt (vgl. **Kapitel 3.4.7**).

3.4.1 Abgrenzung Cloud-Nutzende

Eine Cloud-Umgebung ist im Grunde zunächst wie ein ungenutztes Grundstück. Der Wert von Cloud entsteht v. a. durch Anwendungen, die auf der Cloud entwickelt und betrieben werden, in diesem Sinnbild also mit der Entscheidung, wie das Grundstück genutzt werden soll und vor allem durch wen es „bestellt“ bzw. „bebaut“ wird. Daher waren in der Zielbildentwicklung diejenigen zu involvieren, die die bundeseinheitliche Justizcloud nutzen werden.

Es gibt zwei Typen von Cloud-Nutzenden. Erstens die Anwendungsentwickler- (z. B. Entwicklungsverbünde) und Anwendungsbetriebsteams (z. B. aktuell technischer Anwendungsbetrieb beim IT-Dienstleister). Zweitens die Cloud-Betreibenden (z. B. Container-Plattform) und Infrastrukturteams (z. B. Justiznetzwerk) (vgl. **Abbildung 23**).

Abbildung 23 | Abgrenzung Cloud-Nutzende



Die Anwendungsentwickler sind im Justizkontext die Entwicklungsverbünde, die z. B. durch den einheitlichen Anwendungsentwicklerarbeitsplatz mit einer modernen CI/CD-Pipeline sowie einer einheitliche Ausbringungsumgebung profitieren. Der Anwendungsbetrieb untergliedert sich typischerweise in den fachlichen Anwendungsbetrieb (z. B. Fachpflegestellen, First-/ Second-Level Support) und den technischen Anwendungsbetrieb (z. B. Third-Level Support), welcher bspw. bei schwerwiegenden Problemen eingreift oder Software-Release-Updates koordiniert sowie die Schnittstelle zum Infrastruktur-/ Plattformbetrieb bildet. In der Justizcloud treffen sich Entwicklung sowie der fachliche und technische Anwendungsbetrieb auf einer Plattform. Durch die Befähigung des DevOps-Ansatzes können sich somit Entwicklung und Betrieb nahtlos integrieren und so zu sog. Betriebsverbünden entwickeln.

Den zweiten Typus von Cloud-Nutzenden bilden die Cloud-Plattform- und Infrastrukturateams. Diese entwickeln und betreiben die Justizcloud-Plattformdienste, d. h. die verschiedenen Plattformkomponenten wie das Admin-IAM sowie die Container-, Daten- und Integrationsplattform. Außerdem stellen sie den Anwendungsentwicklerarbeitsplatz bereit und betreuen das Justiz-Code-Repository sowie die CI/CD-Werkzeuge, aber auch Monitoring- und Logging-Komponenten. Bei den Infrastrukturteams muss im Kontext einer Private-Community-Justizcloud berücksichtigt werden, dass es hier zwei Rollen gibt. Für die physische Infrastruktur und deren Virtualisierung sind ausgewählte IT-Dienstleister (sog. Knoten-Provider) verantwortlich. Die Justizcloud-Infrastrukturteams verantworten bspw. Datenbank- und Netzdienste auf der IaaS-Ebene, welche auf virtueller Infrastruktur betrieben werden.

Nicht als Cloud-Nutzende gelten die Endnutzenden von Cloud-Anwendungen, d. h. Justizmitarbeitende (z. B. Richter, Rechtspflegende) bzw. auch die externen Endnutzenden (z. B. Bürger, Notare, Rechtsanwälte). Endnutzende profitieren zwar von modernen Cloud-Anwendungen bspw. durch höhere Verfügbarkeit und Performanz oder auch durch häufigere Releases neuer Features. Sie nutzen aber nicht die Justizcloud an sich, sondern nur die Anwendungen, die die Entwicklungsverbünde auf der Cloud-Plattform ausbringen.

Im fachlichen Panel wurden die Anforderungen der Entwickler und Betreiber moderner Justizanwendungen aus der Ist-Analyse ausgewertet und Implikationen für das Zielbild abgeleitet. So ist bspw. der Bedarf für den integrierten Entwicklerarbeitsplatz priorisiert und detailliert worden (vgl. **Kapitel 3.5.6**). Neben den Anforderungen der Cloud-Nutzenden sind auch die technischen Anforderungen der künftigen Cloud-Anwendungen in die Zielbildentwicklung und insb. den Justizcloud-Servicekatalog (vgl. **Kapitel 3.4.7**) eingeflossen.

3.4.2 Justizcloud-Anwendungslandschaft

Das Zielbild für die Justizcloud-Anwendungslandschaft soll „Greenfield“, d. h. von Grund auf neu, für die modernen, Cloud-fähigen Fachverfahren der Justiz, und alle künftig hinzukommenden Anwendungen (bspw. aus Zukunftsthemen) konzipiert werden. Damit sollen bestehende Komplexitäten der Legacy-IT (z. B. monolithische Verfahren, enge Kopplungen, geringe Flexibilität und hohe Pflegeaufwände) von Beginn aus der Justizcloud herausgehalten werden. Eine schrittweise Transition zur Cloud durch eine sukzessive Modernisierung und/oder Abschaltung von Bestandsanwendungen ist möglich und explizit gewünscht. Das Tempo für die Modernisierung bestimmt die strategische Ebene.

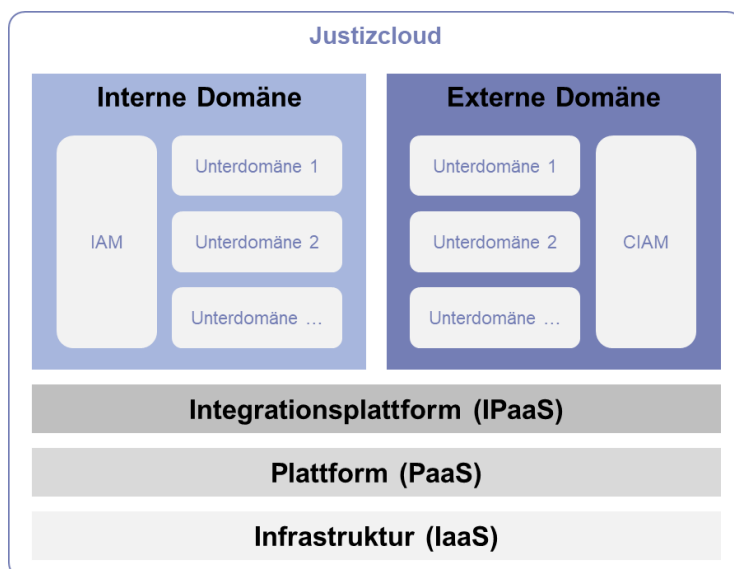
Die Konzeption des Zielbilds erfolgte auf Basis der Standards und Best Practices moderner Cloud-Anwendungsentwicklung nach den Prinzipien des Domain-Driven Design (DDD).

Dabei werden Geschäftsprozesse einer Organisation zunächst in unabhängige Domänen unterteilt. In der Justiz könnte man auf der obersten Ebene zwei Domänen unterscheiden: eine für interne Prozesse (etwa Verfahrensverwaltung) und eine für externe Prozesse (etwa Veröffentlichung von Registerdaten). Unter diesen Domänen können auch weitere Subdomänen wie z. B. für verschiedene Gerichtsbarkeiten definiert werden.

Im *DDD* werden Anwendungen einer Domäne so geschnitten, dass sie ausschließlich Geschäftslogik und Daten beinhalten, die für die spezialisierten Aufgaben ihrer Domäne erforderlich sind (sog. *bounded context*). Zudem haben die einzelnen Domänen ggf. unterschiedliche Anforderungen an Datenhaltung, Netzwerksicherheit, Betrieb, Authentisierung und Autorisierung, etc. Dabei können querschnittliche Anwendungen (z. B. Basiskomponenten), die Funktionalität für verschiedene Subdomänen bereitstellen, auch in eigenen Subdomänen gebündelt werden.

Die Anwendungen verschiedener Domänen können miteinander kommunizieren und Daten austauschen. Die Integration erfolgt dabei allerdings nicht direkt (sog. Punkt-zu-Punkt) zwischen einzelnen Anwendungen, sondern entkoppelt über eine Integrationsschicht. Dabei können je nach Bedarf z. B. APIs, Events oder Messages genutzt werden (**vgl. Kapitel 3.4.4**).

Abbildung 24 | Justizcloud-Domänenmodell



Das Domänenmodell für die Anwendungslandschaft der Justizcloud wurde daher auf der obersten Ebene in eine interne und externe Domäne unterteilt (vgl. **Abbildung 24**). Beide Domänen können dabei in verschiedene Sub-Domänen, z. B. Funktionsblöcke wie Fachverfahren oder Basiskomponenten etc., unterteilt werden und verfügen jeweils über ein dediziertes Benutzer- und Berechtigungssystem (IAM für interne

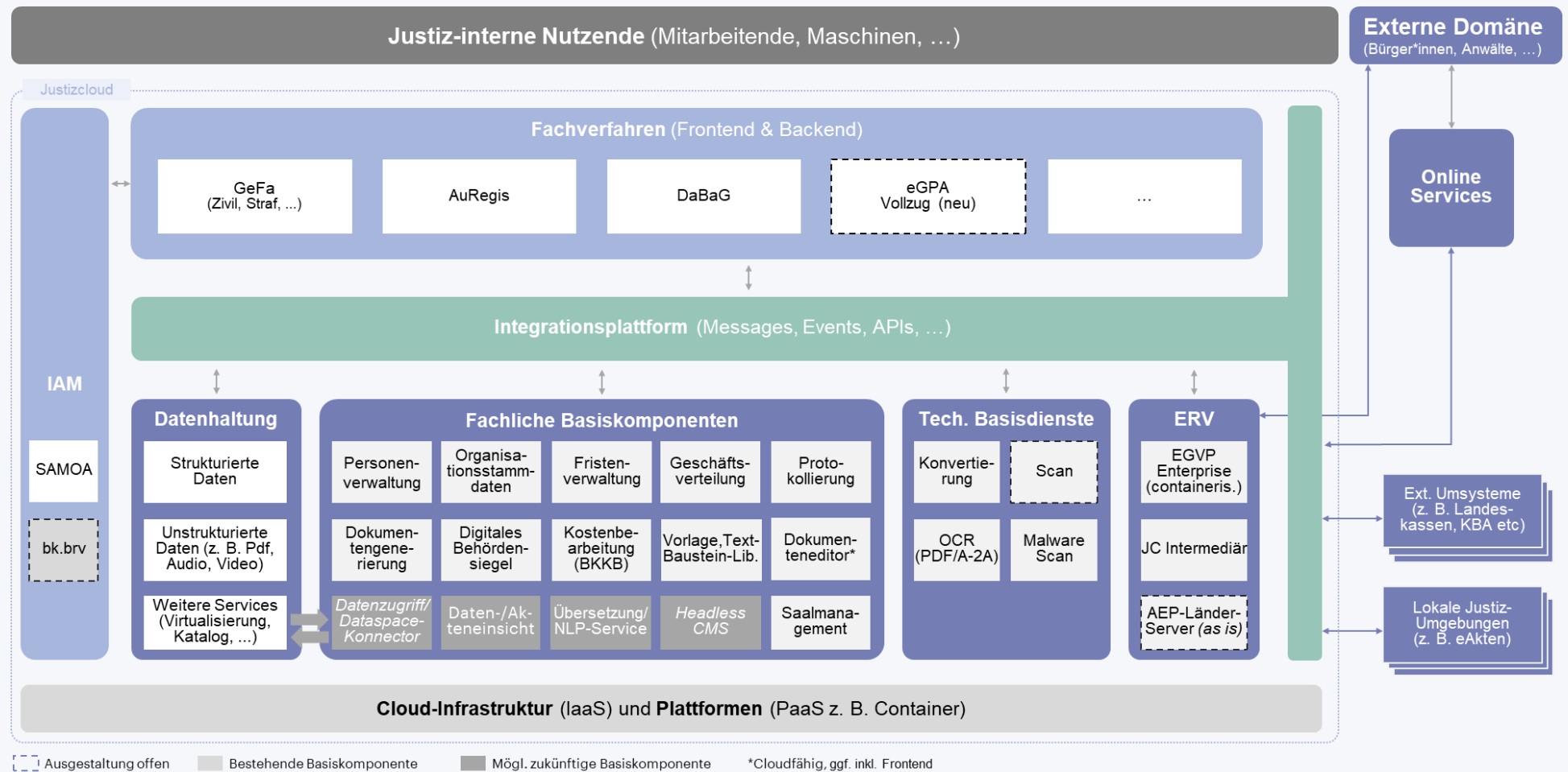
Nutzende und CIAM für externe Nutzende). Die interne und externe Domäne kommunizieren dabei sicher und entkoppelt über eine Integrationsplattform. Alle vorgenannten Elemente nutzen die einheitlichen Plattform- (PaaS) und Infrastrukturdienste (IaaS) der

Justizcloud. Im Folgenden werden die Zielbilder für die Anwendungslandschaft der internen (vgl. **Kapitel 3.4.2.1**) und externen Domäne (vgl. **Kapitel 3.4.2.2**) vertieft.

3.4.2.1 Anwendungslandschaft der internen Domäne

Die Konzeption der internen Domäne der Justizcloud-Anwendungslandschaft erfolgte auf Basis der in der Ist-Analyse erhobenen Anforderungen aus der Bestandslandschaft sowie den Zukunftsthemen. In der Ist-Analyse wurden acht wesentliche Funktionsblöcke identifiziert, die auch im Justizcloud-Zielbild wiederkehren. In jedem Block wurden gemäß dem „Greenfield“-Ansatz nur Anwendungen aufgenommen, die entweder bereits Cloud-fähig sind, aktuell für einen Cloud-Betrieb modernisiert werden oder für das Funktionieren der Gesamtlandschaft essenziell sind und daher noch Cloud-fähig gemacht werden müssen.

Abbildung 25 | Zielbild Anwendungslandschaft der internen Domäne



Kern des Zielbilds der Anwendungslandschaft für die interne Domäne bildet der Funktionsblock der **Fachverfahren** mit den Cloud-nativ entwickelten, modernen Anwendungen wie *GeFa*, *AuRegis* und künftig voraussichtlich auch *dabag*. (vgl.

Abbildung 25) Zudem könnte eine neue Gefangenenpersonalakte (vgl. **Kapitel 2.2.4** siehe Zukunftsthemen) als weiteres Cloud-fähiges Fachverfahren hinzukommen. Die elektronischen Verfahrensakten (eAkten-Systeme) wurden in der Ist-Analyse als nicht Cloud-fähig eingestuft und sind daher in einer ersten Ausbaustufe nicht für einen Betrieb in der Justizcloud vorgesehen. Stattdessen ermöglicht das Zielbild, Cloud-Verfahren mit den eAkten in den lokalen Justizumgebungen über die Integrationsplattform zu integrieren.

Die Zugriffsverwaltung für die Cloud-Anwendungen der internen Domäne soll durch ein einheitliches IAM erfolgen, anstelle dies, wie in der Bestandswelt, in jede einzelne Anwendung zu integrieren. Im Entwicklungsprojekt *GeFa* wird dafür bereits mit der Entwicklung von *SA-mOA* und der IAM-nahen *Basiskomponente Benutzerrechteverwaltung (bk.brν)* wichtige Vorarbeit geleistet, um bspw. moderne Authentisierung und einheitliche Autorisierung nach OAuth 2.0 zu ermöglichen.

Im Sinne der serviceorientierten Architektur umfasst das Zielbild auch einen Funktionsblock für **fachliche Basiskomponenten**. Dies sind Anwendungen, die querschnittliche Dienste für die o. g. Fachverfahren oder andere Basiskomponenten bereitstellen. Die modernen Justizfachverfahren benötigen diverse Basiskomponenten, um ihre volle Funktionalität bereitzustellen. Für einen Cloud-Betrieb der Fachverfahren ist es daher notwendig, die Anwendungen nicht isoliert, sondern gemeinsam in einem Anwendungsgefüge mit den Basiskomponenten zu betrachten. *AuRegis* benötigt bspw. Zugriff auf die Personenverwaltung oder einen Dienst zur Kostenbearbeitung. Damit das Zusammenspiel aus Fachverfahren und Basiskomponenten funktioniert, ist es erforderlich, beide „nah beieinander“ in der Justizcloud zu betreiben. Aktuell sind aber noch nicht alle Basiskomponenten Cloud-fähig bzw. -ready. Einige, wie z. B. *BKKB*, könnten schon heute gemeinsam mit *AuRegis* per CI/CD ausgebracht und auf einer Cloud-Umgebung betrieben werden. Andere, wie z. B. die Textsysteme *e2T* und *bk.text*, müssten noch modernisiert werden. Im Zielbild wurden daher, anstatt bestehende Anwendungen bzw. Komponenten zu benennen, bei einigen Basiskomponenten nur die fachliche Funktion aufgeführt, die in der Justizcloud abgebildet werden muss (z. B. Vorlagen, Textbaustein-Library und Dokumenteneditor). An einigen Stellen wurden vom Fachpanel auch neue, noch nicht existierende Basiskomponenten definiert, die für eine moderne interne Anwendungslandschaft essenziell erschienen (vgl.

Abbildung 25 in grau). Dazu gehören bspw. Dienste wie ein modernes Content-Management-System (CMS) sowie Komponenten für Spracherkennung oder modernen Datenzugriff. (vgl. **Kapitel 2.2.4**).

Teilweise besteht auch die Möglichkeit, verschiedene Basiskomponenten je Land in der Justizcloud zu betreiben. Bspw. könnte je nach Anforderung ein anderes Textsystem an die bundeseinheitlichen Fachverfahren „angeschlossen“ werden. Langfristig ist jedoch eine Einheitlichkeit und Konsolidierung der Anwendungen zu empfehlen.

Als wichtige Querschnittsanforderung aller modernen Anwendungen und Basiskomponenten sowie vieler Zukunftsthemen ist auch der Betrieb einer modernen, Cloud-nativen Datenhaltung vorgesehen. Diese bietet Justizanwendungen sowohl strukturierte (sog. relationale) als auch unstrukturierte (sog. objektorientierte bzw. noSQL), Cloud-native, skalierbare Datenhaltungslösungen sowie moderne Werkzeuge z. B. zur Datenkatalogisierung (sog. Metadaten-Management) und -virtualisierung (vgl. **Kapitel 3.4.5**).

Im Gegensatz zur Integration von Anwendungen in der Bestandslandschaft sollen in der Justizcloud vor allem moderne Integrationsmuster wie RESTful-APIs und Event-basierte Kommunikation Einzug finden. Anstelle direkter Punkt-zu-Punkt-Verbindungen erfolgt die Kommunikation zwischen Anwendungen, Basiskomponenten sowie in die externe Umgebung über eine moderne **Integrations-Plattform**, die u. a. ein modernes Cloud-natives API-Management Gateway sowie einen Event Hub beinhaltet. Details hierzu sind im Schnittstellenkonzept zusammengefasst (vgl. **Kapitel 3.4.4**).

Ein weiterer Funktionsblock ist der *ERV*, über den die Justizcloud elektronische Nachrichten empfangen bzw. senden könnte. Daher ist auch der Betrieb eines „EGVP-Knotens“ und eines Justizcloud-Intermediärs vorgesehen. Beide sind gem. Ist-Analyse noch nicht Cloud-ready, eine Modernisierung ist aber geplant.

Im Rahmen des *ERV* müssen auch einige komplementäre **technische Basisdienste** wie PDF-Konvertierung und Malwareprüfung in der Justizcloud betrieben werden.

Alle vorgenannten Komponenten nutzen bundeseinheitliche Justizcloud-IaaS- und -PaaS-Dienste, insb. die Container-Plattform, für Cloud-native, containerisierte Bestandteile. Diese Ebenen werden im technischen Zielbild detailliert (vgl. **Kapitel 3.5**).

3.4.2.2 Anwendungslandschaft der externen Domäne

Wie in der Ist-Analyse beschrieben (vgl. **Kapitel 2.2.1**), weist auch die Domäne der Online-Services der Justiz ähnliche fachliche und technische Herausforderungen wie die

Anwendungslandschaft der internen Domäne auf. Durch die hohe Heterogenität der Online-Services (z. B. im Interaktions- und Schnittstellenmanagement sowie in der technischen Architektur und Benutzer- und Rechteverwaltung) werden nur wenige Synergien in Entwicklung und Betrieb von Online-Services gehoben, obwohl ähnliche Anforderungen bestehen.

Online-Services werden bereits auf dem Justizportal (*justiz.de*) als Verlinkung aufgeführt, bieten aber in Richtung der Endnutzenden eine wenig moderne und einheitliche Nutzendenerfahrungen. Der getrennte Betrieb von Online-Services in einzelnen Ländern führt zu signifikanten Redundanzen, geringer Einheitlichkeit und mangelnder Nachnutzung gemeinsamer Komponenten.

Die Justiz hat die Notwendigkeit eines einheitlichen, modernen Portals für die Bereitstellung von Online-Services bereits erkannt und will mit dem *Justizportal Deutschland (Arbeitstitel)* eine moderne Plattform schaffen, um ein modernes Service-Ökosystem für externe Nutzende wie Bürger bereitzustellen (vgl. **Kapitel 2.2.4**). Allerdings ist eine Modernisierung von Online-Services, insb. solcher, die auf Anwendungen der internen Domäne zugreifen, komplex, solange die Fachverfahren in heterogenen Länderumgebungen betrieben werden. Ein „Umzug“ von Online-Services in eine bundeseinheitliche Justizcloud könnte also signifikante Synergien und Mehrwerte schaffen, die im Folgenden skizziert werden.

Gemeinsame fachliche Funktionen: Viele Online-Services benötigen ähnliche Basiskomponenten, wie z. B. eine Upload-Funktion für das Einreichen von Dokumenten, Chatfunktionen für den direkten Austausch zwischen Justizmitarbeitenden und Endnutzenden sowie Funktionen zur Terminfindung, Veröffentlichung o. ä. Eine Justizcloud könnte solche querschnittlichen Dienste für alle Online-Services einheitlich und kosteneffizienter bereitstellen.

Gemeinsame Frontend-Technologien: Online-Services benötigen häufig moderne Web-Oberflächen, die speziell für verschiedenen Nutzendengruppen angepasst sind. Ein wichtiges Thema ist dabei z. B. die Barrierefreiheit von UI-Komponenten sowie justizweit einheitlicher Designelemente für eine einheitliche Nutzendenerfahrung. Diese könnten über ein Justizcloud-Code-Repository (vgl. **Kapitel 3.5.6**) für alle Online-Service-Entwickler bereitgestellt werden und somit eine höhere Standardisierung und Effizienz erzeugen.

Gemeinsame Backend-Technologien: Viele Online-Services haben ähnliche Architekturen und technische Anforderungen. Aktuell müssen die Entwicklungs- und Betriebsteams jeweils eigenständig passende Infrastruktur und Plattformen wie Datenbanken, Content-Management-Systeme oder CI/CD-Werkzeuge aufbauen. Auch werden unterschiedliche, teils veraltete Programmiersprachen verwendet. Eine Modernisierung von Online-Services kann

mit der Vereinheitlichung von Backend-Technologien sowie einer Vereinheitlichung der Betriebsplattform für Online-Services kombiniert werden. So können Aufwände für deren Ausbringung drastisch gesenkt und durch die Standardisierung die Pflege vereinfacht und Sicherheit (z. B. durch einheitliche Penetration-Test-Standards) verbessert werden. Gerade Online-Services haben durch ihre externe Exponiertheit ein hohes Risiko, Lastspitzen oder gar DDoS-Attacken zu erfahren und müssen besondere Sicherheitsanforderungen erfüllen. Diese Aufwände zu standardisieren und zentral wahrzunehmen kann nicht nur die Performance, sondern auch Sicherheit der externen Domäne insgesamt steigern.

Gemeinsames Benutzer- und Berechtigungsmanagement: Gerade moderne, personalisierbare Online-Services benötigen ein umfassendes Identitäten- und Berechtigungsmanagement für externe Zugriffe (CIAM), um Nutzende sicher und komfortabel authentisieren und berechtigen zu können. Dazu gehört bspw. die Möglichkeit zum SSO inkl. der Einbindung bzw. Föderation externer Identitäten-Provider (IdP) wie z. B. *Bund-ID eID* für Bürger, von Notaren (*BNotK* IdP), Rechtsanwälten (*BRAK* IdP), Unternehmen und anderen Behörden (z. B. Polizei). Der Aufbau eines modernen CIAM ist notwendig, weil *SAFE-public* nicht zukunftsfähig ist (bspw. keine Multi-Faktor-Authentisierung, Föderation von Identitäten, einfache Integrationsmöglichkeiten, Pflege von Berechtigungen, Self-Service uvm.) und analog der internen Domäne ein *SAMOA-public* aussteht. Dieses CIAM könnte bundeseinheitlich in der Justizcloud für alle Online-Services, ggf. sogar als moderne SaaS-Lösung, bereitgestellt werden.

Gemeinsame Fachverfahrensintegration: Einige Online-Services sind mit den Anwendungen der internen Domäne und damit derzeit mit diversen Landesumgebungen individuell integriert. Gleichzeitig steigen die Anforderungen daran, Daten der Justiz bereitstellen zu können (z. B. als GraphQL-Schnittstelle) und externen Parteien vermehrt die Möglichkeit einer Maschine-zu-Maschine-Kommunikation über APIs („Justiz-API-Ökosystem“) bieten zu können. Für solche modernen Integrationen kann die Justizcloud eine bundeseinheitliche Integrationsplattform, aber insb. sichere und performante Integrationsmuster zwischen Online-Services innerhalb der externen Domäne und zur Integration in die Cloud-Anwendungen der internen Domäne bereitstellen.

Gemeinsame Entwicklung und/ oder Betrieb: Wie für die interne Domäne kann in der Justizcloud die Entwicklung und der Betrieb von Online-Services bundeseinheitlich auf standardisierter Infrastruktur und einem standardisierten Entwicklerarbeitsplatz inkl. moderner Werkzeuge wie CI/CD-Tools erfolgen.

Aus den Synergiepotenzialen für Online-Services ist ein Zielbild für die externe Domäne entstanden, das wesentliche mögliche Komponenten einer Online-Service-Plattform der Justiz zusammenfasst (vgl. **Abbildung 26**).

Der Zugriff auf Online-Services würde durch ein modernes CIAM über Multi-Faktor-Authentisierung und SSO einheitlich und sicher erfolgen. Ein modernes CIAM böte dabei viele Möglichkeiten für Nutzende über Self-Services eigene Rechte anzufragen, ein personalisiertes Benutzerprofil zu pflegen sowie auch Identitäten der eigenen Organisation (z. B. Notare) in der Justiz nutzen zu können (sog. Föderation). Das Justizcloud-CIAM könnte dabei verschiedene Identity Pools für die verschiedenen Nutzendengruppen wie Unternehmen, Bürger sowie Identitäten von Notaren und Rechtsanwälten anbinden. Zudem könnte das CIAM sowohl Identitäten von natürlichen Personen (user-to-application (U2A)) als auch von Maschinen (application-to-application (A2A)) authentisieren und berechtigen.

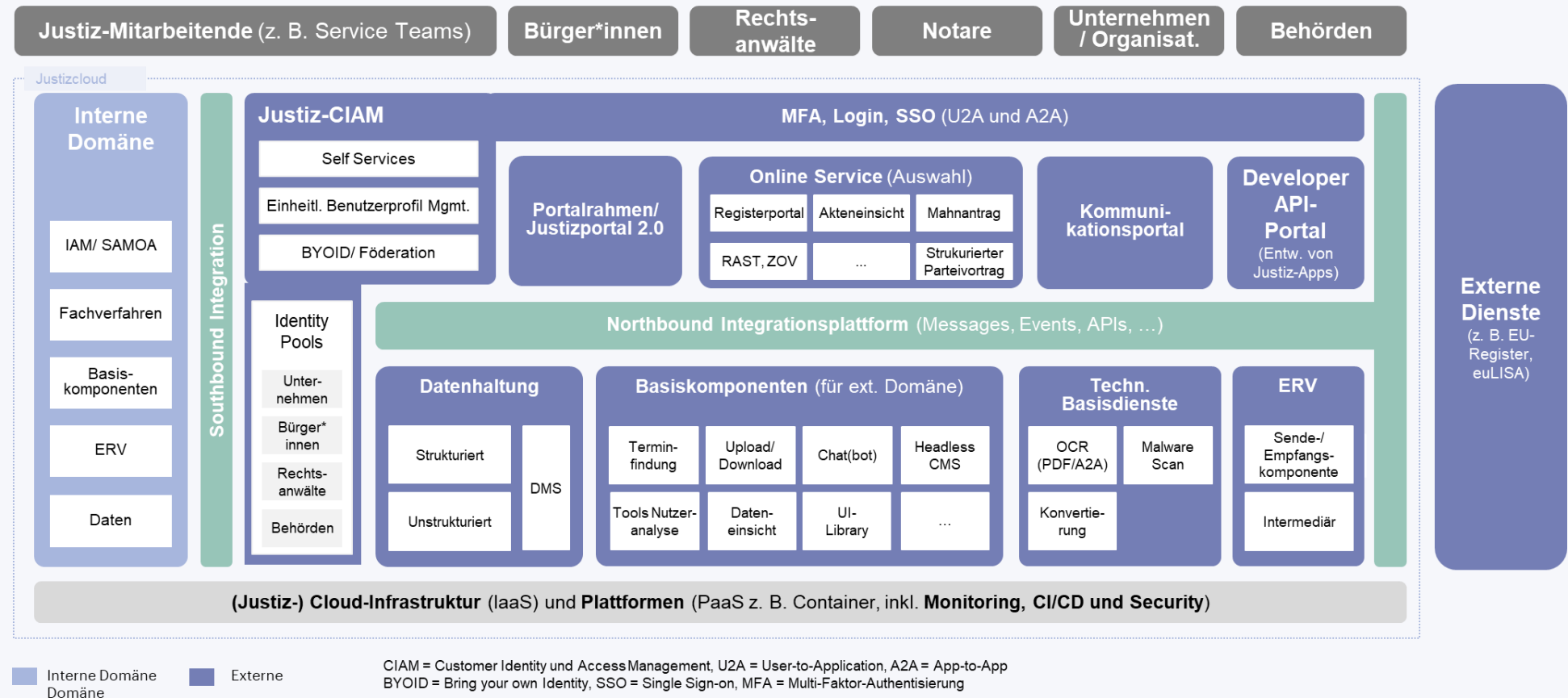
Kernelement der Plattform ist ein einheitlicher Portalrahmen, der eine moderne Nutzeroberfläche und einheitliche UI-/UX-Elemente für verschiedene Online-Services bereitstellt und eine Personalisierung je nach Nutzendengruppe bzw. Nutzenden bietet.

Die Geschäftslogik der einzelnen Online-Services würde in containerisierten, Microservice-basierten, Event-getriebenen und damit echtzeitfähigen Anwendungen auf der Justizcloud und somit auf standardisierter, skalierbarer und einheitlicher Infrastruktur betrieben werden.

Für querschnittliche Funktionen würde zum einen eine standardisierte Kundenschnittstelle als Kommunikationsportal bspw. den Dokumentenaustausch, Support etc. mit Nutzenden der Plattform ermöglichen. Für querschnittliche Funktionalitäten würden Basiskomponenten wie z. B. Terminfindung, Upload/ Download oder ein Content-Management-System bereitgestellt. Zusätzlich können Datendienste für unstrukturierte und strukturierte Datenhaltung bereitgestellt werden, um bspw. eingereichte oder von der Justiz bereitgestellte Daten und Dokumente zwischenzuspeichern. Ein ERV-Knoten erlaubt, klassische *EGVP*-Nachrichten in der externen Domäne sowohl zu empfangen als auch zu verschicken.

Über ein API-Developer-Portal könnten die modernen Schnittstellen der Justiz (sog. Justiz-APIs) publiziert, von Dritten, z. B. den Herstellern von Rechtsanwalts- oder Notarsoftware, übersichtlich eingesehen, beantragt und eingebunden werden. Das CIAM steuert dabei, welche externen Entwickler Zugriff auf welche API haben.

Abbildung 26 | Zielbild Anwendungslandschaft der externen Domäne



Die Integration zwischen den einzelnen Online-Services sowie mit Anwendungen der internen Domäne erfolgt wiederum entkoppelt über die Integrationsplattform mittels API-, Message- und Event-basierten Mustern, je nachdem, wie es die internen Anwendungen benötigen. Hierbei steuert das interne IAM, welche API auf welche interne Anwendung zugreifen darf und mit welchen Berechtigungen.

3.4.3 Mandantenkonzept für Anwendungen

Mandantenfähigkeit

Mandantenfähigkeit ist ein wichtiges Cloud-Konzept, insb. wenn man SaaS-Services erbringen will. Aber auch auf der Plattformebene spielt Mandantenfähigkeit eine tragende Rolle. Mandantenfähigkeit bezeichnet die Fähigkeit von Anwendungen (oder Plattformen) aus einer Instanz heraus verschiedenen Nutzengruppen bzw. Organisationen zu bedienen. Jede bringt dabei jeweils eigene Konfigurationen, Daten und Identitäten mit.

Bisher besteht in der Justiz keine einheitliche Definition des Begriffs Mandantenfähigkeit und es bestehen daher viele verschiedene Umsetzungen. Viele (Alt-)Anwendungen sind nicht mandantenfähig und müssen teilweise pro Gerichtsbarkeit oder pro angeschlossenem Fachverfahren auf eigenen, separaten Instanzen ausgebracht und entsprechend konfiguriert werden. Dadurch entsteht eine sehr hohe Komplexität sowie Redundanz, was schließlich in sehr hohem Betriebsaufwand mündet.

Neue Fachverfahren wie *GeFa* und *AuRegis* werden teilweise schon mandantenfähig entwickelt, weil sie Cloud-nativ skalieren und damit bspw. aus Landessicht mehrere Gerichte aus einer Instanz bedienen können. Diese Anwendungen sind also im Kontext eines länderspezifischen Betriebs mandantenfähig mit jeweils einer Instanz pro Land.

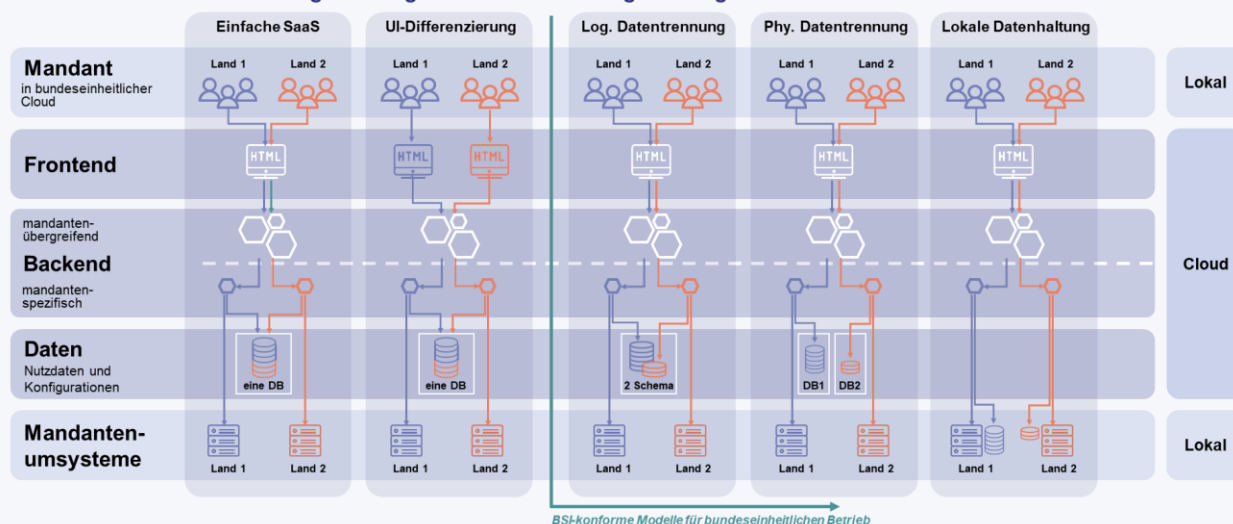
Mit dem Aufbau einer bundeseinheitlichen Justizcloud würde die Möglichkeit bestehen, Anwendungen länderübergreifend zu betreiben, wodurch der Mandant „Land“ hinzukäme. Solche bundesweit mandantenfähigen SaaS-Anwendungen hätten das größte Synergiepotenzial, da alle Länder aus einer skalierbaren Instanz bedient werden könnten und somit weniger personelle und finanzielle Ressourcen für den Betrieb dieser Instanz nötig wären. Es gilt zu beachten, dass bei containerisierten Cloud-Anwendungen die Ausbringung und der Betrieb weiterer Instanzen derselben Anwendung in mehreren Cloud-Tenants oder Namespaces zwar aufwändiger, aber kein Vielfaches des üblichen Aufwands bei klassischen VM-basierten Anwendungen erfordert.

Derzeit ist noch keine Anwendung der Justiz für einen bundeseinheitlichen Betrieb hinreichend mandantenfähig. Um in der Justizcloud die vollen Synergien zu heben, ist daher eine Anpassung von Anwendungen empfehlenswert. Dies kann aber sehr komplex sein und es sollte je Anwendung abgewogen werden, ob eine Anpassung zu länderübergreifender Mandantenfähigkeit fachlich, technisch und wirtschaftlich sinnvoll ist.

Grundsätzlich bestehen verschiedene Architekturen zur Umsetzung von Mandantenfähigkeit. **Abbildung 27** illustriert dies am Beispiel von zwei Ländern, die auf eine Anwendungsinstanz zugreifen. Beide Länder haben unterschiedliche Anforderungen an die Konfiguration einer Anwendung (z. B. Nutzung unterschiedlicher Textvorlagen), greifen auf unterschiedliche Datenbestände zu, müssen mit unterschiedlichen Umsystemen integriert werden und nutzen ggf. unterschiedliche Verschlüsselungszertifikate.

Abbildung 27 | Architekturmodelle für Mandantenfähigkeit

Technisch verschiedene Ausgestaltung von Mandantenfähigkeit möglich



Einfache SaaS-Anwendungen halten die Daten verschiedener Mandanten in einer Datenbank. Dabei wird über die Geschäftslogik und das Zugriffsmanagement der Anwendung sichergestellt, dass Mandanten nur die eigenen Daten sehen und bearbeiten können. Bei Bedarf können pro Mandant unterschiedliche Nutzendenoberflächen bereitgestellt werden, um eine gewisse Differenzierung zu erzielen. Diese Modelle bieten allerdings Sicherheitsrisiken und erfüllen nicht die [BSI-Kriterien](#) an mandantenfähige Anwendungen. Bspw. kann aufgrund der gemeinsamen Datenhaltung nur auf Ebene der Nutzenden und nicht auf Ebene der Anwendungsadministration nach Mandanten unterschieden werden. Ein

technischer Administrator kann grundsätzlich alle Daten der Anwendung einsehen. Eine technische Administration je Mandant ist nicht möglich oder organisatorisch aufwändig. Außerdem können durch Inkonsistenzen in der Datenbank oder Fehler in der Geschäftslogik bzw. in der Zugriffskontrolle unbeabsichtigte Datenzugriffe vorkommen. Auch eine mandantenspezifische Verschlüsselung ist wegen der gemeinsamen Datenhaltung kaum möglich.

BSI-konforme Modelle fordern daher eine durchgängige Mandantentrennung, d. h. sowohl auf Anwendungsebene als auch in der Datenhaltung. Dies kann entweder logisch durch Festlegung mandantenspezifischer Schemata (logische Trennung) oder durch Aufsatz eigener Datenbankinstanzen je Mandant (physische Trennung) erfolgen. Die Datenhaltung ist somit segregiert und bspw. Fehler in der Anwendung können Daten nicht mehr kompromittieren. Zudem lassen sich die Daten jeweils mandantenspezifisch verschlüsseln, wobei jeder Mandant eigene kryptografische Schlüssel hält (Bring- vs. Hold-your-own-key). Bei besonderen Konstellationen gibt es auch die Möglichkeit eine SaaS-Anwendung auf lokal gehaltene Daten zugreifen zu lassen (lokale Datenhaltung sog. Hold-your-own-data). Dies kann aber zu Latenz- und damit Performanzproblemen führen. Moderne Caching-Strategien können diese Herausforderungen teilweise adressieren.

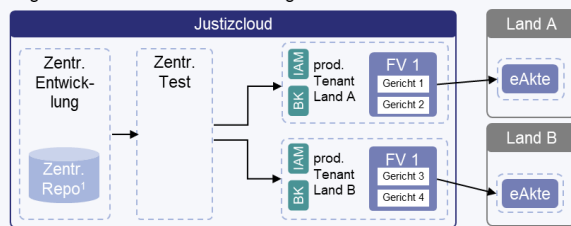
Darüber hinaus muss die Benutzerzuordnung zu Mandanten, z. B. durch getrennte Benutzerverwaltung oder automatisierte Zuordnung, sichergestellt werden. Auch getrennte Protokollierungsmechanismen und mandantenspezifische Log-Auswertungen für Administratoren müssen möglich sein. Die Wirksamkeit der Mandantentrennung muss dabei durch regelmäßige Audits und Penetrationstests nachgewiesen werden.

Mandantenfähiger Cloud-Betrieb

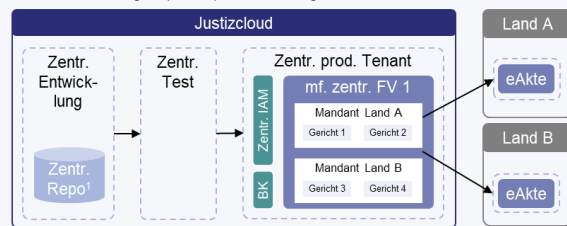
Derzeit gibt es in der Justiz noch keine länderübergreifend mandantenfähigen Anwendungen, die den oben genannten Anforderungen entsprechen. Ein Grund dafür ist, dass bis dato ohne Justizcloud der bundeseinheitliche Betrieb von Anwendungen gar nicht denkbar war. Eine Weiterentwicklung der modernen Anwendungen wie *GeFa* oder *AuRegis* ist aber architekturell grundsätzlich möglich. Allerdings besteht auch die Möglichkeit, Anwendungen, die noch nicht länderübergreifend mandantenfähig sind, in länderspezifischen Tenants zu betreiben.

Abbildung 28 | Multi-Tenant Betrieb vs. Mandantenfähiger Cloud-Betrieb

Option 1: Zentraler Betrieb einer nicht auf BL-Ebene mandantenfähigen sog. multi-instanziierten Anwendung



Option 2: Zentraler Betrieb einer bundeseinheitlich mandantenfähigen (SaaS) Anwendung



Wie in Option 1 von **Abbildung 28** dargestellt, wird dabei für jedes Land ein eigener Tenant aufgebaut und darin eine Anwendung installiert und betrieben. Jeder Tenant muss dabei Umssysteme der Länder wie Basiskomponenten und IAM individuell betreiben, ist aber auch bzgl. Releases autonom zu warten. Dieses Modell ist weniger effizient als der Betrieb einer einheitlichen Anwendung aus einem Tenant (Option 2), da sich geringere Synergien im fachlichen und technischen Anwendungsbetrieb ergeben. Bei Option 2 lassen sich auch Querschnittskomponenten zentral betreiben, sofern sie mandantenfähig sind.

Bereits der Multi-Tenant-Betrieb in der Justizcloud böte erhebliche Effizienzgewinne gegenüber dem aktuellen Betrieb je Land. Denn die Einheitlichkeit von Infrastruktur und Container-Plattform sowie Testautomation und die standardisierte Ausbringung derselben Software in mehrere Tenants via einer gemeinsamen CI/CD-Pipeline mit einem gemeinsamen Repository, adressiert wesentliche Herausforderungen des aktuellen Justiz-IT-Betriebs.

In einer ersten Ausbaustufe der Justizcloud könnte v. a. Option 1, d. h. der Multi-Tenant-Betrieb, gewählt werden, um dann in weiteren Ausbaustufen sukzessive eine Umstellung auf multi-mandantenfähige Anwendungen in einem gemeinsamen Tenant (Option 2) zu forcieren. Mittelfristig sind auch hybride Formen denkbar, in denen parallel zu länderspezifischen Tenants, Querschnittskomponenten in einem gemeinsamen Tenant lägen. So könnten Synergien und Effizienz schrittweise gehoben werden. Aufwand und Nutzen der Umstellung auf volle Mandantenfähigkeit gegenüber einem multi-instanziierten Betrieb in der Justizcloud kann dabei je Anwendung abgewogen werden.

3.4.4 Schnittstellenkonzept

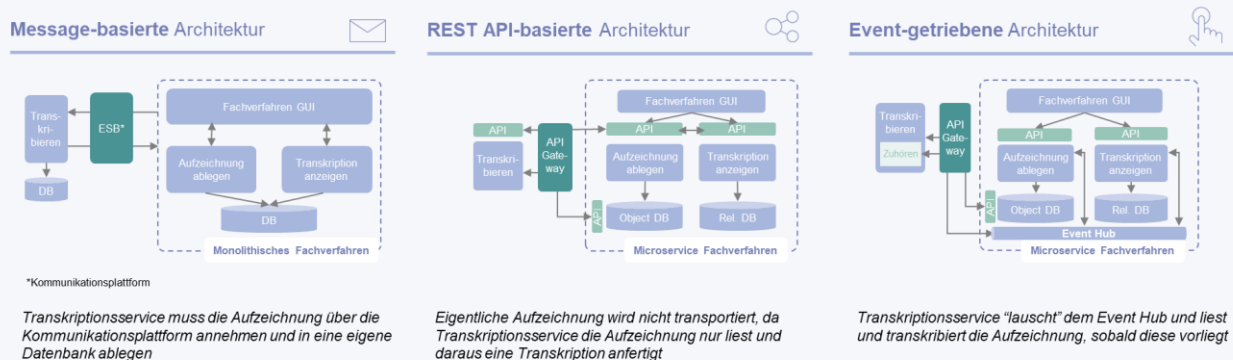
Aktuell findet die Kommunikation von Anwendungen in der Justiz maßgeblich mit Nachrichten (sog. Message-basierte Kommunikation) über Kommunikationsplattformen und den ERV statt. Zur Modernisierung und Flexibilisierung des Justizanwendungsgefüges sollten

ergänzend auch moderne Integrationsverfahren erschlossen werden. Dies sind v. a. moderne APIs (z. B. REST, gRPC) und Event-basierte Kommunikationsmuster, welche auch neue Technologien bzw. Komponenten (z. B. API-Gateway oder Event Hub) erfordern.

3.4.4.1 Schnittstellenarten und -architekturen

Message-basierte Architektur: Bei Message-basierter Kommunikation versenden oder empfangen Anwendungen Nachrichten, z. B. im XML- oder SOAP-Format. Dabei erfolgt der Nachrichtenaustausch entweder direkt (synchron) oder indirekt (asynchron) über eine Kommunikationsplattform (z. B. Enterprise Service Bus (ESB)). Hierfür ist es meist notwendig, die Nachrichten durch spezifische Software zwischen Start- und Zielanwendungen zu konvertieren. Diese Software enthält dabei teilweise komplexe Geschäftslogik (z. B. Übersetzung zwischen zwei Verfahrenssprachen), die fehleranfällig, unflexibel und aufwändig zu warten ist. Über das *XJustiz*-Format standardisiert die Justiz aktuell die Nachrichtenformate.

Abbildung 29 | Typische Integrationsarchitekturen



Auch die Skalierbarkeit und Performanz leiden, denn bei Message-basierter Kommunikation enthält die Nachricht sowohl die Adresse, den Befehl (z. B. fachlichen Zweck der Nachricht) als auch den zu übermittelnden Inhalt (sog. Payload, d. h. Nutzdaten wie Dokumente). Bei großen Nachrichten stößt die Message-basierte Kommunikation daher an technische Grenzen. Mit Blick auf das steigende Datenaufkommen im *ERV* und zukünftige Anforderungen (z. B. digitale Beweismittel, unstrukturierte Daten in Verfahren) ist die Nachrichten-basierte Kommunikation nicht mehr ausreichend. Um zukünftig Skalierbarkeit und Performanz sicherzustellen, wird daher bereits über eine Modernisierung und Vorbereitung technischer Möglichkeiten zur Verarbeitung sehr großer Datenmengen nachgedacht.

Ein weiterer Nachteil des Nachrichtenversands ist, dass mit der Nachricht eine Kopie der Nutzdaten verschickt wird, was insb. bei großen, unstrukturierten Dateien (z.B. großen Akten) zu hohem Traffic und damit Performance-Problemen im Netzwerk sowie bei allen involvierten Systemen entlang der Ende-zu-Ende-Strecke führen kann (bspw. von Intermediär-EGVP über Malwarescanner, Konvertierungsdienst, Kommunikationsplattform bis zur eAkte und Fachverfahren). Darüber hinaus können die Authentizität, Integrität, Aktualität und z. T. auch Vertraulichkeit der Nutzdaten ab dem Moment des Versands nicht bzw. nur teilweise garantiert werden. Der Sender der Nachricht verliert die Datenhoheit über seine Daten.

Moderne, nachrichtenbasierte Technologien wie Message-Queue-Systeme können auch in der Justizcloud genutzt werden. Aber Marktstandard und damit vorrangig für viele Anwendungsfälle im Zielbild sind API- und Event-basierte Integrationen bzw. Technologien.

(REST) API-basierte Architektur: APIs sind standardisierte Schnittstellen, um auf Daten und Services von Anwendungen zuzugreifen. Sie bieten die Möglichkeit, über Standardprotokolle (z.B. http, gRPC oder GraphQL) Daten zu schreiben, abzufragen oder zu verändern (z. B. http GET, PUT, POST, DELETE). API-Aufrufe können synchron und asynchron sein. Bei synchronen Aufrufen belegt die Anfrage Serverressourcen, wartet auf eine Antwort und ermöglicht erst dann einen zweiten API-Aufruf. Bei asynchronen Aufrufen wird dagegen keine Antwort des Servers abgewartet und sie ermöglichen so dem Client direkt weitere Anfragen zu stellen oder Aufgaben wahrzunehmen. Asynchrone APIs können so nahezu beliebig skaliert werden. APIs sind in der Regel standardisiert (z. B. Open API Standard und http-RFC) und damit universell, schnell und flexibel einsetzbar.

APIs sind vielfach auch sicherer als direkte Kommunikationsverfahren, weil man bspw. dem API-Aufruf einen Autorisierungs-Token (vgl. OAuth2.0-Standard) beifügen kann oder die API zwischen Sender und Empfänger per API-Key absichert. API-Zugriffsberechtigungen sind primär Maschine-zu-Maschine Kommunikation und können durch moderne IAMs zentral verwaltet werden. Vorteilhaft ist, dass der Ressource-Server bzw. -Service, auf den zugegriffen wird, nur ein Set von APIs exponiert, auf das Client-Anwendungen, ob Maschine oder Frontend-Client eines menschlichen Nutzers, gleichermaßen, zugreifen können – wenn auch ggf. mit unterschiedlichen Berechtigungen. (REST) APIs können sehr transparent und leicht verständlich dokumentiert und damit publiziert und geteilt werden (z. B. Open-API-Standard bspw. über Tools wie *Swagger*). Sie bieten für Entwickler so einfache Möglichkeiten, ihre Anwendung mit anderen Anwendungen zu integrieren.

Da der API-Aufruf keine Nutzdaten enthält, ist er leichtgewichtiger und damit um ein Vielfaches skalierbarer. Daher werden APIs standardmäßig bei skalierbaren, Cloud-nativen Anwendungen bevorzugt. In einem komplexen Anwendungsgefüge erfolgt die Steuerung von API-Zugriffen zwischen Anwendungen über ein sog. API-Management-Gateway. Dieses bündelt den Umgang mit APIs in der Architektur und dient als zentraler, skalierbarer Knotenpunkt für API-Publikation und Management von API-Zugriffen im laufenden Betrieb. Es übernimmt bspw. das Routing von Anfragen, Authentisierung und Zugriffssteuerung (gemeinsam mit dem IAM) sowie Lastverteilung und verbessert somit die Skalierbarkeit und Sicherheit in der API-Kommunikation. Zudem bieten ein API-Gateway typischerweise viele Funktionen wie Versionierung, Monitoring und Auswertung von API(-Zugriffen). API-Management-Plattformen erlauben zudem den Aufsatz und die Verwaltung von API-Gateways für verschiedenen Domänen, was ein zusätzliches Sicherheitsmerkmal ist. So kann bspw. ein „*Southbound-Gateway*“ die Innenkommunikation der Justiz abbilden und nur dort bestimmte interne APIs veröffentlicht werden, während ein „*Northbound-Gateway*“ die Justiz-APIs für externe Parteien bündeln kann.

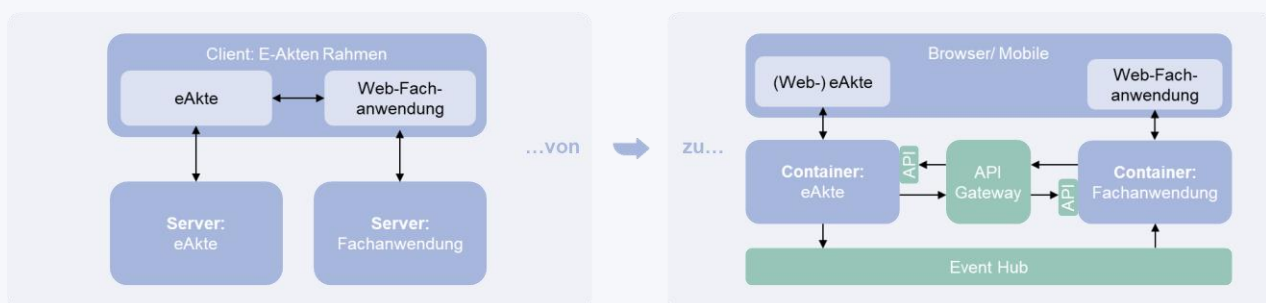
APIs können auch zur Effizienz in der Entwicklung beitragen. Zum einen wird kein Dritter (z. B. ein Kommunikationsplattform-Team) benötigt, um die fachliche Logik der Schnittstelle abzustimmen. Der API-Eigner publiziert seine APIs im API-Gateway und API-Konsumenten können sie dort finden, standardisiert verstehen (vgl. Open-API), testen und Zugriffe beantragen. Zum anderen kommt in modernen Entwicklerteams innerhalb einer Anwendung und auch anwendungsübergreifend der sog. API-First-Ansatz zum Einsatz. Im DDD wird mit dem API-bereitstellenden Team zunächst eine Einigung über die API/ Schnittstelle mit allen Spezifikationen getroffen (z. B. welche http-Befehle erlaubt sind, wie autorisiert wird, welche Parameter möglich sind und wie die Ergebnisausgabe erfolgt, z. B. über Paginierung etc.). Innerhalb einer Anwendung können sich dann Frontend-Teams (verantwortlich für die Single-Page-App oder Micro-Frontend) und Backend-Teams (verantwortlich für die API, Geschäftslogik und Daten des Service) auf diese Schnittstelle (quasi als Vertrag zw. den Teams) beziehen und parallel individuell entwickeln und dagegen testen.

Event-basierte Architektur: Im Gegensatz zu APIs sind Event-basierte Integrationsarchitekturen grds. asynchron und bieten damit besondere Vorteile hinsichtlich Entkopplung, Skalierbarkeit und Performanz. Dabei können Producer-Anwendungen definierte Ereignisse (sog. Events) in einem sog. Event Hub schreiben. Consumer-Anwendungen können dort diese Events abonnieren und damit in Echtzeit auf Ereignisse reagieren. Damit lässt sich das Zusammenspiel verschiedener Anwendungen und Services signifikant verbessern. In

Abbildung 29 ist dargestellt, wie das Zusammenspiel von APIs und Events besonders effektiv für Orchestrierung von Prozessen über mehrere Anwendungen hinweg genutzt werden kann. Dabei erzeugt jede Anwendung bzw. jeder Service zunächst ein Event. Andere können darauf gleichzeitig und somit hoch-skalierbar reagieren und die notwendige Aktion wie bspw. einen API-Aufruf starten oder einfach nur die eigene Datenbasis aktualisieren. Die Anwendungen können so asynchron ihre Aufgaben erledigen und die Flexibilität, Skalierbarkeit und Performanz des Gesamtsystems drastisch verbessern.

Die Verfügbarkeit verschiedener Integrationsverfahren ist also für den Aufbau einer modernen Anwendungslandschaft in der Justizcloud entscheidend. Je nach Anwendungsfall sollte das passende Integrationsmuster gewählt werden. Voraussetzung dafür ist der Aufbau einer Integrationsplattform, die, je nach Anwendungsfall, Messages, APIs oder Events beherrscht. Eine Integrationsplattform besteht daher aus verschiedenen Technologien bzw. Produkten für das Bereitstellen und Betreiben von Message-Queues, API-Gateways und Event-Hubs (vgl. **Kapitel 3.5.4.3.**). Im Folgenden soll die Kombination der modernen Integrationsverfahren zur Lösung eines konkreten Problems in der Ist-Anwendungslandschaft der Justiz illustriert werden (vgl. **Abbildung 30**).

Abbildung 30 | Vergleich Client- vs. Server-Integration für eAkten-Rahmen



Aktuell erfolgt der Austausch von Daten zwischen den eAkten-Systemen (z. B. *e2A*, *eIP*, *eAS*) und dem Fachverfahren (z. B. *GeFa*, *ForumSTAR* oder auch *Textsystem*) innerhalb einer sog. eAkten-Rahmenanwendung auf dem Desktop-/ Client der Justizmitarbeitenden (vgl. **Abbildung 30** links).

Dabei werden sowohl Fachdaten (z. B. Verfahrenskontext über Aktenzeichen/-ID) als auch sicherheitsspezifische Metadaten (z. B. User-Informationen wie SAFE-ID) innerhalb des Rahmens ausgetauscht. Dafür verfügen sowohl die eAkte als auch Fachverfahren über

dedizierte Schnittstellen. Bei Anpassungen von Schnittstellen, z. B. aufgrund neuer Funktionen, müssen oftmals beide Anwendungen angepasst und daher das Zusammenspiel als neue Rahmenanwendungsversion ausgiebig getestet und produktiv auf allen Desktop-/ Clients installiert bzw. ausgebracht (z. B. bei Citrix-Farmen) werden. Dies ist aufwändig, komplex und führt oft zu Problemen, weil bspw. eine der Anwendungen im Aktenrahmen nicht rechtzeitig aktualisiert wurde oder die Anpassung Fehler enthielt. Solche Fehler fallen aufgrund der späten Tests erst spät im Prozess auf, wodurch weitere Verzögerungen eintreten können. Weitere Nachteile der Client-seitigen Integration finden sich in **Kapitel 2.2.1**.

Alternativ könnte eine moderne Architektur mittels APIs und Events die Desktop-/ Client-seitige Integration auflösen und der Datenaustausch zwischen einer modernen, webfähigen eAkte und Fachverfahren auch serverseitig ermöglichen (vgl. **Abbildung 30** rechts).

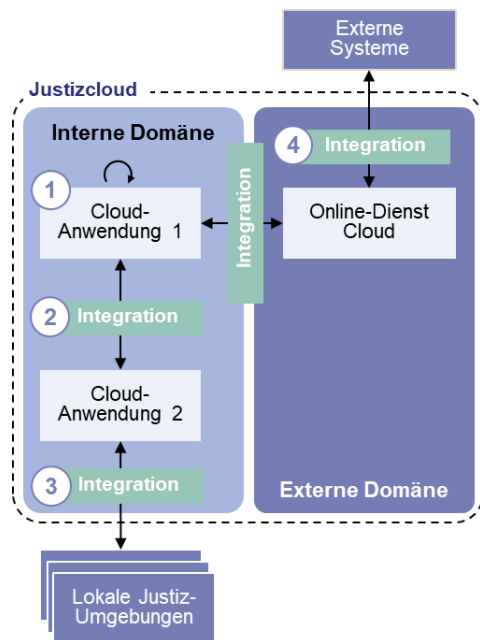
Dabei tauschen eAkte und Fachverfahren Daten per API im Backend über den API-Gateway aus. Dies passiert immer dann, wenn in einer der Anwendungen ein Ereignis (Event, z. B. ein „Klick“) erfolgt. Dabei reagiert die eAkte auf Events im Fachverfahren und das Fachverfahren auf Events in der eAkte. Die Daten könnten so in Echtzeit ausgetauscht werden und beide Anwendungen würden in Echtzeit aufeinander reagieren. Auch die Performanz ist bei dieser Art der Architektur aufgrund hoher Skalierbarkeit der Services und asynchronen Kommunikationsmustern sehr hoch. Somit ist eine flüssige und hoch-performante Arbeitserfahrung gewährleistet. Voraussetzung dafür wäre aber eine Cloud-fähige eAkte. Derzeit sind aber alle eAkten-Systeme nicht Cloud-ready. Das beschriebene Verfahren könnte aber ggf. an der noch zu entwickelnden neuen eGPA(-Plattform) erprobt werden.

Das Anwendungsgefüge würde so auch Endgerät-/ Client-unabhängig aus jedem Browser aufrufbar sein. Auch Entwicklung, Test, Pflege und Weiterentwicklung sowie Ausbringung wären in dieser Architektur deutlich einfacher. Nachteilig könnte sein, dass die Offline-Fähigkeit, die häufig als Anforderung gestellt wird, komplexer umzusetzen ist (bspw. durch moderne, datengetriebene Synchronisation von Datenbeständen).

3.4.4.2 Integrationswege und Architekturprinzipien

Um eine moderne Entkopplung von Anwendungen zu erreichen und somit in Zukunft die Pflege und Flexibilität der Cloud-Anwendungslandschaft gegenüber dem Status Quo zu verbessern, braucht es Architekturprinzipien, die bspw. das Architekturboard für die neue Justizcloud-Anwendungslandschaft durchsetzen könnten. Dabei ist zwischen vier verschiedenen Integrationswegen zu unterscheiden (vgl. **Abbildung 31**).

Abbildung 31 | Überblick Integrationswege



1. Schnittstellen innerhalb von Anwendungen:

Bei Cloud-nativen, Microservice-basierten Anwendungen kommunizieren Microservices innerhalb einer Anwendung (sog. Subdomäne) über Events oder APIs (vgl. **Abbildung 31**). Innerhalb der Anwendungen bzw. Subdomäne wären die Entwicklungsverbünde frei, auch direkte Service-zu-Service-Kommunikation zu nutzen. Die Justizcloud stellt bspw. Basistechnologien, wie einen applikationsspezifischen Event Hub bereit.

2. Schnittstellen zwischen Anwendungen der internen Domäne:

Die anwendungsübergreifende Kommunikation bzw. Integration innerhalb der internen Domäne (Subdomäne-zu-Subdomäne) sollte in der künftigen Anwendungslandschaft

entkoppelt über die Integrationsschicht, d. h. über dedizierte API-Gateways oder Event Hubs, erfolgen. Die Anwendungen publizieren dabei ihre Service-APIs und Events gem.DDD in der Integrationsschicht. Dabei wird kein zusätzliches „Übersetzungspersonal“ in der Integrationsplattform aufgebaut, denn die Nutzenden von APIs und Events kommunizieren direkt mit den Bereitstellern von APIs und Events bei neuen Anforderungen bzw. nutzen die APIs und Events so wie publiziert. Die Integrationsschicht übernimmt dabei wichtige, v. a. technische Sicherheits-, Lastverteilungs-, Monitoring- und Autorisierungsfunktionen. Da in der internen Domäne per Definition v. a. interne Justiz-APIs verwendet werden, sollte bspw. in der Justizcloud ein dedizierter interner API-Gateway (sog. Internal API-Gateway Instanz) betrieben werden, in dem nur interne APIs publiziert sind, der mit den internen IAM- und SIEM-Systemen verbunden ist, die internen API-Bestellungen von internen Nutzenden bearbeitet und somit die interne Kommunikation orchestriert. Das dargestellte Grundprinzip sollte auch für Integrationen innerhalb der externen Domäne (sog. External API-Gateway Instanz) sowie bei Integrationen zwischen Cloud-Anwendungen bzw. Subdomänen der internen mit der externen Domäne (sog. Southbound API-Gateway Instanz). Dies hat den Vorteil, dass immer nur die für den jeweiligen Kontext bzw. für die Domäne notwendigen APIs publiziert sind und mit den jeweils relevanten Authentisierungs- und Autorisierungsverfahren kommunizieren (sog. „Need-to-know“ und „Zero-trust Prinzipien“). Zudem werden die Lasten entsprechend der Domänen verteilt, sodass eine hohe Last in der externen Domäne sich nicht auf die Performanz der internen Domäne auswirkt. Das Architekturboard sollte

darauf achten, dass alle Subdomänen sich an dieses Prinzip halten und sich so sukzessive das interne API-Ökosystem weiterentwickelt.

3. Schnittstellen der internen Domäne zu lokalen Umgebungen: Cloud-native Anwendungen in der Justizcloud müssen bis auf Weiteres mit diversen Bestandsanwendungen in den lokalen Umgebungen der Länder integriert werden. Dies können bspw. andere Justizanwendungen wie die eAkte oder bestehende Fachverfahren, aber auch Anwendungen der Verwaltung, wie z. B. die Landes-Kassensysteme sein. Auch diese Integration sollte künftig über eine dedizierte Integrationsschicht bzw. -plattform erfolgen. (sog. *Legacy-API-Gateway Instanz*). Dabei sind die lokalen Umgebungen der Länder nicht nur auf der http-Ebene (OSI-Layer 6/7), sondern durch das Justizcloud-Netzkonzept (vgl. Netzkonzept) bereits auf OSI-Layer 2/3 abgesichert und entsprechend aus der Justizcloud erreichbar.

Bis auf wenige Ausnahmen (z. B. eAkten) sind die meisten lokalen Anwendungen nur über die bestehenden Kommunikationsplattformen (*e2P* und *eKP*) erreichbar bzw. bieten keine oder veraltete Schnittstellen-/ API-Standards an. Die Integration mit den eAkten kann daher direkt über die Legacy-API-Instanz entkoppelt und gesteuert werden. Dies ist sinnvoll und vorteilhaft, weil jeweils nur die länderspezifischen eAkten-Schnittstellen verwendet („Need to know“) und länderspezifische Sicherheitsmechanismen (z. B. TLS-Zertifikate, IP-Adressen, lokales IAM) umgesetzt werden. Weitere Vorteile bestehen bei der gerichtsspezifischen Steuerung der Kommunikation, denn es muss beachtet werden, dass die eAkten nur auf Gerichtsebene mandantenfähig sind, nicht skalieren und daher meist in vielen Instanzen je Land ausgebracht werden. Das Legacy-API-Gateway muss also ein landesspezifisches Routing beachten, je nachdem mit welchem Gericht und mit welcher lokalen eAkten-Instanz kommuniziert werden soll (vgl. **Kapitel 3.4.4 und 3.5.4.3**).

Bei der Integration mit Verfahren der Bestandswelt über die Kommunikationsplattformen kommuniziert das Legacy-API-Gateway mit der Kommunikationsplattform. Dafür muss die Cloud-Anwendung selbst oder das Legacy-API-Gateway ggf. Nachrichtenformate emulieren (sog. Protokollkonvertierung), die die aktuellen Fachverfahren verstehen und verarbeiten können. Dafür können einerseits Microservices auf dem Legacy-API-Gateway zum Einsatz kommen, die gem. DDD in Hoheit der empfangen Bestandsverfahren (sog. Mediator-Services) sind, oder die Kommunikationsplattformen bieten eine hybride API an, die ggü. der Cloud bspw. RESTful-APIs exponieren und nach Innen Message-basiert kommunizieren. Die Konvertierung der Nachricht erfolgt dabei klassisch in der Kommunikationsplattform und damit meist in der Hoheit einer dritten Partei.

4. Schnittstellen mit externen Parteien bzw. Systemen: Auch die Online-Services der Justiz haben verschiedene Anforderungen zur Integration, sowohl mit Anwendungen der internen Domäne, zur Integration untereinander sowie mit Anwendungen externer Parteien. Insb. die Schnittstellen zu externen Parteien wie Notaren, Rechtsanwälten, Unternehmen sowie zu anderen Behörden (z. B. Polizei) sind von besonderer Bedeutung, da diese APIs neben dem Justizportal den digitalen Zugang zur Justiz darstellen.

Sie bilden einerseits Schnittstellen für diese Parteien, um mit der Justiz zu interagieren, bspw. um digitale Ende-zu-Ende-Strecken mit Notaren für Grundbuchsachen aufzubauen. Andererseits sind dies auch Schnittstellen, mit denen die Justiz Zugriff auf externe Services erhält und sich dementsprechend in das Ökosystem eines digitalen Staats (auch auf EU-Ebene) integrieren kann.

In der Justizcloud-Anwendungslandschaft würden diese Zugriffe über einen sogenannten *Northbound-API-Gateway* orchestriert und gemeinsam mit dem CIAM (vgl. **Kapitel 3.4.6.2**) die API-Aufrufe authentisiert und autorisiert. Im API-Portal des *Northbound-API-Gateway* werden dabei nur die extern verfügbaren Justiz-APIs der Online-Services publiziert und beantragbar gemacht („Need-to-know“). Jede externe Identität/ Maschine (sog. Client) erhält dabei eigene Justiz-Credentials und dedizierte Zugriffsrechte auf eine oder mehrere APIs (API-Sets). Dadurch kann, von Beginn an, ein wesentlicher Beitrag zur Sicherheit und Standardisierung der Justiz-API-Landschaft erfolgen, da es bis dato nur sehr wenige externe APIs (bsp. im Handelsregister) gibt. Die Entkopplung über die Integrationsschicht hat zudem den Vorteil, dass sich die Justiz-APIs sukzessive entwickeln können, da sie im *Northbound-API-Gateway* versioniert und inkrementell publiziert werden können.

Im Falle von externen APIs, an die sich die Justiz anbinden will, ist es auch ratsam, diese über den *Northbound-API-Gateway* (als sog. *Forward-Proxy*) zu kanalisieren. Damit kann ein wesentlicher Beitrag zur sicheren Nutzung und Integration externer Parteien in die Geschäftsprozesse der Justiz geleistet werden. Zudem erfordern die meisten externen Dienste eine moderne Authentisierung und Autorisierung, die ggf. Justizanwendungen noch nicht beherrschen und auch nicht beherrschen müssen. In dem Fall kann der *Northbound-API-Gateway* diesen Schritt übernehmen und die interne Anfrage an einen externen Dienst bspw. um einen OAuth-Token anreichern.

Die Entscheidung, eine serviceorientierte Architektur zu implementieren, wurde in der Justiz bereits durch die Entwicklung von modernen, serviceorientierten Verfahren wie *GeFa* getroffen und wird dort konsequent angewendet. Auch im Integrationskonzept des *BLK-*

Architekturbüros sind entsprechende Standards beschrieben. Aufgrund der historisch sehr engen Kopplung (z. B. Punkt-zu-Punkt) zwischen Verfahren, den hohen Aufwänden zur Anpassung monolithischer Anwendungen (z. B. Kommunikationsplattform) sowie fehlenden modernen Integrationsplattformen sind die dargestellten Ansätze und Konzepte jedoch derzeit nur vereinzelt umgesetzt bzw. umsetzbar.

Über eine moderne Integrationsplattform kann die Justizcloud daher als Katalysator für eine Neuordnung und Vereinfachung des Anwendungsgefüges und somit höherer Flexibilität dienen. Dazu ist es notwendig, dass neben den technischen Voraussetzungen (z. B. Integrationsplattform) auch architektonische und organisatorische Grundsätze und Prinzipien (z. B. API-First-Ansatz, Nutzung von Basiskomponenten, zustandslose/ stateless Microservices) zu etablieren und bei der Einführung von weiteren Cloud-Anwendungen konsequent einzuhalten. Dabei kann ein aus Anwendungsarchitekten der Entwicklungsverbünde bestehendes Architekturboard als organisatorischer Katalysator zur Formulierung und Durchsetzung der o. g. Architekturprinzipien dienen.

3.4.5 Datenkonzept

Eine einheitliche Cloud-Umgebung für die deutsche Justiz kann Grundlage für zahlreiche neue Anwendungsfälle zum Umgang mit Daten sein. Einerseits für neuartige Formen der Datenverarbeitung und -nutzung wie KI, Datenvisualisierung oder „Teilen statt Versenden“, andererseits für die Einbindung moderner Datenplattformen, die diese Anwendungsfälle ermöglichen, wie z. B. relationale, verteilte und objektorientierte Datenbanken, Data Warehouses und Data Lakes. Gleichzeitig bestehen spezifische technische und gesetzliche Anforderungen von Bund und Ländern an die Kontrolle und Sicherheit der Daten. Um vor diesem Hintergrund neue Anwendungsfälle zu ermöglichen, ist ein ganzheitliches Datenkonzept erforderlich. Dazu wurden im Justizcloud-Zielbild sowohl Grundlagen einer Datengovernance, Konzepte zur Datenhaltung und Datenaustausch in der Justizcloud sowie konkrete Anwendungsfälle und benötigte Datentechnologien diskutiert.

3.4.5.1 Datengovernance und Datenhaltung

Die Justiz verarbeitet vielfältige Daten mit unterschiedlichem Schutzbedarf wie personenbezogene Daten (z. B. Namen und Adressen), Verfahrensdaten (z. B. Akten), Beweisdaten (z. B. Bild- und Videoaufnahmen), Verwaltungsdaten (z. B. Personalakten), technische Daten (z. B. Logs von IT-Systemen) uvm. Diese Daten sind dabei meistens in Kontrolle und Verantwortung der jeweiligen Landesjustiz bzw. Bundesgerichte.

Für die Verarbeitung dieser Daten werden in der Regel Datenschutz- und IT-Sicherheitskonzepte erstellt, die unterschiedliche Schutzbedarfe festlegen. Die meisten Anwendungen der Justiz wie eAkte, Fachverfahren etc. sind dabei mit normalem bis sehr hohem Schutzbedarf klassifiziert. Bisher sind die Rechenzentren der einzelnen Länder für die Verarbeitung dieser Daten ausgelegt. Mit der Nutzung einer Justizcloud müssen diese Konzepte ggf. aktualisiert und ergänzt werden.

Im Betrieb einer hybriden Community Cloud-Infrastruktur wie der Justizcloud bieten sich dabei verschiedene Möglichkeiten, den Schutzbedarf der Daten sicherzustellen (vgl. **Abbildung 32**). Dabei können unterschiedliche Maßnahmen, Verfahren bzw. Modelle je nach Schutzbedarf zur Anwendung kommen, bspw. zur Ausgestaltung der Datenhaltung, Einsatz von Verschlüsselungsmechanismen sowie zur Authentisierung und Autorisierung.

Abbildung 32 | Beispielhafte Schutzmaßnahmen nach Schutzbedarf

	Schutzbedarf der Daten		
	Normal Beispiel: Metadaten eines Verfahrens in GeFa (z. B. Länge des Verfahrens)	Hoch Beispiel: Name und Geburtsdatum einer Angeklagten	Sehr hoch Beispiel: Adressen geschützter Zeugen
Beispielhafte Ausgestaltung			
Datenhaltung und Verarbeitung	Datenhaltung und -verarbeitung in der Cloud	Datenhaltung im Land und Verarbeitung in der Cloud	Haltung/ Verarbeitung nur im jeweiligen Bundesland
Verschlüsselung	Geringe Verschlüsselung	Verschlüsselung mit BYOK (Bring your own Key)	Verschlüsselung mit HYOK (Hold your own Key)
Authentisierung	Einfache Authentisierung	2-Faktor-Authentisierung	MFA (z. B. Biometrische Authentisierung)
Autorisierung	Administration durch zentrales Justizcloud Team	Administration nur durch Beamte des jew. BL	Administ. durch kl. Personenkreis und 4-Augen-Prinzip
...			

Zur Sicherstellung des Datenschutzes sollte dazu zunächst eine umfassende Klassifizierung der Daten für den Cloud-Betrieb erfolgen. Anschließend sollte festgelegt werden, welche Daten welche Schutzmaßnahmen auf welcher Ebene und durch wen erfordern.

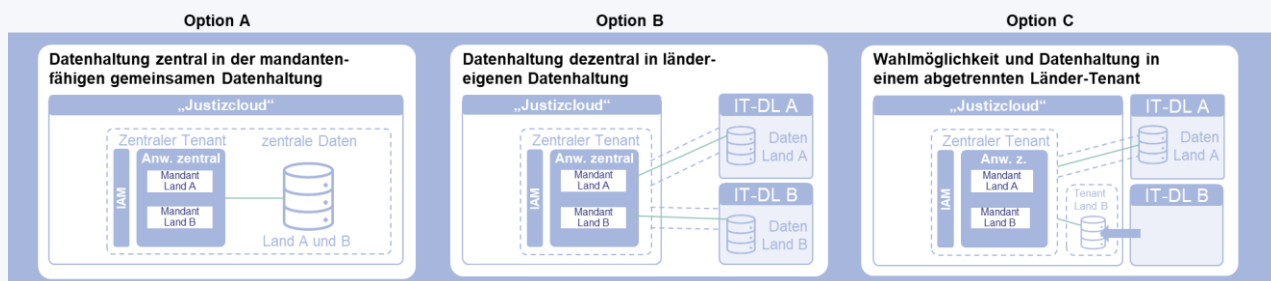
So könnte über alle Phasen der Datenverarbeitung (z. B. at Rest, in Transit) hinweg ein kryptographischer Schlüssel, spezifisch für die Justizcloud bzw. das jeweilige Land (sog. Zertifikate), genutzt werden. Bei länderspezifischem Schlüssel besteht die Möglichkeit, diesen entweder in der Cloud (Bring your own key (BYOK)) oder auf eigener Infrastruktur zu halten (Hold your own key (HYOK)). Auch bei der Authentisierung kann je nach Sicherheitsanforderung ein einfaches Verfahren (z. B. Username und Passwort) oder Zwei- bzw. Multi-

Faktor-Verfahren (2FA/ MFA) mit/ ohne Biometrie sowie mit/ ohne adaptiver Logik (z. B. Geolokation) angewendet werden. Auch für die Autorisierung bieten sich unterschiedliche Verfahren (z. B. Vier-Augen-Prinzip) an.

Mit diesen Maßnahmen sowie dem Community Cloud-Konzept, welches auf bestehender, sicherheitszertifizierter Infrastruktur öffentlicher IT-Dienstleister aufsetzt, kann in der Justizcloud sichergestellt werden, dass alle Daten gemäß ihres Schutzbedarfs, sicher und den gesetzlichen Anforderungen entsprechend verarbeitet werden.

Diverse Beispiele bzw. Anforderungen wurden im Rahmen des fachlichen Zielbilds diskutiert. Eine konkrete Anforderung war z. B. die Möglichkeit, bestimmte landesspezifische Daten auf landesspezifischer Infrastruktur/ Servern zu halten. **Abbildung 33** stellt verschiedenen Optionen hierfür dar:

Abbildung 33 | Modelle der Cloud-Datenhaltung



Bei **Option A** werden die Daten von zwei Ländern in der Justizcloud gehalten und je nach Schutzbedarf mit den o. g. Verfahren gesichert. Die Datentrennung erfolgt dabei BSI-konform durch die Mandantenfähigkeit der Anwendung bzw. Datenhaltung (vgl. **Kapitel 3.4.3**).

Sollten bestimmte Daten auf landesspezifischer Infrastruktur verbleiben müssen, kann in **Option B** die Datenpersistenzschicht der Anwendungen, d. h. die Datenbanken, weiter in den Umgebungen der IT-Dienstleister der Länder verbleiben. So könnte zwar ein Fachverfahren wie *GeFa* in der Justizcloud betrieben, aber Zugriffe aus Land A auf eine Datenbank in Land A und Zugriffe aus Land B in Land B umgeleitet werden (vgl. **Kapitel 3.4.3**).

Im Justizcloud-Community-Cloud-Konzept ist Option B prinzipiell auch innerhalb der Justizcloud denkbar, denn jedem virtuellen Infrastruktur-Knoten kann seine Herkunft, also das bereitstellende Rechenzentrum, als sog. „Tag“ entnommen werden. D. h. auch die Verarbeitung in der Cloud kann auf virtueller sowie der physischen Infrastruktur eines Landes

erfolgen. Ein *GeFa* Betrieb könnte also so konfiguriert werden, dass Daten aus Land A auf Knoten in Land A und Daten aus Land B in Land B verarbeitet werden. Dafür muss aber der IT-Dienstleister dieses Landes auch sog. Knoten-Anbieter sein (vgl. **Kapitel 3.5.2**).

Option C stellt eine hybride Ausgestaltung je nach Anforderungen der Länder dar. Hier könnte z. B. ein Land A seine Daten bereits in der Justizcloud halten, während Land B seine Daten noch im lokalen Rechenzentrum hält. Diese Flexibilität ist insb. dann von Vorteil, wenn die Entscheidungsprozesse in den Ländern bzw. mit den jeweiligen IT-Sicherheitsbetrieben unterschiedlich lange dauern.

3.4.5.2 Skalierbare Speicherkapazitäten

Die steigenden Datenmengen, insb. durch unstrukturierte Daten wie PDF-Anhänge (z. B. aus dem *ERV*) und digitaler Beweismittel, erfordern eine moderne, skalierbare und sichere Speicherinfrastruktur (vgl. **Kapitel 2.2.4**). In der Ist-Analyse wurde auch festgestellt, dass einige IT-Dienstleister der Justiz bereits an Kapazitätsgrenzen bzgl. ihrer Räumlichkeiten und dementsprechend auch der erweiterbaren Server- bzw. Speicherinfrastruktur geraten. Denn das Datenwachstum ist nicht nur auf die Justiz begrenzt, sondern findet sich in allen [Bereichen der Verwaltung und der Privatwirtschaft](#). Einige IT-Dienstleister denken deswegen bereits darüber nach, zusätzliche Rechenzentren zu bauen, oder mieten Räumlichkeiten in Rechenzentren anderer IT-Dienstleister zur Beherbergung der eigenen Infrastruktur an (sog. Housing).

Dementsprechend berücksichtigt auch das Justizcloud-Zielbild Lösungen für eine skalierbare Speicherinfrastruktur. Über das föderierte Community Cloud-Konzept der Justizcloud (vgl. **Kapitel 3.3.2**) kann auf eine breitere Infrastruktur verschiedener IT-Dienstleister zugegriffen und so auch der Speicherbedarf über die gemeinsame Infrastruktur verteilt werden. Damit macht sich die Justizcloud auch unabhängiger von einzelnen Anbietern oder IT-Dienstleistern. Denn auch kommerzielle Anbieter geraten an ihre Kapazitätsgrenzen und müssen regelmäßig neue Kapazitäten und Rechenzentren, vor allem in entwickelten Regionen mit hoher Cloud-Nutzung, oft aber allein schon aus Redundanzgründen, errichten. In einem nationalen Kontext, wie der deutschen Justiz mit der Justizcloud, wäre die Abhängigkeit zu einem einzelnen Anbieter sehr hoch, wodurch die (digitale) Souveränität der Justiz gefährdet sein könnte. Die Kapazitäten eines einzelnen (kommerziellen) Anbieters wären zudem unzureichend, weshalb auch bei einer kommerziellen Justizcloud mindestens zwei, besser sogar drei Anbieter, zu einer Multi Cloud zusammengeschaltet werden müssten.

Das Justizcloud-Konzept beschränkt sich dabei nicht nur auf Infrastruktur von IT-Dienstleistern der Justiz. Es könnte sukzessive auch um weitere öffentliche IT-Dienstleister, aber auch um kommerzielle Cloud-Umgebungen (sog. Hybride Justizcloud), erweitert werden. So könnte schrittweise eine an Datenklassifikation orientierte Datenhaltung umgesetzt werden. Bei dieser könnten bspw. weniger sensible Daten in Speichern der kommerziellen Umgebungen und schützenswerte Daten auf Infrastruktur der Justiz-IT-Dienstleister liegen.

Zusammenfassend könnte die Justizcloud also auf verschiedene Speicherinfrastrukturen skalierbar zugreifen und bei Bedarf neue Anbieter hinzunehmen. Auf der anderen Seite ermöglicht das Justizcloud-Konzept aber auch, weniger Daten in der Justiz zu erzeugen bzw. zu halten. Über das Datenaustauschkonzept (vgl. **Kapitel 3.4.5.3**) wird die Justiz befähigt, Daten mit anderen Parteien (intern sowie extern) zu teilen statt, wie derzeit, multiple Kopien zu versenden. Das Datenaustauschkonzept schafft somit die Grundlagen zum Teilen von Daten mit bzw. von anderen Behörden. So kann die Justizcloud z. B. den Anwendungsfall einer gemeinsamen Beweismittelcloud mit der Polizei fördern.

3.4.5.3 Datenaustauschkonzept

Ein besonders hervorgehobenes Thema bei den Zukunftsanforderungen der Justiz (vgl. **Kapitel 2.2.4**) ist die Schaffung neuer Möglichkeiten zum Datenaustausch und Datenteilen in der internen Domäne oder mit ausgewählten Externen (z. B. mit der Polizei oder EU-Justiz). Mit fortschreitender Digitalisierung steigt auch das Datenaufkommen in der Justiz erheblich. Der Versand von Datenkopien über Message-basierte Kommunikation erzeugt dabei unnötigen Traffic (vgl. **Kapitel 2.2.1**), der durch Möglichkeiten des Datenteilens statt -versendens deutlich reduziert werden könnte.

Durch die abgetrennten Ländernetze sowie heterogene Plattformen und Verfahren ist derzeit der *ERV* mit *EGVP*, von der Versendung physischer Datenträger abgesehen, die einzige technische und rechtliche Möglichkeit, Daten innerhalb der Justiz und mit Dritten durch Versenden von Datenkopien auszutauschen. Hier könnte die Justizcloud durch Schaffung des Fundaments einer bundeseinheitlichen Justizdateninfrastruktur zur Befähigung moderner Datenaustauschmechanismen beitragen. Dafür gibt es zwei Optionen:

Gemeinsame Datenhaltung: Die Justizcloud kann für die Justiz eine gemeinsame Datenhaltung bereitstellen. Dabei würden ausgewählte Daten zentral gehalten und über ein zentrales Berechtigungsmanagement der Zugriff auf die Daten (sog. Row-Level- bzw. Resource-Level-Access-Management) gesteuert (vgl. **Abbildung 33**). Deshalb kann diese Option auch „Dropbox“-Modell genannt werden. In diesem Modell könnte bspw. Gericht A eine Akte

erstellen und z. B. im Instanzenzug Gericht B zur Einsicht und Bearbeitung freigeben. Beide arbeiten dabei am selben Objekt. Gericht B kann entscheiden, sich eine Kopie bei Bedarf zu erzeugen, sofern bspw. die Zugriffsrechte Kopieren erlauben. Handelt es sich um Daten aus den lokalen Bestandsanwendungen (z. B. eAkte) so synchronisiert Gericht A diese Daten regelmäßig mit der Justizcloud-Datenhaltung, da es lokal keine Freigabemöglichkeiten gibt. Sind es bereits zentral gehaltene Daten so wäre ein direktes Teilen machbar.

Dies ist auch für weitere Daten wie Verfahrensdaten oder Beweismittel möglich und würde den Datenaustausch in der Justiz erheblich flexibilisieren. Zusätzliche Voraussetzungen in diesem Modell sind u. a. ein zentrales Metadaten-Management (z. B. Beschreibung und Suchen zentral gehaltener Daten) sowie ein bundeseinheitliches Datenschema für strukturierte, d. h. relationale Daten, um die Daten auch im Kontext von Maschine-zu-Maschine-Kommunikation teilen zu können.

Datenvirtualisierung: Eine Alternative zur zentralen Datenhaltung kann Datenvirtualisierung sein. Dabei verbleiben die Daten beim Dateneigentümer, d. h. den Ländern. Sie können aber ohne eine physische Replikation, anderen Netzwerkteilnehmenden zur Verfügung gestellt werden. Dafür müsste in der Justizcloud spezielle Software zur Datenvirtualisierung aufgebaut und die Datenquellen der Länder katalogisiert und angeschlossen werden (insb. Datenzugriffsprotokoll, -berechtigungen und -beschreibung). Die Datenvirtualisierungs-Plattform enthält daher oft bereits ein Metadaten-Management-Modul, um die virtualisierten Datenquellen zu beschreiben. Dafür muss die Plattform auch an ein zentrales Benutzer- und Berechtigungssystem angeschlossen werden, um die Datenzugriffe fein-granular schneiden und orchestrieren zu können. Damit wären auch eine zentrale Suche und Anfrage sowie Einsicht und Zugriff auf lokal gehaltene Daten möglich.

Datenvirtualisierung bietet damit eine größere Kontrolle, Verringerung des Traffics (v. a. weil Datensynchronisation vermieden wird) und geringere Aufwände, da bestehende Infrastrukturen nachgenutzt und dennoch Datenzugriffe ermöglicht werden. Nachteile können z. B. eine höhere Belastung der Quellsysteme und Inkonsistenzen in Datenmodellen und Datenqualität sein, da Daten verschiedener Systeme nur virtuell zueinander in Beziehung gesetzt werden. Zudem ist der Ansatz etwas komplexer im Aufbau, da individuelle Datenverbindungen zu den lokalen Quellen und gemeinsame Berechtigungssysteme konfiguriert werden.

3.4.5.4 Justizcloud-Datendienste bzw. -Plattform

Für die verschiedenen Anwendungsfälle zum Speichern und Verarbeiten von Daten in der Justizcloud sowie zum Aufbau einer bundeseinheitlichen Datenplattform gibt es diverse

Technologien. **Abbildung 34** gibt einen Überblick aktueller Datenplattform-bezogener Technologien aus Servicekatalogen der Hyperscaler. Einige davon wären bereits in einer ersten Ausbaustufe der Justizcloud essenziell, weil sie von Entwicklungsverbünden bereits genutzt werden. In der Kategorie **Datenhaltung** gehören dazu sowohl eine Cloud-fähige, relationale Datenbanktechnologie für strukturierte Daten als auch ein Objektspeicher (sog. Object Store bzw. NoSQL Datenbank) für unstrukturierte Daten wie digitale Beweismittel, Audiodateien und PDF-Dokumente. Dabei kann die Technologieauswahl während des Justizcloud-Aufbaus auch genutzt werden, um die historisch bedingte Heterogenität an Speichertechnologien in Fachverfahren und eAkten zu harmonisieren. Frühzeitig sollte auch eine Datenvirtualisierungstechnologie in Betracht gezogen werden, wie in **Kapitel 3.4.5.2** dargestellt.

Abbildung 34 | Übersicht Datenplattform-bezogener Cloud-Dienste

Datenhaltung		Datenverarbeitung		Künstliche Intelligenz	
Cloud-native RDBMS	Strukturierte Datenhaltung durch klassische relationale Datenbanken, entweder als managed oder non-managed Service	Data Orchestration	Koordinierte Verwaltung und Automatisierung von Datenflüssen	Speech Recognition	Umwandlung gesprochener Sprache in Text
Non-native managed RDBMS		Data Discovery	Explorative Analyse von Daten z. B. zur syst. Klassifizierung/ Katalogisierung	Vision Recognition	Erkennung und Analyse von visuellen Daten wie Videos und Bilder
No-SQL	Key-Value/Object Store, z. B. für PDFs, Audiodateien, Bilder etc.	Big Data Processing	Verarbeiten besonders großer und komplexer Datenmengen	Language Recognition	Identifikation und Unterscheidung verschiedener Sprachen
Graph Database	Spezielle No-SQL DB zur Analyse von Änderungen, Mustern und Beziehung	Stream Analytics	Echtzeitanalyse von kontinuierlich eingehenden Datenströmen	Text-to-Speech	Umwandlung von geschriebenem Text in gesprochene Sprache
In-memory DB & Caching	SQL/No-SQL für schnellen Lese-/Schreibzugriff (keine Persistierung)	Visualization	Visuelle Darstellung von Daten zur Analyse und Interpretation	Translation	Umwandlung von Text oder Sprache in eine andere Sprache
Data Warehouse	Zentr. Sammlung von Daten versch. Quellen zur Weiterverwendung	Data Quality Service	Dienst zur Sicherstellung der Datengenauigkeit, -konsistenz und -qualität	Machine Learning	Algorithmen, die aus erlernten Mustern intelligente Aufgaben erfüllen können
Data Virtualization	Möglichkeiten zur virtuellen Anbindung und Zugriff auf dezentrale Daten	Predictive Analytics	Vorhersage zukünftiger Trends durch Analyse historischer Datenmuster		

● Akuter Bedarf der Justiz
● Wichtige zukünftige Services
● Noch kein Anwendungsfall

Auch im Bereich der **Datenverarbeitung** sind diverse Technologien für Ausbaustufen der Justizcloud anzudenken. Dazu gehören Möglichkeiten, Datenströme zu integrieren, orchestrieren und automatisieren. Ein wichtiger Baustein ist Stream Analytics, das auf Ereignisse (sog. Events, vgl. **Kapitel 3.4.4.1**) in Echtzeit reagiert und Folgeaktionen auslösen kann.

Zudem werden in der Justiz zunehmend große Datenmengen erhoben, die statistisch und visuell ausgewertet werden müssen. Das können bspw. Daten zu Verfahren sein, aber auch Nutzungsdaten im Bereich der Online-Services. Dafür sind deskriptive sowie visuelle Datendienste erforderlich. Des Weiteren wären auch Technologien für die Messung sowie die

laufende Überwachung und Verbesserung der Datenqualität in einer datengetriebenen Justiz essenziell, damit überhaupt Prozesse auf Basis von Daten automatisiert werden können.

KI wird mit Daten trainiert und generiert wiederum Erkenntnisse über die Daten (z. B. Mustererkennung) bzw. erzeugt neue Daten über diese Daten (z. B. Generative KI). Daher sind auch einige Dienste aus dem Bereich KI relevant für eine bundeseinheitliche Bereitstellung in der Justizcloud, um bspw. in moderne Fachverfahren eingebunden zu werden. Fachlich gibt es Bedarfe für Spracherkennung und Generierung (z. B. Textanalyse, Sprache-zu-Text und Text-zu-Sprache) sowie für Sprachtransformation wie Übersetzung (z. B. ausländischer Anhänge). Mit der KI-Plattform (vgl. **Kapitel 2.2.4**) könnten solche Technologien, Dienste bzw. Anwendungsfälle auf der Justizcloud gebündelt werden.

3.4.6 Identitäten-, Berechtigungs- und Administrationskonzept

Für den bundeseinheitlichen Betrieb von Anwendungen in der Justizcloud ist auch der Aufbau eines bundeseinheitlichen Identitäten- und Berechtigungsmanagementsystems zur Authentisierung und Autorisierung der Zugriffe auf diese Anwendungen notwendig.

Abbildung 35 | IAM und CIAM



Für die interne und externe Domäne wird dabei zwischen einem IAM für interne Zugriffe von Mitarbeitenden der Justiz auf der einen Seite und einem CIAM für die Zugriffe von externen Nutzenden wie Bürgern (sog. Business-to-Customer (B2C)) und Organisationen (Business-to-Business (B2B)) bzw. deren Anwendungen auf der anderen Seite unterschieden. Beide Systeme können in modernen, integrierten (C)IAMS auch aus einer technischen Lösung bzw. Produkt bestehen, werden aber mit

unterschiedlichen Anforderungen und Anwendungsfällen logisch getrennt und daher nachfolgend auch einzeln beschrieben.

3.4.6.1 Internes Identitäten- und Berechtigungsmanagement

Wie in der Ist-Analyse detailliert beschrieben, verwalten die Länder- und Bundesgerichte die Identitäten ihrer Mitarbeitenden in Verzeichnisdiensten (z. B. Active Directory, LDAP als sog. Identity-Provider). Dort werden Mitarbeitende über den gesamten Lebenszyklus von der

Einstellung bis zu Kündigung bzw. Ruhestand geführt und gepflegt. Zudem werden hier grundlegende Berechtigungen auf Basis organisatorischer Rollen vergeben.

In der Regel dienen die Verzeichnisdienste auch der Anmeldung und Authentisierung am Arbeitsplatz-PC des Mitarbeitenden. Nach der Authentisierung können Nutzende bestimmte Anwendungen auf dem Client verwenden. Die Vergabe granularer, anwendungsspezifischer Berechtigungen erfolgt aber meist in den Anwendungen selbst. Dieses System, d. h. der Betrieb der Verzeichnisdienste inkl. Konfigurationen, konkreten Authentisierungsprotokollen und definierten Rollen, besteht aktuell in jedem Land und resultiert in einer hohen technischen, fachlichen und organisatorisch-prozessualen Heterogenität im Bereich des Identitäten- und Berechtigungsmanagements.

Mit der Entwicklung einheitlicher Fachverfahren wie *AuRegis* wurde es erforderlich, auch einen einheitlichen Dienst zur Authentisierung zu entwickeln, der aufbauend auf den Verzeichnisdiensten eine einheitliche Authentisierung und Autorisierung für die modernen Fachverfahren ermöglicht. Dazu wurde *SAFE* als einheitliche Komponente und Standard entwickelt. *SAFE* nutzt dabei den etwas älteren SAML2.0-Standard auf Basis des Open-Source-Produkts *Keycloak* in einer IBM OpenShift Distributionsvariante. *SAFE* ermöglicht dabei SSO sowie über sog. autarke Module das Hinterlegen anwendungsspezifischer Attribute, die in gewöhnlichen Verzeichnisdiensten nicht geläufig sind, aber für den Betrieb der neuen Fachverfahren benötigt werden.

SAFE ist bis auf einige Referenz- und Pilotumgebungen aktuell noch nicht im breitflächigen Produktivbetrieb. Da es den modernen OAuth2.0-Standard noch nicht unterstützt, wird es mit *SAmOA* weiterentwickelt. *SAmOA* ist in der Lage, moderne ID-, Access- und Refresh-Tokens im JWT-Format zu erzeugen. Moderne Webanwendungen wie *AuRegis* und *GeFa* benötigen diese, da die Nutzung von Tokens mittlerweile Markt-, Technologie- und Sicherheitsstandard ist. Ergänzend wurde von Justizentwicklungsverbünden eine Basiskomponente zur anwendungsübergreifenden Verwaltung von Benutzerberechtigungen entwickelt (sog. *bk.brvt*).

Im derzeitigen Identitäten- und Berechtigungskonzept der Justiz soll es pro Land eine *SAmOA*-Instanz geben, mit der sich der jeweilige Landesverzeichnisdienst (z. B. *AD*) föderiert. Dabei werden Identitäteninformationen nach *SAmOA* übertragen und ggf. um weitere berechtigungsrelevante Attribute ergänzt. *SAmOA* kann dann als einheitliche Authentisierungskomponente für moderne Justizwebanwendungen im jeweiligen Land dienen.

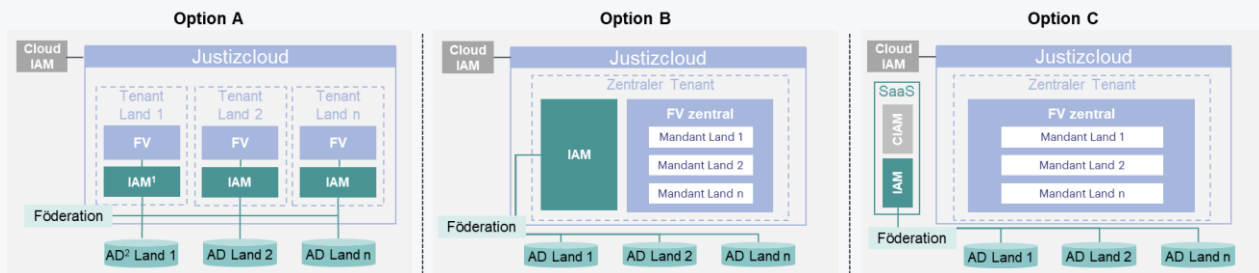
Im Gegensatz zu landesspezifischen *SAM*OAs ohne Justizcloud, wird mit der Justizcloud ein bundeseinheitliches Identitäten- und Berechtigungsmanagementsystem für die Authentisierung und Autorisierung der Justizcloud-Anwendungslandschaft notwendig. Es ist daher fachlich angezeigt, dass die Identitäten weiter in Hoheit der Länder, d. h. den lokalen Verzeichnisdiensten, verbleiben, diese aber mit einem bundeseinheitlichen IAM in der Justizcloud föderieren.

Wenn also etwa ein neuer Mitarbeitender im *AD* seines Landes hinterlegt wird, hat dieser erstmal keinen Zugriff auf ein Cloud-Fachverfahren oder nutzt dieses noch nicht. Sobald er von seinem Land aus zugreifen möchte, werden Identität und Login-Information aus dem Verzeichnisdienst (Identity Provider (IdP)) mit dem zentralen IAM (sog. Service Provider) föderiert, d. h., dorthin übertragen. Dafür muss zwischen Verzeichnisdienst und IAM eine Vertrauensstellung und technische Schnittstelle hergestellt werden. Während der Föderation wird neben der neuen Identität auch ein sog. Account für dieselbe angelegt, um bspw. zu ermöglichen, dass ein Nutzender in verschiedenen Ländern und/ oder IdPs bekannt ist. Bei der initialen Föderation können auch Attribute und Basisberechtigungen ergänzt werden. Im Ergebnis kann der Nutzende Daten zu seiner Identität auch in der Justizcloud nutzen und sich per SSO anmelden. Bei jedem Login/ Föderation wird dabei die Validität der Identität lokal geprüft, ggf. geänderte Attribute aktualisiert (z. B. Nachname bei Heirat) und Basisberechtigungen geprüft.

Dieses Modell der Föderation hat viele weitere Vorteile. Zum einen ist es sicherer, da die Richtigkeit der Identitäten bei jedem Login lokal geprüft wird, zum anderen kann im Authentisierungsprozess entschieden werden, ob die lokale Authentisierung bereits für eine Autorisierung in der Justizcloud ausreicht (sog. SSO) oder ob eine Multi-Faktor-Authentisierung, die es vielfach rein technisch noch nicht lokal gibt, durch das zentrale IAM nachgefragt wird (sog. Step-up-Authentication). Ein weiteres Sicherheitsmerkmal ist, dass immer nur die Identitäten föderiert werden, die auch wirklich Zugriff auf die Cloud-Anwendung brauchen (sog. need-to-know). Wenn sich ein lokaler Mitarbeitender nie zu einem Cloud-Fachverfahren navigiert, wird seine Identität auch nicht föderiert. Technisch bestehen aber verschiedene Modelle der Föderation, die detaillierter in **Kapitel 3.4.6.1** beschrieben werden.

Aus fachlicher Sicht bieten sich zudem drei Optionen für das bundeseinheitliche IAM an (vgl. **Abbildung 36**). Option A „ein IAM pro Landes-Tenant“, Option B „ein zentrales IAM in der Justizcloud“ und Option C „ein zentrales IAM als SaaS außerhalb der Justizcloud“.

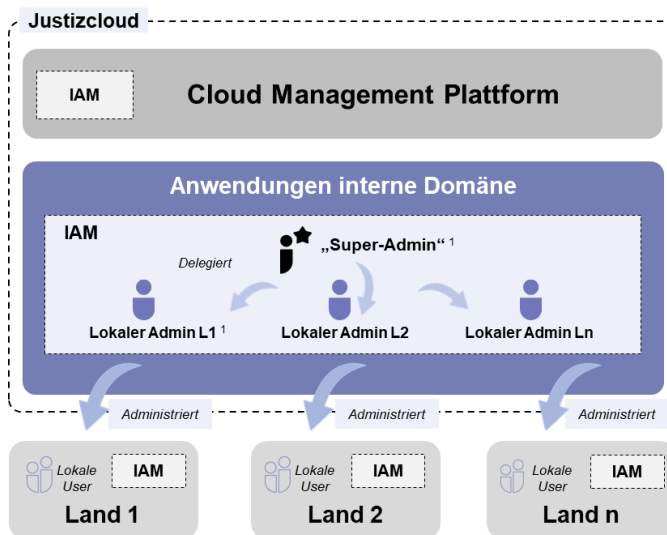
Abbildung 36 | IAM-Ausbringungsmodelle und Föderation



In **Option A** würden in jedem Landes-Tenant, z. B. in einem Betriebsszenario mit vielen, nicht-multi-mandantenfähigen Anwendungen (vgl. **Kapitel 3.4.3**), jeweils eigene IAM-Instanzen betrieben. Die IAMs wären zwar technisch das gleiche Produkte mit gleichen Basisconfigurationen und Ausbringungsprozessen, jedoch müsste jedes IAM dann durch (technische) Administratoren des jeweiligen Landes gepflegt werden. Ein weiterer Nachteil dieser Option ist zudem, dass die baugleichen IAMs mehrfach betrieben und Änderungen mehrfach gepflegt und ausgebracht werden müssten. Auch bei der Vergabe von Rollen, Rechten und Attributen bestünde die Gefahr sukzessiv entstehender Heterogenität. Auch wäre die Schaffung eines Datenraums bzw. das Teilen von Daten über diverse IAM-Instanzen komplexer zu realisieren. Vorteilhaft wäre hingegen, dass die Identitäten-Daten in länderspezifischen Umgebungen (Tenants) lägen und z. B. mit länderspezifischen Schlüsseln verschlüsselt würden.

Alternativ könnte in **Option B** für multi-mandantenfähige Anwendungen auch eine bundeseinheitliche, multi-mandantenfähige IAM-Instanz mit einem bundeseinheitlichen Rollen- und Berechtigungskonzept aufgesetzt werden. Die Identitäten-Pools der Länder würden dabei BSI-konform auf Ebene der Datenhaltung logisch getrennt (vgl. **Kapitel 3.4.3**). Es würden dabei Identitäten aus den IdPs des jeweiligen Landes föderieren und beim Login authentifizieren. Zwar hätte eine bundeseinheitliche Ausbringung des IAM in einer Instanz immense betriebliche Vorteile und würde z. B. die Schaffung eines Datenraums bzw. das Teilen von Daten sowie die Anbindung der Fachverfahren erleichtern, jedoch ist nicht jedes IAM-Produkt multi-mandantenfähig und kommt dadurch als zentrales IAM in Frage. Bspw. müsste das IAM in der Lage sein, einerseits eine Föderation von verschiedenen ADs parallel zu ermöglichen und andererseits im Betrieb die BSI-konforme Administration je Mandant organisatorisch sicherzustellen.

Abbildung 37 | Delegation von Administrationsrechten



Als weitere Anforderungen im Kontext eines modernen, zentralen Berechtigungsmanagement gilt die Möglichkeit, Administrationsrechte an lokale Admins der Länder zu delegieren. Damit könnte das Justizcloud-Team sich alleinig um den Betrieb des IAMs kümmern, während die Vergabe von Berechtigungen an Nutzende oder die Einladung neuer Nutzender zu Justizcloud-Anwendungen weiter aus den fachlichen Betriebsteams (sog. User Manager) der Länder erfolgen kann.

Das hätte viele organisatorische, rechtliche, sicherheitstechnische und fachliche Vorteile. Denn die User Manager kennen ihre jeweiligen Justizmitarbeitenden besser und sind damit effizienter bei der Rechteverwaltung. In der Justizcloud wäre nur ein „Super-Admin“ erforderlich, der die Basiskonfiguration generischer Rollen und Berechtigungen pflegt und zu sog. Admin-Rechte an lokale Administratoren delegiert (vgl. **Abbildung 37**). Da dieses Konzept mittlerweile Marktstandard ist, findet es sich auch insb. im externen Identitäten- und Berechtigungsmanagement für B2B-Kunden wieder (vgl. **Kapitel 3.4.6.2**) und wäre eine signifikante Synergie in beiden Domänen.

SAmOA beherrscht die Föderation von Identitäten aus multiplen Länder-ADs sowie die Delegation von Adminrechten derzeit nicht. Die Anwendung müsste daher für eine Nutzung als zentrales IAM der Justizcloud weiterentwickelt werden. Bei einer Modernisierung sollten auch wichtige Zukunftsanforderungen berücksichtigt werden. Moderne IAMs sollten bspw. verschiedene Sicherheitsmechanismen zur Authentisierung bieten, wie z. B. Multi-Faktor-Authentisierung oder physischer Token. Zudem bieten sie sowohl die Echtzeitauswertung von Zugriffen als auch die adaptive Anpassung der Authentisierungsmechanismen je nach Zugriffsmuster der Nutzenden. Bspw. wird geprüft, von wo sich eine Person einloggt und bei ungewöhnlichen Lokationen wird in Echtzeit eine sog. Step-up-Authentication, also ein weiterer Faktor eingefordert. Unabhängig davon bieten moderne IAM-Systeme viele effizienzsteigernde Komfortfunktionen (z. B. Self-Service-Profilpflege und Rechtebeantragungsprozesse), ohne dabei die Sicherheit zu vernachlässigen.

Moderne kommerzielle IAM-Systeme werden daher vielfach nur noch als SaaS-Lösung in der Cloud angeboten, um der stetig steigenden Bedrohungslage, aber auch den

gestiegenen Kundenanforderungen der IAM-Verantwortlichen, durch eine regelmäßige Verbesserung des Produkts, Echtzeitanpassung von Sicherheitsfeatures sowie eine ganzheitliche Reaktion auf externe Risiken zu ermöglichen.

Die Eigenentwicklung eines solch umfassenden IAM-Systems wäre kostspielig, insb. wenn Wartung und Weiterentwicklung sowie Sicherstellung einer hinreichenden Skalierbarkeit und Bereitstellung stetig verbesserter Sicherheitsfunktionen zu gewährleisten sind. Daher ist in **Option 3** prinzipiell auch die Nutzung eines SaaS-Produkts für das interne IAM der Justizcloud denkbar. Am Markt gibt es dafür zahlreiche Produkte, die teilweise auch auf eigener Infrastruktur (sog. on-premises) betrieben werden können oder als reine SaaS-Lösung an die Kundensysteme angeschlossen werden. Dabei können auch besondere Sicherheitsanforderungen wie etwa die Nutzung eigener Schlüssel (BYOK) genutzt werden, um die Datensouveränität und Sicherheit auch bei Nutzung eines Cloud-SaaS-Produkts sicherzustellen.

3.4.6.2 Externes Kundenidentitäten- und Berechtigungsmanagement

Auch im Bereich des externen Kundenidentitäten- und Berechtigungsmanagements zur Authentisierung und Autorisierung externer Identitäten und Zugriffe bestehen viele Anforderungen, die *SAFE-public* als derzeitiger externer Authentisierungsdienst nur teilweise beherrscht (z. B. Fehlen des OAuth2.0-Standards, vgl. **Kapitel 2.2.1.2**). In der externen Domäne gibt es diverse zu berücksichtigende Nutzengruppen wie z. B. Bürger (B2C), Rechtsanwälte, Notare oder auch Mitarbeitende von Unternehmen und anderen Behörden (B2B). Auch für diese Nutzer-Pools müssen Identitäten und Zugriffsberechtigungen auf Justizanwendungen und -APIs verwaltet werden. Einerseits, um die Sicherheit zu gewährleisten, andererseits, um eine Personalisierung der Justizdienste ggü. diesen Parteien zu ermöglichen. Ein modernes Kundenidentitäten- und Berechtigungsmanagement bildet dabei die Basis für einen einheitlichen Zugang zu digitalen Dienstleistungen und eine einheitliche Kundenerfahrung und könnte auch als zentraler Zugang für ein modernes Justizportal (Arbeitstitel *Justizportal Deutschland*) dienen.

Aktuell stellen dafür die *BNotK* und die *BRAK* multiple *SAFE-public* Instanzen, insb. zur Pflege der Postfächer für die verschiedenen Nutzengruppen bereit. Für das Zielbild der Anwendungslandschaft der externen Domäne (vgl. **Kapitel 3.4.2.2**) wäre der Aufbau eines zentralen CIAM für das integrierte Kundenidentitäten- und Berechtigungsmanagements von externen Parteien zu empfehlen.

Im B2B-Kontext würde das CIAM, wo möglich, die externen Identitäten direkt aus den bestehenden IAMs/ IdPs, d.h. den bestandsführenden Systemen der externen Organisationen (z. B. großen Unternehmen), *BRAC*, *BNotK* und anderen Behörden fördern. So könnte der Pflegeaufwand für alle Parteien und insb. die Justiz signifikant reduziert und gleichzeitig eine höhere Sicherheit beim Zugriff externer Identitäten und deren Maschinen/ Anwendungen sichergestellt werden. Ein weiterer Effizienztreiber wären auch Komfortfunktionen wie Self-Services für Externe, um bspw. selbständig Berechtigungen anzufragen oder Profildaten zu pflegen. Besonders viel Aufwandsersparnis ließe sich durch eine Delegation von Administrationsrechten an vertrauenswürdige Nutzer-Administratoren (sog. User Manager) erzielen. Diese könnten innerhalb eines für sie begrenzten Rahmens die Nutzenden der eigenen Organisation und deren Berechtigungen zu Justizdiensten verwalten. Bspw. könnten die Berechtigungen von Notaren auf Justizanwendungen und -APIs innerhalb gesetzter Grenzen (sog. Admin-Rechte) durch die *BNotK* administriert werden. Dies erhöht gleichzeitig die Skalierbarkeit der Rechteverwaltung, da in der Justiz kein zusätzliches Personal zur Administration aufgebaut werden müsste.

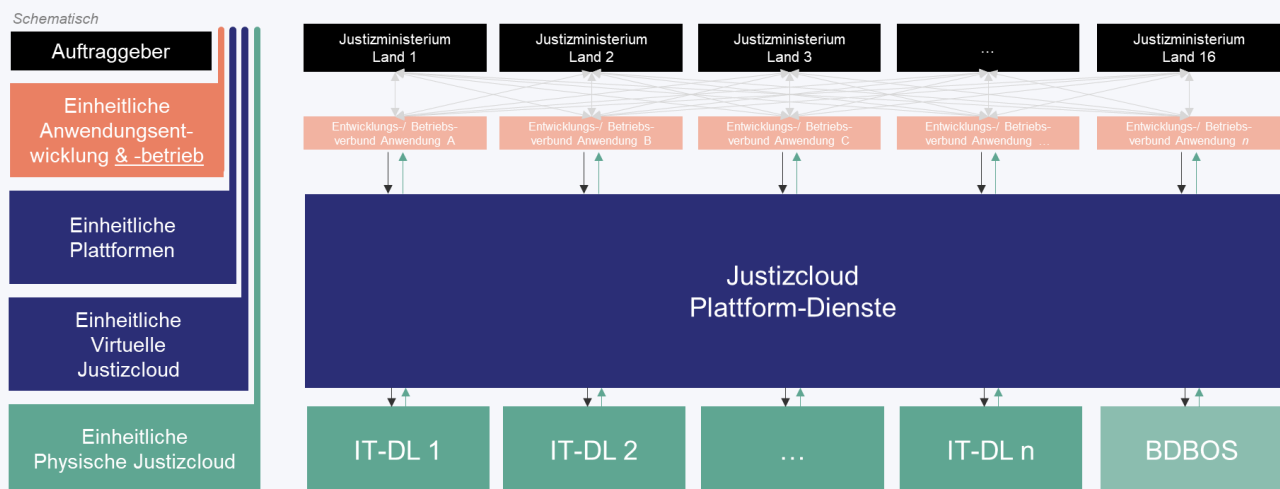
Bei Bürgern würde das CIAM idealerweise mit der *Bund-ID / eID* gefördert, so dass Bürger auch in der Justiz ihre digitale Identität und Authentisierungsfunktionen (z. B. Personalausweis, EUDI-Wallet) nutzen können. Dies wäre auch im Kontext der eGovernment-Prinzipien (insb. Once-Only-Prinzip) zu empfehlen und ist bereits heute punktuell umgesetzt.

Viele moderne IAM-Anbieter bieten sowohl Produkte zur Verwaltung interner Mitarbeitender (Business-to-Employee (B2E)) als auch für die Verwaltung, Föderation und Delegation externer Identitäten im B2B- und B2C-Kontext an. Insbesondere vor dem Hintergrund der stetig steigenden Bedrohungslage investieren kommerzielle IAM-Anbieter regelmäßig signifikante Beträge in neue Sicherheitsfeatures sowie die Absicherung und Überwachung ihrer Cloud-basierten IAM-Lösungen und betreiben teilweise auch dedizierte Security-Operations-Center (SOC) für ihre Kunden (z. B. um DDoS-Attacken abzuwehren). Alle vorgenannten Funktionen im Kontext des immer dynamischeren technologischen Fortschrittes und wachsender Kundenanforderungen für solche IAM-Systeme zu entwickeln und zu pflegen wäre für die Justiz sehr aufwändig und ggf. auch keine Kernkompetenz. Daher wäre im Kontext der Justizcloud-Umsetzung sowie der Weiterentwicklung der externen Domäne auch die Umsetzung einer modernen on-premises- (vgl. **Abbildung 36**, Option B) oder SaaS-basierten CIAM-Lösung (vgl. **Abbildung 36**, Option C) empfehlenswert (vgl. **Kapitel 3.4.2.2**).

3.4.7 Serviceportfoliostrategie und Servicekatalog

Die Justizcloud-Plattform soll künftig vor allem als zentraler Anbieter bundeseinheitlicher IaaS- und PaaS-Dienste für die Entwicklung und den Betrieb der Cloud-nativen Anwendungslandschaft der Justiz fungieren. Die Entwicklungsverbünde entwickeln ihre Anwendungen für die Justizcloud und werden befähigt, diese auch dort zu betreiben. D. h., dass die Entwicklungsverbünde die Anwendungsebene, also SaaS-Dienste, bereitstellen. Ausnahmen davon bilden bspw. die IAM- und CIAM-Dienste, für die noch kein Entwicklungsverbund existiert und die ggf. auch von der Justizcloud bereitgestellt werden könnten. Die primären Kunden der Justizcloud sind also die Cloud-nutzenden Entwicklungsverbünde bzw. Betriebsverbünde (vgl. **Abbildung 38**).

Abbildung 38 | Cloud-nutzende Justizcloud-Plattformdienste



Ziel der Justizcloud muss es demnach sein, vor allem Services bereitzustellen, welche die Entwicklungs- und Betriebsverbünde für ihre Arbeit benötigen. Dies sind insb. virtualisierte, von den IT-Dienstleistern provisionierte Infrastruktur (IaaS) sowie bundeseinheitliche Plattformdienste (PaaS), auf deren Grundlage die Entwicklungsverbünde ihre Anwendungen entwickeln (z. B. Entwicklerarbeitsplatz, Datenbank und Container-Plattform) und betreiben (z. B. Monitoring/ Logging, technische Basisdienste, IAM/ CIAM) können.

Die Auswahl und Entwicklung der Justizcloud-Services sollte sich dabei eng an den Bedarfen und strategischen Prioritäten der Justiz und ihrer Entwicklungsverbünde orientieren und in einen bundeseinheitliche Serviceportfolio und -katalog münden. Dementsprechend sollte die Migration bzw. das Onboarding auf die Justizcloud auch dafür genutzt werden, die

heterogene Technologielandschaft (z. B. eingesetzte Datenbanktechnologien) zu harmonisieren. Die Justizcloud-Services sollten für Entwicklungsverbünde idealerweise über ein Cloud-Serviceportal bzw. -APIs suchbar, buchbar und verfügbar gemacht werden.

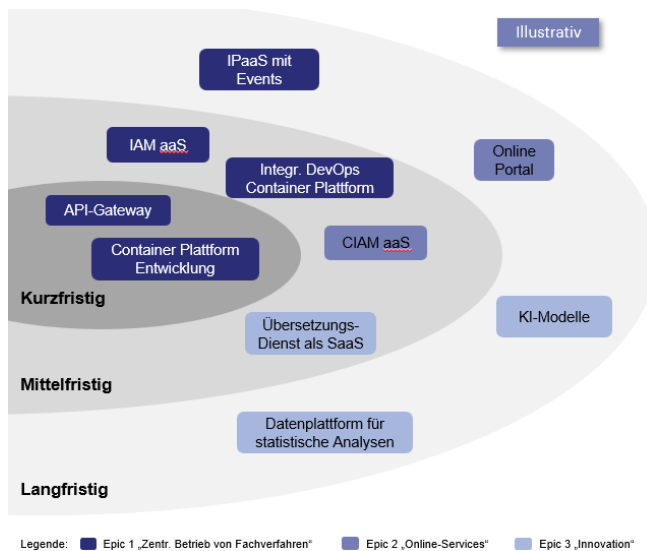
3.4.7.1 Serviceportfoliostrategie der Justizcloud

Welche Services die Justizcloud konkret entwickeln und anbieten soll, muss im Rahmen einer Serviceportfoliostrategie erarbeitet werden. Die Serviceentwicklung sollte sich dabei an der strategischen Zielsetzung der Justizcloud orientieren und die kurz-, mittel- und langfristige Zielsetzung berücksichtigen. Kurzfristiges Ziel sollte sein, genau die Services zu entwickeln, die für die Justiz und ihre Entwicklungsverbünde aktuell die größte Priorität haben. Je nach Anforderungslage kann das Serviceportfolio dann mittel- bis langfristig sukzessive ausgebaut werden.

Dabei ist es wichtig, die Serviceportfolioentwicklung der Justizcloud organisatorisch eng in die übergreifende IT-Organisation der Justiz, bestehend aus dem justizweiten strategischen Anforderungs- sowie dem Architekturmanagement bzw. -board einzubinden (vgl. **Kapitel 3.6.3**). So kann einerseits sichergestellt werden, dass Anforderungen der Entwicklungsverbünde (z. B. an Daten- oder KI-Dienste) (vgl. **Abbildung 34**) auch frühzeitig bei der Entwicklung der Justizcloud-Plattform berücksichtigt werden (vgl. **Kapitel 3.6.3**, Strategisches Anforderungsmanagement). Andererseits kann in diesem Zuge auch auf eine Harmonisierung bzw. Auswahl eines für alle Verbünde passenden sowie für die Justizcloud effizient zu betreibenden Dienstes geachtet werden. So kann das Gesamtsystem graduell erneuert werden und die moderne Anwendungs- und Betriebslandschaft der Justiz entstehen.

Im Rahmen einer justizweiten Portfolioplanung (z. B. analog des Lean Portfolio Managements des *Scaled Agile Frameworks (SAFe)*) könnten strategische Initiativen in sog. Wertströme (value streams) und Epics zusammengefasst und hinsichtlich ihrer Investitionsbedarfe und Nutzenstiftung orchestriert werden. Epics sind zusammenhängende, fachliche Handlungsfelder, die sowohl in der Anwendungsentwicklung (z. B. durch Entwicklungsverbünde) als auch bei der Plattform- (z. B. durch Justizcloud) und Infrastrukturentwicklung (z. B. durch IT-Dienstleister) parallele Umsetzungen erfordern und nur in ihrer Gesamtheit neue Funktionalitäten bzw. Nutzenstiftung für Endnutzende der internen und externen Domäne erzielen. Auf solche Epics könnten durch die integrierte Portfolioplanung gezielt Ressourcen allokiert werden. Im Rahmen der Zielbildentwicklung wurden beispielhaft drei Epics und verschiedene Lieferartefakte (sog. Features) innerhalb der Epics beschrieben (vgl. **Abbildung 39**).

Abbildung 39 | Illustrative Portfolioplanung der Justizcloud



Epic 1 kann bspw. die Schaffung der Kompetenz zum Betreiben der modernen Fachverfahren auf der Justizcloud umfassen. Ein erstes kurzfristiges Feature in diesem Epic wäre z. B. die Verfügbarkeit eines API-Gateways im Kontext der Integrationsplattform. Ein längerfristiges Feature wäre die Verfügbarkeit eines Event Hubs.

Analog wurde auch ein **Epic 2** rund um die Schaffung der Online-Services-Landschaft der externen Domäne definiert, in

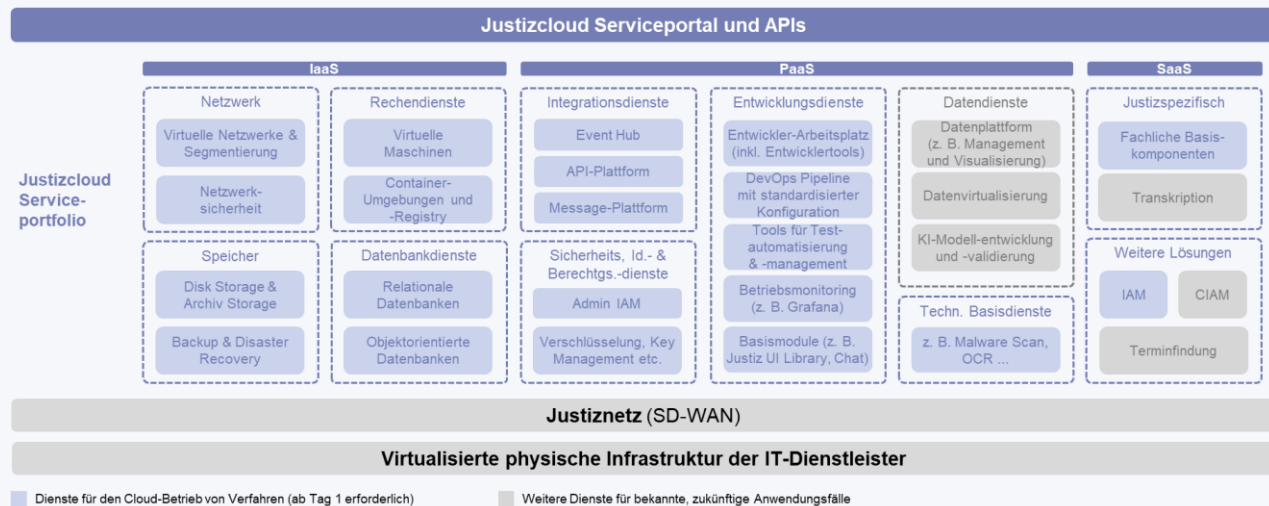
welchem die Verfügbarkeit des CIAM-Systems (vgl. **Kapitel 3.4.6.2**) ein essenzielles, aber aufgrund der Komplexität nur mittelfristig umsetzbares Feature wäre. Dies wäre Voraussetzung für das längerfristige Epic eines modernen *Justizportal Deutschland* (Arbeitstitel). **Epic 3** würde Innovationsthemen der Justiz bündeln. Dieses enthält Features, die Zukunftsfähigkeiten, wie z. B. einen Übersetzungsdienst als SaaS-Lösung, etablieren. Epics können dabei zum Teil individuelle, aber auch querschnittliche Bedarfe bzw. Fähigkeiten adressieren, so dass die zeitliche Anordnung deren Prioritäten aber auch inhärente Abhängigkeiten enthalten kann.

Für eine ganzheitliche Portfoliostrategie müsste die Justiz noch viele weitere Epics, auch außerhalb der Justizcloud, identifizieren und formulieren, damit sie nachhaltig technische und fachliche Weiterentwicklungs-, Modernisierungs- und Digitalisierungsinitiativen steuern und knappe Budgets allokalieren kann.

3.4.7.2 Entwurf Justizcloud Servicekatalog

Auf Basis der Anforderungen der modernen Anwendungen (vgl. **Kapitel 3.4.2.1**) sowie Zukunftsanforderungen der Justiz (vgl. **Kapitel 2.2.4**) wurde ein erster Justizcloud-Servicekatalog erstellt. Dieser enthält Services, deren Verfügbarkeit eine Voraussetzung für ein Onboarding erster Entwicklungsverbünde darstellt. Darüber hinaus werden auch einige Services für künftige Ausbaustufen skizziert. Die Services lassen sich nach drei Cloud-Ebenen gruppieren: Infrastruktur-, Plattform- und Software-as-a-Service (vgl. **Abbildung 40**).

Abbildung 40 | Entwurf eines Justizcloud-Servicekatalogs



Infrastructure-as-a-Service (IaaS): Die Justizcloud soll in Zukunft als zentrale, virtuelle Infrastrukturplattform dienen. Sie baut als Community Cloud auf der physischen, virtualisierten Infrastruktur der IT-Dienstleister und einem gemeinsamen SD-WAN auf. Auf der virtualisierten Infrastruktur werden nun infrastruktur-nahe Komponenten definiert. Dazu gehören einerseits klassische virtuelle Maschinen, auf denen bspw. die skalierbaren Container-Plattform-Umgebungen für den Fachverfahrensbetrieb ausgeführt werden. Auch die Container-Plattform ist ein IaaS-naher Dienst, der oft auch als Container-Plattform-as-a-Service (CaaS) bezeichnet wird.

Eine weitere IaaS-Dienstkategorie bilden virtuelle Netze bzw. Netzwerksegmentierung, bspw. zur Einrichtung unterschiedlicher Netzsegmente je Land und Anwendung (sog. Micro-Segmentierung). Auch Speicherdienste sind eine wichtige IaaS-Kategorie und umfassen schnelle Festplattenspeicher sowie langsamere, aber auch günstigere Dienste für langfristiges Archivieren. Die Speicherdienste bilden die Grundlage für die Datenbankdienstkategorie, in der sich relationale Datenbankdienste und Objektspeicher (bspw. Blob Storage oder noSQL-Datenbanken) befinden (vgl. **Kapitel 3.4.5**).

Plattform-as-a-Service (PaaS): Im Bereich der PaaS-Dienste werden auf der virtualisierten Infrastruktur und in Verbindung mit den IaaS-Diensten wichtige bundeseinheitliche Plattformdienste bereitgestellt. Hierunter fallen insb. technische Basisdienste (z. B. Malware Scanner) sowie Integrationsdienste (z. B. API-Gateway und Event Hub) einer Integrationsplattform (vgl. **Kapitel 3.4.4.1**), um eine moderne und passgenau integrierte Anwendungslandschaft zu befähigen. Zudem fällt auch die Bereitstellung von grundlegenden

Sicherheitsmechanismen wie einem zentralen Admin-IAM zur Administration der Justizcloud-Plattform sowie Verschlüsselungsmechanismen (z. B. Key Management- (sog. Vault) und Zertifikatsdienste) in den Bereich der PaaS-Services.

Darüber hinaus bilden die Entwicklungsdienste einen wesentlichen Teil der PaaS-Ebene der Justizcloud. Dies umfasst insb. Services, die in Summe den Entwicklungsarbeitsplatz ergeben (vgl. **Kapitel 3.5.6**). Diese Services unterstützen Entwickler und Betriebspersonal der jeweiligen Entwicklungs- und Betriebsverbünde dabei, ihre Anwendungen auf der Justizcloud auszubringen, zu überwachen und zu warten. Dazu gehören z. B. eine einheitliche Entwicklungsumgebung (Integrated Developer Interface (IDE)), ein gemeinsames Code- und Artefakt-Repository, ggf. sogar bereits bundeseinheitliche Elementen wie eine barrierefreies UI-Designsystem), eine einheitliche CI/CD-Toolchain, in der Entwickler individuelle Pipelines aufbauen und automatisiert ausführen können. Auch zählen dazu Werkzeuge zur Testautomation sowie das laufende Logging und Monitoring von Anwendungen (z. B. *Prometheus*, *Grafana*).

In verschiedenen Ausbaustufen der Justizcloud können dann weitere Plattformdienste, wie z. B. eine KI- und Datenplattform ergänzt werden (vgl. **Kapitel 3.4.7.1**). Je datengetriebener die Justiz wird, desto mehr könnten Entwickler KI-Modelle auf kuratierten Massendaten trainieren und die Modelle skalierbar in die eigenen Anwendungen einbinden. Die KI-Plattform könnte dabei auch sog. Modellvalidierungsdienste (sog. MLops) umfassen, damit die Justiz von Beginn an auch den erklärbaren und ethischen Einsatz von KI (sog. explainable and ethical AI) technisch berücksichtigen kann.

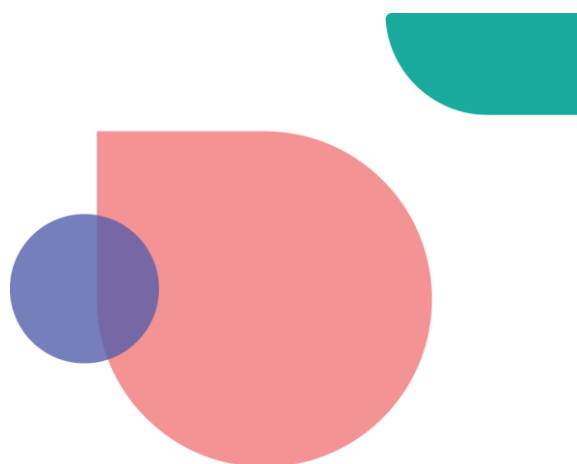
Gleiches gilt für eine moderne Datenplattform, welche die Justiz in die Lage versetzt, große Datenmengen strukturierter und unstrukturierter Daten zu verarbeiten (sog. Big-Data-Analysen). Aber auch Dienste zur Datenvirtualisierung als Grundlage zum Teilen von Daten können sukzessive ergänzt werden.

Software-as-a-Service (SaaS): Die Justizcloud dient primär als Entwicklungs- und Betriebsplattform für die Entwicklungsverbünde der Justiz. Damit werden die Entwicklungsverbünde befähigt, ihre Anwendungen sowie fachlichen Basiskomponenten als SaaS auf der Justizcloud zu betreiben.

Für Komponenten bzw. Dienste ohne aktuellen Entwicklungsverbund wäre denkbar, dass die Justizcloud diese für alle betreibt oder ein neuer Verbund gegründet wird. Bspw. könnten ausgewählte Basiskomponenten (z. B. Übersetzungsdienst, Dienst zum Datenteilen) sowie das zentrale IAM und CIAM hierunter fallen. Auch könnte die Justizcloud als zentrales

Vehikel zur Beschaffung und Integration externer, d. h. kommerzieller oder behördlicher SaaS-Lösungen, dienen (vgl. DVC). Diese werden vom externen Anbieter betrieben und die Justizcloud „betreibt“ dabei den einheitlichen, niederschweligen Zugang zu und die Abrechnung von diesem Dienst sowie die Integrationswege zu dessen Einbindung in die Justizcloud-Anwendungslandschaft. Auf diese Weise könnten über die Justizcloud auch IaaS-, PaaS- und SaaS-Dienste kommerzieller Public Cloud-Umgebungen für die Justiz erschlossen werden (vgl. **Kapitel 3.3.2**).

Der dargestellte Servicekatalog bildet eine erste Grundlage für die Definition und Priorisierung von Justizcloud-Diensten. Im Zuge des Justizcloud-Aufbaus sollte er mit den Cloud-nutzenden Entwicklungsverbünden weiter detailliert und priorisiert werden. Im Folgenden wird das technische Zielbild zur Entwicklung und Bereitstellung der Justizcloud-Services beschrieben.



3.5 Technische Zielbildebene

Das technische Zielbild für die bundeseinheitliche Justizcloud wurde auf Basis der Prämissen (vgl. **Kapitel 3.1.1**), strategischen Zielen (vgl. **Kapitel 3.2**) sowie der fachlichen Zielbildebene abgeleitet. Dabei wurden viele Anforderungen bspw. der Cloud-Anwendungslandschaft (vgl. **Kapitel 3.4.2**), der Mandanten- (vgl. **Kapitel 3.4.3**), Schnittstellen- (vgl. **Kapitel 3.4.4**) und Datenkonzepte (vgl. **Kapitel 3.4.5**) sowie der Cloud-Servicekatalog (vgl. **Kapitel 3.4.7.2**) weiter detailliert und technisch unterlegt. Zudem sind die Erkenntnisse der Ist-Analyse zu bestehenden Cloud-Angeboten der IT-Dienstleister (vgl. **Kapitel 2.2.2**) sowie zu laufenden Cloud-Initiativen (vgl. **Kapitel 2.2.3**, z. B. DVS) maßgeblich in die Ausgestaltung des technischen Bereitstellungsmodells eingeflossen.

Nachfolgend werden zunächst mögliche Bereitstellungsmodelle diskutiert und dabei laufende Cloud-Initiativen und Angebote (vgl. **Kapitel 3.5.1**) aufgegriffen. Anschließend wurde auf Basis der strategischen Ziele und Prämissen ein **Bereitstellungsmodell** (vgl. **Kapitel 3.5.1.4**) ausgewählt. Darauf aufbauend wird ein **Netzkonzept** entwickelt (vgl. **Kapitel 3.5.2**), dass eine einheitliche Verbindung der Bestandumgebungen bei IT-Dienstleistern mit der Justizcloud ermöglicht.

Für die Ausgestaltung der Justizcloud-Plattform wird zunächst das Kernelement, eine bundeseinheitliche **Container-Plattform** (vgl. **Kapitel 3.5.3**) technisch detailliert. Innerhalb des Justiznetzes und der Container-Plattform werden dann **Mandanten-** und **Datenpersistenzkonzept** sowie ein **Administrationskonzept** (vgl. **Kapitel 3.5.5**) definiert. Für eine einheitliche Entwicklung und einen einheitlichen Betrieb auf der Justizcloud wird der integrierte Justizcloud-**Entwicklerarbeitsplatz** (vgl. **Kapitel 3.5.6**) ausgeführt sowie relevante Cloud-native Entwicklungskonzepte wie **DevOps** und **CI/CD** beschrieben. Zudem wird die **Integrationsplattform** (vgl. **Kapitel 3.5.4.3**), wie im fachlichen Zielbild definiert, technisch ausgestaltet. Abschließend wird ein **PoC** (vgl. **Kapitel 3.5.7**) beschrieben, der zusammen mit IT-Dienstleistern der Länder durchgeführt wurde, um viele der o. g. Konzepte nachzuweisen und Erfahrungen für eine mögliche Aufbauphase der Justizcloud zu generieren.

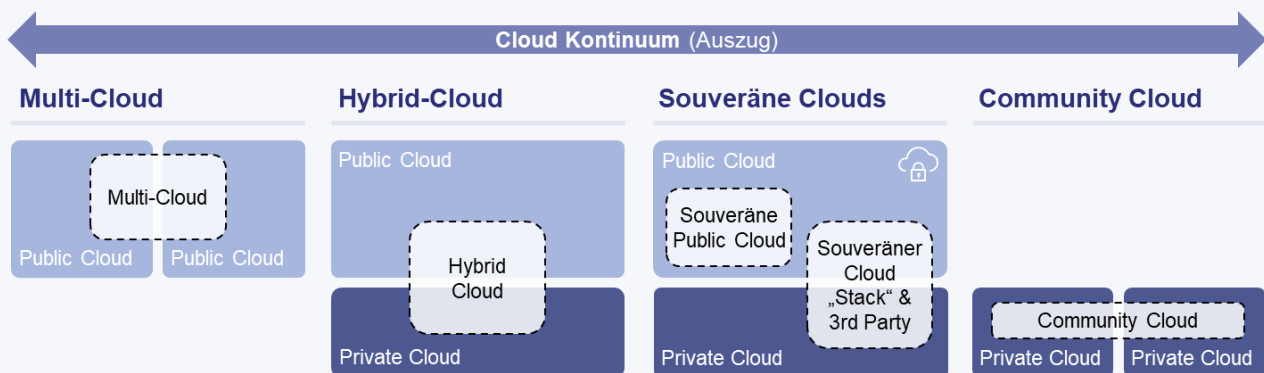
Das technische Zielbild wurde gemeinsam durch ein interdisziplinäres Fachpanel mit Vertretern von IT-Dienstleistern, IT-Stellen der Justiz, Anwendungsbetrieben und Justizministerien in wöchentlichen Workshops konzipiert, diskutiert sowie seine Machbarkeit bewertet. Die im Fachpanel getroffenen Expertenmeinungen und entwickelten Konzepte wurden in der Zielbildentwicklungsphase turnusmäßig dem Sounding Board vorgestellt und deren Machbarkeit bewertet.

3.5.1 Auswahl des Bereitstellungsmodells

3.5.1.1 Bereitstellungsmodelle und Souveränität

Bei der Auswahl des passenden Bereitstellungsmodells, d. h. der Cloud-Umgebung für die Justiz, gibt es im sog. Cloud-Kontinuum viele denkbare Alternativen (vgl. **Abbildung 41**). Dabei kann zunächst zwischen verschiedenen logischen Ausprägungen unterschieden werden. Eine grundlegende Unterscheidung bildet die Public vs. Private Cloud-Kategorie.

Abbildung 41 | Logisches Cloud-Kontinuum



Bereitstellungsmodelle mit Public Cloud

Public Clouds sind kommerzielle Angebote, die grundsätzlich an eine breite Masse von Kunden, d. h. den Markt, gerichtet sind. Als Beispiele für Public Cloud-Anbieter sind allen voran die großen Hyperscaler (*Microsoft*, *Google* und *Amazon*) zu nennen, aber auch größere und kleine (inter-)nationale Cloud-Anbieter (z. B. *Oracle*, *Alibaba*, *OVHcloud* oder *Ionos*, vgl. **Kapitel 2.2.3**). Die Cloud-Anbieter können ihre Public Cloud-Angebote, bzw. Teile davon, auch auf Kunden mit industriespezifischen Anforderungen zuschneiden, z. B. mit bestimmten Zertifizierungen, vertraglichen Sonderbestimmungen (z. B. dedizierte Hardware) oder zusätzlichen Berechtigungen, wie Zutritt zu Rechenzentren. Dabei stehen vor allem Industrien mit besonders sensiblen Daten und Souveränitätsanforderungen im Fokus, bspw. Angebote für Kunden der Finanzindustrie, des Gesundheitswesens oder staatliche Institutionen (sog. Government Cloud-Angebote).

Der kommerzielle Cloud-Anbieter hat mit seinem Cloud-Angebot grundsätzlich eine Gewinnerzielungsabsicht, investiert damit aber auch kontinuierlich in das Cloud-Angebot

(bspw. investiert jeder Hyperscaler jährlich über 1 Mrd. USD in Forschung und Entwicklung), weshalb kommerzielle Public Clouds oftmals auch Innovationsführer mit einem breiten Cloud-Dienste-Portfolio im Cloud-Markt sind (vgl. **Abbildung 42**).

Abbildung 42 | Auszug eines exemplarischen Cloud-Services-Katalogs

Netzwerk	Speicher	Rechen- dienste	Databank- dienste	Integrations- dienste	Sicherheits-, Identitäts- & Berechtigungsmanagement		Administrations- & Automatisierungsdienste		Entwicklungsdienste		App- dienste	Mobile Services	Analytik & Big Data	Künstliche Intelligenz	IoT & VR/AR Dienste	Unternehmens- anwendungen	
Virtual Networking	Attached Disk Storage	Bare Metal / Dedicated Compute	Cloud-native RDBMS	Data Import Export	Account Management	Authentication Authorization	Network Monitoring	Best Practices Advisor	App Deployment Automation	Cloud IDE	Application Hosting	Mobile Apps Development	Data Orchestration	Speech Recognition	IoT Edge	Content Management	
Hybrid Connectivity	Object Storage	Virtual Servers	Non-native managed RDBMS	Data Integration & ETL	Compliance	Security reporting	Resource Monitoring	Fleet Deployment Orchestration	Distributed Apps	API Management	Business Apps	Mobile App Testing	Data Discovery	Vision Recognition	IoT Gateway	Managed Email Services	
Dedicated Connectivity	Shared File Storage	Container Compute	No-SQL	VM Import Export	Directory Services	DDoS Protection Service	Configuration Change Management	Instance Management	App Testing	API Apps	Send Email Notifications	Mobile Identity & Data Sync	Big Data Processing	Language Recognition	IoT Events	Unified Comms	
Network Load Balancing	Archiving – Cool Storage	Container Registry	Graph Database	Data Migration	Information Protection	Application Firewall	Cloud API Log Service	Job Scheduler	DevOps Pipeline	Build Automation	Media Transcoding	Mobile Targeting	Stream Analytics	Text-to-Speech	Virtual & Augmented Reality	Application Streaming	
Web Load Balancing	Hybrid Storage	Event-based Compute	In-memory Database	Integration Services	HSM Security Module	Firewall Management	Operations Analytics & Insights	Infra-as-a-Code Templates	Micro-services	Code Analysis	Messaging Service	Mobile Device Management	Visualization	Translation		Desktop as-a-Service	
Domain Name Service	Backup	Batch processing	Data Warehouse	Server Migration	Certificate Management	Key Management	Exception Reporting	Application Discovery	Managed Source Control	Continuous Delivery	Workflow Service	Mobile Analytics	Data Quality Service	Machine Learning		Market-place	
Internet Traffic Distributor	Disaster Recovery	Scalability	Caching	Enterprise Application Integration		Secrets Management	Service Catalog	Governance and Cost Controls	Web Apps	Game Development	Push Notification		Predictive Analytics	Machine Learning Training		Portal	
Content Delivery Network		Simple Compute	Master Data Management								Managed Search			Intelligent Bots			
IaaS									PaaS							SaaS	

Der kommerzielle Cloud-Anbieter betreibt meist eigene Rechenzentren, in denen die kommerzielle Cloud-Software des jeweiligen Anbieters, quasi das „Betriebssystem“ der Cloud, installiert ist. Dies ist der Fall, weil Rechenzentrum und „Betriebssystem“ eine Einheit ergeben, um die physische Infrastruktur zu virtualisieren und as-a-Service skalierbar anbieten zu können. Da die Cloud-Software per Definition ein proprietäres Gut des Anbieters ist, entsteht bereits allein durch die Nutzung des Public Cloud-„Betriebssystems“ ein gewisser Vendor-LockIn. Bspw. müssen die technische Cloud-Anbindung, Bedienungswissen sowie Verträge und Abrechnungsmechanismen anbieterspezifisch aufgebaut werden. Auch können die Cloud-Dienste des Anbieters nur mit dem Cloud-Betriebssystem des Anbieters konfiguriert werden. So entstehen für die produktive Erschließung (z. B. für Landing Zone, Datentransfer, Verträge, etc.) des Cloud-Angebots bereits signifikante Kosten und Aufwände.

Kunden nutzen die Cloud-Software, um sich innerhalb dieser kommerziellen Cloud-Umgebung eigene Anwendungen auf Basis von Cloud-Diensten des kommerziellen Anbieters zu erstellen. Die dafür verwendbaren Cloud-Dienste umfassen dabei sowohl infrastrukturnahe- (IaaS), Plattform- (PaaS) und Software-as-a-Service (SaaS) Dienste (vgl. **Abbildung 42**)

und sind so miteinander verzahnt, dass sie aufeinander aufsetzen und dementsprechend miteinander abgerechnet werden können (sog. Pay-per-use).

Zwar kann die kommerzielle Public Cloud-Umgebung von vielen Kunden weltweit genutzt werden, jedoch bedeutet das nicht, dass die Kundendaten bzw. Anwendungen durch andere Kunden bzw. Dritte eingesehen werden können oder auf diese zugegriffen werden kann. Denn für jeden Kunden wird innerhalb der Public Cloud-Umgebung eine dedizierte virtuelle Umgebung (sog. Mandant bzw. Tenant) geschaffen, der nur vom jeweiligen Kunden, über ein dediziertes, wenn auch virtuelles Netz (z. B. Virtual Private Network (VPN)), ansprechbar ist. Dieses VPN verbindet die lokale Kundenumgebung mit der kommerziellen virtuellen Umgebung und wird vom Kunden aufgebaut, kontrolliert und mit eigenen Zertifikaten gesichert. Damit ist ein Kunde auch in der Lage, innerhalb der virtuellen Public Cloud-Umgebung viele weitere virtuelle Sub-Umgebungen (bspw. Netzsegmente je Anwendung) zu erzeugen. Das Public Cloud-Netzsegment genießt aber oftmals eine etwas geringere Vertrauensstellung als das lokale Netz im eigenen Rechenzentrum, weil bspw. die Gewährleistung der physischen Sicherheit beim Cloud-Anbieter und demnach in den Händen eines Dritten beruht.

Public Cloud bedeutet nicht, dass Daten automatisch im Internet stehen. Dafür muss der Kunde in einem der o. g. Netzsegmente erst entsprechende Vorkehrungen treffen (z. B. Firewall-Freischaltungen, Reverse Proxies und Loadbalancer sowie DNS-Konfigurationen), damit eine Anwendung überhaupt aus dem Internet erreichbar ist.

Bei der Public Cloud sollten einige besondere Varianten hervorgehoben werden (vgl. **Abbildung 41**). **Multi Cloud** ist eine Nutzungsform, bei der zwei oder mehr Public Cloud-Umgebungen gleichzeitig genutzt, ggf. sogar zusammengeschaltet, werden. Dies kann fachliche Gründe haben, um bspw. Dienste zu nutzen, die einer der Public Cloud-Anbieter nicht anbietet. Auch technische Gründe können dafür sprechen, um bei international tätigen Unternehmen Rechenzentren in der Nähe der eigenen Arbeitsstätten und damit geringere Latenzen zu haben. Finanzielle Gründe können eine Rolle spielen, um mit dem sog. FinOps-Ansatz, je nach Cloud, den günstigsten Cloud-Dienst zu nutzen. Aber auch rechtliche bzw. sicherheitsrelevante Gründe können es erfordern, mehrere (Public) Cloud-Umgebungen zu erschließen, um im Krisenfall wechselfähig und damit unabhängiger zu sein.

Eine weitere Nutzungsform ist die **Hybrid Cloud**. Bei einer Hybrid Cloud wird eine Public Cloud in Verbindung mit einer Private Cloud genutzt. Werden mehrere Public Clouds mit einer Private Cloud verbunden, spricht man wiederum von einer Hybrid Multi Cloud. Die Hybrid Cloud kann einerseits dazu dienen, eine gewisse Rückholfähigkeit in die Private

Cloud und damit eine Anbieterunabhängigkeit zu etablieren. Andererseits können sich die Umgebungen fachlich komplementär ergänzen, so dass man Public Cloud-Dienste nutzt, die in der Private Cloud nur schwer oder gar nicht herstellbar wären. Ein aktuell viel diskutiertes Beispiel ist das Training von KI-Modellen mit hoch-skalierbarer, nahezu unbegrenzter Kapazität in der Public Cloud. Die Nutzung des trainierten Modells (sog. Inferenz) geschieht jedoch in Anwendungen auf der eigenen Private Cloud. Eine weitere Nutzungsform des hybriden Ansatzes ist die Entwicklung von Cloud-nativen Anwendungen mit modernen Werkzeugen der Public Cloud, aber die Ausbringung und Produktion der Cloud-Anwendung in der Private Cloud (vgl. hierzu auch **Kapitel 2.2.3.2**).

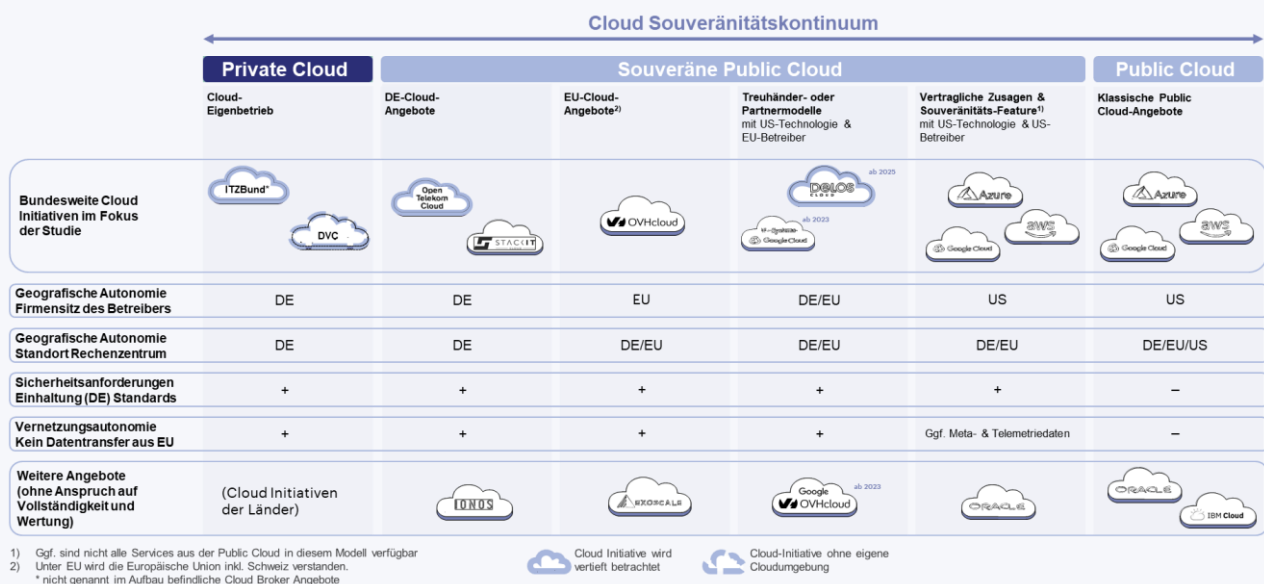
Sowohl der Multi Cloud- als auch der Hybrid Cloud-Ansatz steigern die Anbieterunabhängigkeit und können somit als Elemente einer souveränen Cloud-Strategie verstanden werden. Darüber hinaus können Kunden weitere, z. T. Technische. Maßnahmen ergreifen, um eine souveräne Public Cloud-Nutzung sicherzustellen. Bspw. können sie ihre Anwendungen Cloud-agnostisch entwickeln (sog. technologische Souveränität). Dabei sollten möglichst nur Dienste genutzt werden, die vergleichbar auch bei anderen Anbietern verfügbar sind. Des Weiteren kann entschieden werden, welche Daten überhaupt in der Cloud (d. h. den Rechenzentren des Cloud-Anbieters) gehalten sowie ob und wie sie dort verschlüsselt werden, aber auch wo der Schlüssel dafür liegt (sog. Datensouveränität, vgl. **Kapitel 3.4.5**). Wie dargestellt, entsteht durch die Nutzung von Public Cloud immer eine gewisse Abhängigkeit und immer der Bedarf, Souveränität und Unabhängigkeit für die eigene Organisation auszuprägen und dementsprechende Public Cloud-Angebote zu wählen und/ oder Maßnahmen zur Sicherstellung der Wechsel- und/ oder Rückholfähigkeit zu ergreifen. Daher bieten viele Public Cloud-Anbieter auch innerhalb ihres eigenen Serviceportfolios souveräne Cloud-Angebote mit speziellen Souveränitätsfeatures an, die aber nicht immer in allen Ländern verfügbar sind.

Bei **Souveränen (Public) Clouds** (vgl. **Abbildung 41**) muss man zunächst verschiedene Souveränitätsdimensionen bzw. -ebenen unterscheiden. Zum einen ist entscheidend, wo sich der rechtliche Hauptsitz des Anbieters befindet und unter welchen Rechtsrahmen dieser fällt, d. h. ob er ggf. nicht-europäischen Gesetzen und Behörden unterliegt (vgl. *Alibaba Cloud* oder US-Hyperscaler). Dann sind der Standort des Rechenzentrums und die Backup-Standorte des Anbieters relevant, um zu verstehen, ob die eigenen Daten nationale Grenzen verlassen. Zudem ist auch relevant, welchem nationalen Rechtsrahmen die (Tochter-) Gesellschaft unterliegt und wie rechtlich unabhängig diese von der Firmenzentrale ist. Letztlich ist von Bedeutung, dass der Nutzende Kontrolle über die Übermittlung seiner Daten

in Drittstaaten behält oder ausreichende Sicherheitsmechanismen des Dienstleisters vorgehalten werden. Diese Anforderungen gelten bis auf die Ebene der Meta- und Telemetriedaten (z. B. für Support- oder Abrechnungszwecke).

Weil Souveränität in vielen Industrien und v.a. in der öffentlichen Verwaltung ein wichtiges und z. T. auch sicherheitspolitisches Thema ist, haben kommerzielle Anbieter viele verschiedene **Souveräne (Public) Cloud-Angebote** entwickelt (vgl. **Abbildung 43**).

Abbildung 43 | Cloud-Souveränitätskontinuum und -beispiele (Accenture)



Zum einen bieten viele Cloud-Anbieter sog. Souveränitätsfeatures an. Diese können von lokalen Rechenzentrumsstandorten bis zu vertraglichen Zusagen und Sonderbestimmungen, wie z. B. Besuchs- und Auskunftsrechte, reichen. Andererseits können hierunter auch internationale, regionale (z. B. *ISO27001*, *SOC1-3*, *NIST 800*, *BSI-Grundschutz* und *C5 Kriterien*) sowie industriespezifischen Zertifizierungen (z. B. *HIPAA*, *ENISA*) gefasst werden. Dabei ist zu beachten, dass viele der vorgenannten Zertifizierungen nicht allgemeingültig sind, sondern z. T. für jeden einzelnen Cloud-Service vorliegen müssen und demnach dessen Verfügbarkeit einschränken. So ist bspw. bei vielen Hyperscalern nicht jeder Service auch an jedem Standort verfügbar.

Ergänzend kooperieren einige Public Cloud-Anbieter mit nationalen Gesellschaften in sog. Partner- und Treuhändermodellen. Dabei wird bspw. die Cloud-Software, d. h. das Betriebssystem, in den Rechenzentren eines Dritten installiert, der dann die Cloud betreibt. Beispiele

hierfür sind nationale Angebote der *Delos Cloud*, die speziell für den Bund *Microsoft Azure/ M365* bereitstellen soll oder auch öffentliche Angebote der *T-Systems* oder *OVHcloud*, die neben den eigenen Angeboten auch z. B. jeweils *Google* Cloud-Software in den eigenen Rechenzentren anbieten.

Unabhängig davon sind es auch diese nationalen Anbieter, die sowohl Public Cloud-Angebote EU-weit (z. B. *OVHcloud*, *Ionos*) oder nur in speziellen Ländern (z. B. *StackIT* und *Open Telekom Cloud* in Deutschland, vgl. **Kapitel 2.2.3**) anbieten.

Bereitstellungsmodelle mit Private Cloud

Private Clouds sind im Gegensatz zu Public Cloud-Umgebungen grundsätzlich nur an eine begrenzte Anzahl von Kunden (z. B. Behörden, Forschungseinrichtungen, Unternehmen einer Branche) oder eine einzelne Organisation (z. B. ein Unternehmen) gerichtet. Eine Private Cloud wird daher auch oftmals von den beteiligten Organisationen/ Trägern gesteuert, finanziert sowie auf eigener Infrastruktur in dedizierten Rechenzentren betrieben. Aufgrund dessen ist eine Private Cloud per Definition souveräner als eine Public Cloud.

Zur Errichtung einer Private Cloud muss im eigenen Rechenzentrum spezielle, virtualisierbare (sog. HCI-fähige) Infrastruktur/ Hardware vorhanden sein. Zudem ist eine sog. Hypervisor Software zur Virtualisierung und Orchestrierung dieser Infrastruktur zu IaaS-Diensten erforderlich. Auch in einer Private Cloud werden auf virtueller Infrastruktur Plattformdienste (PaaS) bereitgestellt. Auf den Plattformen werden SaaS-Dienste ausgebracht. PaaS- und SaaS-Dienste sind dabei passgenau auf die Betreiber bzw. die begrenzte Zahl von Kunden zugeschnitten und daher, auch aufgrund der geringeren finanziellen Ressourcen der Betreiber/ Träger, in geringerem Umfang vorhanden als bei großen Public Cloud-Anbietern.

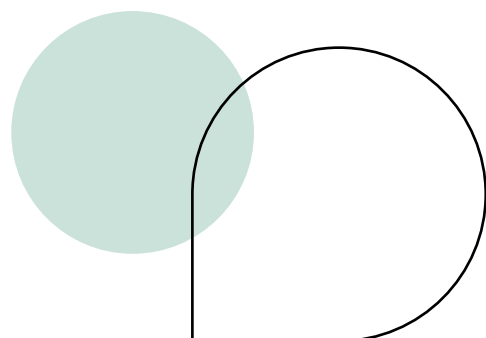
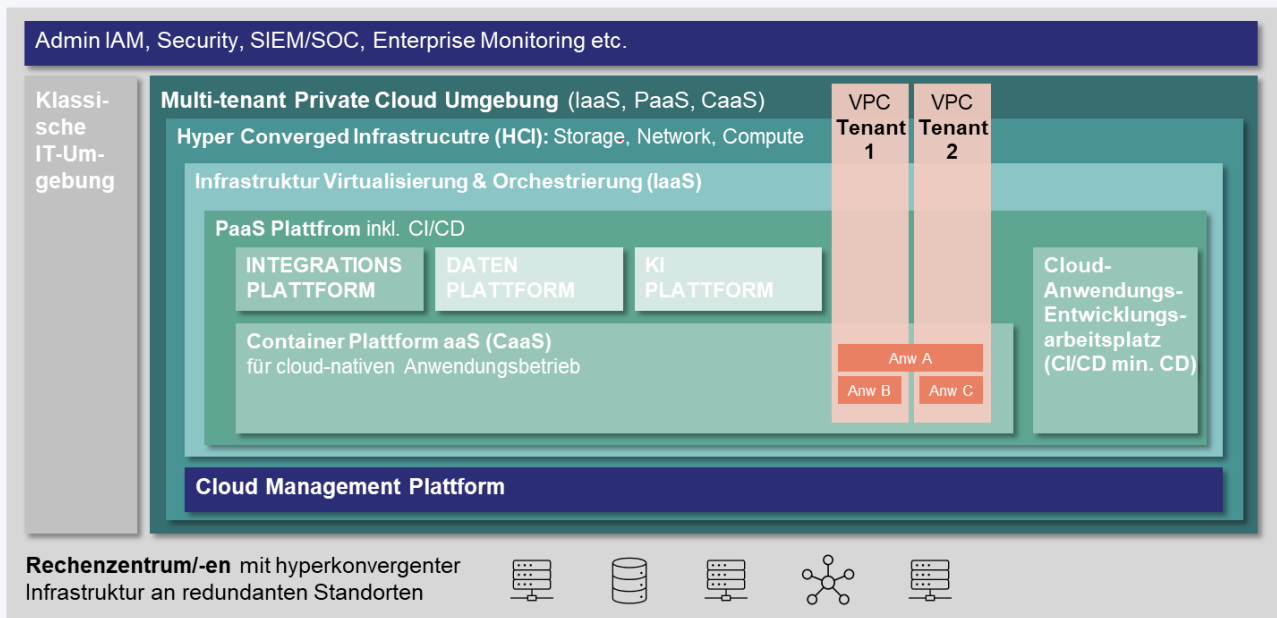
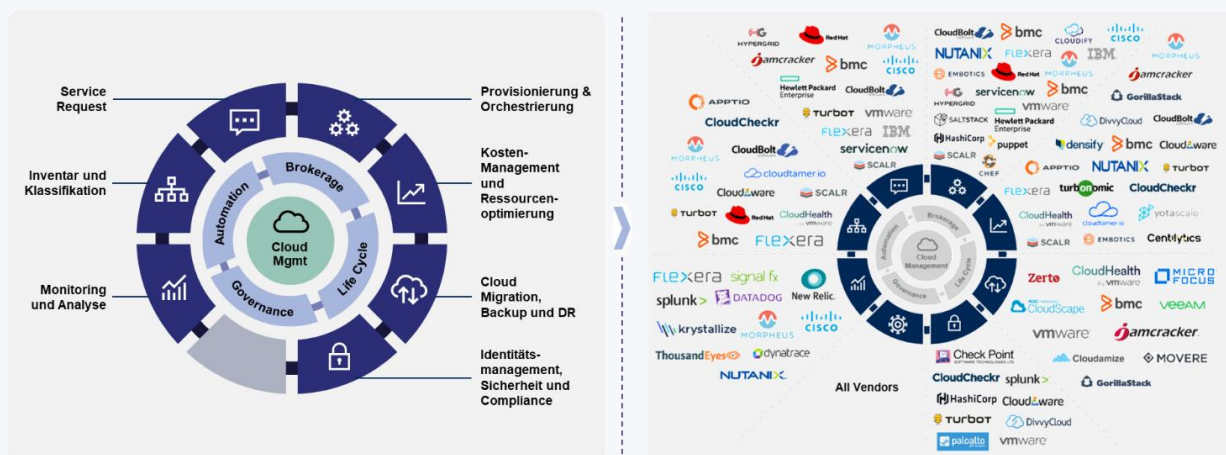


Abbildung 44 | Beispielhafte Private Cloud-Architektur (Accenture)



Eine Private Cloud zu erstellen und zu betreiben ist komplex (vgl. **Abbildung 44**). Abgesehen von der entsprechenden Hardware sind insb. die entsprechenden Softwareebenen und Komponenten (sog. Cloud-Management-Software) eine Herausforderung. Der Markt für Cloud-Management-Software hat sich in den letzten Jahren aber stark weiterentwickelt, denn der Bedarf für Private Cloud-Lösungen, insb. von Organisationen, die bereits über eigene moderne Rechenzentren verfügen, wie z. B. öffentliche IT-Dienstleister oder Großbanken, ist groß.

Abbildung 45 | Cloud-Management-Software Kategorien und Markt (Gartner)



Quelle: Gartner

Aufgrund der inhärenten Komplexität haben sich neben dem eigenen Aufbau einer Private Cloud verschiedene weitere Bereitstellungsmodelle etabliert. Beim sog. **Private Cloud Stack** wird Public Cloud-Software eines Public Cloud-Anbieters auf eigener Infrastruktur installiert und von der eigenen Organisation betrieben. Man holt defacto die Public Cloud ins eigene Rechenzentrum, kann das Gros der Public Cloud-Dienste, meist aber nicht alle, auch lokal nutzen, jedoch nur in den eigenen „Grenzen“ skalieren. Dafür wird oftmals speziell zertifizierte Hardware benötigt und die lokale Installation muss regelmäßig Verbindung zur Cloud (z. B. Telemetriedaten, Incidents) aufnehmen und auch aktualisiert werden. Bei der Aktualisierung des Releases haben Private Cloud-Kunden oft nur begrenzte Zeit, damit sie nicht zu „lang“ vom Hauptprodukt abweichen. Beispiele hierfür sind *Azure Stack Hub* oder *AWS Outpost*. Dieses Modell unterscheidet sich insofern vom o. g. Treuhänder Modell für die Public Cloud, als dass die Cloud-Software im eigenen Rechenzentrum und nicht in dem eines kommerziellen Anbieters ausgeführt wird.

Eine besondere Form des Private Cloud-Modells bietet *Oracle* an. Dabei wird nicht nur die Cloud-Software im eigenen Rechenzentrum installiert, sondern ganze Serverinfrastrukturen mit jeweils vorinstallierter Cloud-Software (vgl. *Oracle OCI*). Der Kunde schafft dafür im eigenen Rechenzentrum einen entsprechend abgeschotteten Bereich, stellt Strom, Kühlung und Netzwerkverbindungen sowie das Betriebspersonal bereit.

Daneben gibt es das sog. **Third Party Private Cloud**-Modell. Dabei betreibt ein Dritter die Private Cloud-Software im eigenen Rechenzentrum. Ein Beispiel hierfür ist die [Private Cloud des ITZBund](#), die von *Ionos* in den Rechenzentren des *ITZBund* betrieben wird. Dabei wird vorrangig die Software des Dritten genutzt. Natürlich haben Organisationen auch die Möglichkeit, generell Dritte mit dem Betrieb der Private Cloud mit Cloud-Management-Software (vgl. **Abbildung 45**) in den eigenen Rechenzentren zu betrauen. Dabei kann die Organisation meist eine passgenaue Produktauswahl für den eigenen Cloud-Betrieb wählen.

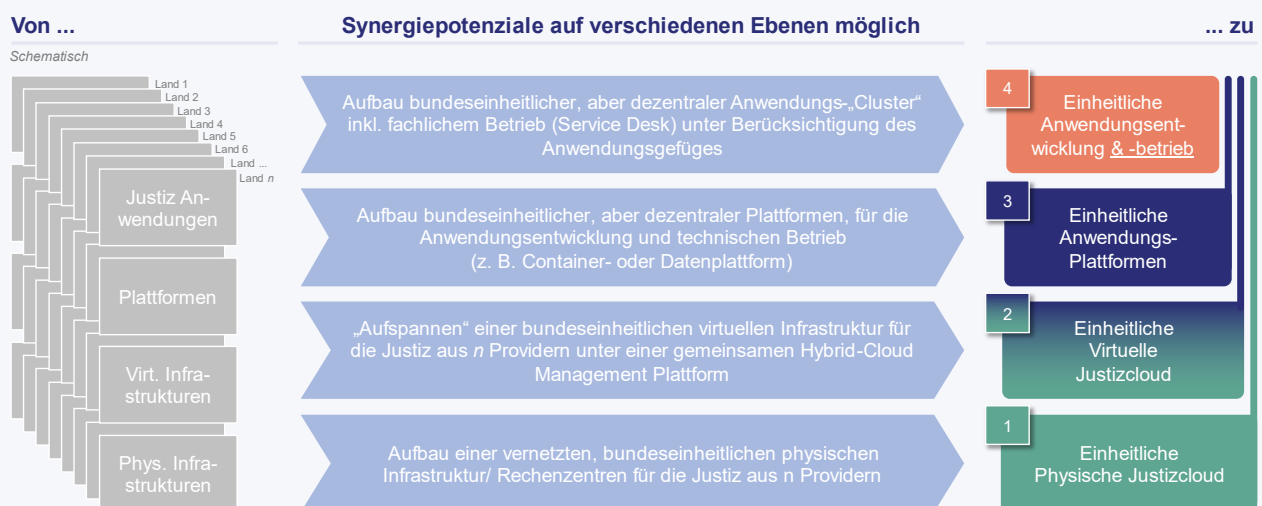
Alternativ dazu teilen sich bei einer (Private) **Community Cloud** (vgl. **Abbildung 41**) mehrere Parteien den Aufwand zum Betrieb der gemeinsamen Private Cloud. In diesem Modell werden die Rechenzentren der teilnehmenden Organisationen miteinander vernetzt und auf der Softwareebene als ein „gespanntes“ Rechenzentrum verwaltet. Dafür stellt jede Organisation virtualisierte Infrastruktur bereit, auf der dann gemeinsame Plattformdienste (PaaS) usw. ausgebracht werden können. Aufgrund der föderierten Infrastruktur werden Community Clouds auch manchmal als Federated Cloud bezeichnet. Dadurch können sich die Beteiligten Kosten und Betrieb der gemeinsamen Private Cloud teilen bzw. jeder bestimmte

Kernkompetenzen einbringen. Die Community Cloud ist damit ähnlich einer Multi Cloud im Public Cloud-Kontext, jedoch zeichnet sie sich dadurch aus, dass die PaaS-Ebene nur einmal anstatt n-Mal existiert. Auf EU-Ebene gibt es verschiedene Beispiele für Private Community Clouds, bei der die Mitglieder ihre virtualisierte Infrastruktur entweder zusammen-schließen oder für Dritte verfügbar machen. So z. B. Universitäten und Forschungseinrichtungen (z. B. [EGI](#)), Zentralbanken, aber auch staatliche Institutionen wie die [G-Cloud](#) (Belgien) oder die [GovCloud](#) (Dänemark). Zudem arbeitet die EU-Kommission mit [Simpl](#) an Konzepten und Toolkits zur Stärkung des Community/ Federtet Cloud-Konzepts.

3.5.1.2 Untersuchte Potenzialebenen

Nachdem die grundsätzlich denkbaren Cloud-Bereitstellungsmodelle und deren Souveränitätscharakteristika untersucht wurden, werden im Folgenden die Potenzialebenen zum Einsatz von Cloud in der Justiz untersucht. Die Potenzialebenen decken sich weitgehend mit den Wertschöpfungsebenen einer Cloud-Umgebung (vgl. **Abbildung 42**), d. h. der physischen Infrastruktur, der virtuellen Infrastruktur, der Plattformanwendungen sowie der Anwendungsebene, also dem eigentlichen Anwendungsgefüge der Justiz (vgl. **Abbildung 46**).

Abbildung 46 | Potenzialebenen und Synergiepotenziale

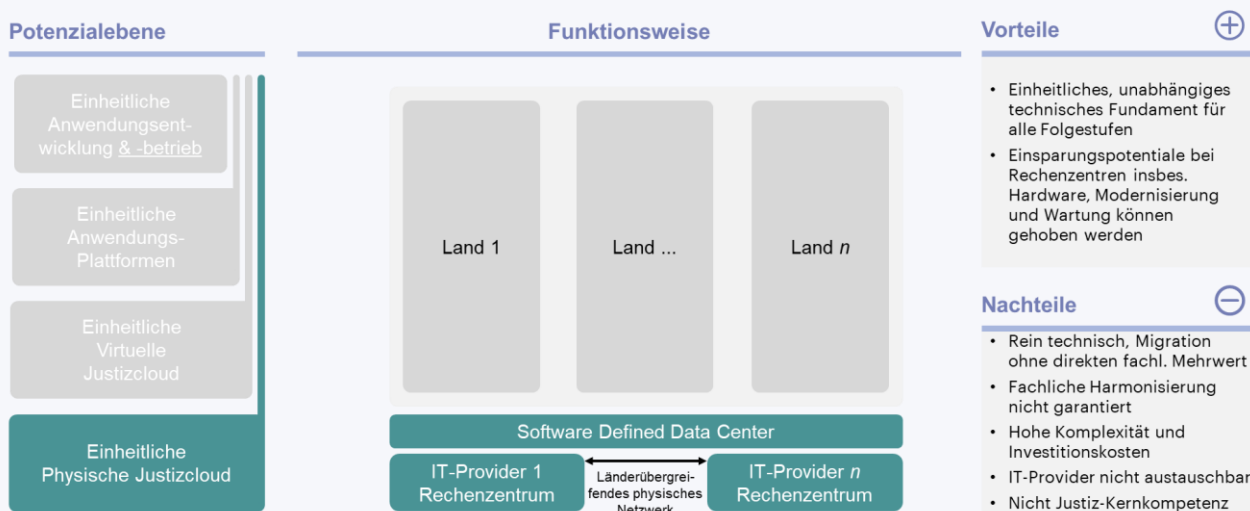


Derzeit besteht eine große Heterogenität auf allen Potenzialebenen. Neben den unterschiedlichen Infrastrukturen und Cloud-Kapazitäten der IT-Dienstleister bestehen viele unterschiedliche Infrastrukturdienste (z. B. eingesetzte Datenbanktechnologien). Auch auf der Plattformebene ist eine hohe Heterogenität zu verzeichnen. So z. B. bei den eingesetzten

Container-Technologien (vgl. **Kapitel 3.5.4.2**). Auch auf der Anwendungsebene besteht, bis auf wenige Ausnahmen (z. B. *AuRegis*), eine hohe länderspezifische Heterogenität bei eingesetzten Justizanwendungen und Technologien. Insofern bestehen grundsätzlich große Synergiepotenziale auf allen vier Ebenen und verschiedene Lösungsansätze für eine bundeseinheitliche Justizcloud sind denkbar. Je mehr Potenzialebenen durch die Justizcloud adressiert werden, desto höher das Synergiepotenzial. Jedoch steigen auch die Kosten der Transformation sowie die technischen (z. B. Daten- und Anwendungsmigrationen), organisatorischen (z. B. Justiz-IT-Betriebsmodelle) sowie rechtlichen Auswirkungen (vgl. Kontrahierungszwänge) auf das bestehende Gesamtgefüge.

Auf Ebene der physischen Infrastruktur ist es denkbar, eine einheitliche physische Justizcloud zu realisieren. Das würde bedeuten, die gesamte Justiz-IT in ein neues justizeigenes Rechenzentrum (RZ) samt Backup-RZ zu verlagern. Dieses Vorgehen kann sowohl den Aufbau eigener RZs als auch die Nachnutzung bestehender (z. B. der Justiz-IT-Dienstleister) oder von Dritten (z. B. dedizierter RZ-Anbieter, *ITZBund*, etc) betriebener RZs beinhalten. Dabei können auch mehrere gleichartige RZs zu einem sogenannten Software Defined Data Center zusammengeschlossen werden. Diese physischen RZs sowie Backup-RZs müssten hinreichend groß dimensioniert sein, um die gesamte Justiz-IT Deutschlands aufnehmen zu können sowie über eine ausreichend große Netzinfrastruktur miteinander verbunden zu werden.

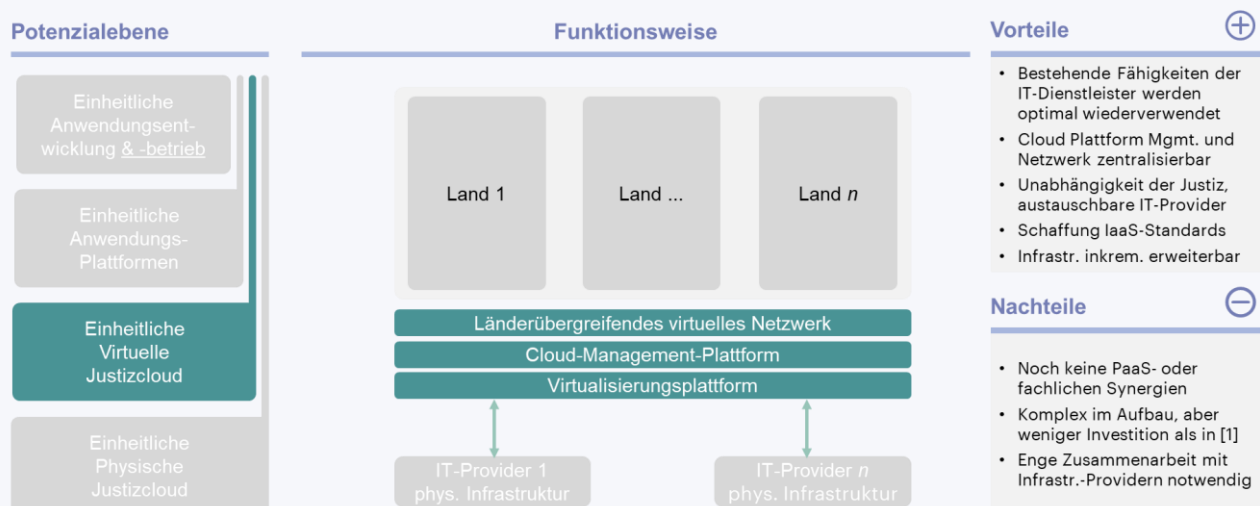
Abbildung 47 | Vor- und Nachteile einer Vereinheitlichung auf physischer Infrastrukturebene



Auf Ebene der physischen Infrastruktur könnte die Justiz zwar Betriebs- und Modernisierungskosten für RZ und Hardware bündeln. Es wären aber rein technische Synergien. Zudem würde es enorme Investitionskosten erfordern, die Justiz-IT-Infrastruktur in das gewählte RZ samt Backup-RZ zu verlagern bzw. ein solches neu aufzubauen. Dabei ist auch zu beachten, dass der RZ-Betrieb keine Kernkompetenz der Justiz ist. Durch die Auswahl mehrere RZ-Betreiber könnte zwar eine gewisse Souveränität und Unabhängigkeit erhalten bleiben, jedoch würde dieses Modell keine der fachlichen Herausforderungen (vgl. **Kapitel 2.2.1**) lösen. Denn nach der Migration würden auf der bundeseinheitlichen Infrastruktur immer noch heterogene Plattformen und Anwendungslandschaften betrieben (vgl. **Abbildung 47**). Daher muss ein Justizcloud-Zielbild Synergien auf höheren Ebenen realisieren.

Ergänzend bzw. auch alternativ dazu ist eine einheitliche, **virtuelle Justizcloud** denkbar. Dabei wird auf bestehender Justizinfrastruktur und/ oder der eines Dritten eine gemeinsame Umgebung bzw. ein Pool bundeseinheitlicher virtueller Infrastrukturdienste für die Justiz geschaffen. Auf dieser könnten dann nachgelagerte Potenzialebenen aufsetzen. Durch die standardisierte, marktübliche Virtualisierung von Infrastruktur wäre es außerdem möglich, die Kapazitäten verschiedener Rechenzentren (zu sog. Availability Zones) zu verbinden. Dies wäre ein wesentlicher Beitrag zu mehr Skalierbarkeit und Nachhaltigkeit, da, je nach Bedarf, weitere Rechenzentren hinzugenommen werden könnten. Nachteil ist, dass man für diesen Ansatz performante Netzwerke zur Verbindung der Rechenzentren benötigt.

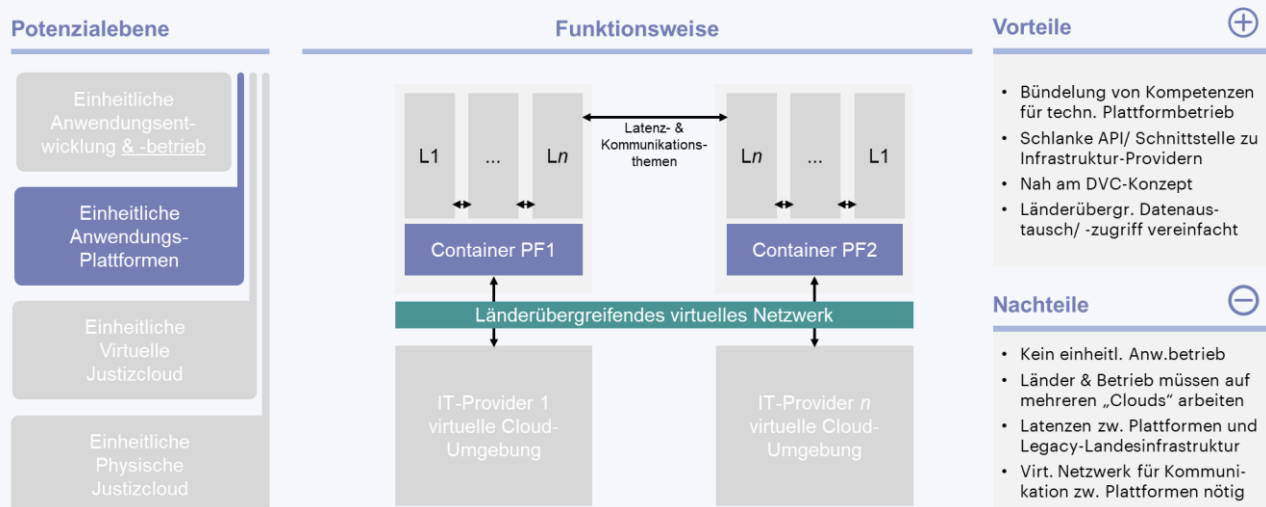
Abbildung 48 | Vor- und Nachteile einer Vereinheitlichung auf virtueller Infrastrukturebene



Der Aufbau einer virtuellen Justizcloud erfordert zusätzliche Komponenten, wie bspw. eine Cloud-Management-Plattform, ein gemeinsames (virtuelles) Netzwerk und einen gemeinsamen Virtualisierungsstandard. Der Ansatz wäre jedoch ggü. der physischen Konsolidierung effizienter und schneller, da Teilnehmer flexibler an das länderübergreifende Netzwerk angebunden werden könnten und die physische Infrastruktur und damit teure Migrationen unberührt blieben. Auch in diesem Modell würden vor allem technische Synergien gehoben. Es wäre aber auch hier nicht garantiert, dass auf dieser bundeseinheitlichen, virtuellen Infrastruktur gemeinsame, bundeseinheitliche Plattformen für eine bundeseinheitliche Anwendungslandschaft entstünden (vgl. **Abbildung 48**). Wiederum könnten landesspezifische Umgebungen verbleiben und die genannten fachlichen Herausforderungen aus der Ist-Analyse (vgl. **Kapitel 2**) würden nur peripher adressiert.

Auch auf der **Plattformebene** sind wesentliche Synergien denkbar. Einerseits könnte man sich auf eine Plattformtechnologie einigen und diese Plattformtechnologie bei allen IT-Dienstleistern der Justiz einführen (vgl. **Abbildung 49**). Dies stünde aber den z. T. erst kürzlich getätigten, landesspezifischen Investitionen der IT-Dienstleister in Cloud-Plattformen entgegen (vgl. **Tabelle 7**). Sofern eine bundeseinheitliche, virtuelle und/ oder physische Justizcloud-Infrastruktur bestünde, wäre auch die Einführung eines bundeseinheitlichen Plattformstandards auf dieser Infrastruktur möglich.

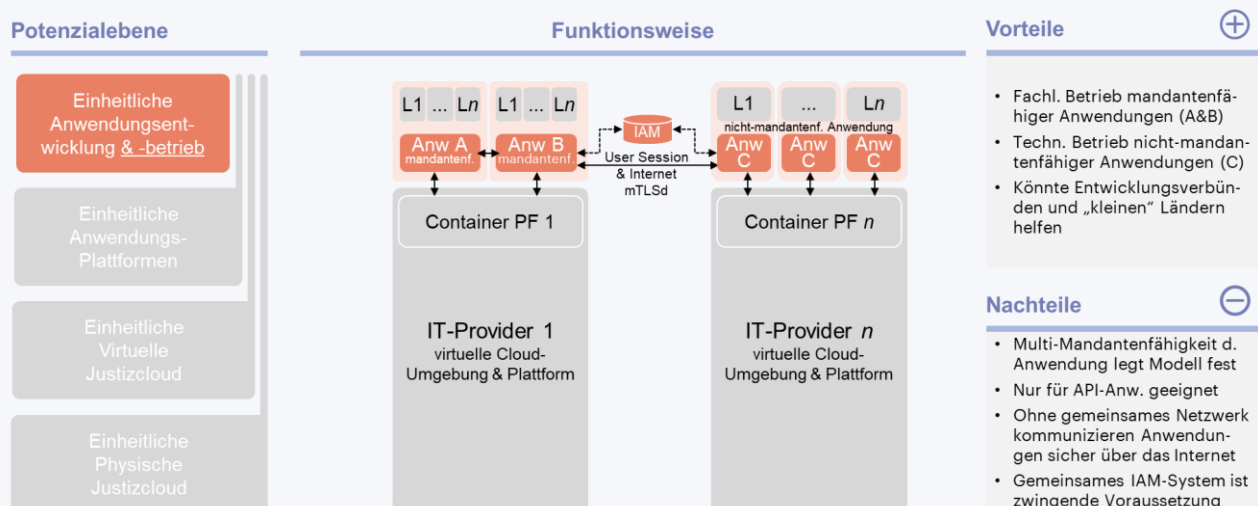
Abbildung 49 | Vor- und Nachteile einer alleinigen Vereinheitlichung auf Plattformebene



Durch einen einheitlichen Plattformstandard würden einige der Herausforderungen aus der Ist-Analyse (vgl. **Kapitel 2**) adressiert, da die Entwicklungsverbünde nur noch gegen diesen einen Plattformstandard entwickeln würden. Aufgrund der fehlenden bundeseinheitlichen physischen und/ oder virtuellen Infrastruktur, müssten aber mehrere Container-Plattformen (und später weitere Platfformdienste) deutschlandweit mehrfach lizenziert, eingeführt und jeweils betrieben werden. Zudem wäre in diesem Modell kein bundeseinheitlicher Anwendungsbetrieb möglich, denn alle Anwendungen würden auf der jeweiligen lokalen Container-Plattform betrieben (vgl. **Abbildung 49**). Auch die Kommunikation und Latenz zwischen den Plattformen (z. B. beim Teilen von Daten) wäre eine Herausforderung.

Abschließend gibt es auch Synergiepotenziale auf der **Anwendungsebene**. Einige davon hebt die Justiz schon, z. B. durch die Entwicklung gemeinsamer Fachverfahren wie *GeFa* und *AuRegis*. Andere plant die Justiz zu heben, wie bspw. die bundeseinheitliche Neuentwicklung der *eGPA* (vgl. **Kapitel 2.2.4**). Mangels einer einheitlichen Ausbringungsumgebung, d. h. Plattformebene, wird aber das bundeseinheitliche Vorgehen erschwert. Denn die bundeseinheitlichen Anwendungen müssen oft auf lokale Plattformanforderungen oder sogar Infrastrukturdienste (z. B. Datenbanktechnologien) angepasst werden. Genau vor dieser Herausforderung steht die Justiz bereits heute. Denn die bundeseinheitlich entwickelten Fachverfahren müssen auf jeweils individuelle Plattform- und Infrastrukturmgebungen der Länder portiert und auf diesen eingeführt werden. Dieser Prozess ist eine enorme Herausforderung für die Entwicklungsverbünde (vgl. **Kapitel 2.2.1 und 2.2.2**).

Abbildung 50 | Vor- und Nachteile einer alleinigen Vereinheitlichung auf Anwendungsebene



Zum Heben von Synergien in diesem Modell wäre es zwar denkbar, die Anwendungslandschaft jeweils auf individuell betriebene Container-Plattformen zu verteilen (z. B. *GeFa* auf Container-Plattform 1 und Basiskomponenten auf Container-Plattform n). In diesem Fall würde aber die Anwendungslandschaft auch per Definition auf verschiedene Rechenzentren verteilt. Da die Anwendungslandschaft aber ein Gefüge bildet, wären Latenz, Kommunikationsschnittstellen und vor allem das Berechtigungsmanagement für Anwendungen eine Herausforderung. Zudem müssten alle Länder mit allen (heterogenen) Plattformen verbunden werden, um die jeweils dort betriebene Anwendung nutzen zu können. Auch die Lokation des zentralen Berechtigungsmanagementsystems (IAM) wäre zu klären. Das Verhältnis von Aufwand und Nutzen wäre in diesem Szenario fragwürdig, denn die Justiz müsste auch weiterhin in verschiedenen Ländern für die Infrastruktur- und Plattformkosten aufkommen.

Wie dargestellt, bestehen Synergiepotenziale auf allen Ebenen. Die Synergiepotenziale verstärken sich, je tiefergehender eine Harmonisierung stattfindet. Jedoch steigen auch die Kosten, je tiefer einer Vereinheitlichung greift. Die größten Synergien bei vertretbaren Kosten und Wahrung des föderalen Charakters würde die Justiz nur durch eine Kombination der vorgenannten Lösungsansätze je Ebene erzielen. Das technische Fachpanel hat dafür folgendes Zielbild entwickelt:

Abbildung 51 | Präferiertes Bereitstellungsmodell

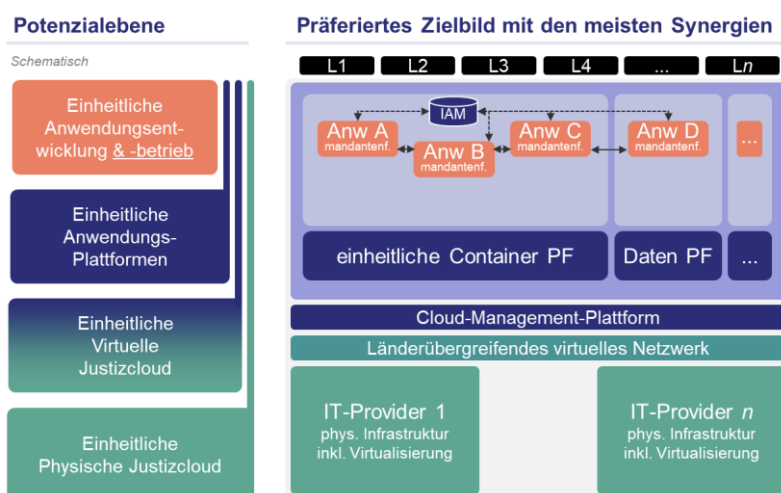


Abbildung 51 zeigt schematisch, wie die strategischen Ziele der Justizcloud (vgl. **Kapitel 3.2**) berücksichtigt und gleichermaßen die aktuellen Schmerzpunkte im Status Quo (vgl. **Kapitel 2**) durch die Kombination von Lösungsansätzen adressiert werden könnten.

Ein strategisches Ziel der Justiz ist es, die einheitliche Aus-

bringung der bundeseinheitlichen Anwendungen (z. B. *GeFa*) zu verbessern und einen bundeseinheitlichen Betrieb von Anwendungen (SaaS) zu ermöglichen. Dies kann nur auf bundeseinheitlichen Plattformen (z. B. Container- und Datenplattform) erfolgen. Die bundeseinheitlichen Plattformdienste benötigen wiederum bundeseinheitliche virtuelle Infrastruktur, um einheitlich betrieben werden zu können. Die virtuelle Infrastruktur hingegen könnte von

einem, aber auch von vielen IT-Dienstleistern gestellt werden, sofern diese über ein länderübergreifendes virtuelles Netzwerk miteinander verbunden sind. Wie so etwas funktionieren kann, hat die *govdigital eG* mit ihrem [gespannten Kubernetes-Cluster](#) für kommunale Anwendungen bereits gezeigt, welches derzeit zu einem vollwertigen, produktiv nutzbaren Plattformservice der *govdigital eG* ausgebaut wird. Für die Justiz ist dabei das Konzept, nicht aber der Service, nachnutzbar, weil die zugrundeliegenden Infrastrukturbetreiber sowie die Mitgliederstruktur der *govdigital eG* selbst die souveräne Nutzung dieses Angebots für die Justiz ausschließen.

Aufgrund des strategischen Ziels, die Souveränität der Justiz zu stärken, sollten bei der Infrastruktur mehrere justiznahe IT-Dienstleister einbezogen werden. Dabei wäre es effizienter, zunächst mit den bestehenden IT-Dienstleistern der Justiz die Ebene der Infrastruktur herzustellen. Zum einen, weil bis auf Weiteres viele Anwendungen der Justiz noch nicht Cloud-ready sind (vgl. **Kapitel 2.2.1**) und damit deren Daten in den Umgebungen der Justiz-IT-Dienstleister verbleiben. Zum anderen, weil viele Justiz-IT-Dienstleister bereits in die Virtualisierung ihrer Infrastruktur investiert haben (vgl. **Kapitel 2.2.2**) und sich über die Netze des Bundes verbinden ließen. Gleichzeitig könnten die Vertrauens- und Vertragsverhältnisse mit diesen IT-Dienstleistern der öffentlichen Hand nachgenutzt werden. Unabhängig davon könnten auch dritte IT-Dienstleister, d. h. auch kommerzielle Anbieter, in diesem Modell angebunden werden, was die Justiz unabhängiger, flexibler und zukunftssicherer aufstellen würde. Zunächst sollten aber alle vom technischen Fachpanel diskutierten, denkbaren Lösungsansätze der physischen und virtuellen Infrastrukturebene betrachtet werden.

Denkbare Optionen auf Ebene der physischen Infrastruktur

Auf der physischen Infrastrukturebene wurden vom technischen Fachpanel sieben Optionen identifiziert und gemeinsam anhand der strategischen Ziele der Justiz (vgl. **Kapitel 3.2**, z. B. Souveränität, Wirtschaftlichkeit usw.) bewertet (vgl. **Abbildung 52**).

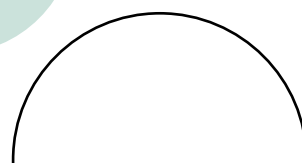
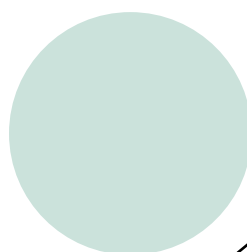
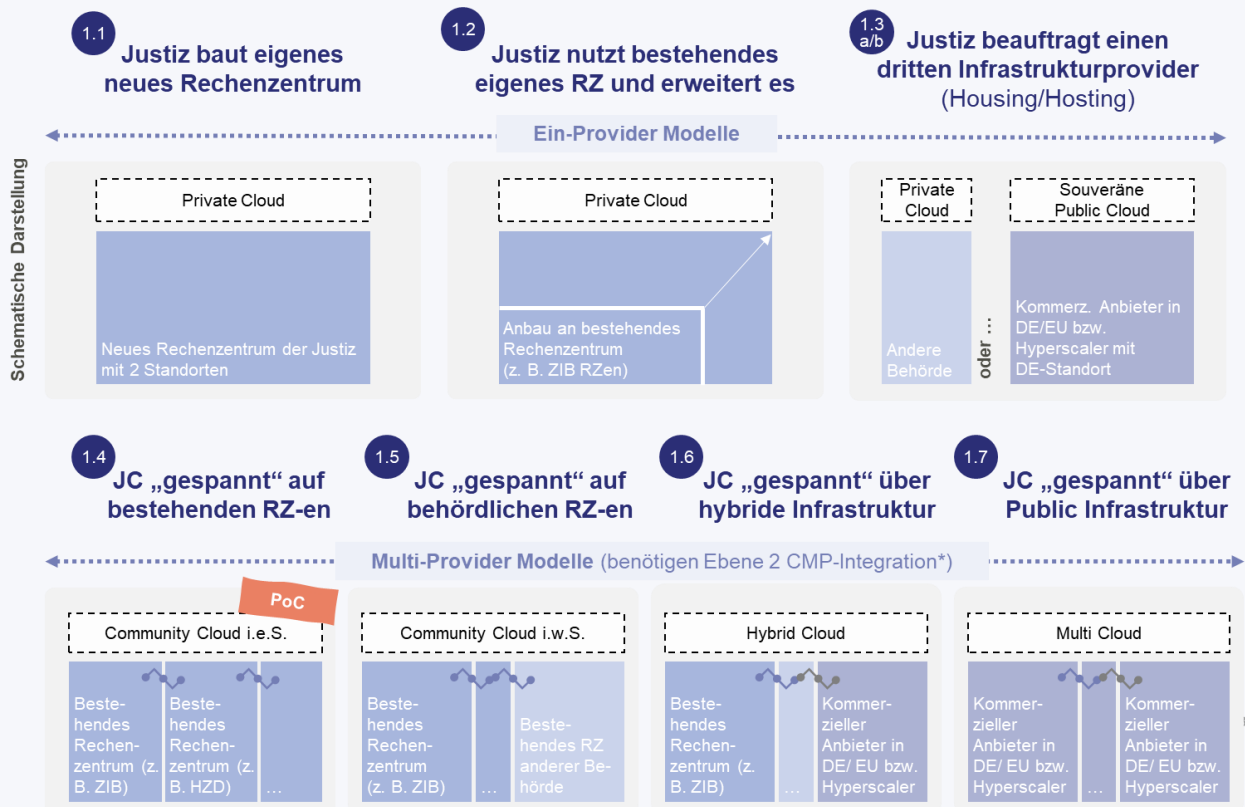


Abbildung 52 | Denkbare Bereitstellungsmodelle auf physischer Infrastrukturebene



Die sieben Optionen unterteilen sich in zwei Gruppen. Einerseits sog. Ein-Provider-Modelle und andererseits Multi-Provider-Modelle. **Ein-Provider-Modelle** bedeuten den Aufbau bzw. die Nutzung der physischen Infrastruktur bei einem einzelnen Provider. Denkbar sind hierbei der Bau eines eigenen RZ (1.1), die Erweiterung eines bestehenden Rechenzentrums (1.2) oder die Beauftragung eines Dritten, bspw. einer anderen Behörde (1.3a) oder eines kommerziellen Anbieters (z. B. Hyperscaler, 1.3b). Während bei 1.1 bis 1.3a jeweils Private Clouds aus Sicht der Justiz entstünden, wäre in 1.3b eine Souveräne Public Cloud als Bereitstellungsmodell zu wählen.

Multi-Provider-Modelle beruhen auf getrennten Infrastrukturen bei mehr als einem Infrastrukturprovider. Daher wird für Multi-Provider-Modelle eine Cloud-Management-Plattform (vgl. **Abbildung 45**) benötigt, um die Infrastruktur über mehrere RZs hinweg an-/ steuern und überwachen zu können. Dabei ist eine Vernetzung bestehender physischer RZs der Justiz (1.4) oder eine Vernetzung der Justiz-RZs mit RZs anderer Behörden denkbar (1.5). In beiden Fällen entstünde eine Community Cloud. Option 1.4 wurde im Rahmen des Justizcloud-PoC (vgl. **Kapitel 3.5.7**) erprobt.

Bei Option 1.6 werden bestehende RZs der Justiz mit einer kommerziellen Infrastruktur zu einer Hybrid Cloud verbunden (vgl. **Kapitel 3.5.1.1**). Das Bereitstellungsmodell 1.7 geht noch weiter und verbindet ausschließlich Infrastrukturen mindestens zweier kommerzieller Anbieter miteinander zu einer Multi Cloud.

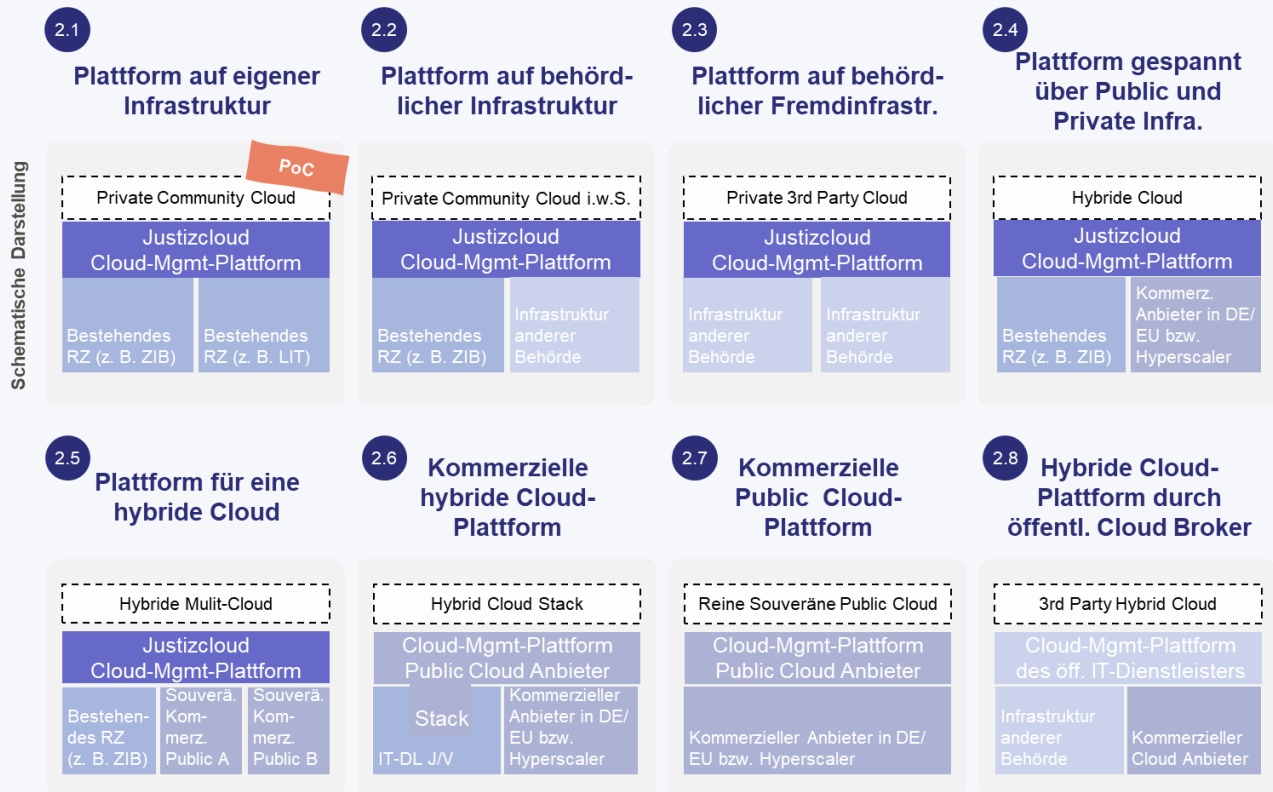
Grundsätzlich sieht das technische Fachpanel im Heben von Synergiepotenzialen rein auf der Infrastrukturebene keine besonders großen Mehrwerte für die Fachebene der Justiz. Schließlich ginge es bei einer solchen Harmonisierung der IT-Infrastruktur rein um technische Synergien; an den Plattformen und Anwendungen würde wenig geändert. Eine bundesweite IT-Konsolidierung stünde auch im Widerspruch zur verfassungsgemäßen Eigenständigkeit der Länder, zu von diesen bereits getätigten Investitionen (z. B. kürzlichen Rechenzentrumsmodernisierungen oder Geschäftsplan des Landesdienstleisters) und wäre insgesamt sehr komplex und teuer. Zudem sind solche einseitigen Ansätze in der Vergangenheit oft daran gescheitert, dass die Komplexität und Kosten der Migration von Daten und Altanwendungen auf neue Infrastruktur den Zeitrahmen und die Budgets der Vorhaben überstieg. Diesbezüglich hat die Justiz schon frühzeitig den „Greenfield“-Ansatz als strategische Prämisse gefasst (vgl. **Kapitel 3.1.1**).

Das technische Fachpanel hat außerdem nachvollziehbar festgestellt, dass die sogenannten Ein-Provider-Modelle aus Sicht von Souveränität und Skalierbarkeit sowie des Migrationsaufwands hin zu einem Provider als nachteilig gegenüber denkbaren Multi-Provider-Modellen zu sehen wären. Selbst bei einer Auslagerung der Infrastruktur an einen Hyperscaler wäre es angebracht, einen zweiten Hyperscaler oder eine Private Cloud als Fallback-Alternative im Sinne der Rückholbarkeit zu erschließen. Auch aufgrund dessen, dass für den Betrieb von Multi-Provider-Modellen jeweils mindestens eine verbindende (virtuelle) Cloud-Management-Plattform benötigt wird, wurden die verbleibenden Multi-Provider-Optionen vom technischen Fachpanel im Kontext der denkbaren Optionen auf Ebene der virtuellen Infrastruktur weiter betrachtet.

Denkbare Optionen auf Ebene virtueller Infrastruktur

Auf der virtuellen Infrastrukturebene wurden vom technischen Fachpanel insgesamt acht Optionen gemeinsam bewertet (vgl. **Abbildung 53**). Bei genauerer Betrachtung finden sich darunter die vier Multi-Provider-Modelle der vorhergehenden Infrastrukturebene sowie zusätzliche denkbare Optionen.

Abbildung 53 | Denkbare Bereitstellungsmodelle auf virtueller Infrastrukturebene



Eine Vereinheitlichung der virtuellen Infrastrukturebene kann auf verschiedene Weise erzielt werden. Option 2.1 spannt eine virtuelle Private Community Cloud über bekannte RZs der Justiz. In 2.2 können auch Rechenzentren einer anderen Behörde hinzukommen. Option 2.3 nutzt ausschließlich Infrastruktur anderer Behörden und schafft somit eine private, nur für begrenzte, öffentliche Kunden zugängliche, Third Party Cloud für die Justiz. 2.4 spannt eine Hybrid Justizcloud über mindestens einen Justiz-IT-Dienstleister und einen kommerziellen Anbieter, um z. B. mehr Skalierbarkeit zu erreichen. Dafür müssten aber beide Rechenzentren die gleiche „Vertrauensstellung“ haben, sodass sensitive Workloads in beiden Umgebungen gleichermaßen betrieben werden können. Alternativ kann ein solches Setup auch dazu dienen, selektiv bestimmte Dienste der kommerziellen Umgebung für bestimmte Anwendungsfälle zugänglich zu machen, nicht aber die kommerzielle Cloud-Umgebung als gleichwertiges bzw. gleich sicheres Pendant zur internen Umgebung zu sehen.

Aufbauend auf Option 2.4, verbindet Option 2.5 weitere kommerzielle Cloud-Umgebungen zu einer Hybrid Multi Cloud zusammen. Dieses Vorgehen kann z. B. vorteilhaft sein, um sensitive Daten in der internen IT-Dienstleister-Umgebung zu verarbeiten und eine

Wechselfähigkeit bei den kommerziellen Cloud-Diensten zu schaffen. Des Weiteren können jeweils die günstigsten kommerziellen Dienste je Anbieter gewählt werden (sog. FinOps).

Option 2.6 ist wiederum ein sog. Ein-Provider-Modell, in dem aber der kommerzielle Anbieter nicht nur die eigene Cloud in den eigenen Rechenzentren bereitstellt, sondern zusätzlich eine sogenannte Cloud-Stack-Lösung (vgl. **Kapitel 3.5.1.1**) bietet. Letztere würden im eigenen, d. h. privaten, Rechenzentrum der Justiz physisch betrieben und so, wie die Infrastruktur der kommerziellen Cloud, über die Cloud-Management-Plattform des kommerziellen Anbieters administriert. Damit könnten sensitive Daten im eigenen Rechenzentrum der Justiz auf eigener Infrastruktur liegen und z. B. Datenübertragungen von on-premises zur kommerziellen Cloud und umgekehrt wären einfacher möglich. Auch ist das Management der gesamten Umgebung effizienter, da dasselbe Betriebssystem genutzt wird. Nachteilig hingegen ist die Abhängigkeit vom singulären Anbieter dieser Lösung.

Denkbar, aber ebenso wenig souverän, wäre das Modell 2.7, bei dem eine spezielle souveräne kommerzielle Public Cloud-Plattform gewählt würde. Im Vergleich zur Option 1.3b, bei der nur die physische Infrastruktur eines kommerziellen RZ-Betreibers (sog. Hosting) oder nur das RZ-Gebäude (sog. Housing) genutzt würde, würde man in Option 2.7 auch das Betriebssystem, also die Cloud-Management-Plattform des Anbieters nutzen.

Abschließend sei Option 2.8 erwähnt, bei der die Justiz die Hybrid Cloud einer dritten Partei (sog. Third Party Hybrid Cloud) nutzen würde. Dies könnte bspw. eine andere Behörde sein, die ihrerseits bereits einen kommerziellen Cloud-Anbieter mit dem eigenen privaten RZ über eine Cloud-Management-Plattform verbunden hat. Im Kontext der Recherchen (vgl. **Kapitel 2.2.2 und 2.2.3**) gäbe es auch hierfür bereits einige Beispiele. So planen bspw. das *ITZBund* oder auch *Dataport* und *IT.NRW* ein ähnliches Setup in der Zukunft. Im Falle einer Verlagerung der gesamten Justiz-IT zu dieser dritten Partei, wäre aber auch hier die Souveränität und Unabhängigkeit der Justiz als Ganzes eingeschränkt.

3.5.1.3 Bewertung möglicher Bereitstellungsmodelle

Um die bundeseinheitliche Plattformebene für eine bundeseinheitlich betreibbare „Greenfield“-Anwendungslandschaft zu errichten (vgl. **Abbildung 51**), hat die Justiz demnach verschiedene denkbare Optionen auf Ebene einer bundeseinheitlichen virtuellen Infrastruktur (vgl. **Abbildung 53**). Die dargestellten Optionen wurden durch das technische Fachpanel, bestehend aus Vertretern der Justiz und der IT-Dienstleister, anhand der vom Sounding Board festgelegten strategischen Ziele der Justizcloud (vgl. **Kapitel 3.2**) bewertet. Unabhängig davon hat auch das Sounding Board die Optionen bewertet. Anschließend wurden

die Bewertungen der Fachpanels dem Sounding Board gespiegelt und festgestellt, dass beide Gruppen zu ähnlichen Ergebnissen kamen. Von den acht Zielen wurden einige als besonders wesentlich zur Bewertung herangezogen:

- Souveränität und Unabhängigkeit der Justiz steigern
- Föderale Bund-Länder-Zusammenarbeit stärken
- Nachhaltig Effektivität, Effizienz und Wirtschaftlichkeit steigern
- Zugang zu innovativen Technologien schaffen

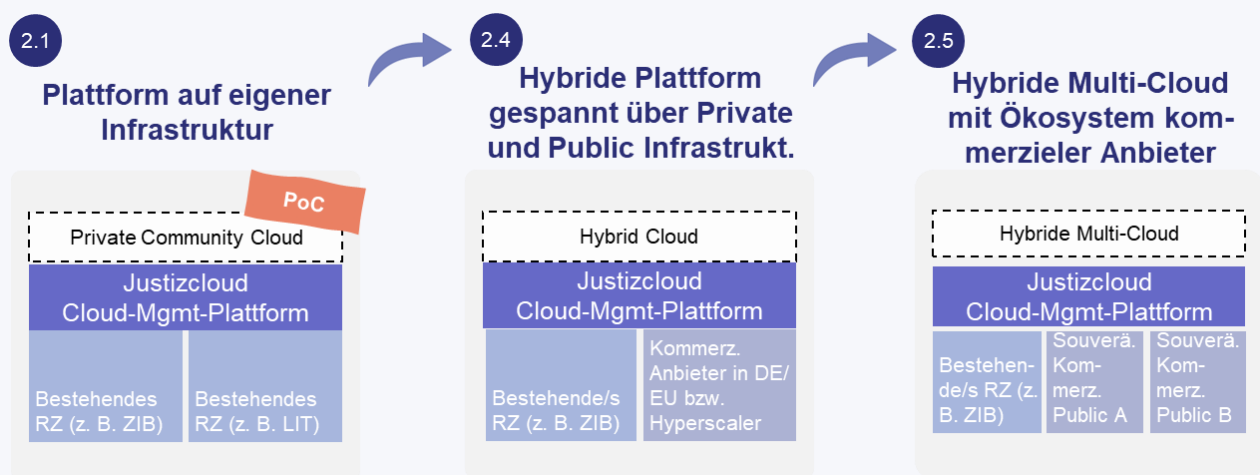
Die anderen vier Ziele sind für die Bewertung der Optionen weniger differenzierend und wurden daher nicht bewertet. Bspw. würden alle Optionen die Standardisierung hin zum zentralen Cloud-Betrieb ermöglichen und in allen Optionen würden auch einheitliche IT-Sicherheits- und Datenschutzstandards etabliert.

Im Rahmen der Bewertung waren sich die Teilnehmenden einig, dass die Ein-Provider-Modelle die Souveränität der Justiz zu stark einschränken und daher ausscheiden. Dabei war es unerheblich, ob nur die Cloud-Management-Plattform (also die virtuelle Ebene) oder die zugrundeliegende physische Infrastruktur bei einem Provider liegt. Auch war es unerheblich, ob es sich dabei um einen kommerziellen Anbieter (vgl. Optionen 2.6 und 2.7) oder eine öffentlich-rechtliche Behörde außerhalb der Justiz handelt (vgl. Optionen 2.3 oder 2.8). Obschon die Souveränität bei den behördlich organisierten Optionen relativ zu den kommerziellen etwas höher bewertet wurde, schnitten diese dafür aber bei Innovationskraft signifikant schlechter ab. Option 2.2 schied aus Effizienzgründen aus, weil keine triftigen Gründe gesehen wurden, beim Aufbau einer Community Cloud auf justizfremde, behördliche Infrastruktur auszuweichen.

Um die Souveränität und Unabhängigkeit der Justiz also sicherzustellen, verbleiben nur Optionen, in denen die Justiz entweder auf Basis bestehender Justizinfrastruktur eine eigene Private Community Cloud schafft (2.1) und diese später zu einer Hybrid Justizcloud mit kommerziellen Angeboten erweitert (2.4) oder direkt eine Multi Cloud-Strategie mit mindestens zwei souveränen Cloud-Angeboten kommerzieller Anbieter verfolgt und eine gewisse Rückholfähigkeit mit eigener Infrastruktur erhält (2.5). In diesen Fällen sollte die Justiz Betreiberin der Cloud-Management-Plattform sein, um einerseits den modularen Ausbau des „Unterbaus“ steuern, andererseits die Kontrolle über die Nutzbarkeit bestimmter Dienste je Umgebung ausüben (z. B. gem. [BSI C5 Kriterien](#)) sowie deren Nutzung überwachen und abrechnen zu können (sog. FinOps).

Das technische Fachpanel hat bei der Bewertung auch festgestellt, dass sich die Optionen 2.1, 2.4 und 2.5 nicht ausschließen, sondern, zeitlich gesehen, Evolutionsstufen einer Justizcloud ergeben könnten (vgl. **Abbildung 54**). Dabei würde die Justiz zunächst eine Private Community Cloud auf Basis bestehender Infrastruktur mit den bestehenden IT-Dienstleistungen schaffen (2.1). Damit könnte die Justiz die wesentlichen Ziele eines bundeseinheitlichen Plattform- und Anwendungsbetriebs bereits heben, die „Kronjuwelen“ der internen Anwendungslandschaft und damit auch die Daten auf eigener Infrastruktur halten und zunächst Cloud-Know-how gebündelt aufbauen.

Abbildung 54 | Mögliche Evolutionsstufen präferierter Bereitstellungsmodelle



Danach könnte eine erste gemeinsame, souveräne und kommerzielle Cloud-Umgebung für bestimmte Anwendungsfälle hinzugenommen werden (2.4), um auch Zugang zu innovativen Plattform- und SaaS-Diensten sowie ggf. günstigerer Infrastruktur dieser Anbieter zu erlangen. Dabei gilt es zu beachten, dass bestehende Infrastruktur derzeit USt-frei ist, kommerzielle Dienste aber umsatzsteuerpflichtig wären.

So könnten sukzessive wesentliche Souveränitätsmaßnahmen erprobt werden (vgl. **Kapitel 3.5.1.1**, z. B. BYOK/ HYOK, Rückholfähigkeit) sowie die Arbeitsteilung und Betriebsmodelle mit kommerziellen Anbietern austariert werden. Mit zunehmender Erfahrung ließen sich dann auch kritischere bzw. sensitive Workloads in der kommerziellen Umgebung verarbeiten. Um dort wechselfähig zu bleiben, könnten weitere souveräne kommerzielle Angebote hinzukommen (2.5), die ihrerseits die Justiz in eine bessere Verhandlungsposition bringen und ein breiteres, aber eben auch komplexeres, Dienste-Spektrum brächten.

3.5.1.4 Auswahl des Bereitstellungsmodells

Sowohl das technische Fachpanel als auch das Sounding Board sahen die Nutzung von Ein-Provider-Modellen (d. h. Zentralisierung) sowie die alleinige Nutzung kommerzieller Angebote im Widerspruch zu den strategischen Zielen der Justiz (vgl. **Kapitel 3.2**).

Sie sahen in einem ausgewogenen Hybrid Cloud-Ansatz (2.4 und 2.5) das größte langfristige Potenzial, um sowohl eine Private Cloud-Umgebung für sensible Verfahren und Daten als auch einen geschützten Raum zum Aufbau von Cloud-Kompetenz, zum Erproben des Cloud-Betriebs und für Mechanismen der Rückholfähigkeit zu etablieren. Eine Private Cloud reicht darüber hinaus vollkommen, um die derzeit bestehenden akuten Ausbringungsprobleme für neue Verfahren (z. B. *GeFa* und *AuRegis*) zu adressieren. Andererseits ist die Benutzung kommerzieller Anbieter (inkl. Hyperscaler) beim Hybrid Cloud-Ansatz explizit vorgesehen, um sukzessive einen bundeseinheitlichen Zugang zu innovativen und ggf. auch günstigeren Cloud-Diensten für alle Länder zu schaffen.

Die **Private Cloud Umgebung** muss dabei per Definition eine Verbindung zu allen bestehenden Justiz-IT-Dienstleistern haben, um im „Greenfield“-Ansatz Cloud-betriebene Fachverfahren (vgl. **Kapitel 3.1.1**) auf weiterhin lokal gehaltene Daten (z. B. in nicht Cloud-fähigen eAkten) zugreifen zu lassen. Dabei müssen lt. *IT-NetzG* auch zwingend die Netze des Bundes (NdB) genutzt werden, um bspw. länderübergreifenden Datenaustausch zu ermöglichen (vgl. **Kapitel 3.5.2.1**). Vor diesem Hintergrund hat sich gezeigt, dass ein Großteil der bestehenden virtuellen Infrastruktur der IT-Dienstleister zügig nachgenutzt werden kann, um eine Private (virtuelle) Community Cloud mit verteilter physischer Infrastruktur aber bundeseinheitlichen Plattformdiensten zu schaffen. Dabei würde die föderale Zusammenarbeit gestärkt (vgl. auch PoC, **Kapitel 3.5.7**) sowie die Möglichkeit zur Bewahrung der Datenhoheit (vgl. **Kapitel 3.1.1**) geschaffen. Durch das Konzept der Private Community-Cloud würde sogar die Souveränität der Justiz weiter gefestigt, weil die Justiz einerseits bundesweit ein justizeigenes, performantes Netz (z. B. analog Verfassungsschutzbehörden) erhielte und andererseits, weil die Justiz mit der Cloud-Management-Plattform (vgl. **Kapitel 3.5.4** bzw. **Abbildung 45**) die Hoheit über den modularen Ausbau der Infrastruktur, die bundeseinheitliche Standardisierung von Cloud-Diensten ohne Abhängigkeit von Entscheidungen sowie eine bessere Verhandlungsposition bei der Beschaffung erhielt (z. B. Volumenrabatte).

Der Ausbau zur Hybrid Cloud mit **kommerziellen Cloud-Umgebungen** ist explizit vorgesehen, um einen bundeseinheitlichen Zugang zu innovativen und ggf. günstigeren Diensten für alle Länder zu schaffen. Jedoch ist die Erschließung eines kommerziellen Anbieters ein

komplexes Vorhaben, das kaufmännische (z. B. Rahmenvertrag, FinOps), rechtliche (z. B. Haftung, Souveränitätsbestimmungen), organisatorische (z. B. SLAs, Arbeitsteilung/ OLAs), technische (z. B. Aufbau von Landing Zones, Netzanbindung, Migrationen, IT-Sicherheit), fachliche (z. B. Datenklassifikation, Berechtigungsmanagement, uvm.) sowie strategische (insb. Anbieterauswahl und Multi Cloud-fähige Wechselfähigkeit) Kompetenzen erfordert. Die Abstimmungen müssten zudem mit allen Ländern geführt und entsprechende Standards definiert werden.

Setzt man voraus, dass die Justiz für ein Minimum an Wechselfähigkeit mindestens zwei Anbieter erschließen müsste, so vervielfachen sich die Komplexität und der Aufwand. Zwar können einige Konzepte und Standards anbieterübergreifend genutzt werden und es gibt auch Angebote zum Nachnutzen, bspw. bestehende kaufmännischer Aspekte (z. B. [govdigital eG Cloud Broker](#)), jedoch gibt es eine vollständige Erschließung einer souveränen kommerziellen Umgebung in der Größenordnung einer „Staatsgewalt“ bisher nicht und müsste daher von der Justiz allein vorangetrieben werden. Insofern wird die Erschließung kommerzieller Umgebungen ein inkrementeller Prozess, zunächst mit einem Anbieter und sukzessive mit weiteren. Auch hierbei ist es von Vorteil, zunächst eine gemeinsame Private Cloud-Umgebung aufzubauen. Denn einerseits gewänne die Justiz dadurch Verhandlungssicherheit gegenüber kommerziellen Anbietern sowie ein besseres Verständnis ihrer langfristigen strategischen Ziele für kommerzielle Umgebungen, andererseits kann auch die Erschließung der kommerziellen Cloud-Umgebungen viel effizienter mit einem einheitlichen Zugang über die Cloud-Management-Plattform der Justiz erfolgen. Bspw. könnte die Justiz ein sog. Hub-and-Spoke-Modell auf Ebene des Netzkonzeptes etablieren und damit einen bundeseinheitlichen Zugang zu kommerziellen Umgebungen schaffen, anstatt 16 Netzanbindungen abzusichern und verwalten zu müssen. Auch die Administration, Überwachung und Abrechnungen der kommerziellen Ressourcennutzung könnte für die Justiz einmal bundeseinheitlich entwickelt werden. Aus Sicht des technischen Fachpanels und des Sounding Boards ergaben sich damit folgende Argumente für die Auswahl einer Private Community Cloud mit anschließenden Evolutionsstufen hin zur Hybrid Multi Cloud:

Effektivität, Effizienz und Wirtschaftlichkeit steigern:

- Da es keine Infrastrukturzentralisierung ist, fallen geringere Migrationsaufwände an.
- Die Nachnutzung virtueller Infrastruktur bestehender IT-Dienstleister ist effizient möglich und viele IT-Dienstleister können mit ihren Infrastrukturen daran teilhaben.

- Das bietet Investitionsschutz, v. a. für IT-Dienstleister, die gerade erst ihre Rechenzentren modernisiert haben.
- Die Infrastrukturressourcen können dabei USt-frei (z. B. via *govdigital eG*) beschafft werden, was etwaige Preisnachteile ggü. kommerziellen Anbietern verringert.
- Die notwendige Bandbreite und die erforderlichen Endgeräte zur Vernetzung der IT-Dienstleister können über die *BDBOS* effizient beschafft werden. Die IT-Dienstleister sind mit den Prozessen vertraut.
- Die kreuzvermaschte Netzanbindung mit allen IT-Dienstleistern (vgl. **Kapitel 3.5.2.1**) müsste technisch, organisatorisch sowie sicherheitsmäßig in allen Modellen erfolgen, um einen gemeinsamen Datenaustausch sowie Konnektivität zu lokalen Daten (z. B. eAkten) zu ermöglichen.
- Für den Aufbau der Community Cloud können [DVC-](#) sowie [EUcloud](#)-Konzepte (z. B. Föderation von Identitäten und Netzkonzepte) nachgenutzt werden. Nationale Beispiele für solche Clouds bestehen in Dänemark und Belgien als Blaupausen.
- Auch das Cloud-Know-how aller IT-Dienstleister kann effizient nachgenutzt werden. Jeder kann seine Kernkompetenzen einbringen, sodass nicht jeder alle Kompetenzen aufbauen muss (vgl. PoC **Kapitel 3.5.7**).
- Aufgrund der Nachnutzung bestehender, vertrauter, vielfach bereits BSI-zertifizierter Infrastruktur sowie der Netze des Bundes werden Sicherheitskonzepte vereinfacht.
- Das Ziel zur Schaffung einer bundeseinheitlichen Plattform für einen bundeseinheitlichen Anwendungsbetrieb ist in diesem Modell möglich.
- Die spätere Erschließung kommerzieller Cloud-Umgebungen wäre viel effizienter.
- Da viele Daten der Justiz noch auf längere Zeit in nicht Cloud-ready Anwendungen in lokalen Umgebungen liegen, werden auch teure Datentransfers in bzw. aus den Rechenzentren Dritter vermieden.
- Die Infrastrukturanbieter stehen langfristig im Wettbewerb, wodurch positive Preiseffekte zu erwarten sind.
- Mittelfristig kann auch ein effizientes Pay-per-use-Konzept für Infrastrukturressourcen mit öffentlichen IT-Dienstleistern erprobt und eingeführt werden, sofern diese die automatisierte Provisionierung beherrschen.
- Die gebündelte Beschaffung von Lizenzen und Fachkräften für den Plattformbetrieb erlaubt wesentliche Synergien und Volumenrabatte.

- Durch einen mit der Private Cloud verbundenen bundeseinheitlichen Entwicklerarbeitsplatz lässt sich viel effizienter entwickeln, Co-Pilot-Lösungen etablieren, Fehler frühzeitiger finden und die Ausbringung von Software auf die Cloud beschleunigen.

Souveränität im föderalen Gefüge stärken:

- Die Kernanwendungen (sog. „Kronjuwelen“) der Justizanwendungslandschaft, d. h. Akten, Verfahren sowie personenbezogene Daten, liegen auf eigener, souveräner Infrastruktur.
- Dabei können auch länderspezifische Bedarfe lokaler Datenhaltung (sog. „meine Daten auf meinen Servern“) ermöglicht werden, sofern der IT-Dienstleister dieses Landes auch Infrastruktur für die Justizcloud (als sog. „Knotenprovider“) stellt.
- Die Justiz würde (analog Verfassungsschutzbehörden) über ein justizeigenes Netz mit justizeigenen Verschlüsselungszertifikaten verfügen und damit bundeseinheitlich Vorgaben der hessischen Netzklage adressieren.
- Resilienz und Skalierbarkeit steigen, denn die Justiz nutzt von Beginn an verschiedene IT-Dienstleister, die jeweils individuell ausbauen können. Zudem kann die Justiz sukzessive weitere Infrastrukturdienstleister, auch kommerzielle, hinzuziehen.
- Die Rückholfähigkeit wird mit der Private Community Cloud vorbereitet und bundeseinheitlich für die Justiz etabliert, sobald erste kommerzielle Public Cloud-Angebote erschlossen werden.
- Die Wechselfähigkeit zwischen kommerziellen Umgebungen wird bundeseinheitlich für die Justiz etabliert, sobald mehr als eine kommerzielle Public Cloud erschlossen ist.
- Die modulare Ausbaufähigkeit der Infrastrukturebene zählt auf die Verhandlungssouveränität der Justiz ein.
- Die Justiz kann im geschützten Raum zunächst Erfahrungen im Cloud-Betrieb sammeln, vermehrt Cloud-ready entwickeln und dann gezielter und souveräner ggü. kommerziellen Cloud-Anbietern und Softwareherstellern auftreten.
- Die Justiz kann vor dem Hintergrund des Fachkräftemangels gezielter und fokussierter Cloud-Know-how an einer Stelle einstellen und ausbilden.
- Durch den Private Community-Cloud-Aufbau und dessen Betrieb mit IT-Dienstleistern und in der Cloud-Management-Plattform der Justizcloud behält die Justiz die Wissens- und Steuerungssouveränität für das Gesamtsystem.

- Finanzielle Ressourcen der Länder verbleiben aufgrund der USt-freien Inhouse-Geschäfte in den Ländern.
- Die Geschäftsmodelle und damit die Souveränität der Landes-/ Justiz-IT-Dienstleister bleiben erhalten, ggf. sogar gestärkt, falls das Justizcloud-Modell Anklang in anderen Ressorts findet.
- Durch einen mit der Private Cloud verbundenen bundeseinheitlichen Entwicklerarbeitsplatz für alle Cloud-fähigen Anwendungen gewinnt die Justiz die Souveränität über ihren Code zurück. Der Entwicklerarbeitsplatz kann souverän in verschiedene Cloud-Umgebungen ausbringen, die Justiz behält somit die Know-how- und Steuerungshoheit über den Ausbringungsprozess.
- Innerhalb der Community Cloud und darüber hinaus kann die Justiz eigenständig moderne IT-Sicherheitsstandards festlegen und sicherstellen, bspw. Multi-Faktor-Authentisierung für alle Endnutzenden moderner Justizanwendungen, auch wenn diese Technologie lokal noch nicht verfügbar ist.
- Insgesamt kann die Justiz schrittweise vorgehen, was einen kontrollierten und agilen Prozess ermöglicht.

Zugang zu innovativen Technologien bieten:

- Durch das Community Cloud-Konzept und die gemeinsame Vernetzung wird erstmals eine bundeseinheitliche Teilhabe aller Länder an Justizcloud-Diensten ermöglicht (sog. Level Playing Field).
- Bereits für die Private Community Cloud sind innovative Plattformdienste vorgesehen, bspw. KI- und Datenplattform sowie modernes Benutzer- und Berechtigungssystem.
- Die Anwendungen für Endnutzende können mit einem modernen Entwicklerarbeitsplatz i. V. m. der Container-Plattform viel häufiger und damit kundenzentrierter weiterentwickelt werden. Die Justiz wird damit für Endnutzende innovativer.
- Der Entwicklerarbeitsplatz selbst erlaubt durch die bundeseinheitliche Bündelung für alle modernen Anwendungen den Einsatz innovativer Deployment-Mechanismen (z. B. Canary- und Blue-Green-Releases) sowie das Training und den Einsatz von Co-Pilot-Funktionen in der Entwicklung.
- Mit der sukzessiven Erschließung von kommerziellen Cloud-Umgebungen wird ein extensives Ökosystem kommerzieller Cloud-Dienste für alle Länder eröffnet.

- Parallel dazu wird auch die Nachnutzung von SaaS-Diensten in der öffentlichen Verwaltung (siehe *DVC-Marktplatz*) ermöglicht.

Föderale Zusammenarbeit stärken:

- Die föderale Zusammenarbeit steckt bereits in Namen und Konzept einer Community Cloud und wird per Definition gestärkt.
- Das Konzept stellt die gleichberechtigte Teilhabe aller Länder sicher. Dabei können Länder mit größeren IT-Dienstleistern mehr Ressourcen einbringen als kleinere Länder, aber alle Länder können gleichermaßen die Cloud-Anwendungen nutzen.
- Die Justiz Community Cloud stärkt nicht nur die Zusammenarbeit innerhalb der Justiz, sondern weit darüber hinaus, z. B. durch die Nachnutzung und damit Validierung von *DVS*-Konzepten sowie die vertragliche Vernetzung über die *govdigital eG*.
- Die IT-Dienstleister könnten jeweils Kernkompetenzen bundesweit im Justizcloud-Aufbau und -Betrieb einbringen und damit Best-of-Breed-Lösungen ermöglichen. Die Arbeitsteilung im Justizcloud-PoC ist das beste Beispiel dafür (vgl. **Kapitel 3.5.7**).
- Die Zusammenarbeit der Entwicklungsverbünde (als Mehr-Länder-Konstrukte) untereinander und mit dem bundeseinheitlichen Infrastrukturbetrieb der Justizcloud wird verbessert.
- Durch das Community Cloud-Konzept werden Betriebsverbünde und bundeseinheitliche Service Desks für Cloud-Anwendungen ermöglicht, was wiederum die länderübergreifende Zusammenarbeit innerhalb der deutschen Justiz stärkt.
- Die Justiz kann ihre IT-Anforderungen besser bündeln und einheitlicher ausschreiben, sodass alle IT-Dienstleister bundesweit gleichberechtigt dafür bieten können.
- Aufgrund der Modularität einer Community Cloud können beim Justizcloud-Aufbau IT-Dienstleister je nach Geschwindigkeit und Reifegrad sukzessive hinzustoßen, somit wird niemand abgehängt.

Für den Aufbau einer Private Community Cloud und den späteren Ausbau hin zu einer Hybrid Cloud werden verschiedene technische Konzepte benötigt, die im Folgenden detaillierter beschrieben werden. Zunächst ein **Netzkonzept** zum Verbinden der IT-Dienstleister-Infrastrukturen (vgl. **Kapitel 3.5.2**), ein **Mandantenkonzept** zur Abbildung länderspezifischer Anforderungen (vgl. **Kapitel 3.5.3**) sowie ein **Administrationskonzept**, mit dem Infrastruktur-IT-Dienstleister mit der Justizcloud-Plattform interagieren können (vgl. **Kapitel 3.5.5**). Weiterhin ist ein **Cloud-Management-Plattform** zur Verwaltung der Umgebungen und Schaffung bundeseinheitlicher **Plattformdienste**, wie einer gemeinsamen **Container-Plattform**

oder **Integrationsplattform** erforderlich (vgl. **Kapitel 3.5.4**). Zudem ermöglicht ein bundeseinheitlicher **Entwicklerarbeitsplatz** die integrierte Entwicklung- und Ausbringung moderner Justizcloud-Anwendungen auf der bundeseinheitlichen Cloud-Plattform (vgl. **Kapitel 3.5.6**), sowohl in die Private Zone als auch perspektivisch in kommerzielle Umgebungen. Abschließend werden Teile dieser Komponenten und Konzepte am Beispiel der Erkenntnisse aus dem **Justizcloud-PoC** illustriert (vgl. **Kapitel 3.5.7**).

3.5.2 Netzkonzept

3.5.2.1 Virtuelles Netzwerk für die Justiz-Community-Cloud

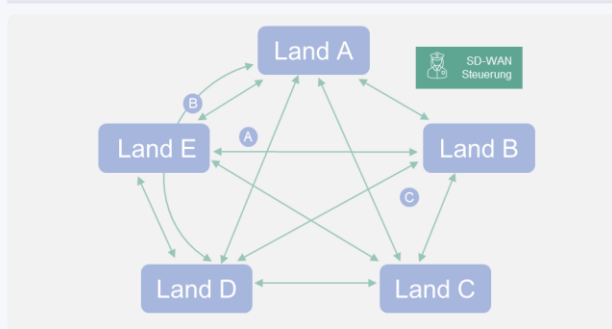
Die Grundlage einer Private Community Cloud ist die Fähigkeit, die teilnehmenden Parteien und deren Rechenzentren performant zu vernetzen. Da man in der Regel keine physischen Kabel bzw. Telekommunikationsleitungen zwischen allen Teilnehmenden eines Verbunds legen kann, da dies prohibitiv teuer wäre, wird in solchen Fällen ein sog. virtuelles Netzwerk zwischen den Parteien gespannt. Dieses private virtuelle Netzwerk kann zwar nur von diesen Parteien genutzt werden, selbst aber verschiedene, verfügbare physische Netze, d. h. Kommunikationsverbindungen (sog. Carrier), zwischen den Parteien nutzen. Im einfachsten Fall werden breitbandige Internetverbindungen zum Aufbau eines virtuellen Netzwerks genutzt, wie es bspw. der [govdigital eG K8s Prototyp](#) vorgeführt hat. Da es sich hierbei um ein virtuelles Netz (sog. Software Defined) diverser, geographisch getrennter Teilnehmer (sog. Wide Area Network) handelt, spricht man auch von einem SD-WAN.

Für den Aufbau des virtuellen Netzwerks zwischen den teilnehmenden Parteien wird in jedem Rechenzentrum entsprechende Netzwerkhardware oder -software eingesetzt, um ein eigenes Netzwerk zwischen diesen Parteien zu definieren. Dafür werden die einzelnen Netzknoten jedes Teilnehmenden konfiguriert und über eine globale Verwaltungsfunktion (sog. SD-WAN Steuerung) das Gesamtnetz gesteuert und überwacht (vgl. **Abbildung 55** links).

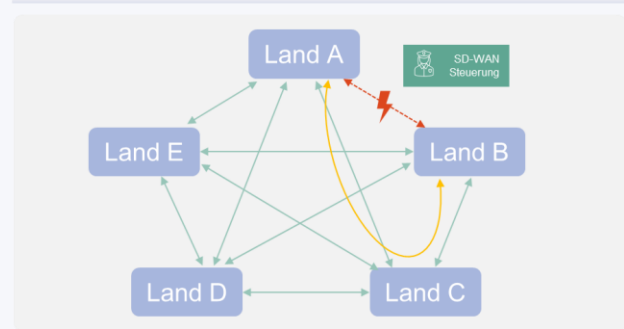


Abbildung 55 | Funktionsweise eines virtuellen, Software Defined Netzwerks

Kreuzmaschiges virtuelles SD-WAN



Funktionsweise bei Ausfall



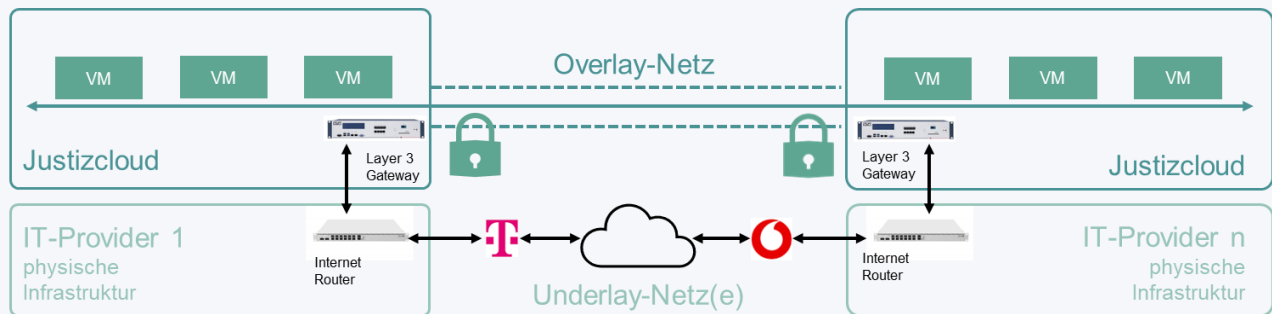
Beim Aufbau des virtuellen Netzwerks wird aus Performanz- und Resilienzgründen außerdem darauf geachtet, dass eine kreuzmaschige Vernetzung etabliert wird. D. h., dass jeder mit jedem Netzknoten potentiell verbunden ist, sich alle Netzknoten kennen und vertrauen sowie Datenpakete sich daher den kürzesten bzw. schnellsten Weg zwischen zwei Punkten suchen können. Die zentrale Steuerung hat dabei die Möglichkeit, bestimmte Routen zu priorisieren bzw. auszuschließen und somit auch eine optimale Lastverteilung innerhalb des Netzes vorzunehmen.

Ein modernes SD-WAN bringt zudem auch einen Zugewinn an Sicherheit, denn die Routen werden dynamisch aufgebaut, d. h. immer nur dann, wenn Datenpakete zu transportieren sind. In einem virtuellen Netz können auf diese Art große Datenpakete performant auf Routen verteilt werden. Angreifer können die Routen a priori nicht kennen und abhören, da sie immer nur zur Laufzeit entstehen.

Besonders beim Ausfall eines Verbindungsglieds (z. B. physischen Defekt an einer physischen Leitung wegen Baggerarbeiten, vgl. **Abbildung 55** rechts) beweist sich die Resilienz des Gesamtsystems. Durch die dynamische Routenfindung suchen sich die relevanten Datenpakete einfach die nächstbesten Wege zum Zielknoten.

Der Aufbau eines virtuellen Netzwerks kann am besten am sog. [OSI-Schichtenmodell](#) erklärt werden (vgl. **Abbildung 56**). Möchten zwei Teilnehmer eine gemeinsame Netzverbindung herstellen, so benötigen sie dafür ein verbindendes (Layer 3) Overlay-Netz und ein zugrundeliegendes (Layer 1-2) Underlay-Netz.

Abbildung 56 | Aufbau eines virtuellen, Software Defined Netzwerks



¹ Anpassung nach Termin mit BMI Referat CI 5

Als Underlay-Netz können dafür beliebige existente Kommunikationsverbindungen zwischen den Teilnehmenden gelten (z. B. Internetanschlüsse sog. Carrier und/ oder Internet Service Provider (ISP)). Dabei können eigene und fremde (sog. gemietete/ leased lines) physische Leitungen (Layer 1) von den Carriern genutzt werden.

Auf dem Layer 2 Underlay-Netz setzt das Level 3 Overlay-Netz auf. Um die Teilnehmenden auf der Layer 3-Ebene zu verbinden, muss jeder Teilnehmende entweder eine physische Hardware (sog. Layer 3 Gateway) oder passende Softwareprodukte im eigenen Rechenzentrum installieren und mit den Kommunikationsleitungen (Layer 2) verbinden.

Die Layer 3 Hard- oder Software-Gateways übernehmen zwei Kernfunktionen. Einerseits den o. g. dynamischen Verbindungsaufbau, immer dann, wenn Datenverkehr zu transportieren ist sowie das Schneiden der Datenpakete und Finden der günstigsten Route. Andererseits verschlüsseln die Gateways den Datenverkehr zwischen den teilnehmenden Parteien mit individuellen Zertifikaten, so dass kein Level 2-Provider Einblick in den Datenverkehr im Layer 3-Netz erhalten kann. Innerhalb des verschlüsselten Netzes können nun die teilnehmenden Parteien untereinander IT-Ressourcen freigeben und gemeinsame Dienste nutzen.

Auch ohne die Justizcloud hätte die Justiz einen großen Bedarf für eine länderübergreifende Vernetzung, um bspw. länderübergreifend Daten teilen zu können, statt sie über *EGVP* und als verschlüsselte Kopien über das Internet zu versenden. Derzeit wird für solche Zwecke das sogenannte Verbindungsnetz (VN) in den NdB genutzt, bzw. kommuniziert *EGVP* über das Internet. Jedoch ist der aktuelle Ausbau des Verbindungsnetz sehr dürrtig und für einen Justizcloud-Aufbau ungeeignet (vgl. **Kapitel 2.2.2**).

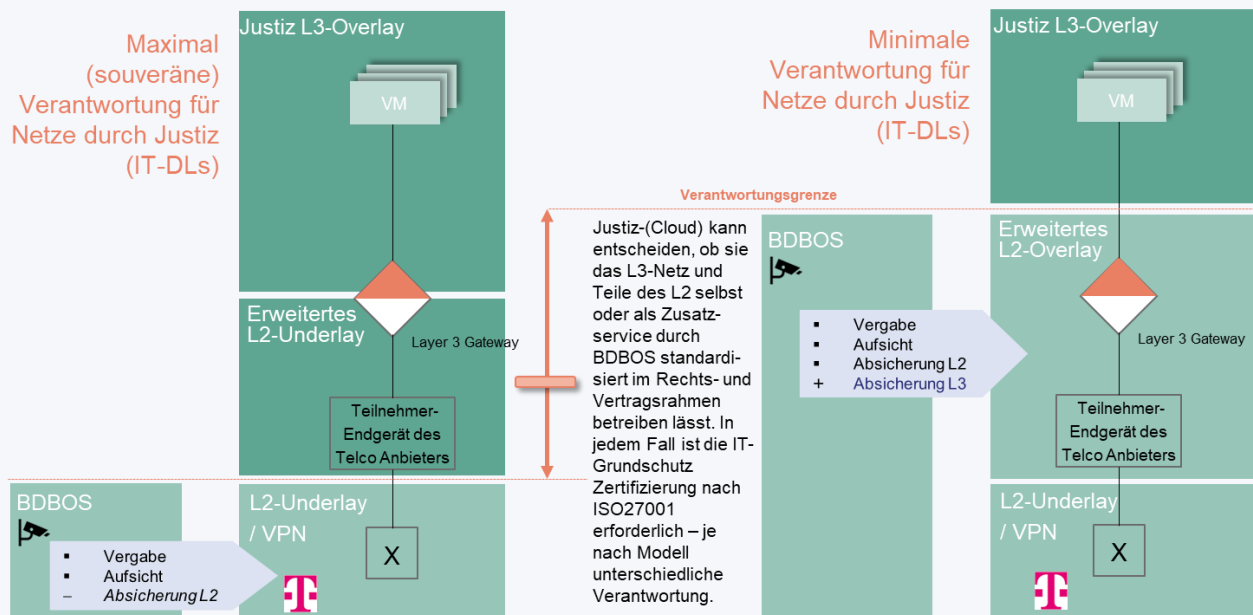
3.5.2.2 Justiznetz in den Netzen des Bundes

Zur länderübergreifenden Vernetzung von Behörden und ihren IT-Dienstleistern der öffentlichen Hand muss gemäß § 3 *IT-NetzG* das Verbindungsnetz verwendet werden. Das Verbindungsnetz als eines der NdB beschreibt dabei kein physisches Netz, sondern stellt einen gemeinsamen Rechtsrahmen (insb. Artikel 91c GG, *IT-NetzG*) dar, der bspw. den behördlichen Datenverkehr vom Telekommunikationsüberwachungsgesetz (vgl. TKÜV, § 170 TKG) entbindet. Zudem werden Rechts-, Vertrags- und Kooperationsrahmen sowie Mindeststandards zwischen den am Netz teilnehmenden Parteien geregelt. Dabei kann der Bund je nach Wunsch der Länder gemeinsame Aufgaben übernehmen, im Zuge dessen z. B. als Schnittstelle zum Netzaufbau fungieren und sich sogar finanziell beteiligen, sofern das Netz als Bundesnetz (analog *BKA*, *BfV/LfV*, *AA*) deklariert wird. Das zu definierende Netz muss aber beim *IT-Planungsrat* vorgebracht und angemeldet werden.

Die einzelnen NdB sind unterschiedlich umgesetzt und geben ausdrücklich keine technische Umsetzung vor. Die behördlichen Netzteilnehmenden haben also viele Freiheitsgrade der Ausgestaltung ihres privaten Netzes in den NdB. Denn die NdB sind nicht bundeseigene physische Leitungen, sondern dedizierte, ebenfalls logisch getrennte, Layer 2-Leitungen bei Carriern, wie z. B. derzeit bei der *Deutschen Telekom*, für welche die *BDBOS* Rahmenverträge hält. Die *BDBOS* kann daher verschiedene Anbindungsarten und flexible Bandbreiten für Layer 3-Netze anbieten. Dabei sind bereits heute standortabhängig sehr hohe Bandbreiten möglich, sofern auch performante Layer 3-Gateway Endgeräte eingesetzt werden. Perspektivisch sind mit dem IVÖV-Breitbandnetz sogar noch performantere Verbindungen möglich, bspw. wenn die *BDBOS* auch Multi-Carrier-Fähigkeit mit breiterer Anbietersauswahl umsetzt und somit noch mehr physische Leitungen genutzt werden können.

Somit kann die Justiz, ebenso wie andere Ressorts (bspw. *BKA*, *BfV/LfV*, *AA*), ein eigenes Justiznetz in den NdB (fortan NdB JN in Anlehnung an das Verbindungsnetz NdB VN) für ihre eigenen Zwecke gründen und betreiben. Dabei hat sie bei der Ausgestaltung der Arbeitsteilung zum Betrieb des Justiznetzes in den NdB mit der *BDBOS* viel Gestaltungsspielraum (vgl. **Abbildung 57**).

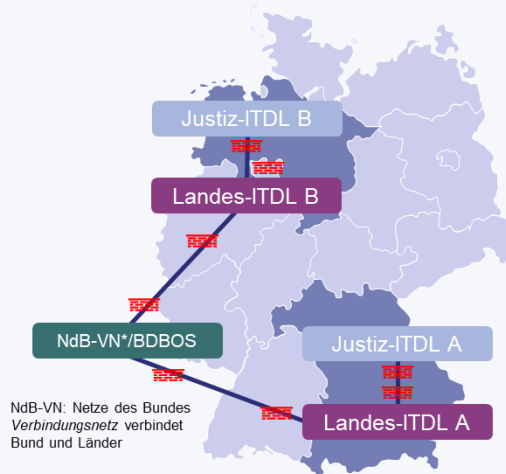
Abbildung 57 | Mögliche Verantwortungsschnitte beim Netzbetrieb mit *BDBOS*



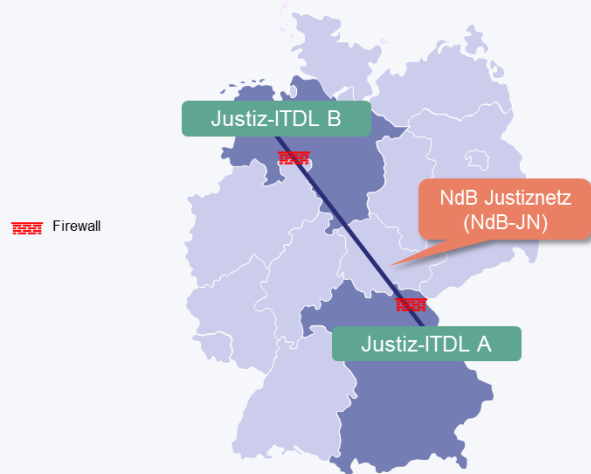
Die Rahmenverträge der *BDBOS* lassen verschiedene Betriebsmodelle zu. In der maximal autarken Ausbaustufe für die Justiz (links) steuert die *BDBOS* nur die Verträge sowie die Aufsicht und Absicherung der Layer 2-Netze bei. Dafür muss die Justiz bspw. die Layer 2-Endgeräte und das gesamte Layer 3-Netz verantworten. Die Justiz kann aber auch das Justiznetz komplett (as-a-Service) von der *BDBOS* betreiben lassen (rechts), dabei würde die *BDBOS* auch den Betrieb der Layer 3-Gateways und die Absicherung des Netzes übernehmen. Dazwischen sind auch Abstufungen vereinbar.

Ein wesentlicher Vorteil des eigenen virtuellen Justiznetzes ist die weitere Stärkung der Souveränität und Unabhängigkeit der Justiz. Einerseits, weil die bundesdeutsche Justiz künftig über ein justizeigenes, mit justizeigenen Zertifikaten gesichertes, Netz kommunizieren würde. Damit wäre auch ein Aspekt der hessischen Netzwerkklage bundeseinheitlich adressiert. Andererseits würden die physischen Verbindungsknoten selbst in Hoheit der Justiz oder, je nach Ausgestaltung, der von der Justiz beauftragten *BDBOS* liegen. **Abbildung 58** (links) zeigt, dass derzeit viele Justiz-IT-Dienstleister nicht über eigene Netzanschlüsse (zum Internet oder NdB VN) verfügen, sondern Anschlüsse der Landes-IT-Dienstleister oder gar dritter IT-Dienstleister nutzen, die wiederum über Verbindungsknoten des NdB Verbindungsnetzes kommunizieren. Würde sich die Justiz in diesem Setup eine Änderung wünschen, wäre dies nicht ohne intensive Abstimmung, viele Herausforderungen und vor allem viel Zeit möglich.

Verbindungsnetz über Verwaltungsknoten



Justiz-eigenes virt. Netzwerk (NdB-JN)



Beim Aufbau eines eigenen virtuellen Netzes zwischen Justiz-IT-Dienstleistern können direkte Kommunikationskanäle in Hoheit der Justiz geschaffen werden (vgl. **Abbildung 58** rechts). Dabei lägen Erweiterungen, Konfiguration, Steuerung und Überwachung des gesamten Netzes in Hoheit der Justiz. Allein die physische Platzierung innerhalb eines ggf. verwaltungsnahen Rechenzentrums sowie die physische Wartung dieser Endgeräte durch IT-Dienstleister wäre zu regeln. Diese kann die *BDBOS* entweder selbst übernehmen (siehe oben) oder die Fähigkeit zum sicheren Betrieb der Endgeräte durch entsprechende Zertifizierungen der IT-Dienstleister (z. B. ISO27001) überwachen.

Innerhalb des bundeseinheitlichen Justiznetzes ist die Justiz nun frei, beliebige Plattformdienste zu etablieren und dafür gleichermaßen dedizierte virtuelle Infrastruktur in allen verbundenen Rechenzentren zu nutzen. Bei den am Justiznetz teilnehmenden IT-Dienstleistern unterscheidet man in sogenannte Knoten-Provider und Netzteilnehmenden. Knoten-Provider sind IT-Dienstleister, die nicht nur am Netz teilnehmen, sondern auch dedizierte virtuelle Infrastruktur zur Justizcloud beisteuern. Netzteilnehmende hingegen sind IT-Dienstleister, die nur mit dem Justiznetz verbunden sind, aber keine eigene virtuelle Infrastruktur stellen.

Es ist klar, dass Knoten-Provider eine entsprechend performante Netzverbindung benötigen, da auf ihrer Infrastruktur die bundeseinheitlichen Plattformen und Anwendungen betrieben werden. Dafür sollten Endgeräte mit ca. zwei bis fünf Gigabit geplant werden, wohingegen einfache netzteilnehmende IT-Dienstleister mit einem Gigabit-Bandbreite

auskommen sollten. Die initiale Recherche ergab, dass die benötigten Layer 2-Bandbreiten durch die *BDBOS*-Rahmenverträge möglich wären. Im Rahmen des Justiznetz-Aufbaus sollten jedoch insb. bei den Knoten-Providern sogenannte Site Surveys durch von der *BDBOS* beauftragte Carrier erfolgen, um die größtmöglichen physikalischen Bandbreiten zu ermitteln. Die entsprechenden Layer 3-Endgeräte zum Justiznetzaufbau sind via *BDBOS* beschaffbar und wurden gem. *BDBOS*-Preisliste in der Justizcloud-Wirtschaftlichkeitsbetrachtung bereits berücksichtigt (vgl. **Kapitel 4.2.1**).

3.5.2.3 Justizcloud Zertifikate-Provider

Zur Absicherung des Layer 3-Justiznetzes benötigt die Justiz eigene bundeseinheitliche Verschlüsselungszertifikate. Dafür sollte die Justiz eine eigene zentrale Root-CA (Certificate Authority), also eine Hauptquelle zur Ausstellung, Verteilung und Validierung dieser Zertifikate, besitzen. Dies ist auch wichtig, weil die Zertifikate für eine bessere Sicherheit regelmäßig ausgetauscht werden müssen (sog. Key Rotation). Dies sollte idealerweise automatisch erfolgen.

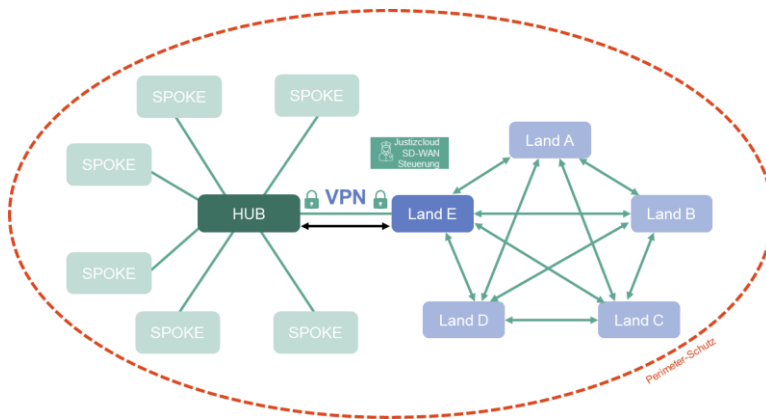
Die Zertifikate werden verwendet, um den Datenverkehr in den Layer 3-Gateways der Sender zu verschlüsseln und vom Gateway des empfangenen Netzteilnehmenden entschlüsselt zu werden. Da die Justiz noch keine eigene Root-CA hat, könnten Vertrauensdienste bspw. des *BSI* (sog. V-PKI) oder der *Bundesdruckerei* (sog. D-Trust) genutzt werden.

Sollte die Justiz das Layer 3-Netz von der *BDBOS* absichern lassen (vgl. **Kapitel 3.5.2.2**) und für das Justiznetz selbst keine Root-CA benötigen, wäre ein solcher Dienst trotzdem relevant, um auch Zertifikate für andere Komponenten und Dienste der Justizcloud verfügbar zu haben, bspw. für eine Datenverschlüsselung (sog. at rest) in der Justizcloud oder in kommerziellen Cloud-Umgebungen (sog. BYOK/ HYOK). Auch werden Zertifikate zur Verwendung in den Justizanwendungen, z. B. Browser-Kommunikation (*https*), benötigt.

3.5.2.4 Justizcloud-Netzwerksegmentierung

Bereits bei der Untersuchung der Bereitstellungsmodelle wurde vom technischen Fachpanel der Vorteil einer sogenannten Hub-and-Spoke-Netzarchitektur erkannt (vgl. **Kapitel 3.5.1.3**). Diese kann bei Erweiterung des Justiznetzes bspw. in kommerziellen Umgebungen verwendet werden, um einen bundeseinheitlichen, souveränen und vor allem effizienten Zugang zu diesen Umgebungen für alle Länder zu schaffen (vgl. **Abbildung 59**).

Abbildung 59 | Netzwerkerweiterungen durch Hub-and-Spoke-Modell



Dabei etabliert die Justizcloud-SD-WAN-Steuerungseinheit einen sog. Virtual-Private-Cloud-Hub-Netzknoten beim kommerziellen Cloud-Anbieter. Dafür wird anforderungsabhängig von einem zu definierenden IT-Dienstleister (hier: Land E) eine gesicherte VPN-Verbindung zum kommerziellen Anbieter er-

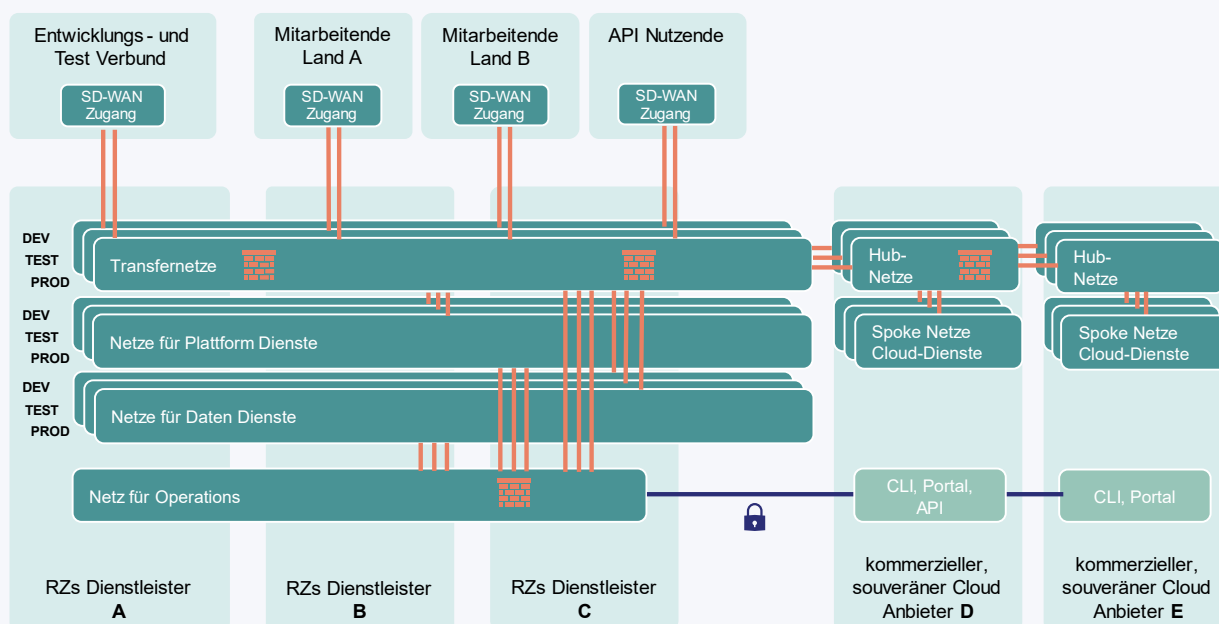
stellt und dafür der Internetanschluss oder auch dedizierte Layer 2-Netze (sog. Standleitungen, dedicated cloud access (DCA)) für eine breitbandige Anbindung genutzt bzw. angeschafft. Diese Verbindung würde in der Regel nicht über die NdB aufgebaut, denn der kommerzielle Anbieter ist keine Behörde.

Aus dem Hub heraus können nun sogenannte Spoke-Netzwerksegmente bzw. virtuelle Subnetze aufgebaut werden, um bspw. anwendungsspezifische Netzsegmente oder Netzsegmente für Innen- und Außenkommunikation sowie zur Datenhaltung abzuscheiden. Die Kontrolle und Konfiguration (z. B. IP-Adressvergabe) dieser Netze behält dabei immer die Justizcloud-Steuerungseinheit. Sie kann Netze erstellen, erweitern oder löschen sowie Intra- und Inter-Netzkommunikation erlauben und überwachen (z. B. bzgl. ungewöhnlicher Aktivitäten). Mit dem Hub-and-Spoke-Modell lassen sich so auch weitere Hubs bei anderen kommerziellen Anbietern etablieren, konfigurieren, absichern und steuern.

Ein ähnliches Verfahren böte sich auch bei der Anbindung der Bundesgerichte an. Die Bundesgerichte kommunizieren als Bundesbehörden über die NdB und sind netzwerkseitig nicht direkt von den Ländern erreichbar. EGVP-Nachrichten werden den Bundesgerichten via deren Internetanschluss zugestellt. Um Justizcloud-Dienste zu nutzen oder am Datenaustausch innerhalb des Justiznetzes teilzunehmen, hätten die Bundesgerichte im Grunde zwei Möglichkeiten. Einerseits könnten sie sich jeweils selbst an das Justiznetz anschließen, indem sie selbst Layer 3-Gateways im eigenen IT-Betrieb bzw. bei ihrem IT-Dienstleister installieren. Andererseits wäre es auch denkbar, dass die Justiz einen Hub als Netzübergang in die NdB definiert und von dort aus jeweils Spoke-Segmente je Bundesgericht ansteuern kann. In beiden Fällen könnten die Bundesgerichte mit der Justiz in den Ländern über das Justiznetz kommunizieren, entweder miteinander oder mit anderen Bundesbehörden, aber weiterhin über die NdB.

Im Rahmen des technischen Fachpanels wurde neben diesen übergreifenden Festlegungen auch ein grobes Netzwerksegmentierungskonzept entwickelt. **Abbildung 60** zeigt am Beispiel von drei Justiz-IT-Dienstleistern (A-C) sowie zweier kommerzieller Umgebungen (D und E), wie die Netzsegmentierung aussehen könnte.

Abbildung 60 | Typische Netzwerksegmentierung für Hybrid-Cloud



Das Konzept sieht vor, dass innerhalb der Private Community Cloud mindestens vier Netze unterschieden werden müssen. Das Hauptnetz, welches alle Anwendungen und Anwender miteinander verbindet, wird als Transfernetz bezeichnet. Die bundeseinheitlichen Justizcloud-Plattformdienste werden in einem separaten Netz ausgebracht. Ebenso separiert wird ein Netz für Datenhaltungsdienste. Im sogenannten Operations- bzw. Managementnetz liegen administrative Dienste der Justizcloud-Administratoren (vgl. **Kapitel 3.5.5**), bspw. um die vorgenannten Netze zu administrieren. Von dort aus haben die Administratoren auch Zugriff auf die Hub-and-Spoke-Netze in kommerziellen Umgebungen, die sie über sichere Verbindungen via der Cloud-Portalanwendungen oder direkt per API der kommerziellen Anbieter administrieren können.

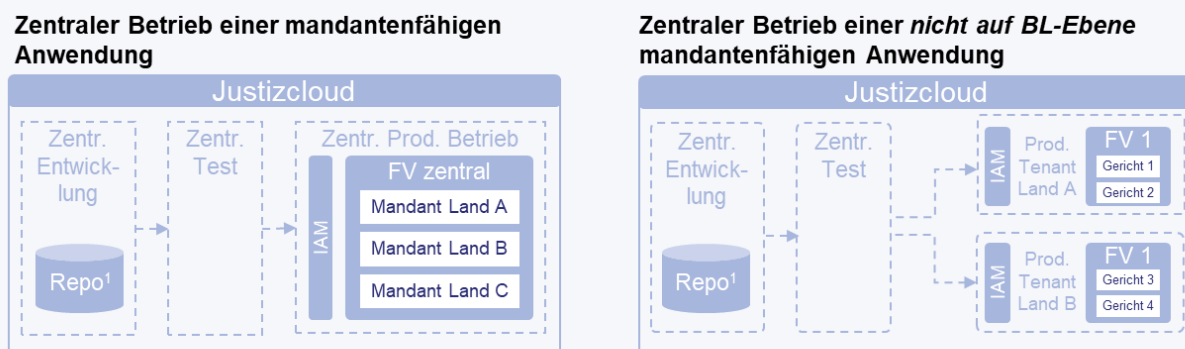
Die meisten vorgenannten Netze gibt es zudem jeweils dreimal. Denn auch die Netzwerksegmentierung muss entwickelt, getestet und für den produktiven Wirkbetrieb ausgebracht werden. Das spiegelt sich sowohl in der internen als auch in den kommerziellen Umgebungen wider.

3.5.3 Mandantenkonzept der Plattform

Innerhalb des bundeseinheitlichen Justizcloud-Netzes können nun zwei verschiedene Varianten der Mandantentrennung umgesetzt werden. Ein Mandant (sog. Tenant) im Sinne der Justizcloud ist ein Land oder ein Bundesgericht. Im Cloud-Kontext ermöglicht ein Mandant, die vollständige Trennung bspw. von Benutzern, Anwendungen, Konfigurationen und Kostenabrechnungen. Auch die Festlegung und Erbringung von Service Level Agreements (SLAs) kann bei Bedarf mandantenspezifisch erfolgen. Da die Justiz mit der bundeseinheitlichen Justizcloud vor allem das Ziel eines bundeseinheitlichen Betriebs moderner Anwendungen verfolgt (vgl. **Kapitel 3.1.1**), wird zunächst davon ausgegangen, dass für alle Länder die gleichen Bedingungen gelten sollen.

Da nicht alle Anwendungen der Justiz multi-mandantenfähig sind (vgl. **Kapitel 2.2.1**), müsste die Justizcloud zwei Mandantenkonzepte bereitstellen. Erstens bundeseinheitliche Bereiche zum Ausbringen multi-mandantenfähiger Anwendungen zur Nutzung durch alle Länder. Zweitens länderspezifische Mandantentrennung für Anwendungen, die nicht multi-mandantenfähig sind, zur Nutzung durch ein Land oder Bundesgericht (vgl. **Abbildung 61**).

Abbildung 61 | Varianten der Mandantentrennung



¹ Repository für Code, Artefakte (z. B. Container Images), automatisierte Tests, Ausbringungs-Templates ...

Länderübergreifend mandantenfähige Anwendungen könnten in **bundeseinheitlichen Mandantensegmenten** betrieben werden. Multi-mandantenfähige Anwendungen können innerhalb der Anwendung unterscheiden, aus welchem Land bzw. Gericht ein Nutzender stammt bzw. worauf er berechtigt ist. Dafür hat die Anwendung Zugriff zum zentralen Benutzer- und Berechtigungsmanagement (IAM), wo diese Informationen hinterlegt sind. Multi-mandantenfähige Anwendungen trennen die Datenhaltung auf logischer oder physischer

Ebene und können dadurch eine länderspezifische Datenverschlüsselung auf Datenebene realisieren (vgl. **Kapitel 3.4.3**).

Die Umgebung für solche bundeseinheitlich betreibbaren, multi-mandantenfähigen Anwendungen wird mit einem bundeseinheitlichen Zertifikat gesichert. Zur Betreuung dieser bundeseinheitlichen Umgebungen sollten ausgewählte Administratoren festgelegt werden sowie die Administratoren der Länder zumindest lesend berechtigt werden. Die Abrechnung der Nutzung in solchen Umgebungen sollte pro rata bzw. per use erfolgen oder klassisch per *Königsteiner Schlüssel*.

Die Ausbringung multi-mandantenfähiger Anwendungen in diese bundeseinheitlichen Mandanten erfolgt zweistufig. Aus einem zentralen Entwicklungssegment wird in eine bundeseinheitliche Testumgebung ausgebracht und nach erfolgreichem Test durch alle Länder die zentrale Produktivumgebung aktualisiert.

Da noch nicht alle Anwendungen multi-mandantenfähig sind, müssen in der Justizcloud auch **länderspezifische Mandanten** möglich sein. Eine länderspezifische Mandantenumgebung ist dadurch gekennzeichnet, dass in ihr nur Anwendungen für das jeweilige Land ausgebracht werden können und diese Anwendungen auch nur Nutzende aus dem jeweiligen Land verwenden können. Dafür kann das zentrale IAM dienen. Es ist aber auch möglich, eine individuelle IAM-Instanz in diesem Mandanten auszubringen und diese nur mit dem jeweiligen lokalen IdP zu föderieren. Solche Umgebungen sind auch mit länderspezifischen Zertifikaten gesichert und können daher nur vom jeweiligen Land eingesehen und auf Ebene des Tenants vom Land administriert werden. Die Justizcloud-Administratoren sollten in dem Fall Unterstützungs- und Standardisierungsfunktionen sowie Basiskonfigurationsaufgaben übernehmen. Die Abrechnung von der Cloud-Nutzung in solchen Mandantensegmenten sollte pro Land erfolgen.

Auch die Ausbringung unterscheidet sich von bundeseinheitlichen Mandantensegmenten (vgl. **Abbildung 61**). Da es sich in der Justizcloud um bundeseinheitliche Cloud-fähige Anwendungen handelt, werden diese wie zuvor aus der zentralen Entwicklungsumgebung in eine zentrale Testumgebung ausgebracht. Nach erfolgreichem Test, werden dann gleiche Instanzen, d. h. jeweils Kopien der Anwendungen, in die länderspezifischen Produktivumgebungen ausgebracht. Das ist zwar etwas aufwändiger als ein bundeseinheitliches Deployment, kann aber sehr effizient mit heutigen CI/CD-Werkzeugen als sog. Pipelines umgesetzt und gesteuert werden. Es ist auch denkbar, für bestimmte Anwendungen länderspezifische Testumgebungen im Kontext des länderspezifischen Mandanten zu ermöglichen. Dies

würde vor allem darauf einzahlen, dass länderspezifische Mandanten als erweitertes Serviceangebot der Justizcloud die Umsetzung länderspezifischer Bedarfe, wie z. B. nicht-bundeseinheitliche Verfahren, ermöglichen.

3.5.4 Justizcloud-Plattformdienste

Die Justizcloud-Plattform soll bundeseinheitliche Plattformdienste bereitstellen, die auf bundeseinheitlicher Infrastruktur von Justiz-IT-Dienstleistern (Private Community Cloud) und perspektivisch ergänzend von kommerziellen Anbietern (Hybrid Justizcloud) basieren (vgl. **Kapitel 3.5.1.3 ff.**). Auf der Plattformebene sind dabei vor allem eine **Cloud-Management-Plattform** (vgl. **Kapitel 3.5.4.1**), eine **Container-Orchestrierungs-Plattform** (vgl. **Kapitel 3.5.4.2**) sowie eine **Integrationsplattform** (vgl. **Kapitel 3.5.4.3**) relevant. Um auf der CaaS-Plattform Anwendungen ausbringen zu können, bedarf es eines **Entwicklerarbeitsplatzes** auf der Justizcloud-Plattform (vgl. **Kapitel 3.5.6**). Zur Festlegung von Administrationsrechten in allen vorgenannten Plattformdiensten wird zudem ein **Benutzer- und Berechtigungsmanagement für Administratoren** benötigt (sog. Admin-IAM, vgl. **Kapitel 3.5.5**).

3.5.4.1 Cloud-Management-Plattform

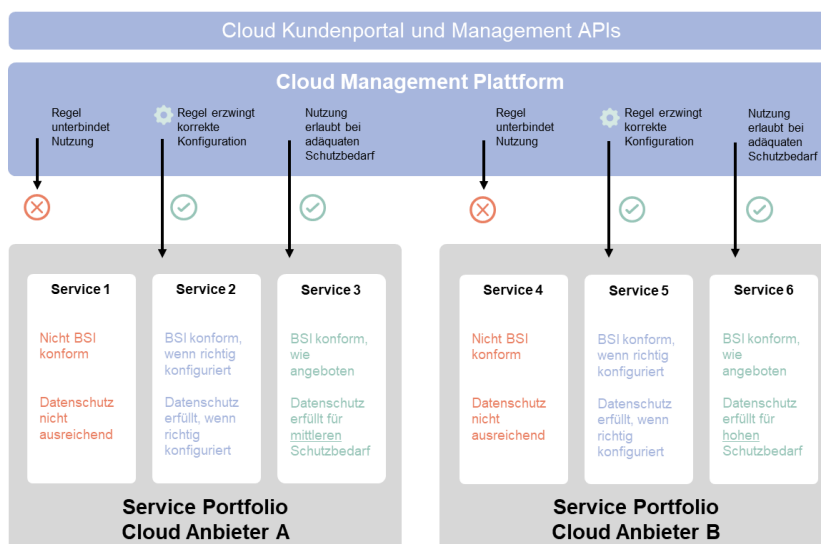
Eine Cloud-Management-Plattform (CMP) stellt verschiedene Funktionen bereit, um den Cloud-Betrieb zu ermöglichen sowie die einheitliche und integrierte Verwaltung verschiedener Cloud- bzw. Infrastrukturdienste verschiedener Anbieter bzw. Umgebungen im Multi/Community bzw. Hybrid-Cloud-Kontext. Für die verschiedenen Funktionsbereiche einer CMP gibt es diverse Softwarelösungen, einige davon decken mehrere Funktionen ab, andere spezialisieren sich auf einzelne (vgl. **Abbildung 45**).

Die wesentlichen Funktionen einer CMP umfassen verschiedene miteinander integrierte Bereiche: Der **Service Request** umfasst z. B. ein Portal oder APIs zur Beauftragung und automatisierten Bereitstellung von Cloud-Diensten oder zusätzlicher Ressourcen. Dabei können nur Dienste und Ressourcen verwendet werden, die im **Inventar** entsprechend zur Nutzung **klassifiziert** wurden. Die eigentliche Bereitstellung findet durch den **Provisionierungs- und Orchestrierungsbaustein** statt. Die Cloud-Dienste und Ressourcennutzung werden über das **Kostenmanagement und die Ressourcenoptimierung** abgerechnet. Hier geht es auch darum, Transparenz über die Cloud-Ressourcennutzung herzustellen, um Entwicklungsverbünden Hinweise zur Kosten- und Performanz-Optimierung zu geben und vorausschauende Planungen zu ermöglichen.

Der Funktionsblock **Cloud-Migration, Backup und Disaster Recovery** stellt Werkzeuge bereit, um die Cloud selbst sowie die Daten und Anwendungen der Endnutzenden regelmäßig zu sichern und im Notfall wiederherstellen zu können. Der Bereich **Monitoring und Analyse** stellt Funktionen für den Cloud-Plattformbetrieb und den Betrieb der Anwendungen durch Entwicklungsverbünde bereit und ist vor allem an Entwickler und Betriebspersonal gerichtet, um technische Auswertungen, z. B. zur Stabilität und Performanz von Cloud-Diensten und Anwendungen, zu ermöglichen. Abschließend stellt der Bereich **Identitätsmanagement, Sicherheit und Compliance** Funktionen bereit, die Berechtigungen und Auditierbarkeit der vorgenannten Funktionsbereiche ermöglichen. Dabei werden diese Werkzeuge mit dem Admin-IAM integriert (vgl. **Kapitel 3.5.5.1**).

Gerade die Inventarisierungs- und Klassifikationsfunktion nimmt beim Hybrid- und insb. Multi Cloud-Betrieb (vgl. Justizcloud-Evolutionsstufen, **Kapitel 3.5.1.4**) eine wesentliche Rolle ein, da jeder kommerzielle Anbieter ein heterogen definiertes Dienste-Portfolio und Preismodelle mitbringt. Auch ist die Zertifizierung (z. B. BSI C5) der Dienste nicht immer gleich, selbst innerhalb eines Cloud-Anbieters. Daher ist es essenziell, dass die Justiz über die CMP individuell steuert, welche Dienste in welchem Umfeld freigegeben sind (vgl. **Abbildung 62**).

Abbildung 62 | Cloud-Service-Governance mit Cloud-Management-Plattform



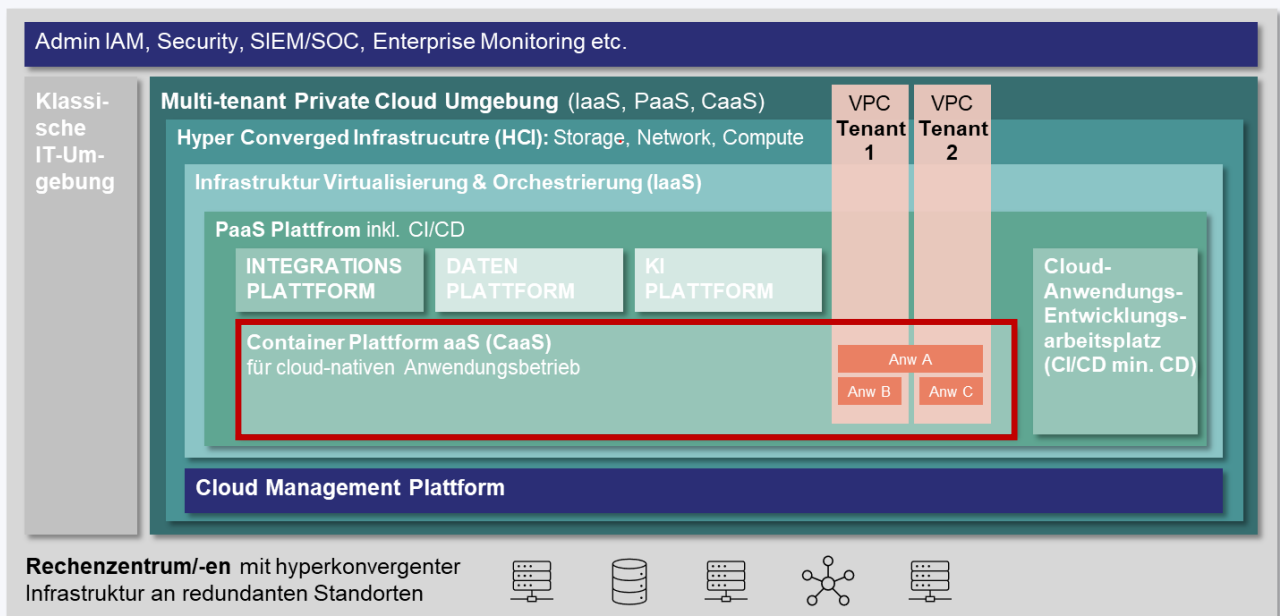
Die CMP übernimmt dabei die Sicherstellung dieser Einschränkungen, die Vereinheitlichung der Buchbarkeit und Abrechnungsfunktionen über heterogene kommerzielle Anbieter hinweg, sowie die Provisionierung der Cloud-Dienste für die Beantragenden, bspw. die Entwicklungsverbünde.

Damit kann die CMP auch länderspezifische Datenhoheit sicherstellen, indem bestimmte Mandanten oder Anwendungen nur auf freigegebene länderspezifische Datendienste zugreifen können. Auch die Ausführung von Container-Workloads kann durch ein entsprechendes Tagging-Konzept an den zugrundeliegenden Diensten bzw. virtuellen Maschinen administriert werden.

3.5.4.2 Container-Plattform

Eine Container-Orchestrierungsplattform ist Kernstück einer Cloud-Plattform, denn die Container-Technologie hat sich de facto als Marktstandard für den Betrieb Cloud-nativer, containerisierter Anwendungen etabliert. Cloud-native, containerisierte Anwendungen können ohne dedizierte Server bzw. virtuelle Maschinen (VM) ausgeführt werden, weil im jeweiligen Container bereits alle notwendigen Bestandteile zum Ausführen der Anwendung, inkl. eines leichtgewichtigen Betriebssystems (sog. Basis Image), enthalten sind. Dadurch können die Container von der Container-Plattform nahezu autark aus dem Code- bzw. Artefakt-Repository entnommen und auf verschiedenen Umgebungen ausgebracht werden. Jedem Container liegt dabei eine Ausbringungsanweisung bei, bspw. um die Ressourcenanforderungen oder Abhängigkeiten zu anderen Containern zu definieren. Zudem kann jeder Container signiert werden. Der Signatur (sog. Tagging) kann bspw. entnommen werden, auf welcher Umgebung dieser Container bereits erfolgreich getestet wurde und wo er daher wiederverwendet werden kann. Eine Container-Plattform bildet dabei das Bindeglied zwischen der virtuellen Infrastruktur und den containerisierten Anwendungen, um die Anwendungscontainer auszubringen und im Betrieb deren Verfügbarkeit, Stabilität und Wiederherstellung zu garantieren (vgl. **Abbildung 63**).

Abbildung 63 | Container-Plattform im Kontext einer Cloud-Architektur (Accenture)

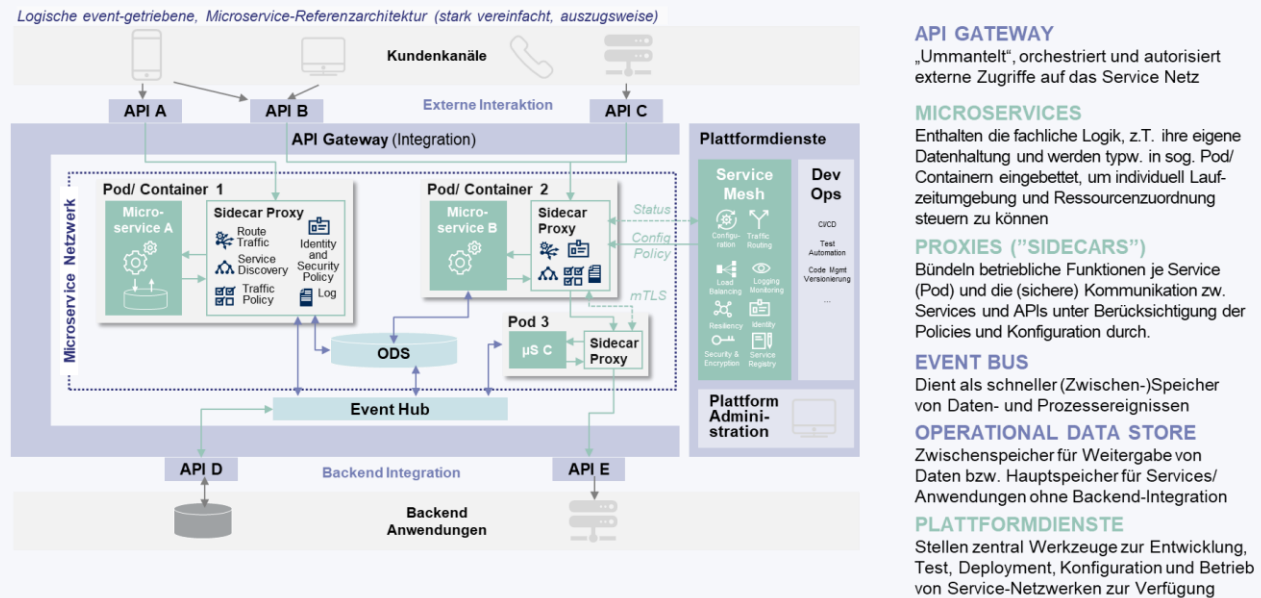


Durch den Zugriff auf die virtuelle Infrastruktur kann eine Container-Plattform, je nach Bedarf, Anwendungen horizontal bzw. vertikal skalieren, sogar voll automatisiert mit sog. Auto-Scaling. Vertikale Skalierung bedeutet, dass der Anwendung zusätzliche virtuelle Infrastruktur (z. B. CPU-/ Rechenleistung) zugewiesen wird. Horizontale Skalierung bedeutet, dass Kopien desselben Containers mehrfach ausgebracht werden und der Datenverkehr auf diese neuen Container-Instanzen durch die Container-Plattform umgeleitet, d. h. orchestriert, wird. Die Container-Orchestrierungsplattform kann dadurch eine hohe Parallelisierung von Anwendungen ermöglichen, um etwa eine große Rechenlast oder Nutzendenlast effizient zu verteilen. Sollte ein Container aufgrund von Fehlern oder zu hoher Last abbrechen, orchestriert die Container-Plattform die Wiederherstellung neuer Container, sodass jederzeit ausreichend Kapazität im Container-Cluster vorliegt. Nicht zuletzt aufgrund dieser Fähigkeiten vereinfacht eine Container-Plattform den technischen Anwendungsbetrieb erheblich.

Wie dargestellt, arbeitet die Container-Plattform sehr eng mit dem Entwicklerarbeitsplatz zusammen. Dabei können Entwicklerarbeitsplatz und Container-Plattform so miteinander integriert werden, dass Entwickler selbst steuern können, welche Umgebungen (sog. Namespaces) existieren und welche Container auf welche Umgebungen ausgebracht werden sollen. Dies tun sie mit sogenannten CI/CD-Pipelines (vgl. **Kapitel 3.5.6**). Die CI/CD-Werkzeuge benötigen dafür wiederum administrative Rechte auf dem Namespace des Entwicklers, nicht aber auf der Container-Plattform selbst oder gar den darunter liegenden VM-Betriebssystemen, um je nach Bedarf Umgebungen hoch- oder herunterzufahren (vgl. **Kapitel 3.5.3**). In diesem Zusammenhang wird daher oft von CaaS gesprochen, da viele Funktionen und damit Flexibilität und Agilität in festgesetzten Grenzen in die Hände der Entwickler gegeben werden.

Zudem bieten Container-Plattformen über die Orchestrierung im Betrieb hinaus viele Zusatzfunktionen. Einige Produkte bringen ihr eigenes Artefakt-Repository mit, dass auch Container-Images externer Quellen sanitisieren kann. Andere Produkte bringen sog. Operatoren zum standardisierten Ausbringen von containerisierten Drittprodukten (z. B. Kafka als Event Hub oder ELK-Stack für Logging und Monitoring) mit. Andere spezialisieren sich auf sicherheitsspezifische Aspekte und integrieren bspw. ein sog. Service Mesh im Kontext der Container-Plattform, mit dem die Service-zu-Service-Kommunikation innerhalb eines Clusters abgesichert (z. B. *mTLS*) und überwacht werden kann. Diese Zusatzdienste kann man auch als Plattformdienste bezeichnen, da sie allen auf der Container-Plattform laufenden Anwendungen dienen können (vgl. **Abbildung 64**).

Abbildung 64 | Beispielhaftes Container-Cluster mit Service Mesh und Plattformdiensten



Auch für den Aufbau der Justizcloud muss ein entsprechendes, passgenaues Container-Plattform-Produkt ausgewählt werden. Die IT-Dienstleister setzen derzeit viele verschiedene Produkte ein. Für die Justizcloud sollte ein bundeseinheitliches gewählt werden, das die Anforderungen der Justiz und insb. der Entwicklungsverbünde abdeckt, entsprechend skaliert und für das bestenfalls die entsprechende Betriebskompetenz bereits vorliegt. Dabei ist zu beachten, dass die Justizcloud eine multi-mandantenfähige Plattform ist und dementsprechend auch die Container-Plattform multi-mandantenfähig aufgesetzt wird. Im PoC wird noch simuliert, dass jedes Land einen sogenannten Namespace innerhalb des Container-Clusters bekommt (vgl. **Kapitel 3.5.7**). Perspektivisch kann man aber auch Container-Cluster pro Land bzw. auch Mandanten pro Land definieren, in denen jedes Land eigene Cluster und wiederum in jedem Cluster eigene Namespaces verwalten kann.

3.5.4.3 Integrationsplattform

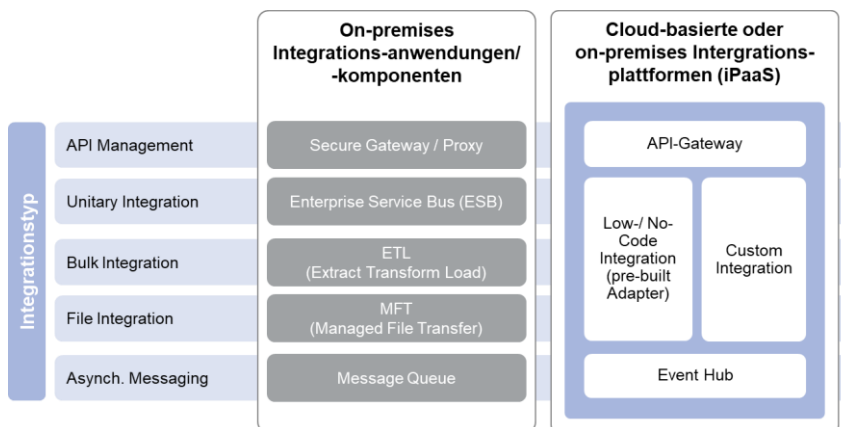
Integrationsplattformen sind Komponenten, um die Kommunikation zwischen Anwendungen zu entkoppeln, dabei verschiedene Mechanismen (sog. Protokolle) und Mehrwertdienste (z. B. Sicherheitsfunktionen und Lastverteilung) anzubieten und die einheitliche Verwaltung und Versionierung dieser Integrationen zu ermöglichen (vgl. **Kapitel 3.4.4.1**).

Man unterscheidet synchrone und asynchrone Kommunikation. Bei synchroner Kommunikation wird die Zielanwendung während des Zugriffs blockiert, wogegen bei asynchroner Kommunikation die Nachrichten konsekutiv abgearbeitet werden. Für eine hohe Performanz

sollten Zugriffe möglichst asynchron gestaltet werden. Dies funktioniert jedoch nicht immer, z. B. bei Zahlungssystemen, die eine direkte Bestätigung einer Buchung erfordern.

Integrationsplattformen sollten in der Regel drei Protokollarten unterstützen. Message-, also Nachrichten-basierte Kommunikation, API-basierte (z. B. REST, gRPC) und Event-basierte Kommunikation (vgl. **Kapitel 3.4.4.1**). Eine Integrationsplattform stellt dafür jeweils individuelle Technologien bereit, ermöglicht aber deren einheitliche Steuerung (vgl. **Abbildung 65**).

Abbildung 65 | Funktionsumfang von Integrationsplattformen

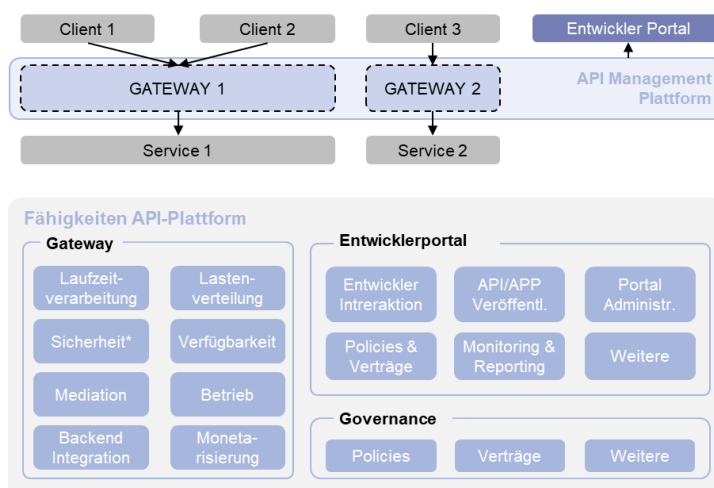


Quelle: Gartner

Am Markt haben sich dazu bereits sog. iPaaS-Produkte (Integration Plattform as a Service) entwickelt, die teils Cloud-basierte, teils auch on-premises betreibbare Varianten enthalten. Grundsätzlich kann die Justiz aber auch einen hybriden Ansatz verfolgen

und für jede Kommunikationsart das optimale Produkt wählen. Als Platfordmdienste liegen die sog. „Control Planes“ dieser Komponenten in einem separaten Netzsegment. Von da aus können verschiedene Instanzen, z. B. die eines API-Gateways (z. B. North- und Southbound, vgl. **Kapitel 3.4.4.2**), administriert und überwacht werden (vgl. **Abbildung 66**).

Abbildung 66 | Funktionsumfang eines API-Gateway



Bisher hat die Justiz vor allem Erfahrung mit Message-basierter Kommunikation gesammelt, da der Großteil der Kommunikation von Altverfahren sowie des elektronischen Rechtsverkehrs über Nachrichten via der bestehenden, Kommunikationsplattformen stattfindet. API-basierte Kommunikation findet langsam Einzug in die Justiz, z. B. bei Online-Diensten (vgl. **Kapitel 2.2.1.2**) und den neuen bundes-

einheitlichen Verfahren (z. B. *GeFa* und *AuRegis*). Jedoch wird dabei mangels einer API-

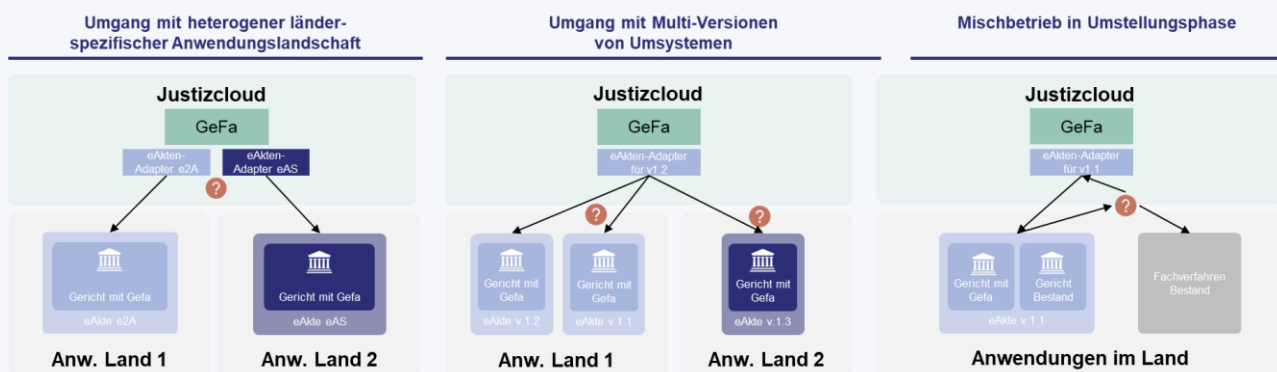
Management-Plattform, vielfach eine komplexe, fehleranfällige und schwer zu wartende Punkt-zu-Punkt-Verbindung zwischen Anwendungen (bspw. Fachverfahren und eAkte) hergestellt (vgl. **Kapitel 2.2.1**). Event-basiert Kommunikation findet mangels Verfügbarkeit einer Event-Hub-Komponente nahezu nirgends statt, obschon dies für Microservice-basierte, Cloud-native Anwendungen als Standard gilt, um Echtzeit-Reaktionen in Frontend-Applikationen zu ermöglichen oder die Datenkommunikation zwischen Microservices asynchron zu entkoppeln.

Im Rahmen der Modernisierung der Legacy-Kommunikationsplattformen sollten daher unbedingt auch moderne Formen der Kommunikation und damit Plattformprodukte in Betracht gezogen werden. Unabhängig davon wäre eine Integrationsplattform auch essenziell, um den sukzessiven Rückbau des veralteten eAkten-Rahmenkonzepts (vgl. **Abbildung 30**) sowie die skalierte Integration der Justizcloud-Anwendungslandschaft in die lokale Länderumgebungen effizient zu ermöglichen.

Integration mit lokalen Umgebungen

Bei der Integration mit lokalen Bestandsanwendungen müssen mehrere Integrationsherausforderungen gelöst werden (vgl. **Kapitel 3.4.4.1**).

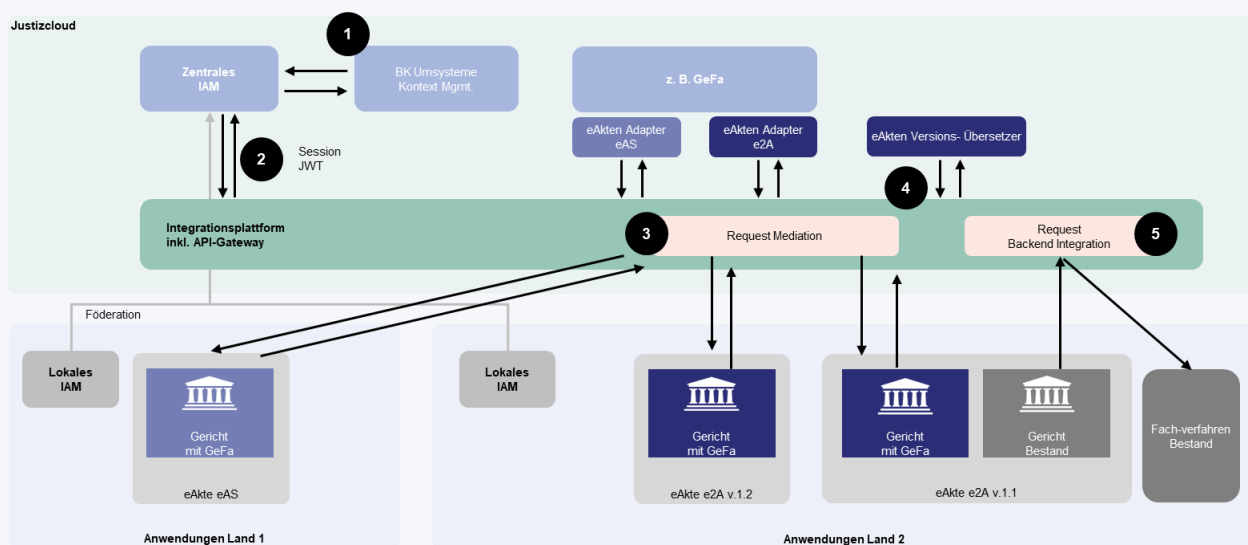
Abbildung 67 | Integrationsherausforderungen im Länderkontext



Zunächst stellt der Einsatz verschiedener Anwendungen je Land im Kontext der modernen Cloud-fähigen Fachverfahren, insb. der eAkten-Systeme, eine Herausforderung dar. Eine multi-mandantenfähige Cloud-Anwendung muss daher parallel mit drei verschiedenen eAkten-Systemen sprechen können.

Zudem kann es vorkommen, dass Länder mit demselben eAkten-System unterschiedliche Versionen einsetzen oder sogar mehrere Versionen in einem Land existieren. Somit könnten innerhalb eines Landes ein Teil der Gerichte auf eine neue eAkte und das neue Fachverfahren (z. B. *GeFa* oder *AuRegis*) migriert sein, während andere noch ein Bestandsverfahren mit der dazugehörigen älteren eAkten-Instanz nutzen. Über eine Integrationsplattform kann dieses Problem adressiert werden (vgl. **Abbildung 68**).

Abbildung 68 | Ablaufsequenz einer Anbindung von Länderumgebungen



Auf Basis des Funktionsumfangs von API-Management-Plattformen (z. B. Lastverteilung, Mediation, Sicherheit) lassen sich für die genannten Integrationsherausforderungen Lösungen entwickeln. Im Kontext der Integrationsplattform können bspw. Mediations-Microservices in Hoheit der anwendungsverantwortlichen Entwicklungsverbünde entwickelt werden. Die Schnittstellen der Anwendungen werden im API-Developer-Portal publiziert und können dort von neuen API-Nutzenden recherchiert, getestet und Zugriffsrechte angefordert werden. Die Integrationsplattform übernimmt auch das sog. Token-Handling und orchestriert die Abfrage entsprechender Zugriff-Tokens beim zentralen IAM. Außerdem kann die Integrationsplattform in der Cloud auch für die Backend-Integration in Altverfahren als sog. Redirect bzw. Umleitung aufgebaut werden. Damit könnte die Justizcloud-Integrationsplattform einen wesentlichen Beitrag zur Unterstützung und Belastbarkeit von Migrationsvorhaben leisten.

3.5.5 Plattform-Administrationskonzept

3.5.5.1 Administration und Admin-IAM

Administratoren sind im Grunde Entwicklungs- und Betriebspersonal mit besonderen, teilweise sehr weitgehenden Rechten auf der technischen (z. B. Errichtung oder Löschung neuer Netzwerksegmente) und z. T. auch fachlichen Ebene (sog. Last Level Support).

Die Justizcloud als virtuelle Community Cloud basiert auf physischer, virtualisierter Infrastruktur von IT-Dienstleistern und bündelt diese zu einer homogenen virtuellen Infrastruktur- und Plattformebene. Dadurch ergibt sich eine besondere Arbeitsteilung zwischen den IT-Dienstleistern, der Justizcloud und den Cloud-nutzenden Entwicklungsverbünden, die ihre Anwendungen mit und auf der Justizcloud ausbringen. Auch das vorgestellte Mandantenkonzept (vgl. **Kapitel 3.5.3**) bringt eine zusätzliche Anforderung für eine länderspezifische Administrationstätigkeit mit sich. Dadurch entstehen verschiedene Bedarfe, administrative Tätigkeiten im Gesamtkontext zu betrachten und ein Administrationskonzept von Beginn an mitzudenken. Einige davon sollen hier beispielhaft ausgeführt werden.

Zum einen bedarf es eines administrativen Zusammenspiels auf der Infrastrukturebene. Dabei müssen Justizcloud-Dienste idealerweise festgelegt administrative Rechte bei Knoten-Provider-IT-Dienstleistern haben, um z. B. automatisiert, d. h. via API, zusätzliche virtuelle Infrastruktur provisionieren zu können. Andererseits sollten Administratoren der Knoten-Provider zumindest lesenden Zugriff auf die Justizcloud-Infrastrukturebene erhalten, um das Verhalten ihrer bereitgestellten virtuellen Maschinen überwachen zu können.

Das alle Parteien verbindende Justiznetz wird zentral durch die Justizcloud-Einheit in Zusammenarbeit mit der *BDBOS* betrieben und gesteuert. Jedoch liegen die entsprechenden physischen Knoten in den Rechenzentren der Justiz-IT-Dienstleister, sodass physische, administrative Tätigkeiten in den Verantwortungsraum der IT-Dienstleister fallen.

Auch auf der Justizcloud-Plattformebene sind gemeinsame administrative Tätigkeiten notwendig. Bspw. bei der vorgenannten Zulassung länderspezifischer Administratoren auf länderspezifische Umgebungen bzw. Mandanten (vgl. **Kapitel 3.5.3**). Auch ist es denkbar, dass perspektivisch bestimmte IT-Dienstleister selbst PaaS für die Justizcloud erbringen und deren administratives Personal entsprechende Zugriffe erhält.

Abschließend bedarf es in Verbindung mit dem Anwendungsentwicklerarbeitsplatz auch administrativer Tätigkeiten auf der Anwendungsebene. Personal der Entwicklungsverbünde (sog. DevOps-/ Plattformteams) muss für eine effektive Tätigkeit relevante administrative

Rechte erhalten. Diese können sehr eng, aber auch sehr weit definiert werden. Bspw. ist es üblich, dass Entwickler eigene Testumgebungen autark „hochziehen“ und „abreißen“ können. Andererseits müssen diese Umgebungen bzgl. ihrer Ressourcennutzung administriert und beschränkt werden, sodass ausgeschlossen wird, dass Entwicklungstätigkeiten die produktiven Kapazitäten der Justizcloud negativ beeinflussen. Auch innerhalb eines Entwicklungsverbunds kann klar geregelt werden, welcher Entwickler welche Rechte auf der Codebasis usw. erhält.

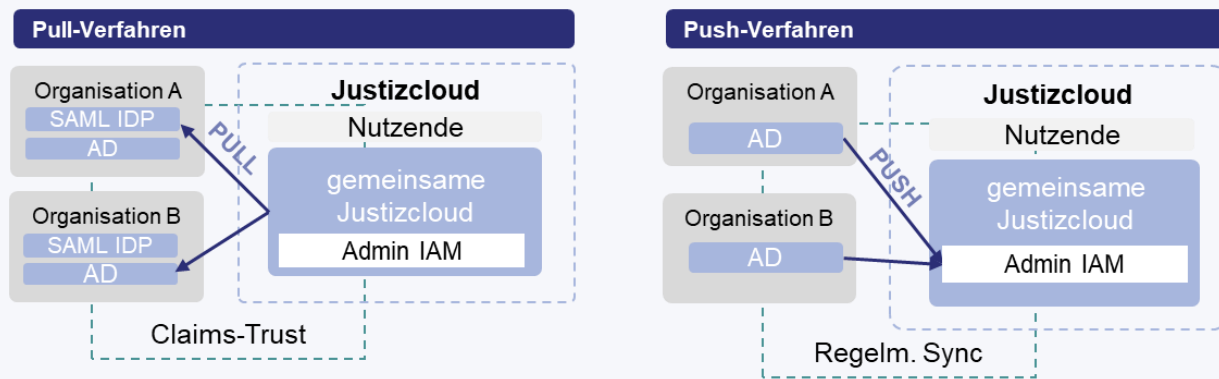
Um solche administrativen Nutzenden der Justizcloud und der Länder verwalten und deren Rechte auf Plattform, Infrastruktur und Netzwerk steuern sowie Administratoren und Entwickler und von den Endnutzenden der Anwendungen selbst unterscheiden zu können, wird ein sog. **Admin-IAM** im Plattformzielbild benötigt (vgl. **Kapitel 3.3.2**). Teil eines Admin-IAMs ist auch ein so genanntes Privileged Access Management (PAM). Dies ist ein (Sub-)System, dass die sichere Verwaltung der Authentisierungsfaktoren und Zugriffsberechtigungen für Administratoren ermöglicht und bspw. zeitbeschränkte Zugriffe ermöglicht, administrative Tätigkeiten aufzeichnet und rechtlich erforderliche Audit-, Governance und Reportingfunktionen bietet.

Dies bedeutet, dass administrative Tätigkeiten auf der fachlichen Anwendungsebene, d. h. erweiterte Rechte in Anwendungen (bspw. *GeFa* und *AuRegis*), nicht unter das Plattformadministrationskonzept fallen. Diese Art von Berechtigungen von Endnutzenden sowie deren fachliche Administration lokaler Nutzerpools findet im Benutzer- und Berechtigungsmanagement für Nutzende auf der Anwendungsebene statt (vgl. IAM / CIAM, **Kapitel 3.4.6**).

3.5.5.2 Föderation von Administratoren

Wie im vorangegangenen Kapitel dargestellt, ist es an verschiedenen Stellen notwendig, dass nicht nur Administratoren der Justizcloud tätig werden, sondern auch Administratoren der Länder (ggf. Dritte) auf der Justizcloud-Plattform bekannt und berechtigt sind. Die Administratoren der Justizcloud können dabei direkt im Admin-IAM der Justizcloud gepflegt werden. Die Identitäten der Administratoren der Länder hingegen werden führend in den Länder-IdPs verwaltet und sollten daher ins Admin-IAM föderiert werden. Dafür bieten sich grundsätzlich zwei Verfahren (sog. Push- vs. Pull-Verfahren) an (vgl. **Abbildung 69**).

Abbildung 69 | Identitäten-Föderationsverfahren für Administratoren



Das **Pull-Verfahren** zeichnet sich dadurch aus, dass sich das Admin-IAM zur Laufzeit rückversichert, ob ein Administrator im Länder-IdP (Identity Provider) oder -AD (Active Directory) existiert, welche Basisrechte er hat und wie er sich authentisiert. Dabei können Standardprotokolle wie SAML oder OIDC/OAuth2.0 verwendet werden. Dafür muss zwischen dem Justizcloud-Admin-IAM und den lokalen Identitätsquellen vorher eine Vertrauensstellung (sog. Claims-Trust) sowie die gegenseitige Erreichbarkeit sichergestellt werden. Bspw. sind nicht alle Länder-IdPs aus dem Internet erreichbar, sodass diese Form der Kommunikation im Justiznetz erfolgen muss. Da die Länder-IdPs häufig aber in den internen Netzzonen der IT-Dienstleister liegen, muss auch eine Vertrauensstellung zwischen Justiznetz und internen Netzen bspw. in Form von Firewall-/ Port-Freischaltungen existieren oder die Kommunikation über eine API-Management-Plattform entkoppelt werden. Nachteil des Pull-Verfahrens ist, dass die Länderseite per Definition „online“ sein muss, damit sich ein Länder-Admin in der Justizcloud betätigen kann. Um diesen Nachteil zu mitigieren, verwenden Organisationen das sog. Push-Verfahren.

Im **Push-Verfahren** werden die lokalen Identitäten der Administratoren von den lokalen IdPs regelmäßig ins Admin-IAM gepusht bzw. damit synchronisiert. Der Rhythmus sollte dabei mindestens täglich sein, kann aber auch je nach Setup häufiger erfolgen. Dementsprechend sind die Administratoren nicht in Echtzeit, aber hinreichend aktuell, um Risiken (z. B. gekündigter Administrator) zu vermeiden. Zudem liefern die meisten IdP häufig auch Metadaten mit, in denen sich Berechtigungsdauern, Vertragslaufzeiten und Löschkennzeichen abbilden lassen. Durch die regelmäßige Synchronisation sind die Administratoren jederzeit in der Justizcloud handlungsfähig, auch wenn zum lokalen IdP keine Verbindung besteht.

In beiden Verfahren werden die Rechte der Administratoren auf bzw. innerhalb der Justizcloud-Ebenen und -Dienste im Admin-IAM der Justizcloud vergeben. Zudem können auch im Admin-IAM zusätzliche Anforderungen an die Authentisierung (sog. Step-up-Authentification) festgelegt und zur Laufzeit von Administratoren abgefordert werden.

3.5.6 Justizcloud-Entwicklerarbeitsplatz

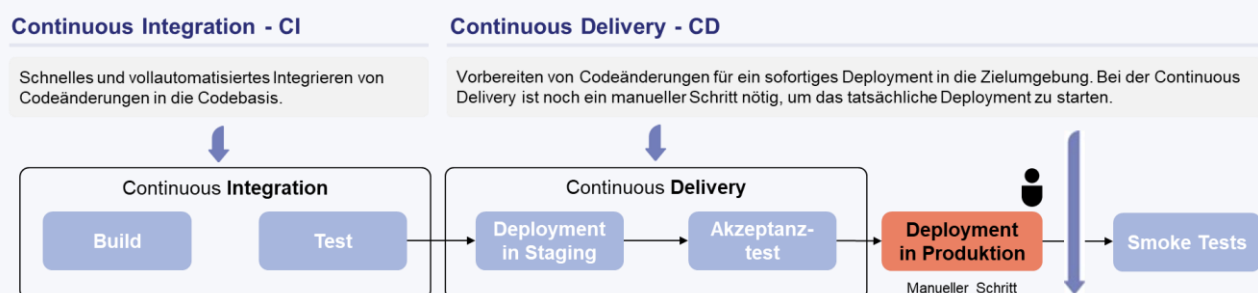
Ein wesentliches Kernelement der Justizcloud ist der sogenannte integrierte Entwicklerarbeitsplatz. Dieser ermöglicht es Entwicklungsverbünden, ihre Anwendungen auf Justizcloud-Umgebungen sowohl in der Private Cloud als auch perspektivisch in kommerziellen Umgebungen über die Justizcloud auszubringen.

Bei Cloud-nativen Anwendungen spricht man im Kontext der Ausbringung auch vom sogenannten CI/CD. CI steht für Continuous Integration und bedeutet, dass Entwickler kontinuierlich ihre Anwendungen weiterentwickeln und ihre Änderungen unabhängig von anderen Entwicklern kontinuierlich testen lassen (vgl. Testautomation) können.

CD steht für Continuous Delivery und bedeutet, dass erfolgreich getestete Anwendungen oder Bestandteile von Anwendungen automatisiert auf höherstufige Umgebungen ausgebracht werden, um dort im Gesamtkontext bzw. Zusammenspiel mit anderen Komponenten und Anwendungen weiter getestet zu werden.

Sobald auch diese Akzeptanztests positiv verlaufen, kann ein Entwicklungsverbund dann das automatisierte Deployment auf eine Produktivumgebung veranlassen. Das kann teilautomatisiert, zu Beginn aber eher manuell, gesteuert werden (vgl. **Abbildung 70**).

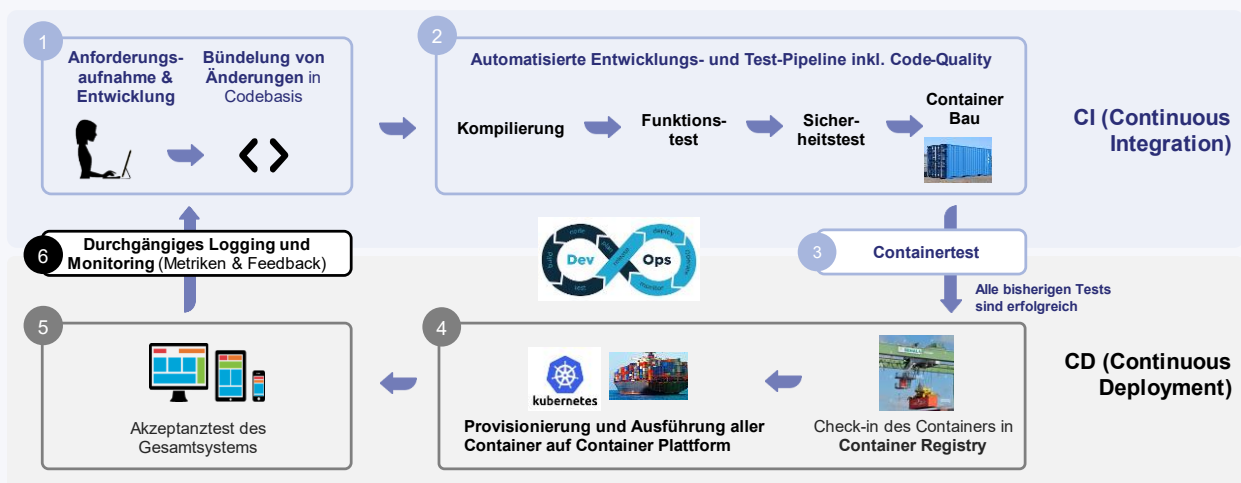
Abbildung 70 | Aufgabenschnitt bei Continuous Integration und Delivery



Da man bei Cloud-nativen Anwendungen eine häufigere und damit auch kundenzentriertere Ausbringung anstrebt, sind diese Anwendung oftmals Service-orientiert und aus diesem

Grund oft mit einer Microservice-basierten Architektur entwickelt. Dies bedeutet, dass die parallelisierte kontinuierliche Integration und kontinuierliche Ausbringung einer Vielzahl von Komponenten sehr komplex werden kann. Daher wird CI/CD durch dedizierte Werkzeuge unterstützt, die die Entwickler bei der Integration, bei den Tests und der Ausbringung unterstützen und wichtige Hinweise und Erkenntnisse entlang der Wegstrecke geben (vgl. **Abbildung 71**).

Abbildung 71 | DevSecOps Zyklus entlang einer CI/CD-Prozesskette



Diese Werkzeuge decken dabei nicht nur den eigentlichen Integrations- und Ausbringungsprozess ab, sondern bieten entlang des Prozesses verschiedene Testwerkzeuge, z. B. für Funktions-, Codequalität-, Sicherheits- und Performanztests. Des Weiteren werden entlang des Prozesses Metriken und Feedback gesammelt und in Reporting- und Monitoring-Werkzeugen für die Entwickler und den Betrieb zusammengefasst.

Durch die häufige parallelisierte Ausbringung entsteht ein Feedback-Loop (sog. DevOps Zyklus), der jedem Entwickler individuelles Feedback entlang der Wegstrecke bietet und sogar Hinweise aus dem produktiven Umfeld der Endnutzenden und des Betriebs sammelt (z. B. Stabilität, Nutzungsverhalten, Skalierbarkeit). Dieses Feedback und die Metriken nutzen die Entwickler wiederum, um Produkte oder Services weiter zu verbessern und wiederum den Integrations- und Ausbringungsprozess anzustoßen.

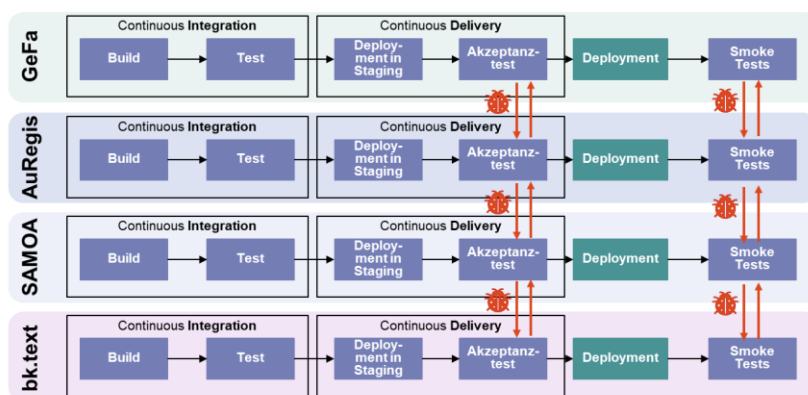
Moderne Entwicklungsverbünde, z. B. *GeFa* und *AuRegis*, nutzen bereits heute CI/CD-Verfahren. Allerdings setzt jeder Entwicklungsverbund eigene Werkzeuge und Standards dafür

ein und kann innerhalb seiner isolierten Umgebung prinzipiell den CI- und CD-Schritt nur auf der eigenen, „künstlichen“ Testumgebung durchführen.

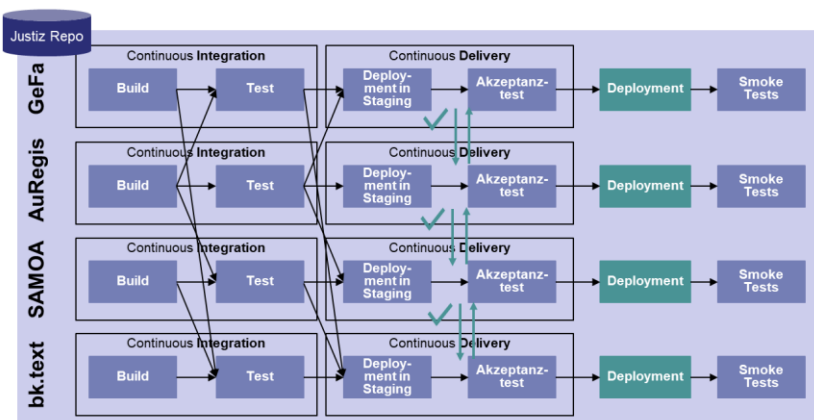
Zudem sehen Entwicklungsverbünde jeweils immer nur ihren eigenen Code und ihre eigene CD-Pipeline. Das Justizanwendungsgefüge basiert aber maßgeblich auf dem Zusammenspiel der Anwendungen bzw. Komponenten (vgl. **Kapitel 3.4.2.1**). So fallen Fehler und Inkonsistenzen per Definition immer erst sehr spät im Prozess auf, denn die Anwendungen und Komponenten finden im Status Quo erst sehr spät im Prozess zusammen, bspw. in fachlichen Akzeptanztestumgebungen der Länder oder sogar erst in Produktion (z. B. bzgl. Performanz von Schnittstellen im Wirkbetrieb). Zudem ist dieser Prozess enorm aufwändig für alle Beteiligten und Entwickler erhalten teils erst nach Monaten Feedback zu ihren Neuentwicklungen (vgl. **Abbildung 72** oben).

Abbildung 72 | CI/CD ohne (vorher) und mit Justizcloud (nachher)

CI/CD ohne Justizcloud



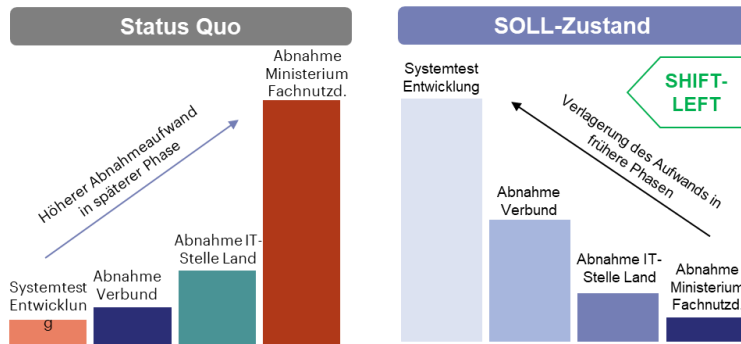
CI/CD mit Justizcloud



Demgegenüber kann der Entwicklerarbeitsplatz in der Justizcloud die Entwicklungsverbünde zu integrierter Entwicklung und Ausbringung befähigen (vgl. **Abbildung 72** unten). Mit einem gemeinsamen Justiz-Repository für Code und Artefakte, wie bspw. Container-Images, wäre damit eine zusammenhängende Integration und Ausbringung von Anwendungen mit einer gemeinsamen CI/CD-Toolchain möglich. Entwickler könnten so frühzeitig gegen Komponenten und Schnitt-

stellen anderer Anwendungen testen (sog. *Shift-Left-Ansatz*). Damit fielen Fehler viel früher auf und ließen sich viel effizienter beheben. Zudem könnte eine viel höhere Güte der Ausbringung in Abnahmetest- und Produktivumgebungen gewährleistet sowie der Aufwand für fachliche Tester und den Betrieb signifikant gesenkt werden (vgl. **Abbildung 73**).

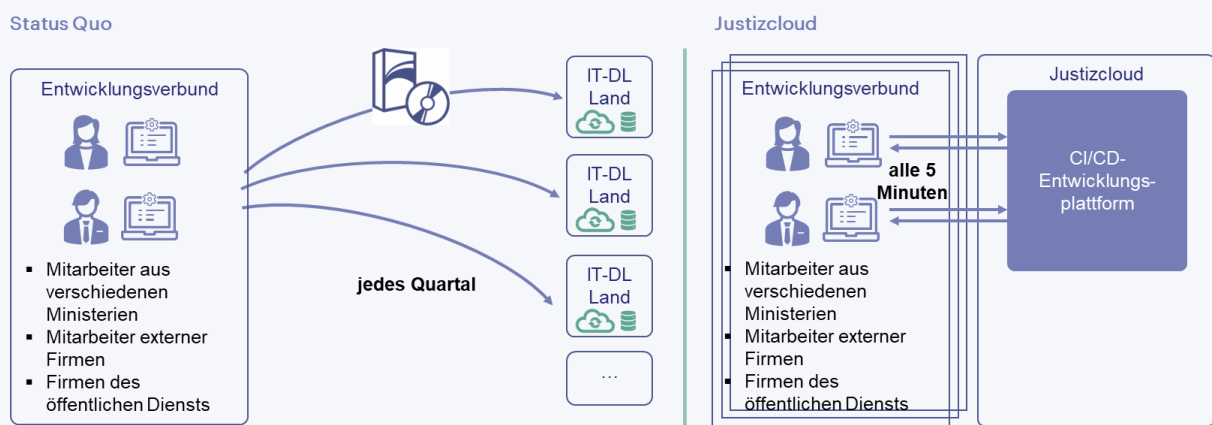
Abbildung 73 | Mehrwerte des „Shift-Left“-Ansatzes



Auch der Ausbringungsprozess an sich würde sich fundamental verändern. Derzeit verschicken Entwicklungsverbünde ihre Anwendungen an die IT-Dienstleister der Justiz. Diese installieren die Anwendung mit CD-Werkzeugen auf verschiedenen Umgebungen, testen und

betreiben diese dann individuell. Bei Problemen kontaktieren die IT-Dienstleister die Entwicklungsverbünde ebenfalls individuell. Entwicklungsverbünde erhalten dadurch teils stark zeitlich verzögertes Feedback. Jeder Entwicklungsverbund hat dafür eigene Issue-Management-Werkzeuge und -Prozesse. Eine ganzheitliche Übersicht aller Probleme (sog. Issues) gibt es nicht. Demgegenüber kann mit einem integrierten Entwicklerarbeitsplatz eine kontinuierliche Integration neu entwickelter Anwendungsbestandteile durch die Entwicklungsverbünde auf der bundeseinheitlichen Plattform erfolgen. Die Entwicklungsverbünde wären dabei frei in der Wahl ihrer IDE, denn die Justizcloud normiert nur die CI/CD-Kette nachdem die IDE einen sog. Merge-Request an das Justizcloud-Repository veranlasst hat. Perspektivisch kann die Justizcloud auch eine sog. Cloud-IDE, also einen virtuellen Entwicklerarbeitsplatz anbieten, der vor allem von KI-unterstützten Entwicklungs-Co-Piloten profitieren und damit die Produktivität und Fehlervermeidung steigern kann (vgl. **Abbildung 74**).

Abbildung 74 | Integration und Ausbringung im Status Quo vs. mit Justizcloud

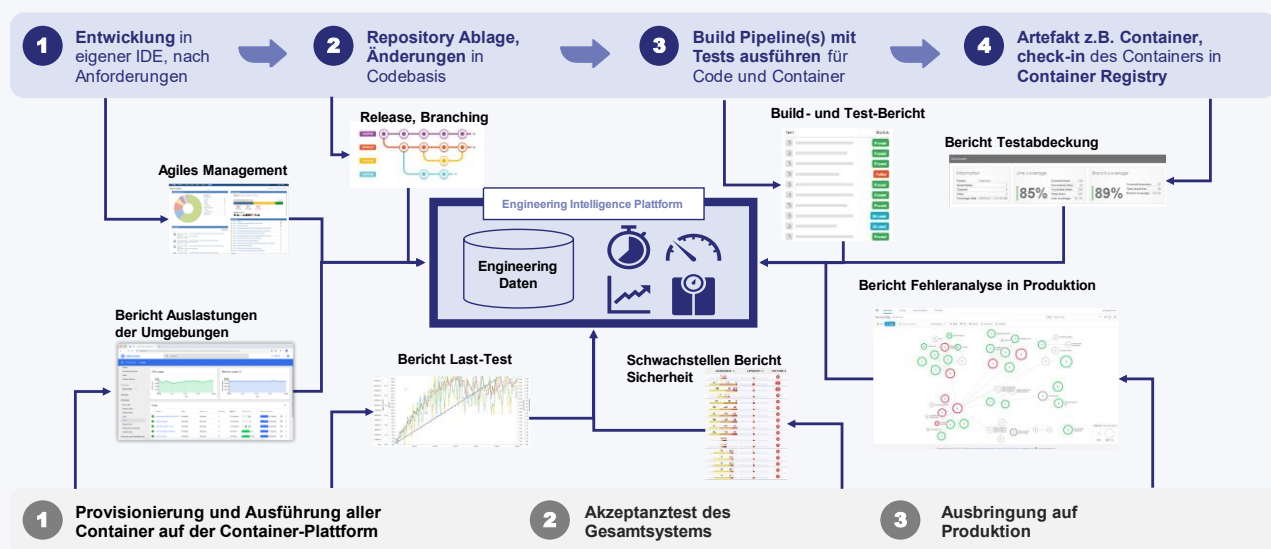


Durch die Integration von Cloud-Umgebung und Entwicklerarbeitsplatz erhielten Entwickler zudem künftig auch Metriken direkt aus Akzeptanztest- und Produktivumgebungen. Sie

könnten dann zeitnah darauf reagieren, was einen wesentlichen Beitrag zu mehr Stabilität, Performanz und Kundenzentriertheit bedeuten sowie zur Zufriedenheit von Entwicklern und Betrieb beitragen würde.

Der integrierte Entwicklerarbeitsplatz für die Entwicklungsverbünde der Justizcloud-Anwendungslandschaft bietet darüber hinaus noch viele weitere Vorteile. Besonders erwähnenswert ist, dass er die Grundlage für eine sog. Engineering Intelligence Plattform schafft (vgl. **Abbildung 75**).

Abbildung 75 | Integrierte Engineering Intelligence Plattform



Eine solche Plattform sammelt kontinuierlich Metriken zu allen relevanten Anwendungen und Komponenten sowohl aus der Entwicklung als auch aus dem Betrieb, d. h., aus den CI/CD-Pipelines und den Betriebsumgebungen. Sie führt diese an einer Stelle zusammen und erlaubt es Entwicklungsverbünden und Betrieb, wichtige Zeitreihen- und Abhängigkeitsanalysen über die gesamte Anwendungslandschaft der Justizcloud durchzuführen. So könnten bspw. unerwartetes Anwendungsverhalten und Abhängigkeiten zwischen Anwendungen besser identifiziert werden. So würde nicht mehr übersehen, wenn etwa eine Anwendung eine Schnittstellenänderung einführt, diese Änderung aber Effekte in anderen Anwendungen hat (z. B. diese verlangsamt). Dieser Umstand sowie ähnliche Zusammenhänge sind im Status Quo vollkommen intransparent, können aber von Beginn an bei der Justizcloud-Anwendungslandschaft adressiert und entsprechend unterfüttert werden. Dies wird umso wichtiger, je größer die Justizcloud-Anwendungslandschaft wird.

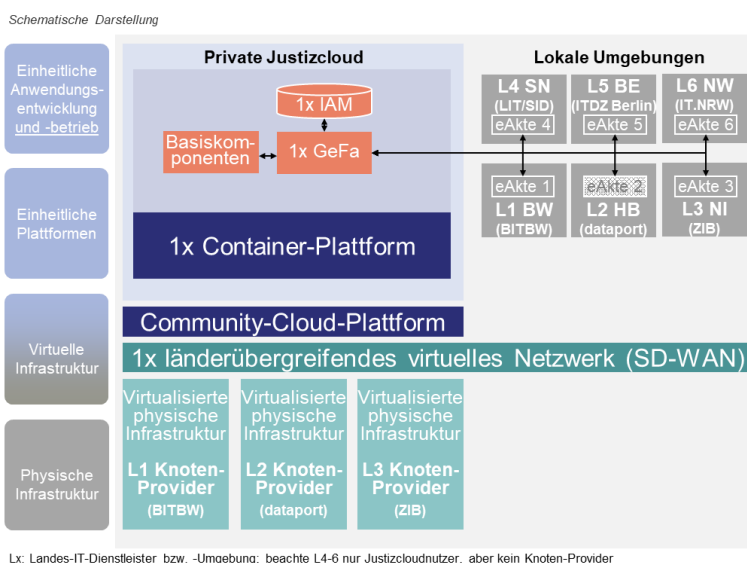
3.5.7 Justizcloud-PoC im Schichtenmodell

Ein Länder- und Dienstleister-übergreifender PoC soll die Justizcloud-Mehrwerte und das notwendige Kooperationsmodell greifbar machen. Mit dem PoC will die Untersuchung der Machbarkeit erste greifbare Mehrwerte und frühzeitigen Erkenntnisgewinn erreichen und gemeinsam mit den IT-Dienstleistern Momentum aufbauen. Mit der Durchführung des PoC wird gezeigt, dass die praktische Zusammenarbeit über die IT-Dienstleister der Länder im Zielbild der Justizcloud funktioniert und, dass das fachliche und technische Zielbild grundsätzlich umsetzbar sind. Ebenfalls wesentliches Ziel des PoC war es, bereits so viele praktische Lernerfahrungen wie möglich für eine spätere Umsetzung zu sammeln, sowohl technischer Natur als auch aus Prozess- und organisatorischer Sicht.

Konkret wird im PoC das Fachverfahren *GeFa* sowie ein gemeinsames Identitätensystem durch ein zentrales Team bundeseinheitlich ausgebracht. Über *GeFa* werden dann die unterschiedlichen eAkten-Systeme und Datenbanken in den sechs Ländern angebunden. Im PoC werden dabei nur eAkten-Testsysteme und Testdatenbanken ohne echte Nutzdaten verwendet. Damit wird gezeigt, dass ein gemeinsamer Cloudbetrieb möglich ist, die erstellten Daten und Akten aber in den Ländern verbleiben können.

Für den PoC haben sich sechs IT-Dienstleister der Länder engagiert (vgl. **Abbildung 76**). Das LID aus Rheinland-Pfalz unterstützt zusätzlich als Sparrings-Partner.

Abbildung 76 | Justizcloud-PoC im Schichtenmodell



Lx: Landes-IT-Dienstleister bzw. -Umgebung; beachte L4-6 nur Justizcloudnutzer, aber kein Knoten-Provider

Der PoC umfasst eine gemeinsame Cloud-Infrastruktur mit mehreren Knoten. Drei IT-Dienstleister, *BITBW*, *Dataport* und *ZIB*, haben diese gemeinsame, gespannte Cloud-Infrastruktur als Cloud-Knotenanbieter umgesetzt. Durch Netzwerktechnologie der *BITBW* wird dazu exemplarisch ein virtuelles Netz (SD-WAN) zwischen allen sechs PoC-Teilnehmenden etabliert. Über dieses Netz kom-

muniziert die gemeinsame, gespannte Cloud-Infrastruktur. Ebenso kommunizieren über dieses Netz die Nutzenden aller sechs Länder: die drei Infrastruktur-anbietenden Länder sowie

die Infrastruktur-nutzenden Länder bei den IT-Dienstleistern *LIT*, *ITDZ Berlin* und *IT.NRW*, die selbst keine eigene Infrastruktur zur Verfügung stellen, sondern nur lokale eAkten-Systeme und Datenbanken im Land. Damit wird gezeigt, dass nicht jedes Land im Zielbild Cloud-Know-how aufbauen muss. Das Know-how kann für die Justiz gebündelt werden.

Mit dem PoC werden auch erstmals exemplarisch die Kernherausforderung einer Umsetzung praktisch simuliert. Der Aufbau eines länderübergreifenden virtuellen Netzwerks sowie die Bereitstellung einer gespannten Container-Plattform (für *GeFa*). In der Zusammenarbeit mit den teilnehmenden IT-Dienstleistern wurde eine Netzwerkarchitektur erarbeitet, welche eine gemeinsame, virtuelle Netzwerkzone mit verbundenen PoC-Segmenten bei jedem IT-Dienstleister schafft. Gleichzeitig sind bei jedem IT-Dienstleister Komponenten der IT-Sicherheit wie z. B. Firewalls, Proxy-Server im Einsatz, um das gemeinsame Netz von den Bestandsnetzen zu trennen. Die Kommunikation zwischen IT-Bestandsnetzen den Netzsegmenten des PoC muss individuell ausgestaltet werden und freigegeben sein.

Ende November 2024 wurde der PoC erfolgreich abgeschlossen und die Ergebnisse auf dem *Bund-Länder-Digitalgipfel* vorgestellt. Dabei wurden viele Erkenntnisse und Impulse für die Umsetzung der Justizcloud mit den Teilnehmenden gesammelt. Dazu gehören insb.:

Strategisch: Das Justizcloud-Konzept ist machbar und greift die Idee der *govdigital eG* des gespannten Container-Clusters sowie diverse *DVC*-Konzepte auf und entwickelt sie weiter.

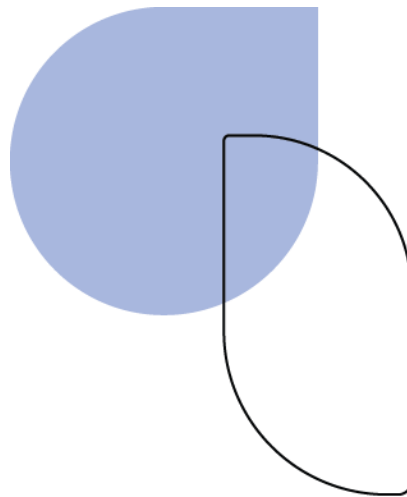
Fachlich: Die Anbindung der eAkten der Bestandswelt ist auch im PoC herausfordernd und die in der Ist-Analyse (vgl. **Kapitel 2.2**) beschriebene hohe Komplexität der heterogenen Anwendungslandschaften mit Artefakten verschiedener Entwicklungsverbünde tritt auch im PoC bereits in der praktischen Arbeit auf. Scope des PoC war die Anbindung von drei eAkten Systemen (*eAS*, *e2A*, *eIP*) in sechs unterschiedlichen Konfigurationen. Darüber war die oft unklare Verantwortung für die richtige Konfiguration zur Verbindung zweier Anwendungen herausfordernd.

Technisch: Entwicklungsverbünde müssen in Zukunft in Plattform- und CI/CD-Kompetenz befähigt werden. Die Verantwortung für die Konfiguration zur Ausbringung von Anwendungen muss klar verortet sein. Es muss ein gemeinsames IT-Sicherheitsrahmenwerk erstellt werden, das Verantwortung und Zuständigkeiten gemeinsam verbindlich festlegt.

Rechtlich-organisatorisch: Im PoC konnte eine erste Teillandkarte der IT-Sicherheitsorgane von sechs Ländern erstellt werden. Die Zielorganisation der Justizcloud muss gemeinsam mit den IT-Sicherheitsorganen aller Länder eine funktionierende, dauerhafte

Arbeitsstruktur und Aufgabenteilung aufbauen. Dabei muss jeweils die IT-Sicherheitsstelle der IT-Dienstleister, des Landes und der Justiz mit einbezogen werden.

Die fachliche, technische und organisatorische Zusammenarbeit und vor allem Arbeitsteilung bei der Lösung der Herausforderungen hat zwischen den IT-Dienstleistern gut funktioniert. Die beteiligten Dienstleister haben mit wichtigen Ideen und Vorschlägen zum Erfolg des PoC und zur Lösungsfindung beigetragen. Diese Vorschläge wurden in einem gemeinsamen „Lessons Learned“-Workshop gesammelt und für die Justizcloud-Umsetzung zusammengefasst.



3.6 Rechtlich-organisatorische Zielbildebene

Die rechtlich-organisatorische Ebene beschreibt aufbauend auf den strategischen, fachlichen und technischen Zielbildelementen, welche u. a. die Stärkung der föderalen Zusammenarbeit, den gemeinsamen Anwendungsbetrieb sowie den Aufbau eines gemeinsamen Netzwerks umfassen, wie diese organisatorisch realisiert werden können und welche rechtlichen Rahmenbedingungen hierbei zu beachten sind. Dabei wird z. B. definiert, welche Prozesse und Fähigkeiten für den Betrieb der Justizcloud-Services notwendig wären, wie eine effektive Beschaffung sichergestellt werden könnte und wie die Justizcloud in den organisatorischen und rechtlichen Rahmen der föderalen Justiz eingebettet werden könnte.

Dazu legt die rechtlich-organisatorische Ebene zunächst die den Zielen der Justizcloud entsprechende Wertschöpfungstiefe entlang des Cloud-Schichtenmodells (IaaS, PaaS, SaaS) (vgl. **Kapitel 3.6.1**) fest. Daraus wurden Anforderungen, Aufgaben sowie notwendige Rahmenbedingungen für eine Justizcloud abgeleitet. Dabei wurde im Rahmen der Fachpanelarbeit die Notwendigkeit der Gründung einer eigenen Justizcloud-Einheit festgestellt (vgl. **Kapitel 3.6.2**). Darauf aufbauend wird zunächst die Einbettung der Justizcloud-Einheit in die übergreifenden Strukturen der Justiz ausgestaltet, wie z. B. durch ein justizweites Anforderungsmanagement. Zudem werden die Schnittstellen mit anderen Parteien wie Entwicklungsverbünden, IT-Dienstleistern sowie bspw. der *BLK* bzw. ihrer AGs vorgedacht (vgl. **Kapitel 3.6.3**). Auf Basis der Anforderungen und Aufgaben der Justizcloud werden anschließend Rahmenbedingungen für den Aufbau einer Justizcloud-Einheit selbst definiert (vgl. **Kapitel 3.6.4**). Dabei werden zum einen relevante Funktionen und Rollen definiert und zum anderen der Personalbedarf und eine Strategie zum Personalaufbau entwickelt (vgl. **Kapitel 3.6.5**). Darüber hinaus wird beschrieben, welche Rechtsformen für die Justizcloud-Einheit geeignet sein könnten (vgl. **Kapitel 3.6.6**).

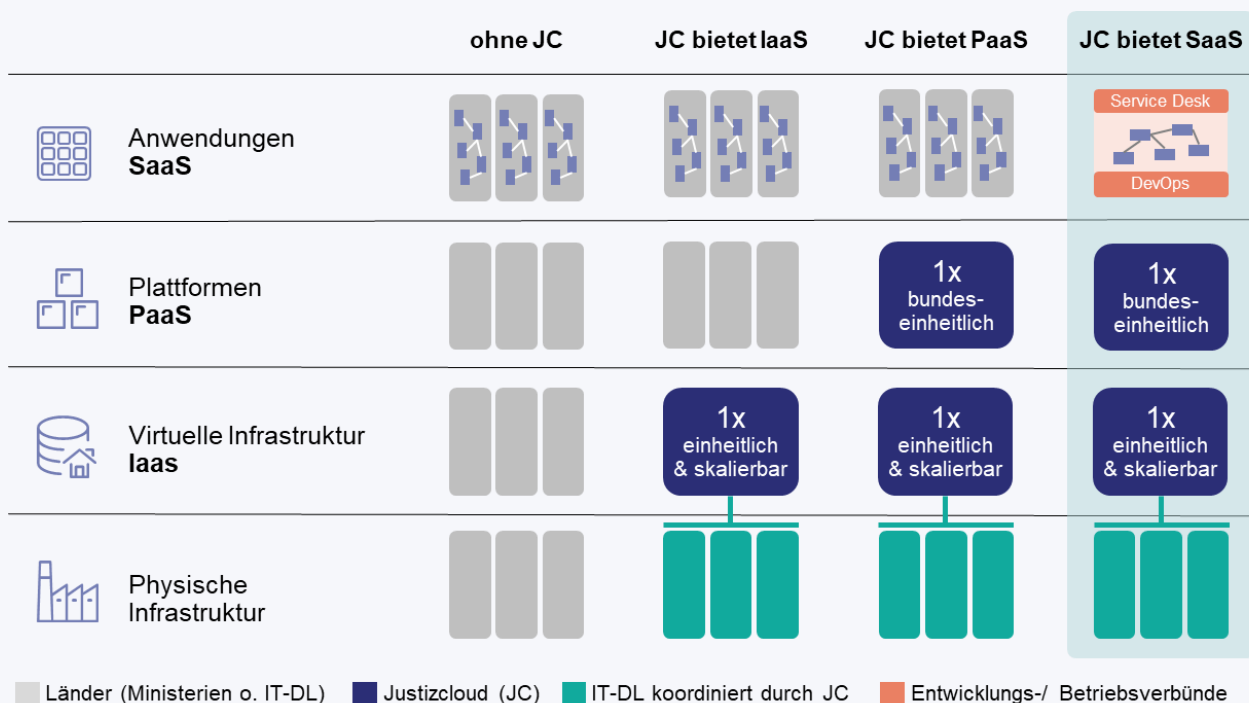
Die Ausgestaltung der einzelnen Elemente erfolgte im Rahmen des rechtlich-organisatorischen Fachpanels. Dabei wurden für alle Elemente des Zielbilds verschiedene Lösungsoptionen vorgestellt, diskutiert und jeweils die Option ausgewählt, die dem fachlichen und technischen Zielbild sowie den strategischen Zielen am meisten entsprach und als rechtlich-organisatorisch machbar angesehen wurde.

3.6.1 Wertschöpfungstiefe der Justizcloud

Um die organisatorischen und rechtlichen Aspekte der Justizcloud auszugestalten, musste zunächst festgelegt werden, welche Services die Justizcloud eigentlich bereitstellen soll.

Dazu wurden im organisatorischen Panel systematisch die Vor- und Nachteile verschiedener Servicemodelle diskutiert. Im Rahmen des iterativen Vorgehens flossen dabei auch Erkenntnisse aus den anderen Zielbildebeneen ein: aus der strategischen Ebene bspw. die Zielsetzung, Anwendungen gemeinsam zu betreiben und bestmöglich Effizienzpotenziale zu realisieren, aus dem fachlichen Panel z. B. die Anforderung des Multi-Mandantenbetriebs oder aus dem technischen Panel die Machbarkeit bspw. eines gemeinsamen virtuellen Justiznetzwerks. Auf Basis dieser Erkenntnisse wurden das strategisch, fachlich und technisch machbarste Wertschöpfungsmodell auch organisatorisch auf Machbarkeit überprüft und notwendige Implikationen für die organisatorische Ausgestaltung der Justizcloud abgeleitet. Grundsätzlich kann die Wertschöpfungstiefe einer Cloud sehr unterschiedlich ausgeprägt sein und entlang der vier Ebenen des Cloud-Schichtenmodells beschrieben werden.

Abbildung 77 | Wertschöpfungstiefe der Justizcloud



Auf der untersten Ebene bildet die physische Infrastruktur (bspw. Rechenzentren, Server-Hardware, Speichersysteme und Netzwerkinfrastruktur) das Fundament jeder Cloud, die anschließend virtualisiert für den Plattform- und Anwendungsbetrieb bereitgestellt wird. Die Justizcloud soll, wie bereits im technischen Zielbild dargestellt, aus mehreren Überlegungen (u. a. Wirtschaftlichkeit, Datenhoheit der Länder, Nachnutzung von bestehenden Strukturen)

nicht über eigene Infrastruktur verfügen (vgl. **Kapitel 3.5**). Stattdessen baut die Justizcloud auf der vorhandenen Infrastruktur der IT-Dienstleister auf. Damit wird die Justizcloud die unterste Ebene der Wertschöpfungsebenen einer Cloud nicht selbst stellen, sondern im Gegenteil selbst physische Infrastruktur von IT-Dienstleistern beziehen.

Auf der Ebene der Virtualisierung bietet IaaS Zugang zu virtualisierter Infrastruktur, d. h. virtuelle Maschinen (VMs), virtuelle Speicher und virtuelle Netzwerke. Hier können durch effiziente Skalierung, das Setzen von Standards sowie eine Vereinheitlichung des Betriebs (d. h. Konfiguration, Wartung, Monitoring etc.) Synergieeffekte entstehen. Statt wie bisher auf eigenen virtuellen Umgebungen pro Land könnte die Justiz in Zukunft auf einer einheitlichen virtuellen Umgebung arbeiten. Über ein gemeinsames Netzwerk wären so bspw. auch neue Anwendungsfälle möglich, wie die Schaffung eines gemeinsamen Datenraums. Um diese Mehrwerte zu heben, soll die Justizcloud standardisierte, virtuelle Infrastruktur durch die IT-Dienstleister beziehen und diese über ein gemeinsames Netzwerk als einheitliche, virtuelle Umgebung bereitstellen.

Die Wertschöpfungstiefe der Justizcloud umfasst daher zumindest einheitliche, virtuelle IaaS. Allerdings wäre der Aufbau von Plattformdiensten wie Container-, Daten-, Integrations- und KI-Plattformen (PaaS) sowie der Betrieb von Anwendungen weiter im Aufgabenbereich der einzelnen Länder. Viele Mehrwerte wie ein gemeinsamer Aufbau und Betrieb von Cloud-Plattformen und Synergien im Anwendungsbetrieb wären nicht realisiert.

Aus diesem Grund wurde festgelegt, dass die Justizcloud Plattformdienste (PaaS) bereitstellen soll, insb. eine Container-Plattform, die für die Entwicklung, Tests, Ausbringung und den Betrieb von Anwendungen genutzt werden kann. Für die Entwicklungsverbünde der Justiz könnte die Justizcloud eine einheitliche, hoch standardisierte Umgebung bereitstellen. Auf dieser könnten die Länder in Zukunft Anwendungen zunächst gemeinsam entwickeln und dann jeweils auf länderspezifischen Umgebungen (sog. Tenants) betreiben. Dies würde erhebliche Synergieeffekt bei Aufbau sowie im Betrieb der Plattform heben. Gleichzeitig wären so durch die Standardisierung der Infrastruktur moderne CI/CD-Pipelines und damit echte Cloud-Mehrwerte sowie moderne Entwicklung und Betrieb möglich. Allerdings würden nach wie vor länderspezifische Betriebsteams eine Anwendungslandschaft pro Land betreiben, mögliche Mehrwerte im technischen und fachlichen Anwendungsbetrieb sowie hohe Effizienzgewinne durch ein einheitliches, modernes, mandantenfähiges Anwendungsgefüge (vgl. **Kapitel 3.4**) wären nicht realisiert.

Um auch diese Effizienzpotenziale voll auszuschöpfen, ist vorgesehen, auf der Justizcloud auch SaaS zu ermöglichen. Dabei würde nicht mehr ein länderspezifisches Anwendungsgefüge pro Land betrieben werden. Stattdessen würde ein einheitliches Bündel an Anwendungen für alle Länder aus einer Cloud-Umgebung bereitgestellt werden. Somit würden nicht nur der Aufbau und Betrieb der Cloud-Plattform vereinheitlicht und damit einmal statt n-Mal erfolgen, sondern es könnte auch der laufende Betrieb des Cloud-fähigen Justizanwendungsgefüges durch einen einheitlichen technischen und fachlichen Betrieb erfolgen.

Dieses Modell vereinheitlicht aber nicht nur den Softwarebetrieb der Justiz entlang der Infrastruktur-, Plattform- und Anwendungsebene. Über die einheitliche Entwicklung und den einheitlichen Betrieb eines Anwendungsgefüges innerhalb einer Umgebung könnten weitere wesentliche Cloud-Mehrwerte gehoben werden. Zum einen wäre die Möglichkeit von DevOps gegeben, bei dem ein gemeinsames Entwicklungs- und Betriebsteam Anwendungen kontinuierlich entwickelt, ausbringt und betreibt (vgl. **Kapitel 3.5.6**).

Organisatorisch wurde dabei im Rahmen der Untersuchung eine Weiterentwicklung von Entwicklungs- zu Betriebsverbünden diskutiert. Statt wie bisher Software in Entwicklungsverbünden zu entwickeln und dann in separaten Betriebsteams pro Land zu betreiben, könnten integrierte Entwicklungs- und Betriebsverbünde in Zukunft das Anwendungsgefüge der Justiz nach dem DevOps-Ansatz als SaaS einheitlich bereitstellen. Dieser Ansatz hätte viele Vorteile wie bspw. eine schnellere Ausbringung, direkteres Feedback von Nutzenden für die Entwicklungsteams sowie Effizienzgewinne, da das Know-how über die Anwendungen in Entwicklung, Ausbringung und Betrieb in bundeseinheitlichen Teams gebündelt wäre. Auch die fachliche Administration der Anwendungen könnte über die Betriebsverbünde auf einer Service Desk-Infrastruktur (z. B. Serviceportal) der Justizcloud erfolgen. Insgesamt könnte so vermieden werden, neue Betriebsteams in der Justizcloud aufzubauen. Stattdessen würde der Betrieb durch Ländervertreter in den Verbünden auf einer einheitlichen Plattform und mit einheitlichen Prozessen erfolgen (vgl. **Kapitel 3.5.5**, Administrationskonzept).

Zusammenfassend würde die Wertschöpfungstiefe der Justizcloud auf der Ebene der virtualisierten Infrastruktur (IaaS) mit der Vernetzung und Standardisierung virtueller Maschinen der Justiz-IT-Dienstleister beginnen. Darauf werden einheitliche PaaS aufgebaut und für die Entwicklungs- und Betriebsverbünde bereitgestellt. Diese entwickeln und betreiben auf dieser Plattform das Cloud-fähige Justizanwendungsgefüge als SaaS inkl. DevOps und Service Desk für die Justiz.

3.6.2 Aufgaben, Anforderungen und Rahmenbedingungen

Aus der beschriebenen Wertschöpfungstiefe, nach der IaaS- und PaaS-Dienste für die Entwicklungs- und Betriebsverbünde bereitgestellt werden sollen, ergibt sich ein umfassendes Aufgabenprofil sowie Anforderungen an eine Justizcloud. Zudem müssen einige Rahmenbedingungen erfüllt sein, damit die Justizcloud in der Justiz ihre definierten Aufgaben erfüllen sowie die definierten Services erbringen kann.

Serviceerbringung nach Außen: Die zentrale Aufgabe der Justizcloud soll es sein, Infrastruktur und Plattformdienste bereitzustellen. Dazu müssen diese zunächst aufgebaut bzw. beschafft werden und skalierbar, standardisiert und v. a. auf die Bedarfe der Entwicklungs- und Betriebsverbünde angepasst, ausgebracht werden. Die benötigten IaaS- und PaaS-Produkte ergeben sich dabei aus dem fachlichen- und technischen Zielbild (siehe Serviceportfolio). In Zukunft sollen diese Dienste fortlaufend produktiv durch Entwicklungsverbünde bereitgestellt werden. Dabei ist der Aufbau einer ganzheitlichen Infrastruktur zur kontinuierlichen Entwicklung, Test und produktiven Ausbringung von Plattformdiensten erforderlich. Dienste wie eine Container-Plattform müssen bspw. durch Produktupdates oder neue Anforderungen (z. B. fachliche oder technische Sicherheitsanforderungen) weiterentwickelt werden. Dazu ist auch ein umfassendes Netz- und Integrationskonzept für die Plattformen umzusetzen.

Um diese Dienste technisch zu entwickeln, sind eine Reihe fachlicher Aufgaben erforderlich. Bspw. müssen Kundenbedarfe systematisch über ein Anforderungsmanagement erhoben werden und dazu ein enger Austausch mit den Entwicklungs- und Betriebsverbünden erfolgen. Zudem muss ein Servicekatalog gepflegt und etwa Serviceerbringung, Bestellprozesse sowie laufender Support der Nutzenden prozessual ausgestaltet werden. Teil dessen ist auch das Onboarding neuer Entwicklungs- und Betriebsverbünde, der Aufbau der Kundenbeziehung, die Freischaltung zu Entwicklerarbeitsplätzen, die Festlegung erforderlicher Dienste sowie die Bereitstellung und Erläuterung der Dienste für neue Nutzer uvm. In diesem Zusammenhang ist auch eine enge Abstimmung mit bzw. Rücksichtnahme auf die Release-Pläne der Entwicklungsverbünde relevant, um Bereitstellung von Diensten, Freischaltungen, Sicherheitsfreigaben etc. gemäß den Zeitplänen der Verbünde zu ermöglichen.

Aufgaben nach Innen: Um diese komplexen Services nach außen zu erbringen, muss eine Justizcloud viele querschnittliche Aufgaben nach innen erfüllen. Dazu gehört u. a. die Beschaffung. Nicht alle Dienste müssen durch die Justizcloud selbst entwickelt werden. Es besteht auch die Möglichkeit, Cloud-Dienste von externen Anbietern zu beschaffen, z. B.

über die *DVC*, oder bestehende Services der IT-Dienstleister nachzunutzen und in der Justizcloud zentral und einheitlich zu erbringen. Auch die Beschaffung virtueller Infrastruktur der IT-Dienstleister muss fortlaufend erfolgen und über Service-Level-Agreements (SLAs) eine Leistungserbringung für einen unterbrechungsfreien Betrieb rechtlich sichergestellt sein. Auch die Beschaffung des eigenen Personals für den Betrieb der Justizcloud-Services ist für die Justizcloud wichtig (siehe **Kapitel 3.6.5**).

Aus den vielfältigen Aufgaben, insb. Beschaffung und Personalbedarf, ergibt sich für die Justizcloud auch die Notwendigkeit, rechtsfähig zu sein, eigene Verträge abschließen zu können und bspw. SLAs nachzuhalten. Um diese Aufgaben wahrzunehmen, ist zu empfehlen, dass die Justizcloud mit einem eigenen Haushalt ausgestattet wird.

Aufgaben im Rahmen der übergreifenden Justizorganisation: Die Justizcloud fügt sich in einen bestehenden organisatorischen Rahmen der Justiz ein. In diesem Kontext fallen strategische und operative Aufgaben an. Besonders wichtig ist dabei eine Berücksichtigung der übergreifenden strategischen Ziele der Justiz. Entscheidungen wie bspw. der Fokus auf eine zentrale Bereitstellung bestimmter Verfahren oder Investitionen in neue Technologien wie KI können nicht durch die Justizcloud gefällt werden. Dennoch könnte die Justizcloud zur Umsetzung dieser Ziele in Zukunft eine wichtige Rolle spielen und z. B. das technische Fundament bereitstellen. Auch muss die Justizcloud in ein übergreifendes Infrastruktur-, Plattform- und anwendungsübergreifendes Architekturkonzept inkl. Architekturstandards und Roadmap einbezogen werden bzw. sich daran orientieren. Nicht zuletzt ist auch die Frage der richterlichen Kontrolle, wie sie in der Hessischen Netzklage angelegt ist, für die Justizcloud zu beantworten.

Insgesamt ergeben sich aus den vielfältigen Aufgaben, Anforderungen und Rahmenbedingungen wichtige rechtlich-organisatorische Implikationen an die Justizcloud und ihre Einbettung in die übergreifenden Organisationsstrukturen der Justiz. Diese sind in ein Organisationsmodell der Justizcloud eingeflossen, das im Folgekapitel dargestellt wird.

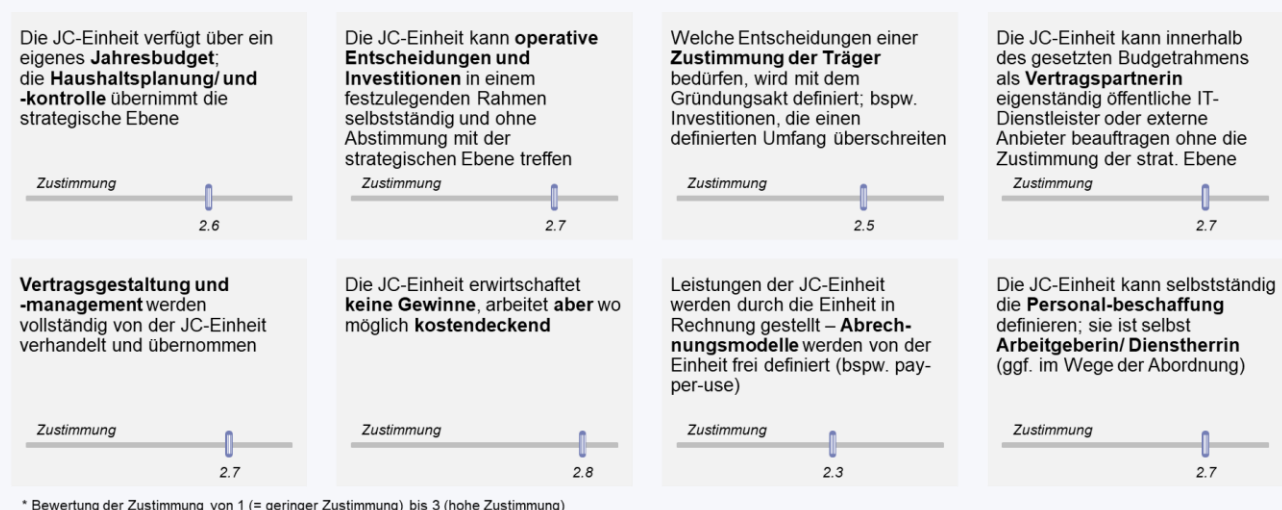
3.6.3 Organisationsmodell der Justizcloud

Das Organisationsmodell definiert die Organisationsstrukturen der Justizcloud selbst sowie in welche organisatorischen Strukturen die Justizcloud eingebettet sein sollte, damit alle oben genannten Aufgaben effizient wahrgenommen werden können. Es bildet damit alle Gremien und Einheiten ab, die bspw. für Steuerung und Kontrolle, den unmittelbaren Betrieb sowie Verwaltung, die Beschaffung notwendiger Infrastruktur bzw. Produkte sowie für die

reibungslose Leistungserbringung gegenüber Entwicklungs- und Betriebsverbünden notwendig sind, und setzt sie in Beziehung zueinander.

Dabei ist die Untersuchung zu dem Ergebnis gelangt, dass eine eigenständige Justizcloud-Einheit gegründet werden sollte. Um zu diesem Ergebnis zu kommen, wurde zunächst entlang der Aufgabenbereiche der Justizcloud sondiert, ob eine Justizcloud diese Aufgaben nur ausführend, d. h. ohne eigene Flexibilität und Entscheidungsspielraum, wahrnehmen kann oder inwiefern ein gewisser Grad der Eigenständigkeit erforderlich ist. Die Einschätzung wurde sowohl in den Fachpanels als auch gemeinsam mit dem Sounding Board erhoben und gespiegelt (vgl. **Abbildung 78**).

Abbildung 78 | Einschätzung erforderlicher Eigenständigkeit der Justizcloud



In den jeweiligen Aufgabenbeschreibungen wurde dabei zwischen operativen sowie strategischen Entscheidungen unterschieden. Strategische Entscheidungen und Aufgaben, wie die Festlegung eines Jahresbudgets sowie der Haushaltsplanung, müssen durch strategische Einheiten und Gremien innerhalb der E-Justice-Strukturen getroffen werden. Für operative Entscheidungen hingegen, wie Vertragsgestaltung und -management, Definition von Abrechnungsmodellen, Personalbeschaffung etc. wurde eine stärkere Eigenständigkeit der Justizcloud befürwortet.

Grundsätzlich standen verschiedene Organisationsformen für die Justizcloud zur Auswahl: (1) eine virtuelle Mischorganisation aus verschiedenen Ländern/ „Häusern“ wie z. B. die Entwicklungsverbünde, (2) eine Aufhängung in einer bestehenden Organisation (z. B. einem

IT-Dienstleister oder Ministerium), (3) eine Auslagerung der Einheit an Dritte oder (4) die Gründung einer eigenständigen Einheit.

Da die vorliegende Untersuchung keine Rechtsberatung durchführt, ist eine umfassende rechtliche Bewertung der Optionen nicht vorgenommen worden. Allerdings wurden die Optionen (1) bis (3) aus nachfolgenden, praktischen Überlegungen verworfen.

Option (1) wurde verworfen, weil virtuelle Organisationen, z. B. die Entwicklungsverbünde, in der Regel nur auf Zeit für die Entwicklung und ggf. Pflege von Anwendungen bestehen. Sie verfügen dabei nicht über ein eigenes Budget und können bestimmte Beschaffungsprozesse nicht eigenständig tätigen. Zudem können sie kein eigenes Personal einstellen, da die Mitarbeitenden der virtuellen Organisation typischerweise nur aus anderen Organisationen abgeordnet sind bzw. ihre Arbeitskraftanteile bereitgestellt werden. Diese Aspekte widersprechen den Zielen der Justizcloud, langfristig Know-how zu bündeln und eigenständige Vertragsbeziehungen mit Partnern wie z. B. IT-Dienstleistern einzugehen.

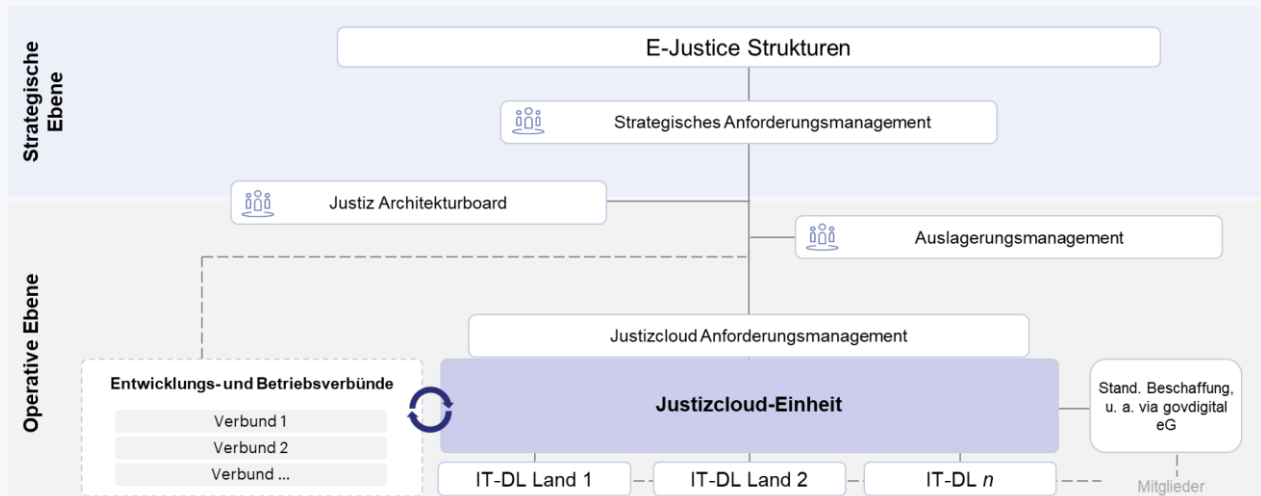
Option (2) wurde verworfen, weil eine Auf- bzw. Unterhängung (z. B. als Bereich bzw. Abteilung) bei einer bestehenden Organisation ebenfalls die Eigenständigkeit der Justizcloud und aller teilnehmenden Länder beschränkt. So könnten bspw. bestimmte Entscheidungen durch konkurrierende Ziele der jeweiligen Organisation beeinflusst sein. Auch kann das Personal nicht verlässlich langfristig aufgebaut und gehalten werden, da der Personalbedarf mit den Anforderungen der aufnehmenden Organisation als Ganzem ermittelt würde und ggf. konkurrieren könnte. Viel wichtiger ist aber, dass derzeit keine bestehende Organisation in Frage kommt, hoheitliche Aufgaben für die Länder und den Bund gleichberechtigt zu übernehmen. Die IT-Dienstleister gehören bspw. entweder Ländern oder dem Bund.

Zuletzt wurde Option (3), eine Auslagerung an Dritte, aus zwei zentralen Gründen verworfen. Erstens widerspräche sie zentralen Zielen der Justizcloud, wie bspw. dem langfristigen Aufbau von Cloud-Know-how innerhalb der Justiz und nicht bei Dritten, um so die Souveränität dieser zu stärken. Zweitens wäre unklar, ob eine Auslagerung bspw. im Kontext bestehender Kontrahierungszwänge rechtlich möglich wäre. Dritte sind insb. kommerzielle Anbieter von Betriebs-Dienstleistungen im Cloud-Bereich wie z. B. IT-Systemhäuser.

Basierend auf diesen Überlegungen wurde Option 4, die Gründung einer eigenen Justizcloud-Einheit, als Empfehlung für das Organisationsmodell der Justizcloud festgelegt und im Rahmen eines übergreifenden Organisationsmodells ausgestaltet. Das Organisationsmodell Justizcloud-Einheit ist in eine strategische und eine operative Ebene unterteilt und

nachfolgend mit allen notwendigen Gremien, Einheiten und Beziehungen dargestellt (vgl. **Abbildung 79**).

Abbildung 79 | Justizcloud-Organisationsmodell



3.6.3.1 Strategische Organisationsebene

Auf der strategischen Ebene bilden die bestehenden **E-Justice-Strukturen** (vgl. **Kapitel 2.2.2**) mit dem *E-Justice-Rat* und der *BLK* den strategischen Entscheidungsrahmen, über den u. a. die Bund-Länder-übergreifende Zusammenarbeit koordiniert wird. Sie legen u. a. Vorgaben und Standards zu übergreifenden Fragen der Justiz-IT fest, wie bspw. für die Entwicklung von service-orientierten Architekturen, Containern und offenen Schnittstellen mit dem Ziel, „die immer noch divergente IT-Landschaft der Justiz zunehmend in bundesweiten Projekten zu vereinheitlichen, um unnötige Redundanzen und Mehrfachentwicklungen zu vermeiden“ ([Webseite des E-Justice-Rat](#)). Auch wichtige strategische Ziele wie die Sicherstellung digitaler Souveränität und Innovationszielen, z. B. dem Einsatz von KI, werden über den *E-Justice-Rat* vorangetrieben. Auch die bundeseinheitlichen Entwicklungsprojekte *GeFa* und *AuRegis* sind über den *E-Justice-Rat* initiiert worden.

Zukünftig dürfte auch die Justizcloud und ihr strategischer Auftrag in den Entscheidungs- bzw. Kompetenzbereich des *E-Justice-Rat* und der *BLK* fallen. Dabei würden die E-Justice-Strukturen maßgeblich die strategische Ausrichtung vorgeben. Zudem würden Sie als höchste Entscheidungs- und Eskalationsinstanz für strategische Fragen fungieren. Operative Aufgaben und Entscheidungskompetenzen sollen jedoch bei der Justizcloud-Einheit

bzw. den anderen Organen des Organisationsmodells, wie bspw. dem strategischen Anforderungsmanagement, dem Architekturboard und den Entwicklungsverbünden, liegen.

Eine Eingliederung der Justizcloud in die Organisationsstrukturen der Justiz-IT würde den Handlungsrahmen deutlich verändern und erweitern. Während auch bislang sowohl strategische als auch fachliche Entscheidungen sowie Entwicklungsprojekte bereits über den *E-Justice-Rat* initiiert wurden, sind viele operative Fragen des Betriebs dezentral in den Ländern umgesetzt worden. So wurde etwa die Entscheidung zur Entwicklung von *GeFa* bundeseinheitlich getroffen, aber der Aufbau entsprechender Betriebsumgebungen und die Planung des zukünftigen Betriebs erfolgte inkl. technischer Grundsatzentscheidungen, wie z. B. der Auswahl und dem Aufbau von Container-Plattformen, pro Land.

Zukünftig könnte nicht nur die Entwicklung, sondern auch der Betrieb in der Justizcloud bundeseinheitlich erfolgen. Damit wäre der Lebenszyklus der Softwareentwicklung bis zum Betrieb im Verantwortungsbereich der Bund-Länder-Zusammenarbeit im Rahmen der E-Justice-Strukturen. Um dabei effizient und planvoll vorzugehen, sind auf der strategischen Ebene zwei weitere neue Einheiten, ein strategisches Anforderungsmanagement und ein Justiz Architekturboard zu empfehlen.

Strategisches Anforderungsmanagement: Aus den strategischen und fachlichen Zielen der Justiz, die im Rahmen der E-Justice-Strukturen entwickelt werden (wie z. B. bundeseinheitlicher Betrieb, Einsatz von KI in der Justiz, elektronische Gefangenenpersonalakte, Modernisierung des ERV etc.), müssen konkrete Anforderungen abgeleitet und ggf. durch verschiedene Parteien umgesetzt werden. Je nach strategischer Anforderung (sog. Epics) kann dies bedeuten, dass Entwicklungsverbünde, Justizcloud, aber auch Dritte, wie bspw. Governikus (z. B. für *EGVP*) oder die BNotK (z. B. für *SAFE*), tätig werden müssen.

Das strategische Anforderungsmanagement ist damit die Schnittstelle zwischen den strategischen Prioritäten der Justiz und der operativen Umsetzungsebene. Daher ist zu empfehlen, das strategische Anforderungsmanagement als Gremium sowohl aus Beteiligten der *BLK* sowie der Leitungsebene der in Umsetzungsverantwortung stehenden Einheiten (z. B. Entwicklungsverbünden und Justizcloud) zu besetzen.

Das strategische Anforderungsmanagement (bspw. als Design Authority) bearbeitet zusammen mit dem Architekturboard priorisierte strategische Themen und leitet daraus gemeinsam mit den betroffenen Parteien Umsetzungsvorschläge, konkrete Aufgaben, etwaige Abhängigkeiten sowie grobe Aufwandsschätzungen und Roadmaps ab. Damit werden die E-Justice-Strukturen zu nachhaltigeren und nutzenmaximierenden Entscheidungen befähigt.

Dazu müssen auch Fragen der Budgetierung geklärt bzw. eine effektive und den priorisierten Anforderungen entsprechende Ressourcenverteilung vorgenommen werden.

Nach einem Beschluss verteilt das strategische Anforderungsmanagement die Aufgaben, stößt die Umsetzung bei den relevanten Organisationseinheiten an, koordiniert Abhängigkeiten und hält die übergreifende Umsetzung nach.

Justiz Architekturboard: Das Anforderungsmanagement sollte dabei durch ein justizweites Architekturboard eng unterstützt werden. Dieses würde die Gesamtsicht auf die Justizanwendungslandschaft, die zugrundeliegende Plattformarchitektur sowie ein Zielbild zu deren Weiterentwicklung nachhalten. Mit dem Ziel der Technologieharmonisierung, Standardisierung und Sicherstellung von Wirtschaftlichkeit durch die Vermeidung von Redundanzen arbeitet das Architekturboard auch eng mit den thematischen AGs der *BLK* zusammen, z. B. zu Themen der IT-Sicherheit. Das Architekturboard sollte als cross-funktionales Team arbeiten und das Architektur-Zielbild der Justiz gemeinsam mit leitenden Lösungsarchitekten der Justiz auf Basis der übergreifenden Ziele und Anforderungen weiterentwickeln. Dabei sollten sowohl die Lösungsarchitekten der Entwicklungsverbünde, weiterer relevanter Kernkomponenten (wie bspw. *ERV*) sowie der Justizcloud-Einheit zusammenarbeiten.

3.6.3.2 Operative Organisationsebene

Aus den strategischen Zielentscheidungen von *EJR* und *BLK*, konkreten und priorisierten Anforderungen des strategischen Anforderungsmanagement und technischen Anwendungs- und Plattform-Zielbildern des Architekturboards, werden konkrete Umsetzungsentscheidungen in die operative Ebene übergeben. Auf dieser arbeiten die Entwicklungsverbünde und die Justizcloud-Einheit gemeinsam an der Umsetzung von Anforderungen und orchestrieren den laufenden Betrieb des Justizanwendungsgefüges. Für die Justizcloud sind dabei ein eigenes Anforderungsmanagement sowie ein Auslagerungsmanagement aufzubauen. Die Justizcloud arbeitet zudem eng mit den IT-Dienstleistern im Rahmen der Infrastrukturbereitstellung sowie mit weiteren Partnern im Rahmen eines standardisierten Beschaffungsprozesses (z. B. *govdigital eG*) zusammen.

Justizcloud-Anforderungsmanagement

Die Justizcloud benötigt ein eigenes Justizcloud-Anforderungsmanagement. Dieses bildet den Brückenkopf zum justizweiten, strategischen Anforderungsmanagement und dem Architekturboard und orchestriert die Umsetzung von Anforderungen durch Konkretisierung, Priorisierung und Sicherstellung benötigter Ressourcen. Das Justizcloud-

Anforderungsmanagement leitet dabei bspw. aus der strategischen Vorgabe, eine Betriebsumgebung für einen bundeseinheitlichen Betrieb aufzubauen, konkrete Umsetzungsthemen ab. So müsste etwa der Auf- und Ausbau der Container-, Integrations- und Datenplattform erfolgen. Zudem muss gemeinsam mit der Justizcloud-Architektur überlegt werden, welche Anforderungen an Datendurchsatz, Verschlüsselung oder Administration erforderlich sind. Auch fachliche Anforderungen, wie ein Ausbau der Fachbetreuung von Betriebsverbänden, müssen hier vorgedacht werden. Weiterhin müssen Beschaffungsprozesse in Gang gesetzt werden und Serviceteams konkrete Anforderungen zur Umsetzung erhalten. Das Justizcloud-Anforderungsmanagement besteht daher v. a. aus Justizcloud-internen Funktionen (insb. Leitung, Strategie und Architektur), Vertretern des Justizarchitekturboards sowie des strategischen Anforderungsmanagements. Zudem könnten beschaffungsrelevante Partner wie die Entwicklungsverbünde, die IT-Dienstleister und ggf. *govdigital eG* als wesentliche Schnittstelle für die Beschaffung eingebunden werden.

Auslagerungsmanagement

Da die Justiz durch die dargestellte neue Form der Zusammenarbeit hoheitliche Aufgaben an die Justizcloud-Einheit übertragen würde, sollten hierfür Beaufsichtigungsmechanismen eingerichtet werden. Insb. muss sichergestellt werden, dass die Anforderungen von Bund und Ländern, etwa an IT-Sicherheit oder Datenlokalisierung, eingehalten werden. Hierfür könnten innerhalb eines Auslagerungsmanagement z. B. Vorgaben für SLAs festgelegt werden. Am Auslagerungsmanagement beteiligt werden sollten Vertreter der Justizcloud-Einheit in beratender Rolle sowie, ggf. gebündelt über die *BLK*, die Justizverwaltungen der Länder, die diese Aufgabe heute für die Gerichte wahrnehmen.

IT-Dienstleister

Die IT-Dienstleister stellen im Rahmen des Wertschöpfungsmodells die physische Infrastruktur bereit und bilden das Fundament für die Justizcloud (vgl. **Kapitel 3.3.2**). Sie sind somit ein wesentlicher Akteur im Justizcloud-Ökosystem. Des Weiteren ist eine enge und frühzeitige Einbindung sowie vertrauensvolle Zusammenarbeit zwischen Justizcloud-Einheit und IT-Dienstleister erfolgsentscheidend. Die Zusammenarbeit zwischen IT-Dienstleistern und der Justizcloud-Einheit wird durch Vertragsverhältnisse geregelt, die den Gegenstand der Leistungserbringung (bspw. den Bezug der virtuellen Infrastruktur) sowie die Bedingungen dafür (bspw. durch SLAs) definieren. Die Ausarbeitung, Initiierung und Kontrolle der Leistungserbringung erfolgt dabei durch eine Funktionseinheit für Beschaffungs- und Lieferantenmanagement innerhalb der Justizcloud-Einheit (vgl. **Kapitel 3.6.4**). Das

Beschaffungs- und Lieferantenmanagement stellt gemeinsam mit den IT-Dienstleistern die Einhaltung dieser SLAs sowie den vertragskonformen Leistungsabruf sicher.

Eine weitere wichtige Rolle der IT-Dienstleister neben der Bereitstellung von Infrastruktur ist das Einbringen von Services sowie ggf. die Übernahme von Betriebsaufgaben. Mit bestehenden und teilweise marktreifen und bewährten (Cloud-)Lösungen können die IT-Dienstleister ein wichtiger Lieferant beim Aufbau des Justizcloud-Serviceportfolios sein. Denkbar wäre bspw. die Nachnutzung von Container-Plattformen sowie von Logging- und Monitoring-Infrastruktur für die Justizcloud oder auch bestimmter SaaS-Produkte. Auch könnten die IT-Dienstleister durch die Justizcloud beauftragt werden, bestimmte Plattform-Komponenten wie Logging und Monitoring nicht nur auf der Justizcloud aufzubauen, sondern auch einheitlich im Auftrag der Justizcloud zu betreiben. Mit ihrer Erfahrung im Betrieb von Services für die öffentliche Hand und dem im Ausbau befindlichen Produktportfolio können die IT-Dienstleister zudem Innovationstreiber für die Justiz sein und dabei helfen, Synergien zwischen Verwaltung und Justiz zu heben.

Standardisierte Beschaffung

Für den Bezug von Produkten und Dienstleistungen wie bspw. Standard- und Spezialsoftware oder auch Beratungsleistungen, wird für die Justizcloud-Einheit eine dedizierte Einheit für standardisierte Beschaffung empfohlen. Sie legt hierfür Standards und Richtlinien (inkl. Sicherheitsstandards, SLAs, Datenschutzbestimmungen, Compliance-Anforderungen) in Abstimmung mit dem Cloud-Plattform-Management der Justizcloud-Einheit fest und trifft basierend darauf die Auswahl geeigneter Anbieter. Sie kann dabei auf etablierte Strukturen wie die *govdigital eG* zurückgreifen. Die Inhouse-Fähigkeit der *govdigital eG* ermöglicht es der Justizcloud-Einheit, auf Leistungen aller relevanten Justiz-IT-Dienstleister, die Mitglied der Genossenschaft sind, sowie deren Rahmenverträge zuzugreifen. Die durch die *govdigital eG* aufgebauten Kooperationsmodelle mit den IT-Dienstleistern minimieren zudem den administrativen Aufwand. Darüber hinaus eröffnet sich ggf. zu einem späteren Zeitpunkt die Möglichkeit, die *govdigital eG* als Cloud-Broker zu nutzen und somit Zugang zu Leistungen weiterer Cloud-Anbieter zu erhalten.

Entwicklungs- und Betriebsverbünde

Die Entwicklungsverbünde bilden im vorgesehenen Organisationsmodell ein operatives Kernelement der Justiz-IT. Während die Justizcloud-Einheit die Plattform für Softwareentwicklung und -betrieb bereitstellt, wären die Entwicklungs- und Betriebsverbünde diejenigen, die Software auf der Justizcloud für die Justizcloud entwickeln und betreiben. Damit

sind die Entwicklungs- und Betriebsverbünde auch diejenigen, die die Services der Justizcloud beziehen und nutzen.

Bisher haben die Entwicklungsverbünde Software für die Justiz entwickelt, welche anschließend durch die multiplen IT-Dienstleister individuell betrieben wurde. Da die moderne Cloud-native Software der Justiz zukünftig aber in der Justizcloud betrieben werden soll, musste definiert werden, wer diesen Betrieb operativ durchführt. Eine Möglichkeit wäre der Aufbau eines Betriebsteams pro Anwendung in der Justizcloud-Einheit. Gemäß moderner Cloud-Anwendungsentwicklung sollte Software aber durch sog. DevOps-Teams sowohl entwickelt als auch betrieben werden. Dies hat immense Vorteile, da z. B. das Informations- und Koordinationsproblem zwischen Entwicklung und Betrieb deutlich reduziert wird. So bündeln DevOps-Teams das Know-how für Entwicklung und Betrieb organisatorisch in einer Einheit, Herausforderungen bei der Ausbringung können in der Entwicklung aufgenommen werden (z. B. bei der Fehlerbehebung), technische Anforderungen an die Betriebsplattform können schneller identifiziert und umgesetzt werden und die Planung von Release- und Testzyklen wird deutlich verkürzt. Weitere Vorteile von DevOps sind auch ein effizienterer Ressourceneinsatz, mehr Zeit für die Exploration von Innovationen und den Aufbau neuer Features sowie schnellere Problemlösung und geringere Ausfallzeiten. All dies verbessert auch die Nutzendenerfahrung und insgesamt die Qualität Cloud-nativer Software.

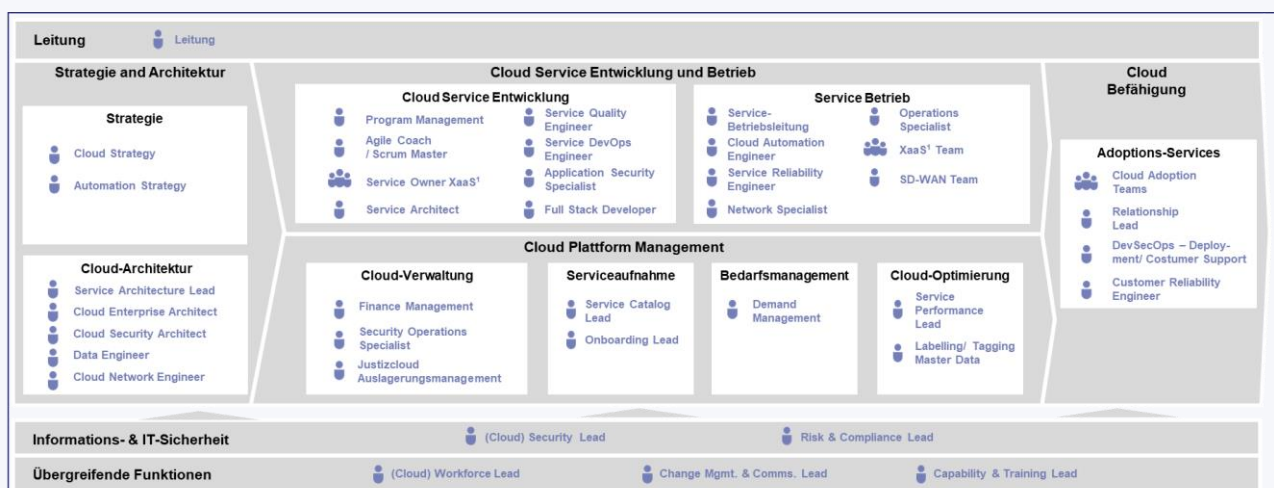
Aus diesem Grund wurde im Zielbild eine Weiterentwicklung von Entwicklungs- zu Betriebsverbünden vorgesehen. Dabei ist eine enge Zusammenarbeit und Abstimmung zwischen Betriebsverbünden und Justizcloud ein entscheidender Erfolgsfaktor. Voraussetzung dafür sind die Etablierung gemeinsamer strategischer Entscheidungs- und Koordinationsstrukturen wie bspw. dem strategischen Anforderungsmanagement und einem gemeinsamen Architekturboard (vgl. **Kapitel 5.1.3**). Aufbauend auf den strategischen Anforderungen müssen die Entwicklungs- und Bereitstellungaktivitäten zwischen Verbünden und Justizcloud eng koordiniert werden. Bspw. müssen Entwicklungs- und Releasezyklen mit der Plattformentwicklung abgestimmt werden. Wichtig ist dabei etwa, dass zum Releasezeitpunkt alle benötigten Plattformkomponenten zur Verfügung stehen und dafür auch die entsprechenden Freigaben (z. B. IT-Sicherheit) vorliegen. Wichtig ist auch, dass die Entwicklungs- und Betriebsteams über die für sie wesentlichen Werkzeuge verfügen. Dabei ist die Ausgestaltung des integrierten Entwicklerarbeitsplatzes in der Justizcloud und die Festlegung auf standardisierte Entwicklungs-, Test- und Releasewerkzeuge entscheidend. Auch für die Betriebsteams müssen betriebsrelevante Werkzeuge (z. B. Logging/ Monitoring) verfügbar sein. Darüber hinaus könnte für einen bundeseinheitlichen Support (1st/ 2nd/ 3rd-level) ein

gemeinsames Ticketing-System auf der Justizcloud bereitgestellt werden. So könnten an einer zentralen Stelle Nutzendenanfragen (beachte: die Nutzenden der Justizcloud sind die Entwicklungsverbünde) bspw. bei Störungen oder Freischaltungen gebündelt und gezielt je nach Anfrage an die benannten fachlichen und technischen Justizcloud-Betriebsteams weitergeleitet werden. Entwicklungsverbünde würden im Verlauf auch die Länder-spezifischen Migrations- und Einführungs-Roadmaps mit dem Justizcloud-Betriebsteam abstimmen, damit diese bspw. die Ressourcenvolumina mit den IT-DL bündeln und abstimmen können.

3.6.4 Ausgestaltung der agilen Justizcloud-Einheit

Die Justizcloud-Einheit bündelt das Cloud-Know-how für die Justiz an einer Stelle und verfügt über ein breites Fähigkeitsprofil, um ihre Aufgaben innerhalb der Gesamtorganisation zu erfüllen. Dabei muss die Justizcloud (1) Aufgaben gegenüber ihren Kunden, den Entwicklungs- und Betriebsverbünden, (2) Aufgaben nach Innen (d. h. Services gegenüber den eigenen Mitarbeitenden) sowie (3) Aufgaben im Rahmen der übergreifenden Justizorganisation erfüllen. Abgeleitet aus diesen Aufgaben wurde ein Zielbild für eine Aufbau- sowie Ablauforganisation inkl. initialer Rollenbeschreibungen für die Justizcloud-Einheit konzipiert (vgl. **Abbildung 80**). Die Justizcloud soll dabei von Anfang an als agile Organisation (z. B. aufbauend auf dem Scaled Agile Framework (SAFe)) aufgesetzt werden.

Abbildung 80 | Zielbild der agilen Justizcloud-Einheit inkl. Rollen



¹ XaaS = IaaS, PaaS, SaaS, CaaS

Aufbau- und Ablauforganisation

Als eigenständige Organisation verfügt die Justizcloud über eine **Leitung**, die die Gesamtverantwortung für den Betrieb und Verwaltung der Justizcloud trägt. Sie stellt dabei sicher, dass die Justizcloud ihre Aufgaben in der übergreifenden Justizorganisation wahrnimmt, klare Anforderungen und strategische Ziele formuliert und die Justizcloud in alle relevanten übergreifenden Gremien und Entscheidungen eingebunden ist. Zugleich verantwortet die Leitung den laufenden Betrieb, d. h. die Besetzung interner Rollen, stellt Finanzierung und Ressourcenverteilung entsprechend den strategischen Zielen sicher und fungiert als Aufsichts- und Eskalationsinstanz für strategische und operative Fragen.

Neben der Leitung sind insb. zwei Rollen zu institutionalisieren, die Bereiche Strategie und Architektur.

Der Bereich **Strategie** verantwortet u. a. die übergreifende Cloud-Vision für die Einheit und definiert hierfür (Teil-)Strategien, die für einen modernen Cloud-Betrieb relevant sind. Dazu muss der Bereich Strategie sowohl die Anforderungen der Justiz an eine Justizcloud (bspw. Fachbedarfe, Anforderungen der Entwicklungsverbünde) als auch Marktentwicklungen wie Angebote von IT-Dienstleistern und externen Anbietern im Auge behalten. Auch eine Weiterentwicklung von Services auf Public Cloud-Angebote könnte durch einen Strategiebereich vorgedacht werden. Allerdings würde bei Entscheidungen dieser Tragweite auch einen Auftrag oder eine Zustimmung der strategischen Ebene, d. h. *EJR*, *BLK* etc., erfordern. Dagegen können Strategien zur Optimierung der Leistungserbringung innerhalb der Justizcloud etwa durch (Prozess-)Automatisierung, KI oder mögliche notwendige personelle (Re-)Strukturierungen, auch durch den Strategiebereich, unter Beteiligung der Leitung initiiert werden. Auch die kontinuierliche Optimierung des Serviceportfolios und bspw. Aufnahme innovativer Technologien und Services sind Teil der strategischen Aufgaben.

Das Strategieteam besteht zu Beginn aus einem Experten für Cloud-Strategie sowie Fachexperten für Automation. Letztere Rolle wurde gemeinsam mit den Fachpanels definiert, da als neue Organisation mit hohen Effizienzzielen der Einsatz von Automatisierung (mit und ohne KI) für repetitive Aufgaben (sog. Automation-by-Default) in der Justizcloud als wichtige strategische Maßnahme zur Optimierung interner Prozesse definiert wurde.

Der Bereich **Architektur** verantwortet die fachliche und technische Konzeption der Justizcloud-Plattform. Das Architekturmanagement definiert bspw. die notwendigen Plattformkomponenten wie eine Container-, Integrations- und Datenplattform. Gemeinsam mit der Serviceentwicklung und auf Basis der Kundenbedarfe werden Anforderungen und

Standards für die jeweiligen Plattformkomponenten definiert, die anschließend in der Beschaffung und Entwicklung berücksichtigt werden müssen. Weiterhin wird sichergestellt, dass alle Plattformkomponenten sicher, performant und flexibel miteinander integriert werden. Auch das Netzwerkkonzept für die Plattform sowie weitere Plattformkonzepte wie die übergreifende Daten- und Sicherheitsarchitektur liegen im Verantwortungsbereich des Architekturteams.

Das Architekturteam besteht in einer ersten Ausbaustufe der Justizcloud aus einer Leitung, sowie spezialisierten Architekten für die Themen Cloud-Enterprise-Architecture, Sicherheitsarchitektur und Netzwerk sowie einem Data Engineer für das Thema Datenarchitektur.

Kern der Justizcloud-Einheit ist der Bereich **Cloud-Serviceentwicklung und -betrieb**. Dieser Bereich verantwortet die operative Planung, den Aufbau, die kontinuierliche Weiterentwicklung sowie den laufenden Produktivbetrieb der Cloud-Dienste. Der Bereich arbeitet dabei gemäß dem DevOps-Ansatz in einem integrierten, agilen Setup bestehend aus zwei Sub-Teams, jeweils für Entwicklung und Betrieb. Das Entwicklungsteam besteht dabei aus einem Programmmanager und einem oder mehreren agilen Coaches, um die agile Serviceentwicklung zu unterstützen. Zudem gibt es, wie im agilen *SAFe-Framework* vorgesehen, für die verschiedenen as-a-Service-Dienste (z. B. Container- und Integrationsplattform) einzelne Service-Owner die die funktionalen und nicht-funktionalen Anforderungen an die Plattformdienste, gemeinsam mit der Architekturmanagement, definieren. Für die Entwicklung besteht das Team aus spezialisierten DevOps Entwicklern, die auf die Entwicklung von Cloud-Plattformen spezialisiert sind. Zudem sind ein Sicherheitsanalyst sowie ein Quality Engineer Teil des Teams.

Der laufende Plattformbetrieb erfolgt durch das Betriebsteam. Neben einer Leitung besteht das Team aus Experten für Automatisierung, z. B. für automatisierte Plattformbereitstellung durch Infrastructure-as-Code (IaC), einem Service Reliability Engineer, der die Überwachung der Services sicherstellt, einen Netzwerk-Spezialisten, der die Netzwerkauslastung überwacht und einem Fachbetrieb, der die Bereitstellung und Kundenbetreuung für alle Services übernimmt.

Der Servicebetrieb arbeitet dabei eng mit einer Einheit zur Cloudbefähigung zusammen. Dieses Team bildet die Kundenschnittstelle zu den Entwicklungs- und Betriebsverbünden. Die Nutzung von Cloud verändert die Arbeit in Anwendungsentwicklung und Betrieb deutlich. Die Nutzenden müssen zunächst die Prozesse der Justizcloud kennenlernen, verstehen welche Services die Justizcloud bereitstellt und wie diese funktionieren (wie z. B. den

Entwicklerarbeitsplatz und die verschiedenen Plattformdienste) und müssen sowohl in der Anfangsphase als auch während der laufenden Nutzung Support erhalten. Dafür besteht das Team zur Cloud-Befähigung aus Spezialisten für Cloud-Adoption, d. h. Ansprechpartnern die neue Nutzende während des Onboardings, also in der Anfangsphase der Cloud Nutzung, unterstützen. Zudem bildet eine DevSecOps-Kundentreuung kontinuierliche Unterstützung bei Fragen zu den Plattformdiensten sowie zu den standardisierten DevSecOps-Prozessen auf der Justizcloud, die die Entwicklungs- und Betriebsverbünde zur Ausbringung ihrer Anwendungen nutzen.

Die interne Verwaltung der Justizcloud erfolgt durch ein **Cloud Plattform Management**. Dieses stellt alle Verwaltungs-, Beschaffungs- und Betriebsaufgaben, die für das Funktionalisieren der Plattform benötigt werden. Ein Team für Cloud-Verwaltung übernimmt dabei alle Verwaltungsaufgaben wie etwa Finanzen und Auslagerungsmanagement. Ein Team für Serviceaufnahme pflegt, gemeinsam mit dem Strategiebereich, den Servicekatalog und das Portfoliomanagement der Justizcloud. Ein Team für Bedarfsmanagement ist für die kundenspezifische Bedarfsaufnahme und Verwaltung des Kundenverhältnisses inkl. Abrechnung verantwortlich. Das Bedarfsmanagement unterstützt bspw. gemeinsam mit dem Cloud-Adoption-Team die Festlegung des Portfolios an Cloud-Diensten, die ein Kunde benötigt, sowie die Festlegung von Finanzierungs- bzw. Abrechnungsmodellen. Auch die laufende Abrechnung und Rechnungsstellung erfolgt über das Bedarfsmanagement. Zuletzt analysiert das Team Cloud-Optimierung fortlaufend die Nutzung der Cloud-Dienste inkl. Betriebsdaten, Auslastung, Kunden etc. Das Team leitet auf dieser Basis Optimierungspotenziale für die Cloud-Landschaft ab, priorisiert Handlungsempfehlungen und stellt sie der Leitung, Architektur und Strategie der Justizcloud-Einheit in Form von Berichten zur Verfügung. Die Cloud-Optimierung umfasst darüber hinaus auch die Preisgestaltung der Cloud-Services.

Der Bereich **Informations- und IT-Sicherheit** verantwortet übergreifend sowohl die Sicherheit der Justizcloud-Einheit selbst sowie der erbrachten Cloud-Services. Für die Justizcloud wird dabei ein eigenes Informationssicherheitsmanagementsystem (ISMS) sowie ein Security-Incident- und Event-Management (SIEM) etabliert. Zudem müssen für die verschiedenen Services etwa Zertifizierungen (z. B. IT-Grundschutz) inkl. Sicherheitskonzepten, Risikomanagement und Lösungen für Ausfall- und Exitszenarien entwickelt werden.

Abschließend sind einige querschnittliche Aufgaben gebündelt in **Übergreifende Funktionen** dargestellt. Hierzu zählen u. a. die Personalgewinnung und -verwaltung, der Rechtsbereich der Justizcloud sowie Kommunikations- und Change-Management-Funktionen.

Gremien in der Justizcloud

Neben den beschriebenen Teams existieren in der Aufbauorganisation zudem **vier Gremien**, die im Rahmen der internen Governance spezifische Abstimmungs- und Entscheidungsfunktionen wahrnehmen. Sie setzen sich querschnittlich aus Vertretern verschiedener Bereiche zusammen und sind in der Aufbauübersicht der Justizcloud-Einheit daher nicht explizit abgebildet.

Das **Strategie- und Architekturgremium** setzt sich aus Vertretern der Bereiche Strategie, Architektur, Cloud-Serviceentwicklung, Cloud-Optimierung sowie Cloud-Befähigung zusammen. Es sorgt dabei für eine enge Abstimmung zwischen allen relevanten Bereichen im Zusammenhang mit der fachlichen und technischen Ausgestaltung der Cloud-Plattform und den dazugehörigen Diensten inkl. der Architektur-, Portfolio- und Produktentscheidungen.

Das **Gremium Lieferantenmanagement** verantwortet die Kontrolle der Auslagerungen von Produkten und Services, z. B. von genutzten SaaS-Produkten, an IT-Dienstleister und externe Anbieter. Das Gremium setzt sich aus Vertretern des Justizcloud-Auslagerungsmanagements, der Justizcloud-externen IT-Provider sowie den Bereichen Informations- & IT-Sicherheit, Bedarfsmanagement und Cloud-Optimierung zusammen. Es überwacht z. B. die Einhaltung der vereinbarten Sicherheitsvorgaben und Standards sowie SLAs.

Das Gremium **Cloud-Service-Projektsteuerung** verantwortet das Management aller Projekte, die neue Services aufbauen (z. B. Datenbanken) inkl. Leitung der Planungsinkremente und Reporting bspw. bei Verzögerungen. Es übernimmt somit im Rahmen des Auf- und Ausbaus der Justizcloud eine wichtige Steuerungsfunktion. Das Gremium besteht aus der Leitung der Justizcloud-Einheit sowie Vertretern der Bereiche Strategie und Cloud-Serviceentwicklung.

Zuletzt überwacht ein **Cloud-Betriebsgremium** die unterbrechungsfreie und sichere Erbringung der Cloud-Services. Dabei werden u. a. die Einhaltung von SLAs kontrolliert, Risiken besprochen oder Sicherheits- und Betriebs-Incidents diskutiert und Maßnahmen abgeleitet. Hierfür stimmen sich Vertreter der Bereiche Servicebetrieb, Cloud-Verwaltung, Cloud-Optimierung, Cloud-Service-Entwicklung, Cloud-Architektur sowie Cloud-Sicherheit ab.

3.6.5 Personalbedarf und -strategie

Als eigenständige Organisationseinheit muss die Justizcloud-Einheit auch eigenes Personal einstellen. Der Personalbedarf leitet sich dabei aus den Aufgaben und definierten Rollen der Justizcloud-Einheit ab, die im vorangegangenen Kapitel beschrieben wurden (vgl. **Kapitel**

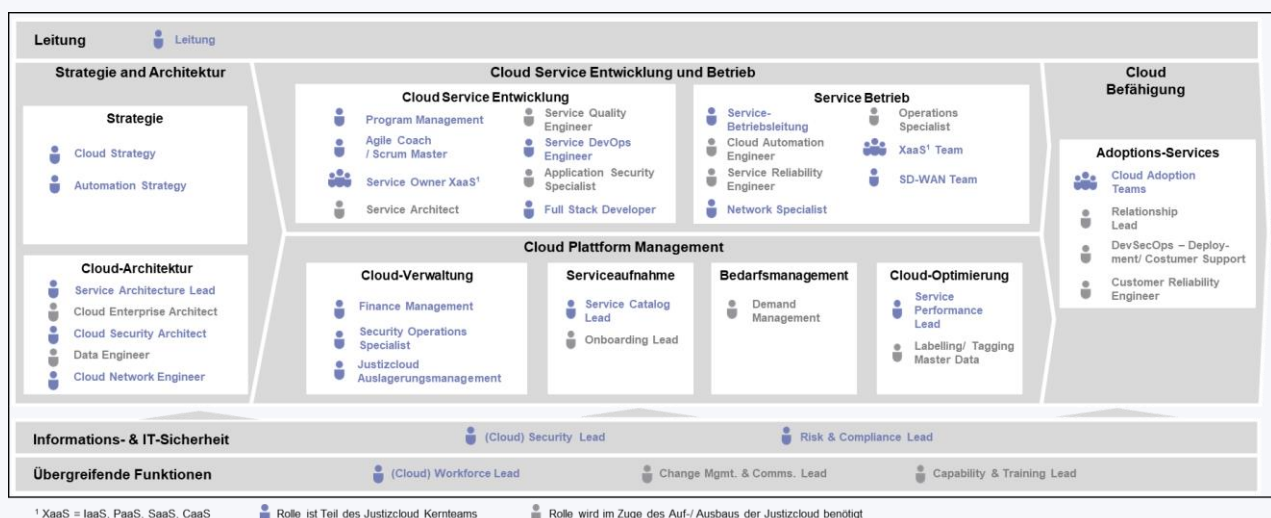
3.6.4). Die in **Abbildung 80** dargestellten Rollen entsprechen dabei nicht notwendigerweise einer Person. Je nach Aufgabenumfang kann eine Person auch mehrere Rollen wahrnehmen bzw. eine Rolle kann auch durch mehrere Personen wahrgenommen werden. Um die beschriebenen Aufgaben vollumfänglich zu erfüllen, wurde für die Justizcloud-Einheit ein Personalbedarf von 50 bis 60 Personen bei voller Realisierung des Zielbilds geschätzt. Dieser Personalbedarf wird jedoch nicht ab Tag 1 erforderlich sein. Stattdessen ist vorgesehen, während des Justizcloud-Aufbaus Personal schrittweise und bedarfsorientiert aufzubauen. Im Rahmen des rechtlich-organisatorischen Panels wurden sowohl der phasenweise Aufbau von Personal sowie verschiedene Herausforderungen, Erfolgsfaktoren und Strategien zur Personalgewinnung detailliert.

Personalbedarf und -aufbau

Der Personalaufbau wurde entlang von drei Phasen im Rahmen des Aufbaus und der Skalierung der Justizcloud-Einheit beschrieben: Initiierung und Vorbereitung, Aufbau und Pilotierung sowie Ausbau und Skalierung (vgl. **Kapitel 5.1.1**).

In der ersten Phase, Initiierung und Vorbereitung, ist die Justizcloud-Einheit noch nicht gegründet und kann daher auch kein eigenes Personal einstellen. Die Initiierung und Vorbereitung erfolgt durch einen Aufbaustab und ggf. externe Unterstützung. Der Personalbedarf für diese Phase wird in **Kapitel 4** „Wirtschaftlichkeitsbetrachtung“ sowie in **Kapitel 5.1** „Roadmap“ beschrieben.

Abbildung 81 | Kernteam der Justizcloud-Einheit



In der zweiten Phase, Aufbau und Pilotierung, arbeitet die Justizcloud darauf hin, erste Plattform-Services sowie den Betrieb erster Anwendungen zu pilotieren. Die Phase beginnt mit der Gründung der Justizcloud-Einheit und zielt darauf ab ein MVP vorzubereiten. Dieses sieht eine produktive Nutzung der Justizcloud-Plattform durch eine Justizanwendung bzw. den Betrieb eines ersten Anwendungsbündels vor. Dazu werden während des Aufbaus schrittweise die definierten Rollen des organisatorischen Zielbilds besetzt. **Abbildung 81** stellt das Kernteam der Justizcloud-Einheit dar, d. h. Rollen, die zum Zeitpunkt eines MVP besetzt sein sollten. Besonders wichtig sind dabei die wesentlichen Entscheidungsträger in Leitung, Strategie und Architektur, die idealerweise direkt aus dem Aufbaustab in den Regelbetrieb der Justizcloud wechseln. Zudem sind für die Entwicklung der Kerndienste, die bereits zum MVP verfügbar sein müssen, die Rollen des Programmmanagement, der Service-Owner sowie Entwicklerrollen zu besetzen. Im Betriebsteam müssen für die MVP-Services erste Betriebsrollen besetzt werden und insb. das Netzwerk sicher betrieben werden können. Eine umfassende Besetzung des Betriebsteams ist zu diesem Zeitpunkt noch nicht erforderlich. Dagegen muss die Cloud-Verwaltung bereits etabliert werden, da schon während des Aufbaus Kosten anfallen und erste SLAs und die Übernahme von Betriebsverantwortung im MVP erfolgen soll. Auch ein erster Servicekatalog sollte für das MVP verfügbar sein und die Rolle des Service-Catalog-Lead besetzt sein. Insg. kann der Personalkörper im laufenden Betrieb und der Kundenbetreuung bzw. Cloud-Befähigung noch schlank bleiben, da nur wenige Entwicklungsverbünde zum Zeitpunkt des MVP die Cloud nutzen. Der Gesamtbedarf an Personal beläuft sich zum Zeitpunkt des MVP auf ca. 40-50 Personen.

In der dritten Phase, Ausbau und Skalierung, werden die Cloud-Dienste weiter ausgebaut, sukzessive weitere Cloud-Dienste hinzugefügt und der Betrieb von Anwendungen skaliert, d. h. die Anzahl von Entwicklungs- und Betriebsverbünden, die Anwendungen auf der Justizcloud entwickeln und betreiben, steigt. Mit der Skalierung von Plattform und Anwendungen wächst auch der Bedarf an Kundenbetreuung, Onboarding. Die laufenden Betriebsaufwände der Plattform steigen ebenfalls. Gleichzeitig erreicht der Ausbau der Plattform aber einen hohen Reifegrad, daher sinkt der Bedarf für Entwicklung, wobei insgesamt die Plattform fortlaufend weiterentwickelt wird und daher auch konstant Entwickler in der Justizcloud arbeiten. Erwartungsgemäß greifen in dieser Phase auch erste Maßnahmen der Cloud-Optimierung sowie Automatisierung durch gezielte Maßnahmen zur Prozessoptimierung, die in der Justizcloud von Anfang an mitgedacht werden sollen. Nach anfänglichen hohen Aufwänden im Onboarding der Entwicklungsverbünde sinken diese Aufwände im Zeitverlauf wieder.

Insgesamt wird erwartet, dass der Personalbedarf temporär auf 70+ Personen ansteigt, aber sich mit wachsendem Reifegrad der Justizcloud auf ca. 50-60 einpendelt.

Personalbedarfsdeckung

Einer der großen Mehrwerte und Ziele der Justizcloud ist eine mögliche Bündelung und der nachhaltige Aufbau von Cloud-Know-how in der Justiz. Insb. durch den Fachkräftemangel und knappe Budgets ist die Einstellung und Ausbildung hochqualifizierter Cloud-Experten herausfordernd. Um den Personalbedarf in der Justizcloud-Einheit zu decken, wurden im Rahmen des rechtlich-organisatorischen Panels vier Strategien diskutiert. Diese können je nach Bedarf und Ausbaustufe der Justizcloud unterschiedlich relevant sein und sollten kombiniert werden, um den gewünschten Personalmix zu erreichen.

Abbildung 82 | Strategien zur Personalbedarfsdeckung



Die Justizcloud kann als eigenständige Einheit über **Neueinstellung** ihren langfristigen Personalbedarf mit qualifizierten Fachkräften decken. Dies ist insb. für Personal relevant, das bereits kurzfristig benötigt wird, langfristig gebunden werden soll, aber in der Justiz aktuell noch nicht oder nicht in ausreichendem Maße vorhanden ist. Dies könnte bspw. für Rollen gelten, die im Kontext des Fachkräftemangels sowie dem hohen Bedarf von Wirtschaft und Verwaltung im Bereich Cloud aktuell besonders nachgefragt sind (bspw. Cloud-Architekten, Cloud-Entwickler oder Cloud-Sicherheitsexperten). Diese Stellen sind erfolgskritisch für den effektiven Auf- und nachhaltigen Ausbau einer modernen Justizcloud-Plattform. In der Vorbereitungsphase der Justizcloud (vgl. **Kapitel 5.1.1.1**) sollten daher zeitnah Stellenprofile für diese Rollen entwickelt werden und Ausschreibungen erfolgen.

Parallel dazu sollten die Justiz und die Justizcloud in die **Fort- und Weiterbildung bestehenden Personals** investieren. Beim Zukunftsthema Cloud müssen viele neue Fähigkeiten erlernt werden und es bieten sich große Chancen für Personal, neue technische sowie organisatorische Rollen zu erschließen. Dazu sollte in der Justizcloud die Möglichkeit bestehen, über Schulungen neue Fähigkeiten, wie z. B. Cloud-native Anwendungsentwicklung oder Know-how im Bereich agiler Methoden, zu erlernen. Zudem sollte ein funktionierendes Wissensmanagement etabliert werden, etwa durch die konsequente Nutzung von Dokumentationswerkzeugen, um neues Personal schnell onboarden zu können und gleichzeitig Abhängigkeiten zu einigen wenigen Wissensträgern zu reduzieren.

Als dritte Option besteht die Möglichkeit **zeitlich begrenzter Beauftragung** von Arbeitskräften, bspw. von externen Dienstleistern oder durch Abordnung von Fachkräften aus Bund und Ländern. Insb. die Abordnung ist eine gute Möglichkeit, in der Aufbau und Skalierungsphase der Justizcloud schnell Know-how zu akquirieren und zu nutzen, das in der Justiz bereit besteht. Viele IT-Dienstleister haben bereits umfassendes Wissen im Bereich Cloud aufgebaut. Über Inhouse-Sourcing und befristete Abordnungen könnten IT-Dienstleister ihr Wissen und Expertise beim Aufbau der Justizcloud einbringen. Zudem könnten IT-Dienstleister auch langfristig den Betrieb einzelner Service-Komponenten übernehmen.

Ergänzend ist als vierte Option der konsequente Einsatz von **Robotic-Process-Automation (RPA) und KI** in der Justizcloud von Beginn an angedacht (*Automation-by-Default*). Dazu sollen schon während der Planung und Implementierung von Prozessen im Rahmen des Cloud-Aufbaus Automatisierungslösungen geprüft und implementiert werden. Dies ist eine wichtige Komponente, um die Justizcloud möglichst effizient aufzustellen, Personal zu entlasten und die Justizcloud als Arbeitsplatz attraktiver zu gestalten.

Je nach Phase des Justizcloud-Aufbaus sind diese Strategien unterschiedlich relevant. Neueinstellungen sollten insb. in der Aufbau- und Skalierungsphase für sehr spezialisiertes Know-how und langfristig benötigtes Personal erfolgen. Für punktuelle Unterstützung beim Aufbau der Cloud sollte über zeitlich begrenzte Beauftragung u. a. von externen Dienstleistern nachgedacht werden. Am wichtigsten und nachhaltigsten ist aber der langfristige Auf- und Ausbau von Fachwissen bei bestehendem Personal durch Schulungen und Weiterbildungen. Insg. sind für die langfristige Gewinnung von Personal bestimmte **Erfolgsfaktoren** zu berücksichtigen.

Besonders wichtig ist die Ausrichtung der Justizcloud als attraktiver Arbeitsgeber. Dazu sollten bspw. flexible Arbeitsmodelle (Teilzeit, Home Office etc.) angeboten werden. Hier kann

die Justizcloud auch auf Erfahrungen anderer Behörden im öffentlichen Sektor (bspw. *FITKO*) zurückgreifen, die durch eine Reduzierung von Anwesenheitspflicht ein breiteres Spektrum an potenziellen Mitarbeitenden ansprechen und gewinnen konnten. Weiterhin ist auch ein breites Angebot von Schulungen, Fortbildungen und anderen Entwicklungsmaßnahmen (bspw. durch Mentoring-Programme für Führungskräfte) inkl. Aufstiegs- bzw. Aufstiegsperspektiven besonders attraktiv für neue Mitarbeitende. Auch ein Arbeitsplatz mit modernen Werkzeugen (Software und Hardware) sowie eine moderne Arbeitskultur trägt zur Arbeitgeberattraktivität bei.

Darüber hinaus ist auch eine vorausschauende Personalplanung und -strategie wichtig, um bspw. sicherzustellen, dass Bedarfe frühzeitig an IT-Dienstleister kommuniziert werden und so Bestandspersonal auch entsprechend freigestellt werden kann. Zudem sollte Personal bundesweit gesucht werden, was auch durch flexible Remote-Modelle befördert werden kann, um den Pool passender Interessenten zu erhöhen. Eine detaillierte Personalplanung und Strategie zur Personalgewinnung sollte in der Aufbauphase der Justizcloud angegangen werden.

3.6.6 Rechtsform und Finanzierung

Aus den beschriebenen Aufgaben und Anforderungen an die Justizcloud ist Handlungs- und Geschäftsfähigkeit innerhalb eines abgesteckten Rahmens sowie personelle und rechtlich-organisatorische Eigenständigkeit erfolgsentscheidend. Die gewählte Rechtsform für die Justizcloud muss dieses Ziel maßgeblich unterstützen.

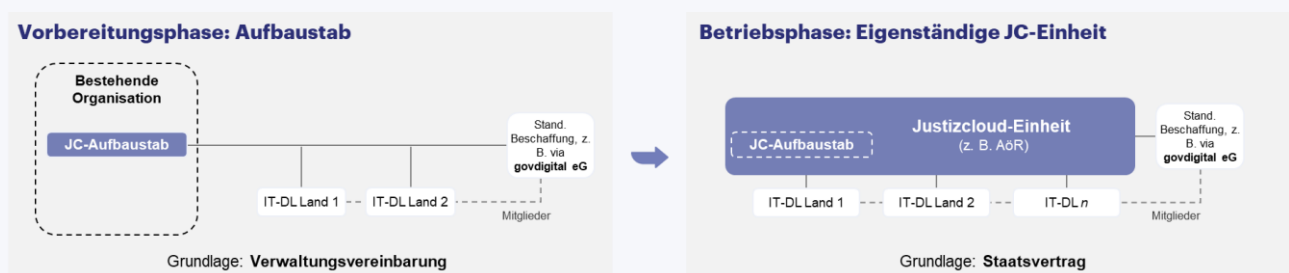
Das Spektrum möglicher Rechtsformen reicht von juristischen Personen des privaten Rechts (z. B. *GmbH*, *Aktiengesellschaft* oder *Verein*) und des öffentlichen Rechts (z. B. *Stiftung des öffentlichen Rechts* oder *Anstalt des öffentlichen Rechts (AöR)*) über die vollständige Auslagerung an externe Dienstleister bis hin zu Mischformen der vorgenannten Optionen. Die Optionen wurden im Rahmen des rechtlich-organisatorischen Panels diskutiert und auf Basis praktischer Überlegungen und organisatorischer Implikationen des Zielbilds eine initiale Einschätzung für eine passende Rechtsform abgeleitet. Eine rechtliche Beratung und Bewertung ist nicht erfolgt.

Im Zielbild wird dabei die Gründung einer **juristischen Person des öffentlichen Rechts** favorisiert (vgl. **Kapitel 3.3.3**). Naheliegend scheint dabei die *AöR*, die per Definition eine Sammlung von Sach- und Personalmitteln zur Erfüllung öffentlicher Aufgaben darstellt. Eine juristische Person des öffentlichen Rechts wurde von den Fachpanelisten favorisiert, da die

Aufgaben des IT-Betriebs für die Justiz dem Spektrum öffentlicher Aufgabenwahrnehmung zugerechnet wurden. Ferner wäre eine juristische Person des öffentlichen Rechts eine Grundvoraussetzung für Abordnung. Schließlich darf nicht außer Acht gelassen werden, dass mit einer juristischen Person öffentlichen Rechts Inhouse-Beziehungen mit weiteren Behörden entstehen würden.

Für die Gründung einer juristischen Person des öffentlichen Rechts bzw. einer AöR bedarf es eines Gründungsakts. Für die Justizcloud-Einheit ist analog zur Gründung der FITKO AöR die Verabschiedung eines Staatsvertrags durch Bund und Ländern sowie die weitere Ausgestaltung durch ein Gesetz des Sitzlandes vorgesehen.

Abbildung 83 | Übergang von Aufbaustab zu eigenständiger Justizcloud-Einheit

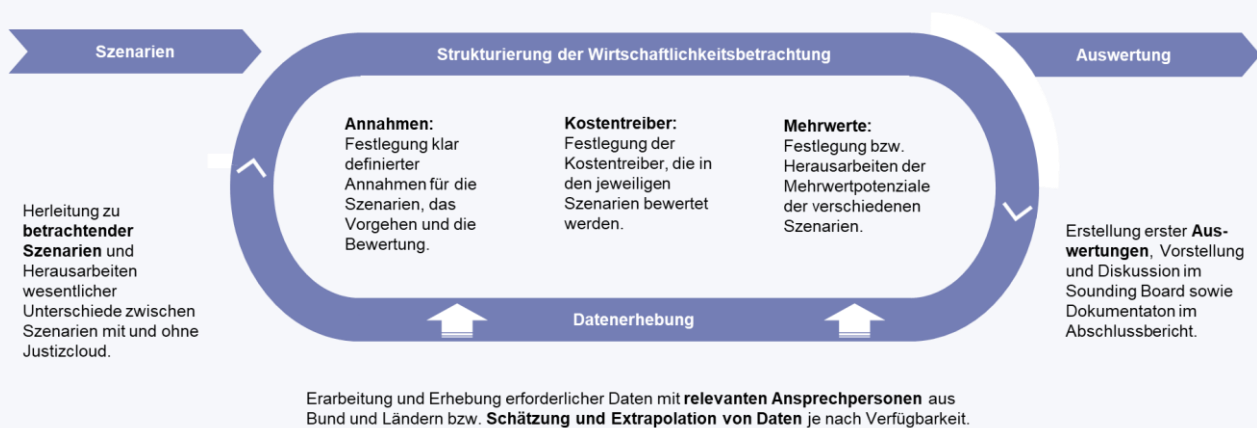


Die Justizcloud-Roadmap (vgl. **Kapitel 5.1**) sieht bereits ab 2025 eine Initialisierungs- und Vorbereitungsphase vor. In dieser soll ein Aufbaustab mit ersten Leitungsfunktionen und weiterem Personal den Aufbau der Justizcloud vorantreiben. Um dies organisatorisch zu ermöglichen, soll der Aufbaustab in einer bereits existierenden Organisation ausgebracht werden. Über eine **Verwaltungsvereinbarung** sollen dabei die Handlungsfähigkeit gesichert und vertragliche Vereinbarungen mit (ersten) IT-Dienstleistern und Externen geschlossen werden. Im Verlauf der Vorbereitungsphase wird der Aufbaustab sukzessive ausgebaut und nach Verhandlung und Zeichnung des Staatsvertrags in die eigenständige Justizcloud-Einheit übergehen (siehe **Abbildung 83**).

4 Wirtschaftlichkeitsbetrachtung

Gegenstand der vorliegenden Untersuchung ist auch eine Betrachtung der Wirtschaftlichkeit des Justizcloud-Zielbilds (vgl. z. B. **Kapitel 3.3**) und Auftrag des *BLDG*. Dazu wurden die erwarteten finanziellen Mehrwerte einer Justizcloud den dafür notwendigen Investitionen gegenübergestellt. Dies erfolgte entlang eines strukturierten Vorgehens gemeinsam mit Ansprechpartnern aus Bund und Ländern analog zur wöchentlichen Zusammenarbeit in den Fachpaneln während der Zielbildentwicklung (vgl. **Kapitel 3**).

Abbildung 84 | Vorgehensmodell der Wirtschaftlichkeitsbetrachtung



Zunächst wurden Zukunftsszenarien eines Infrastruktur-, Plattform- und Anwendungsbezugs der Justiz mit bzw. ohne Justizcloud erarbeitet (vgl. **Kapitel 4.1**). Darauf aufbauend wurde eine Methodik zur Schätzung der Investitions- und Betriebskosten in beiden Szenarien erarbeitet. Dies erfolgte in einem iterativen Prozess, in dem die Szenarien über Annahmen und relevante Kostenblöcke geschärft und auf Basis verfügbarer Daten ein Schätzvorgehen erarbeitet wurde (vgl. **Kapitel 4.2**). Abschließend erfolgte eine Schätzung der Kostenentwicklung in den Szenarien und eine Quantifizierung der gesamthaften finanziellen Vorteile einer Justizcloud. Ergänzend wurden zusätzliche Mehrwerte identifiziert, die mit einer bundeseinheitlichen Justizcloud realisiert werden könnten, wie z. B. einfaches Teilen

statt Versenden von Daten (vgl. **Kapitel 2.2.4.2**). Diese wurden nicht quantifiziert, sollten aber als Zusatzmehrwerte ergänzend zu den finanziellen Vorteilen einer Justizcloud berücksichtigt werden.

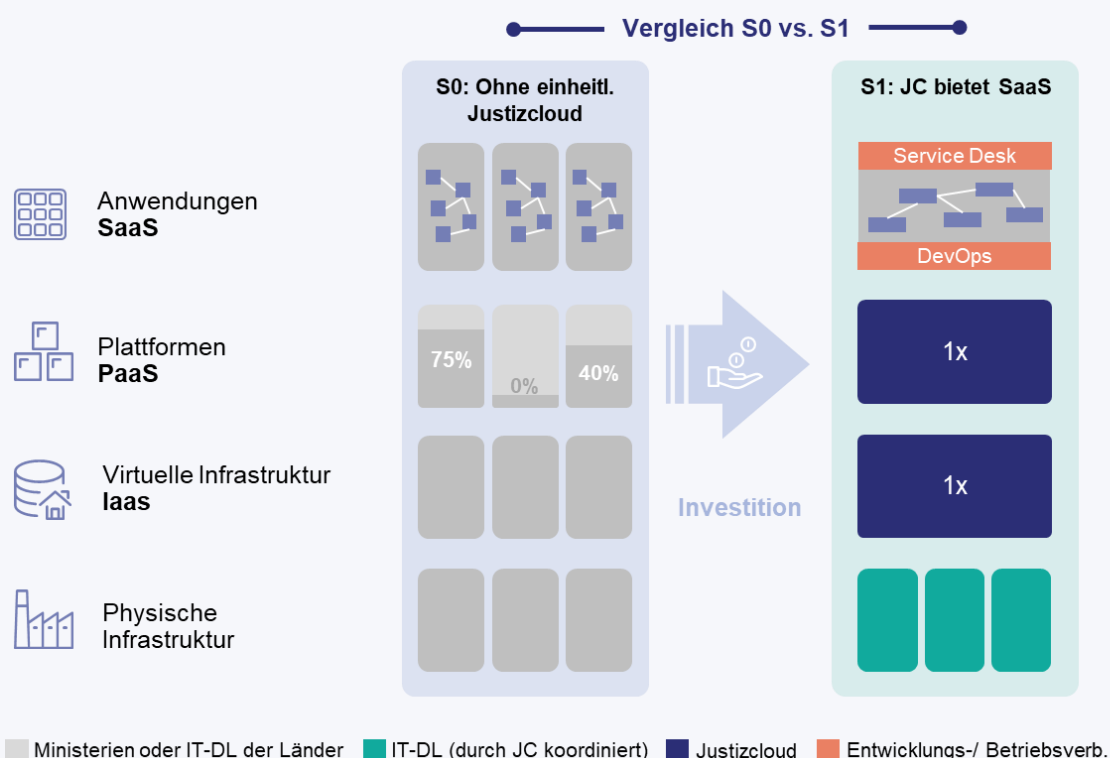
4.1 Szenarioentwicklung und Annahmen

4.1.1 Szenarioentwicklung

Die Wirtschaftlichkeitsbetrachtung soll zeigen, dass sich eine einmalige Investition in die Justizcloud durch erwartete jährliche Betriebseinsparungen amortisiert. Dazu wurden zwei Szenarien für einen Betrieb der Cloud-Anwendungen der Justiz definiert und dafür die jährlichen Betriebskosten geschätzt. Zudem wurden die erforderlichen Investitionen in eine Justizcloud quantifiziert. Die Justizcloud ist wirtschaftlich, wenn die Einsparungen durch eine Justizcloud in einem vertretbaren Zeithorizont die Investitionen übersteigen.

Zunächst wurden dazu Szenarien eines Betriebs der Cloud-Anwendungen der Justiz ohne bundeseinheitliche Justizcloud (Szenario 0) sowie mit Justizcloud (Szenario 1) konkretisiert. Die Szenarien sind in **Abbildung 85** dargestellt und werden nachfolgend beschrieben.

Abbildung 85 | Cloud-Anwendungsbetrieb mit und ohne bundeseinheitliche Justizcloud



Beschreibung Szenario 0: Ohne einheitliche Justizcloud

Die Ist-Analyse hat ergeben, dass die Bestandsanwendungen der Justiz inkl. physischer als auch virtualisierter Infrastruktur (Rechner, Speicher und Netzwerk) sowie Plattformkomponenten (z. B. Datenbanken) und Anwendungen in jedem Land bzw. Bundesgericht betrieben werden. Das bedeutet, dass für die Länder mind. 13 IT-Betriebe (vier Länder betreiben bei Dataport) und für die Bundesgerichte sechs IT-Betriebe bestehen. Daher fielen für den Betrieb der Justizanwendungen auch in jedem IT-Betrieb Kosten für physische und virtualisierte Infrastruktur, für die Container-Plattform sowie im technischen und fachlichen Anwendungsbetrieb an.

Die Ist-Analyse hat auch ergeben, dass durch die Entwicklung moderner, Cloud-fähiger Fachverfahren wie *GeFa* und *AuRegis* ein akuter Bedarf in der Justiz besteht, diese Anwendungen in Zukunft auch betreiben zu können. Dafür bauen viele IT-Dienstleister aktuell Cloud-Plattformen auf und bereiten sich darauf vor, zusätzlich zu bestehenden Infrastrukturen, Plattformen und Anwendungen, in Zukunft eine Cloud-/ bzw. Container-Plattform für die neuen Fachverfahren zu betreiben. Somit besteht der Bedarf in allen Ländern in neue Betriebsfähigkeiten zu investieren. Zudem würden in Zukunft, ohne den Aufbau einer bundeseinheitlichen Justizcloud, in jedem Land laufende Kosten für den Betrieb der neuen Cloud-fähigen Fachverfahren anfallen. Diese sind ggf. bei Archetyp 2 Ländern durch Synergien geringer. Dieses Szenario wurde im Rahmen der Wirtschaftlichkeitsbetrachtung Szenario 0 (S0) genannt.

Beschreibung Szenario 1: Justizcloud bietet SaaS

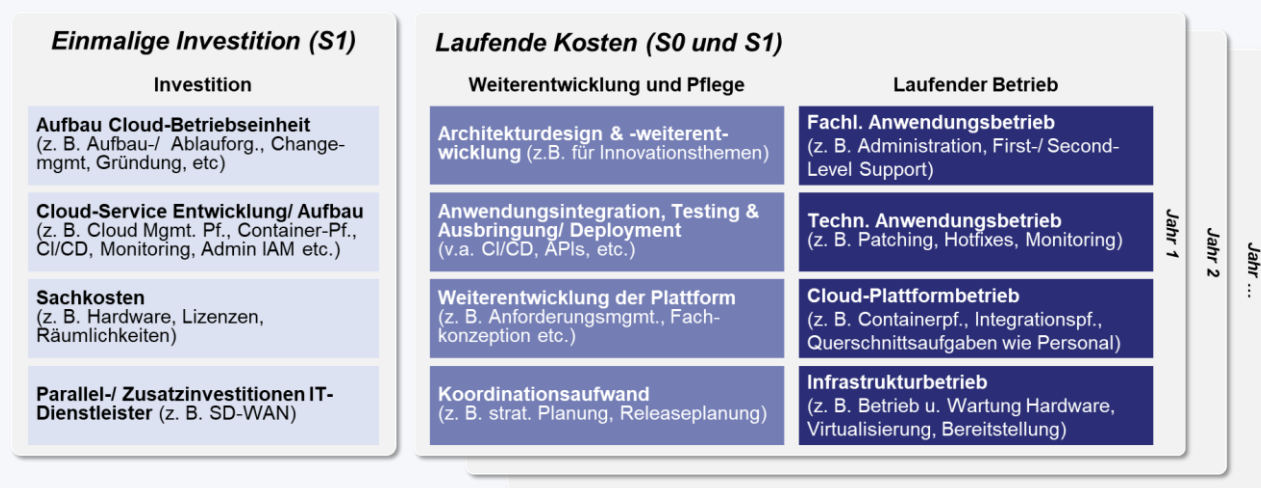
Um dem zu begegnen, wurde im Rahmen der Machbarkeitsuntersuchung einer bundeseinheitlichen Justizcloud ein Zielbild für eine Alternative zum Betrieb der modernen Cloud-fähigen Fachverfahren entwickelt. Das Zielbild sieht dabei vor, dass der Betrieb der Cloud-Anwendungen der Justiz nicht pro Land, sondern stattdessen einheitlich, d.h. auf einer einheitlichen Plattform sowie einer einheitlichen virtuellen Infrastruktur, basierend auf der physischen Infrastruktur der Länder, erfolgt. Dabei würden die Kosten für den Betrieb der virtuellen Infrastruktur, der Plattform sowie der Anwendungen nur ein Mal anfallen. Zudem würden durch einheitliche CI/CD-Prozesse und Standardisierung die Entwicklung- und Ausbringung von Software deutlich einfacher, da die hohen Integrations- und Anpassungsaufwände auf heterogene Anwendungsgefüge und Infrastruktur aller Länder (vgl. **Kapitel 2**) wegfallen würden. Auch die Fähigkeiten zum Betrieb von Cloud-Verfahren würden nurmehr einmal statt n-Mal pro Land aufgebaut werden müssen.

Gleichwohl ist zu erwarten, dass der Betrieb von Cloud-Infrastruktur, -Plattform und -Anwendungen für die gesamte Justiz teurer wäre als für ein einzelnes Land. Und auch der Aufbau der Justizcloud wäre komplexer und umfangreicher als der Aufbau einer lokalen Cloud-Umgebung. Das Szenario eines Aufbaus und zukünftigen Betriebs der Cloud-Anwendungen der Justiz auf einer bundeseinheitlichen Justizcloud wurde Szenario 1 (S1) genannt.

4.1.2 Annahmen zu Kostenblöcken

Um die Szenarien und die laufenden Betriebs- und Investitionskosten zu errechnen, wurde ein Modell der Kostenblöcke erstellt, die im Cloud-Betrieb sowie zum Aufbau einer Justizcloud anfallen. Die jährlichen Kosten wurden dabei in laufende Betriebskosten sowie regelmäßig anfallende Kosten für Weiterentwicklung und Pflege unterteilt (vgl. **Kapitel 2.2.1.1**).

Abbildung 86 | Übersicht relevanter Kostenblöcke in den Szenarien



Laufende Betriebskosten: Die jährlich anfallenden Kosten für Szenario 0 und Szenario 1 ergeben sich aus Aufwänden für den Betrieb von Cloud-Anwendungen entlang des Cloud-Stack. Dazu gehören der Betrieb von Infrastruktur (physisch und virtuell), der Cloud-Plattform sowie der Anwendungen selbst (technischer und fachlicher Anwendungsbetrieb). Der Infrastrukturbetrieb umfasst dabei sowohl Hardware wie Rechner, Speicher und Netzwerk und deren Wartung sowie Aufwände für die Virtualisierung und Bereitstellung dieser Infrastruktur als virtuelle Maschinen. Der Cloud-Plattformbetrieb umfasst die Kosten für den Betrieb der verschiedenen Plattformkomponenten wie Integrations- oder Container-Plattform. Der technische Anwendungsbetrieb verantwortet das technische Monitoring von

Anwendungen im laufenden Betrieb sowie der Container in denen Anwendungen laufen. Auch der sog. Third-Level Support bei technischen Problemen (z. B. Hot-Fixes, Backup und Recovery) wird vom technischen Anwendungsbetrieb übernommen. Der fachliche Betrieb verantwortet die fachliche Administration der Anwendungen, vergibt bspw. Berechtigungen, schaltet Nutzer frei und übernimmt den First- und Second-Level-Support. Die laufenden Betriebskosten ergeben sich auf allen Ebenen insb. durch Personalkosten (für internes und externes Personal) sowie Sachkosten für z. B. Hardware und Lizenzkosten für Software.

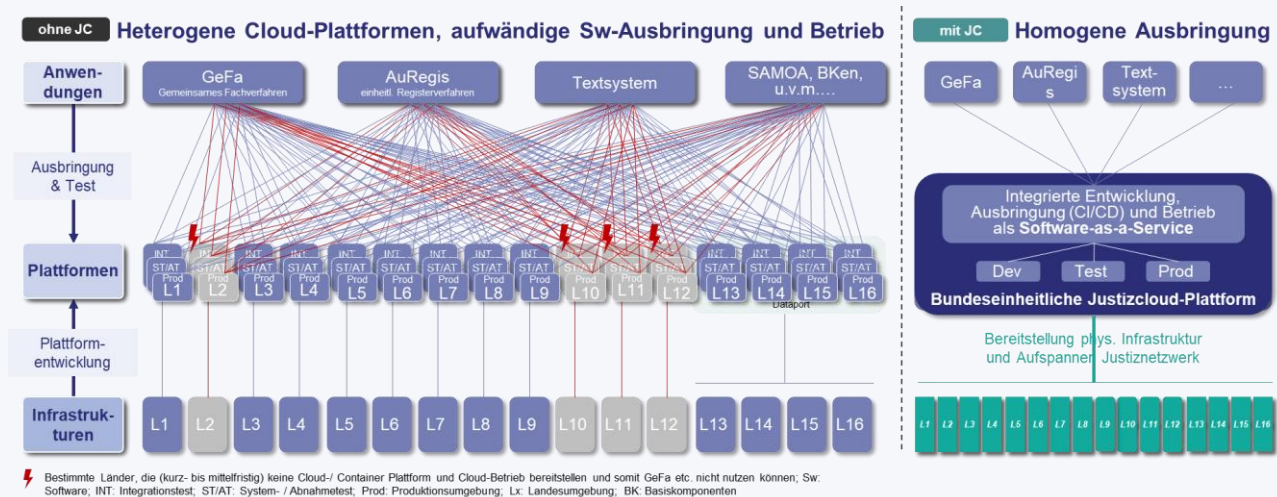
Eine Quantifizierung der Aufwände für den laufenden Betrieb erfolgt in **Kapitel 4.2.2**.

Weiterentwicklung und Pflege: Neben der Sicherstellung des laufenden Betriebs, fallen auch laufende Kosten für die Weiterentwicklung und Pflege von Anwendungen an. Die Ist-Analyse hat ergeben, dass viele Anwendungen der Justiz konstant weiterentwickelt werden und jährlich zwei Updates und Releases erfolgen. Gleichzeitig müssen auch die IT-Plattformen in allen Ländern weiterentwickelt werden, wie aktuell bspw. durch den Aufbau von Container-Plattformen in allen Ländern für den Betrieb von *GeFa* und *AuRegis*. Die Aufwände zur Weiterentwicklung und Pflege von Plattform und Anwendungen wurden in vier Kostenblöcke unterteilt. Der Kostenblock Architekturdesign/ -weiterentwicklung bündelt alle fachlichen Aufgaben zur Definition neuer Anforderungen an Anwendungen und Plattformen sowie die Entwicklung technischer Zielbilder. Wenn Anforderungen definiert sind, müssen diese durch die IT-Dienstleister (bei Plattformen) oder die Entwicklungsverbünde (bei Anwendungen) umgesetzt werden. Dabei fallen Aufwände für Integration, Testing und Ausbringung an. Zudem ist bei Bund-Länder-übergreifenden Vorhaben wie der gemeinsamen Entwicklung von Verfahren oder der Justizcloud ein Koordinationsaufwand, z. B. für die strategische Planung oder die Abstimmung von Releaseplänen, zu berücksichtigen. Der Aufwand für Weiterentwicklung und Pflege wird maßgeblich in Personalkosten geschätzt.

Der Unterschied der Aufwände in Weiterentwicklung und Pflege in S0 und S1 wird in **Kapitel 4.2.3** dargestellt. Dabei wird für S0 angenommen, dass für die Ausbringung von Cloud-fähigen Fachverfahren wie *GeFa*, *AuRegis* und zukünftig weiteren Anwendungen wie Textsystemen, SAMOA etc. zunächst eigene Plattformumgebungen in jedem Land aufgebaut werden müssen. Die Ausbringung jeder Anwendung erfolgt anschließend pro Land (vgl. **Abbildung 87**). Im ersten Schritt erfolgt dabei die Ausbringung in eine Integrationsumgebung (INT). Nach erfolgreichen Integrationstests erfolgt die Ausbringung in eine Testumgebung für System- und Abnahmetests (ST/AT). Letztlich erfolgt die Ausbringung auf einer Produktivumgebung je Land. Für jeden Schritt fallen dabei in jedem Land Personalaufwände an.

Zu berücksichtigen ist auch, dass aufgrund der Heterogenität der Integrationsanforderungen je Land die Integrationstests und v. a. auch erforderliche Anpassungen durch die Entwicklungsverbünde komplexer sind als in Szenario 1.

Abbildung 87 | Software-Ausbringungsmodelle in den Szenarien S0 vs. S1



Für S1 muss die Integration der Verfahren nur einmal erfolgen, da ein einheitliches Cloud-Anwendungsgefüge der Justiz betrieben wird. Zudem wird angenommen, dass durch die einheitliche Plattform schon die Entwicklung in einer produktionsnahen Umgebung auf der Justizcloud erfolgt. Integrationstests müssen somit nur einmal erfolgen und können schon während der Entwicklung durchgeführt werden. Durch moderne CI/CD können aus der Entwicklungsumgebung auch die System- und Abnahmetests teilweise automatisiert erfolgen. Der gesamte CI/CD-Prozess, von der Entwicklung, über Test bis zur Ausbringung, ist also einheitlich und somit schneller und effizienter. Die Quantifizierung der Aufwände für Weiterentwicklung und Pflege erfolgt in **Kapitel 4.2.3**.

Investitionskosten: Die Investitionskosten fassen alle Kosten zusammen, die für den Aufbau der Justizcloud-Plattform sowie der Justizcloud-Einheit gemäß des Zielbilds erforderlich sind. Für den Aufbau der Einheit sind dabei bspw. Kosten für die Projektsteuerung, das Design der Aufbau- und Ablauforganisation, Changemanagement und die Kosten für die Gründung der Justizcloud-Einheit erforderlich. Für die Plattform müssen die verschiedenen Plattformdienste aufgebaut und miteinander integriert werden. Zudem ist der Aufbau des gemeinsamen Justiznetzwerks zwischen den IT-Dienstleistern zur Provisionierung der physischen Infrastruktur erforderlich. Dazu kommen Sachkosten in Form von Hardware (z. B. PC

der Mitarbeitenden), Lizenzkosten, Gebäudekosten und bspw. die virtualisierte Infrastruktur für den Aufbau der Plattform. Die Quantifizierung der Investition in die Justizcloud erfolgt in **Kapitel 4.2.4.**

4.1.3 Annahmen zur Cloud-Plattform

Um die Investitions- und Betriebskosten für die Plattform zu schätzen, mussten einige Annahmen zum Umfang der Plattform getroffen werden (vgl. **Abbildung 88**). In der Wirtschaftlichkeitsbetrachtung wurde der Betrachtungsrahmen auf den Teil des Zielbilds beschränkt, der für den Betrieb der neuen Cloud-fähigen Verfahren der Justiz, *GeFa* und *AuRegis*, und damit für die erste Ausbaustufe der Justizcloud, erforderlich ist. Auf Ebene der Infrastruktur gehört dazu das gemeinsame Justiznetzwerk inkl. Provisionierung virtueller Infrastruktur für die Justizcloud. Auf der Plattformebene sind in der ersten Ausbaustufe eine Container-Plattform, ein Admin-IAM, eine Integrations-Plattform sowie ein Logging und Monitoring-System erforderlich. Darauf wird das Cloud-Anwendungsgefüge betrieben, für das im folgenden Kapitel Annahmen getroffen werden. Zudem ist der Entwicklerarbeitsplatz zur bundeseinheitlichen Entwicklung-, Test-, Ausbringung- und Betrieb via CI/CD ein zentrales Element der Plattform.

Nicht im Betrachtungsrahmen inbegriffen ist die externe Domäne. Diese wird aktuell bereits in einem Land betrieben und es sind insgesamt geringere Kosteneffekte zwischen S0 und S1 im Vergleich zur internen Domäne zu erwarten. Weiterhin ist der Betrieb der Bestandsanwendungen der Justiz sowie eine notwendige Integration von Cloud-Verfahren mit lokalen Legacy-Systemen nicht Teil der Betrachtung, da diese Kosten unabhängig von der Entscheidung für oder gegen eine Justizcloud anfallen. Sowohl in Szenario S0 als auch in S1 ist eine Integration neuer Cloud-fähiger Verfahren mit bestehenden nicht Cloud-fähigen Verfahren notwendig (z. B. *GeFa* mit *eAkten*). Die Kosten sind daher in Szenario 0 und Szenario 1 gleich und werden in der Wirtschaftlichkeitsbetrachtung nicht betrachtet. Zuletzt ist auch die Nutzung kommerzieller Public Cloud-Angebote nicht im Betrachtungsrahmen, da diese für die erste Ausbaustufe der Justizcloud nicht vorgesehen sind.

Durch die neuen Cloud-fähigen Verfahren der Justiz wird nicht nur in der Justizcloud, sondern auch in jedem Land der Aufbau und Betrieb einer Private Cloud-Plattform erforderlich. Daher werden die Betriebskosten für Container-, Integrations- sowie Logging und Monitoring-Plattformen sowohl in S0 als auch S1 berechnet. Ein Admin-IAM besteht in den Ländern bereits und ein SD-Wan wäre in S0 nicht erforderlich. Daher sind diese Komponenten nur in S1 zu berechnen.

Abbildung 88 | Komponenten der Cloud-Plattform in S0 und S1

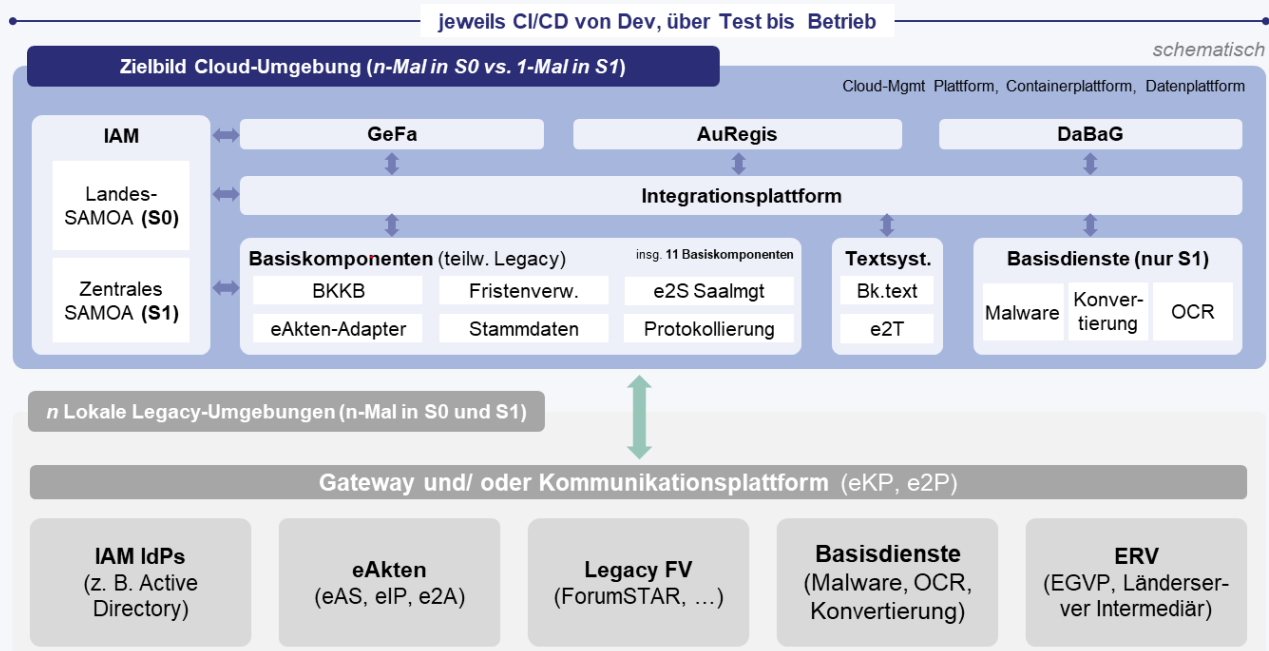


4.1.4 Annahmen zur Cloud-Anwendungslandschaft

Zur Schätzung der Kosten im Anwendungsbetrieb mussten Annahmen getroffen werden, welche Anwendungen auf der Justizcloud (S1) sowie in den Ländern (S0) als Teil des Cloud-Anwendungsgefüges betrachtet werden (vgl. **Abbildung 89**). Dabei ist wichtig, dass Verfahren wie *GeFa* und *AuRegis* nicht autark sind, sondern im Zusammenspiel mit vielen Basiskomponenten (z. B. *BKKB*) sowie einem Cloud-fähigen IAM (*SAmOA*) bzw. Berechtigungsmanagement (*bk.bv*) betrieben werden müssen. Für jede Anwendung sind in S1 oder S0 zukünftig sowohl technische als auch fachliche Betriebsfähigkeiten aufzubauen.

In der Wirtschaftlichkeitsbetrachtung wurde angenommen, dass sowohl *GeFa* als auch *AuRegis* Teil des Cloud-Anwendungsgefüges sind. Zudem ist *dabag* im aktuellen Entwicklungsstand noch nicht Cloud-ready, wird dies aber voraussichtlich zukünftig werden. Als IAM wird angenommen, dass in jedem Land (S0) *SAmOA* für die Authentisierung genutzt wird. In der Justizcloud (S1) würde eine „zentrales *SAmOA*“, also eine Weiterentwicklung inkl. Möglichkeiten der Föderation von Identitäten und Delegation von Admin-Rechten, benötigt (vgl. **Kapitel 3.4.6**). Darüber hinaus sind insgesamt mind. elf Basiskomponenten erforderlich, wie *BKKB*, Fristenverwaltung, die *eAkten-Adapter* etc. Als Textsysteme sind sowohl *bk.text* als auch *e2T* betrachtet worden, da beide Textanwendungen aktuell in verschiedenen Ländern weiterentwickelt werden (z. B. *e2T* in Niedersachsen und *bk.text* in Bayern). Zuletzt sind einige Basisdienste nur in der Justizcloud (S1) aufzubauen und neu zu betreiben. Diese Basisdienste werden in den Ländern sowohl mit (S0) als auch ohne Justizcloud (S1) für die Bestandsverfahren betrieben und sind daher nicht eingerechnet.

Abbildung 89 | Mittelfristig angenommenes Cloud-Anwendungsgefüge in S0 und S1



Die bestehenden Legacy-Umgebungen der Länder werden nicht in der Wirtschaftlichkeitsbetrachtung eingerechnet, da sich der Legacy-Betrieb durch den „Greenfield“-Ansatz in S0 und S1 gleich entwickeln würde. Nicht Cloud-fähige Verfahren, für die es noch keine Nachfolger gibt, würden weiter betrieben werden (z. B. *eAkten*) und Verfahren, für die es Nachfolger gibt (z. B. Fachverfahren wie *ForumSTAR*), würden voraussichtlich mit der Einführung von *GeFa* abgeschaltet. Dabei ist es unerheblich, ob *GeFa* pro Land oder in der Justizcloud ausgerollt würde. Die notwendige Integration mit nicht Cloud-fähigen Legacy-Verfahren der Länder würde ebenfalls sowohl in S0 als auch in S1 durchgeführt werden.

4.2 Datenerhebung und Schätzung

Auf Basis der Szenarien, Annahmen und definierten Kostenblöcke wurden gemeinsam mit Vertretern von Bund und Ländern Daten erhoben und eine Quantifizierung bzw. Schätzung der Kostenblöcke vorgenommen. Dazu wurden für die Kostenblöcke Betrieb, Weiterentwicklung und Pflege sowie Investition (vgl. **Kapitel 4.2.2, 4.2.3, 4.2.4**) zunächst Personal- und Sachaufwände erarbeitet. Anschließend wurden die Personal- und Sachaufwände mit durchschnittlichen Kosten für Personal (intern und extern) sowie Sachkosten (Hard- und Software) verrechnet, um die Gesamtkosten in Euro zu erhalten.

Die Quantifizierung erfolgte, soweit möglich, auf Basis erhobener Daten der Länder. Kostenblöcke, für die Daten vorhanden waren, wurden auf Basis dieser Daten quantifiziert (z. B. durchschnittliche Kosten einer virtuellen Maschine). Bei Kostenblöcken, für die noch keine Daten vorhanden sind (z. B. Personalbedarf für den Fachbetrieb von *GeFa*), wurden annahmebasiert Schätzwerte erarbeitet. Dabei wurden die Bedarfe konservativ geschätzt.

Für die Personal- sowie Sachkosten wurden ebenfalls Daten erhoben, teils mit den Ländern teils durch Recherche, sowie bewährte Schätzmethoden, wie z. B. Berechnungsmethodik des *BMF* für die Personalkosten im öffentlichen Sektor, herangezogen.

4.2.1 Schätzung Personal- und Sachkosten

Personalkosten

Personal und Sachkosten sind die wesentlichen Kostentreiber beim Aufbau einer Cloud-Infrastruktur sowie im laufenden Betrieb von Infrastruktur, Plattform und Anwendungen.

Tabelle 8 | Übersicht Sach- und Personalkosten

Personalkosten	
Interne VZÄ (pro Jahr)	~100.000€
Externe VZÄ (pro Jahr)	~260.000€
Arbeitstage (pro Jahr)	202
Sachkosten	
SD WAN Investition (Einmalig)	480.000€
SD WAN Betrieb (pro Jahr)	250.000€
Virtuelle Maschine (pro Jahr) (16 Kerne/ 64GB Ram/ 300 GB Speicher)	10.800€
Lizenzkosten inkl. USt. (pro Jahr)	~2 M€

Sowohl während der Aufbau- und Investitionsphase der Justizcloud (S1) als auch im laufenden Betrieb (S0 und S1) beschäftigt die Justiz internes und externes Personal. Der Personalbedarf wird dabei im Folgenden in Jahres-Vollzeitäquivalenten (VZÄ) ausgedrückt.

Die Schätzung der internen VZÄ wurde dabei auf Basis einer [Berechnungsmethodik des BMF](#) vorgenommen. Dabei wurde ange-

nommen, dass keine Beamten, sondern insb. Angestellte, in der Justiz-IT arbeiten. Anschließend wurden die Tarifgehälter entsprechend einer typischen Zusammensetzung von Gehaltsstufen zu einem Durchschnittssatz verrechnet. Im Ergebnis wurde für interne VZÄ ein Durchschnittssatz von 100.000 € jährlich errechnet.

Zudem wurde berechnet, dass eine VZÄ der durchschnittlichen Arbeitsleistung von 202 Arbeitstagen entspricht (berücksichtigt sind dabei 104 Wochenendtage, 9 Feiertage, 20 Krankheitstage und 30 Urlaubstage). Ein VZÄ entspricht dabei einer Vollzeitstelle, kann aber auch durch zwei oder mehr Teilzeitstellen ausgefüllt werden.

Für externes Personal wurden ebenfalls 202 Arbeitstage pro Jahr angenommen und auf Basis bestehender Rahmenverträge und einem typischen Senioritäten-Mix (Stufe 1: Partner/ Senior Architekt, Stufe 2: Manager/ Junior Architekt/ Senior Entwickler, Stufe 3: Consultant/ Junior Entwickler) ein durchschnittlicher Tagessatz von 1.080 € (1285 € inkl. USt.) errechnet. Daraus ergeben sich Jahreskosten von ca. 260.000 € pro Jahr für externe VZÄ.

Die durchschnittlichen Personalkosten pro VZÄ sind in Szenario 0 und Szenario 1 identisch.

Sachkosten

Die Sachkosten für den IT-Betrieb ergeben sich aus Infrastrukturkosten für den Betrieb von Plattform und Anwendungen sowie Lizenzen für benötigte Software. Dieses Kosten fallen sowohl in S0 als auch S1 an. Dazu kommen nur in S1 Zusatzkosten für den Aufbau und laufenden Betrieb des gemeinsamen Justiznetzwerks (SD-WAN).

Die Infrastrukturkosten ergeben sich aus dem Betrieb der Hardware (insb. Speicher und Rechner). Diese werden heutzutage bei den IT-Dienstleistern virtualisiert und als virtuelle Maschinen für Plattform- und Anwendungsbetrieb provisioniert. Für die Berechnung wurde angenommen, dass die Kosten für eine virtuelle Maschine die Kosten für die physische Infrastruktur sowie für die Virtualisierung und Provisionierung beinhalten. Für eine standardisierte, marktübliche virtuelle Maschine mit 16 Kernen, 300 GB Speicher und 64 GB Ram wurden Jahreskosten von ca. 10.800 € pro VM errechnet. Dieser Wert wurde von Vertretern der IT-Dienstleister im Rahmen der Wirtschaftlichkeitsbetrachtung bestätigt.

Für den Betrieb einer Cloud-Plattform sind zudem umfassende Softwareprodukte erforderlich, für die Lizenzen zu entrichten sind. Dabei wurden in der Wirtschaftlichkeitsbetrachtung zehn verschiedenen Softwareprodukte erhoben: SIEM, Code Repository mit CI/CD, Artefakt Repository, Integrationsplattform, Event Hub, Anforderungsmanagement wie Jira, Ticketing-Tool, Container-Plattform, Service Mesh sowie eine Cloud Management Plattform. Auf Basis einer Recherche mit etablierten Anbietern dieser Produkte sowie Annahmen für die Lizenzmodelle (z. B. erwartete Größe der Container-Cluster) wurde ein jährlicher Gesamtbetrag von ca. 2 M€ für die Justizcloud errechnet (S1). In den Ländern wären in S0 aufgrund der etwas einfacheren Ausgestaltung der Cloud-Plattform einige Tools nicht erforderlich, wie z. B. eine Cloud Management Plattform. Für die Länder wurden zudem je nach Größe des Landes Annahmen für die Lizenzmodelle getroffen. Bspw. benötigt ein kleineres Land eine weniger umfangreiche Container-Plattform und zahlt daher auch weniger Lizenzgebühren. Die jährlichen Lizenzaufwände pro Land sind in **Tabelle 8** aufgeführt.

Zuletzt sind für S1 die Kosten für das Justiznetz berechnet worden. Dazu muss zunächst neue Hardware zur Absicherung des Justiznetzes in den Ländern beschafft werden. Anschließend fallen für den Betrieb des Netzwerks Kosten in jedem Land an. Die Gesamtkosten für die Beschaffung beläuft sich für alle Länder und die Justizcloud auf einmalig 480.000 €. Anschließend kostet der Betrieb 250.000 € pro Jahr. Die individuellen Personalkosten der IT-Dienstleister zur Anbindung an das Justiznetz sind nicht enthalten.

4.2.2 Schätzung Betriebskosten

Die Betriebskosten umfassen die jährlichen Kosten für den Betrieb der Cloud-Plattform sowie des Anwendungsgefüges. Die Betriebskosten ergeben sich aus übergreifenden Funktionen des Cloud-Betriebs, dem Plattformbetrieb, dem technischen und fachlichen Anwendungsbetrieb sowie jährlichen Sachkosten. Die geschätzten Gesamtaufwände für den Betrieb in S0 und S1 sind in **Tabelle 9** dargestellt.

Tabelle 9 | Jährliche Kosten im laufenden Betrieb (Aggregierte Sicht)

	Justizcloud (S1)	Alle Länder (S0)
Personalkosten pro Jahr	18,2 M€	60,9 M€
Übergreifende Funktionen	24	69
Plattformbetrieb	28	97
Anwendungsbetrieb (Fachlich/Technisch)	43 / 34	174 / 88,5
GeFa	12 / 8	54 / 14
AuRegis	4 / 3	26 / 6,5
dabag	4 / 3	26 / 6,5
Weitere Anwendungen (ca. 12)	23 / 20	68 / 61,5
Sachkosten pro Jahr	3,6 M€	21,2 M€
Virtuelle Maschinen	1,6 M€	8,6 M€
Lizenzkosten	1,7 M€	12,6 M€
Netzwerk/ SD-WAN	0,3 M€	-
Betriebskosten JC (Übergr. Funk., Plattform, Sachk.)	10,5 M€	
Betriebskosten Entw. Verbünde (Anw. Betr.)	11,3 M€	
Gesamtkosten	21,8 M€	82,1 M€
Einsparpotenzial pro Jahr	60,3 M€	

Kosten in Millionen € (M€); Personalaufwände in Vollzeitäquivalenten (VZÄ) aufgeteilt nach fachlichem und technischem Anwendungsbetrieb; Anteil interner Mitarbeitender: Übergreifende Funktionen = 90%, Fachlicher Anwendungsbetrieb = 90%, Technischer Betrieb = 50%, Plattformbetrieb = 75%; Tagessätze pro Jahr: Intern = ~100.000€; Extern: ~260.000€

Die übergreifenden Funktionen für den Cloud-Betrieb entsprechen den in **Kapitel 3.6.4** beschriebenen erforderlichen Rollen für eine Justizcloud. Dazu gehören bspw. die Leitung, ein Strategiebereich, Architekturmanagement, IT-Sicherheit, das Cloudmanagement inkl. Beschaffung, Lieferantenmanagement, Finanzen, Personal etc. Für S1 wird geschätzt, dass 24 VZÄ für diese Funktionen erforderlich sind. Auch in den Ländern sind für einen Cloud-Betrieb neue Funktionen aufzubauen, bspw. im Bereich Anforderungsmanagement, Cloud-Architektur, Cloud-Sicherheit sowie in den Bereichen Beschaffung, Finanzen, Personal und Servicemanagement. Insgesamt wurde geschätzt, dass in jedem Land 5,3 VZÄ zusätzlich erforderlich sind. Insgesamt sind in S0 damit 69 VZÄ im Bereich übergreifender Funktionen für den Betrieb lokaler Cloud-Plattformen erforderlich.

Beim Plattformbetrieb sind für alle Plattform-Dienste wie Container- und Cloud Management-Plattform, CI/CD sowie Logging- und Monitoring zusätzliche VZÄ für den Betrieb erforderlich. In S1 wird davon ausgegangen, dass 28 VZÄ pro Jahr für den Plattformbetrieb erforderlich sind. Diese Personen übernehmen bspw. Provisionierung, Monitoring/ Logging, Kundenbetreuung, Problembehebung usw. In S0 wird davon ausgegangen, dass pro Land 7 VZÄ (13 VZÄ bei Dataport) im Plattformbetrieb neu für die Justiz aufgebaut werden müssen. Insgesamt ergibt sich dadurch ein Personalbedarf pro Jahr von 97 VZÄ.

Im Anwendungsbetrieb wird zwischen technischem und fachlichem Anwendungsbetrieb unterschieden. Für den Betrieb des gesamten Cloud-Anwendungsgefüges wurden in S1 ein Personalbedarf von 43 VZÄ im fachlichen und 34 VZÄ im technischen Betrieb geschätzt. Für S0 wurde pro Land ein Wert von 13 VZÄ im fachlichen und 6,5 VZÄ im technischen Betrieb geschätzt (18 VZÄ bzw. 10,5 VZÄ für Dataport). Diese Werte sind für den Betrieb von 15 Verfahren sehr konservativ angesetzt. Insgesamt ergibt sich in S0 ein Wert von 174 VZÄ im fachlichen und 88,5 VZÄ im technischen Betrieb für alle Länder zusammen.

Im Bereich der Sachkosten wurde für S1 ein jährlicher Bedarf von 110 VMs angenommen sowie 1,7 M€ Lizenzkosten (ohne USt.) und 0,3 M€ jährlicher Betriebskosten für das SD-WAN. Insgesamt ergeben sich damit Sachaufwände von 3,6 M€ für S1. In S0 wurden die benötigten virtuellen Maschinen bzw. Lizenzkosten entsprechend der Größe des jeweiligen Landes angepasst, die genauen Werten sind in **Tabelle 9** aufgelistet. Damit ergeben sich geschätzte Sachkosten in S0 von 21,2 M€.

Insgesamt belaufen sich die jährlichen Betriebskosten in S1 damit auf 21,8 M€ und die Kosten in S0 auf 82,1 M€. Damit ermöglicht die Justizcloud jährliche **Einsparungen von 60,3 M€ pro Jahr** im laufenden Betrieb der Cloud-Verfahren und Cloud-Plattform.

Tabelle 10 | Jährliche Kosten im laufenden Betrieb (Detailsicht)

	S1	S0													
	JC	Länder	BE	Dataport	BB	TH	SN	RP	MV	BY	BW	NW	NI	HE	SL
Personalkosten (Intern 50%)	10,2 M€	33,7 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€	2,6 M€
Personalkosten (Extern 50%)	8 M€	27,7 M€	1,8 M€	5,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€	1,8 M€
Übergr. Funktionen	24	69	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3	5,3
Plattformbetrieb	28	97	7	13	7	7	7	7	7	7	7	7	7	7	7
Anwendungsbetrieb	77	262,5	19,5	28,5	19,5	19,5	19,5	19,5	19,5	19,5	19,5	19,5	19,5	19,5	19,5
GeFa	20	68	5	8	5	5	5	5	5	5	5	5	5	5	5
AuRegis	7	32,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5
dabag	7	32,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5
weitere Anwendungen (ca. 12)	43	129,5	9,5	15,5	9,5	9,5	9,5	9,5	9,5	9,5	9,5	9,5	9,5	9,5	9,5
Sachkosten Jahressicht	3,6 M€	21,2 M€	1,3 M€	3,8 M€	1,6 M€	1,2 M€	1,7 M€	1,3 M€	1,2 M€	1,4 M€	1,4 M€	1,9 M€	1,7 M€	1,3 M€	1,6 M€
Virtuelle Maschinen	1,6 M€	8,6 M€	0,7 M€	2,3 M€	1,1 M€	0,7 M€	1,1 M€	0,7 M€	0,7 M€	0,7 M€	0,7 M€	1,1 M€	1,1 M€	0,7 M€	1,1 M€
Lizenzkosten	1,7 M€	12,6 M€	0,6 M€	1,5 M€	0,5 M€	0,5 M€	0,6 M€	0,6 M€	0,5 M€	0,7 M€	0,7 M€	0,8 M€	0,6 M€	0,6 M€	0,5 M€
Netzwerk/ SD-WAN	0,3 M€	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Gesamtkosten	21,8 M€	82,1 M€													
Einsparpotenzial p. a.	60,3 M€														

Kosten in Millionen € (M€); Personalaufwände in Vollzeitäquivalenten (VZÄ) aufgeteilt nach fachlichem und technischem Anwendungsbetrieb; Anteil interner Mitarbeitender: Übergreifende Funktionen = 90%, Fachlicher Anwendungsbetrieb = 90%, Technischer Betrieb = 50%, Plattformbetrieb = 75%; Tagessätze pro Jahr: Intern = ~100.000€; Extern: ~260.000€

4.2.3 Schätzung Kosten für Weiterentwicklung und Pflege

Die Kosten für Weiterentwicklung- und Pflege wurden für Anwendungen sowie Plattformkomponenten getrennt geschätzt. Wie in **Kapitel 2.2.1.1** beschrieben, erfolgt der Ausbringungsprozess entlang der Integrations-, Test- sowie Produktionsumgebung. Zudem erfolgen verschiedene Tests wie Integrations-, Regressions-, Abnahme- sowie Performance-Tests. Im Falle von Fehlern in der Software kann in einigen Fällen auch eine komplexe Fehleranalyse sowie Überarbeitung der Software (Refactoring) durch den Entwicklungsverbund notwendig sein.

Für die Schätzung der Kosten der Ausbringung wurden zunächst die Personentage (PT) für die Ausbringung **einer komplexen Anwendung** entlang aller oben genannten Schritte geschätzt. Dabei wurde geschätzt, dass in der Justizcloud (S1) 93 Personentage benötigt werden. Dagegen wurde in den Ländern angenommen, dass pro Land etwa 19 PT (37 PT für Dataport) erforderlich sind. Für ein Land ist die Ausbringung annahmebasiert daher weniger aufwändig als in der Justizcloud. Insgesamt ist der Aufwand über alle Länder für die Ausbringung einer Anwendung allerdings mit 265 PT deutlich höher als in der Justizcloud. Anschließend wurde gemäß der Kosten pro Personentag (Kosten VZÄ/ Arbeitstage) ein durchschnittlicher Betrag für die Ausbringung einer Anwendung in der Justizcloud bzw. in allen Ländern errechnet. Eine komplexe Anwendung kostet dabei 74,4 M€ in der Justizcloud (S1) und 207,3 M€ in allen Ländern (S0). Bei einfachen Anwendungen bzw. einfachen Deployments (Major vs. Minor Updates) wurde von 25% der Kosten ausgegangen.

Insgesamt wurde davon ausgegangen, dass ca. sechs Deployments pro Jahr erreicht werden sollten, was eine Verbesserung von vier Deployments gegenüber den aktuellen Verfahren der Justiz bedeuten würde. Zudem wurde angenommen, dass fünf komplexe und zehn weniger komplexe Anwendungen gemeinsam gepflegt werden müssen (siehe Anwendungsbündel). Insgesamt wurden dabei ein Betrag für Weiterentwicklung und Change von Anwendungen von 3,3 M€ in der Justizcloud und 9,3 M€ in den Ländern errechnet.

Die erwarteten **Gesamteinsparungen pro Jahr für Weiterentwicklung und Pflege von Anwendungen** belaufen sich daher auf 6 M€ pro Jahr.

Tabelle 11 | Jährliche Kosten für Weiterentwicklung und Pflege

	Justizcloud (S1)	Länder (S0)
Weiterentwicklung und Pflege Anwendungen		
Personentage pro Deployment (für komplexe Anwendung)	93	265
Ausbringung (Integrations-/Test-/Prod.-Umgebung)	32	56
Testing (Integr.-, Regression-, Abnahme-, Performance-Tests)	50	165
Fehleranalyse/ Refactoring	11	44
∅ Gesamtkosten pro Deployment	74,4 k€	207,3 k€
Aufwand p. a. (komplexe Anwendungen)	2,2 M€	6,2 M€
Aufwand p. a. (einfache Anwendungen, 25% des Aufwands)	1,1 M€	3,1 M€
Gesamtkosten für 15 Anwendungen pro Jahr	3,3 M€	9,3 M€
Einsparpotenzial pro Jahr	6 M€	

Weiterentwicklung und Pflege Plattformdienste		
Personentage pro Deployment	92	351
Weiterentwicklung, Updates, Fehleranalyse	40	151
Ausbringung (Test- und Produktions-Umgebung)	24	94
Testing (Integr.-, Regression-, Performance-Tests)	28	106
∅ Gesamtkosten pro Deployment	65,3 k€	249,6 k€
Aufwand Deployment p. a. (einfache Anwendung)	2,4 M€	9 M€
Gesamtkosten für 6 Plattformdienste pro Jahr	2,4 M€	9 M€
Einsparpotenzial pro Jahr	6,6 M€	

Kosten in Mio. € (M€); Tagessätze pro Jahr: Intern = ~100.000€; Extern: ~260.000€; Anteil interner Mitarbeitender: Fachl. Anwendungsbetrieb = 90%, Techn. Betrieb = 50%, Plattformbetrieb = 75%, Entwicklungsverbund = 20%; Kosten errechnen sich anteilig aus eingesetzten Tagen fachlicher und technischer Anwendungsbetrieb, Entwicklungsverbund oder Plattformbetrieb)

Für die Plattformdienste ist das Vorgehen, abgesehen von einigen Anpassungen, analog zu den Anwendungen. Auch Plattformdienste müssen in einer Test- sowie Produktionsumgebung aufgebracht werden und anschließend umfassend getestet werden. Wichtig ist bei der Schätzung der Plattformdienste, dass die Justiz in einigen Ländern gemeinsame IT-Dienstleister mit der Verwaltung nutzt (vgl. Archetyp 3 in **Kapitel 2.2.2**). Hier entstehen dadurch hohe Synergien mit der Verwaltung für die Weiterentwicklung und Pflege von Plattformdiensten. Hier wurde angenommen, dass die Justiz nur 30% der Kosten für die Weiterentwicklung der Cloud-Plattform in diesen Ländern trägt. Im Umkehrschluss bedeutet dies aber auch, dass einige Länder, die über einen justizspezifischen IT-Dienstleister verfügen, die gesamten Cloud-Kosten und -Aufwände selbst tragen.

Für S1 wurde angenommen, dass die Ausbringung eines Plattform-Dienstes ca. 92 PT beansprucht. Aufgrund der geringeren Komplexität und der Synergien mit der Verwaltung, ist der Aufwand mit 14 PT in sieben Ländern deutlich geringer. Fünf Länder müssten ihre Plattform dagegen ohne Synergien mit der Verwaltung weiterentwickeln, dabei wird ein Wert von 46 PT pro Ausbringung geschätzt. Bei Dataport wird von 22 PT pro Ausbringung ausgegangen. Insgesamt wird pro Ausbringung über alle Länder von 351 PT ausgegangen.

Insgesamt wurde geschätzt, dass mit Container- und Integrationsplattform, CI/CD und Logging/ Monitoring sowie IAM und Admin-IAM sechs Plattformdienste gepflegt werden müssen und dazu sechs Deployments pro Jahr erforderlich sind. Verrechnet mit den durchschnittlichen Kostensätzen für einen Personentag belaufen sich die Gesamtkosten für die Pflege der Plattform auf 2,4 M€ in S1 und 9 M€ in S0.

Das jährliche Einsparpotenzial durch die Justizcloud bei **Weiterentwicklung- und Pflege der Plattform** beläuft sich damit auf 6.6 M€.

4.2.4 Schätzung Investitionskosten

Die Investitionskosten für die Justizcloud ergeben sich insb. aus dem Aufbau der Justizcloud-Einheit sowie dem Aufbau der Justizcloud-Plattform (vgl. **Kapitel 3.3.3 und 3.5.4**). Der Aufbau soll über sechs Jahre von 2025 bis 2030 erfolgen. Dafür ist ein Umsetzungsprogramm geplant, dessen genauer Aufbau und Ablauf noch ausgestaltet werden müsste. Die Schätzung der Investitionskosten erfolgte daher auf Basis von Erfahrungswerten vergangener Cloud-Transformationen und den Anforderungen des Zielbilds.

Der Aufbau der Cloud-Einheit umfasst alle rechtlich-organisatorischen und teilweise konzeptionelle fachliche und technische Aspekte. Für den Aufbau ist ein Aufbaustab vorgesehen und eine Programmsteuerung, inkl. strategischer Begleitung und Programmmanagement-Office (vgl. **Kapitel 3.6.6**). Der Kostenblock Gründung umfasst alle Aufgaben zur rechtlichen Prüfung und Durchführung der Gründung. Der Bereich Stakeholder-Kommunikation umfasst alle Aufgaben zur Einbindung des komplexen Stakeholder-Netzwerks wie Ministerien, IT-Dienstleister, Entwicklungsverbünde sowie teilweise Außenkommunikation (z. B. Pressearbeit, Einstellungskampagnen etc.) falls erforderlich. Im Bereich Aufbau- und Ablauforganisation erfolgt die operative Ausplanung und Umsetzung der Einheit sowie ihrer Prozesse. In der Umsetzung arbeitet dieser Arbeitsstrang eng mit einem Bereich für Change-Management und Befähigung zusammen, der methodisch und kommunikativ die Mitarbeitenden und Teams dabei unterstützt, z. B. neue agile Arbeitsweisen umzusetzen. Das

Team Architekturkonzeption übernimmt die technische Konzeption der Plattform inkl. Netzwerkkonzept. Der Arbeitsstrang IT-Sicherheit verantwortet z. B. das Grundschutzkonzept, den Ausbau eines Security Operation Center, Risikomanagement sowie die Sicherstellung einer BSI-Zertifizierung. Abschließend sind agile Rollen wie Release Train Engineers zur Koordination und Fachverantwortung für die Service-Entwicklung erforderlich. Ein Arbeitsstrang Beschaffung kümmert sich um die Einbindung der IT-Dienstleister und Beschaffung von Personal, Software sowie Hardware für den Aufbau. Insgesamt wird für den Aufbau der Einheit von einem **Personalbedarf von 121,5 VZÄ** über sechs Jahre ausgegangen.

Tabelle 12 | Investitionskosten für Szenario S1

	Justizcloud (S1)
Aufbau Cloud-Einheit (in VZÄ)	121,5
Aufbaustab + Programmsteuerung (inkl. Strategie, Governance, PMO etc.)	25
Gründung (inkl. Rechtliche Aspekte etc.)	12
(Stakeholder-)kommunikation	12
Aufbau- und Ablauforganisation (Design/ Umsetzung)	13
Changemanagement, Befähigung	11,5
Architekturkonzeption & Anforderungsmanagement	13
IT-Sicherheit (inkl. Grundschutz, SOC, Risikomanagement)	14
Agile Rollen (Release Train Engineers, Scrum Master)	14
Beschaffung (inkl. Vertrags- und Lieferantenmanagement.)	7
Serviceentwicklung (PaaS/ IaaS) (in VZÄ)	137
Cloud Management Plattform	10
Container-Plattform	36
Entwicklerarbeitsplatz (CI/CD)	17,5
Logging/ Monitoring (inkl. SIEM/SOC)	12,5
Integrationsplattform & Datenplattform	21,5
Zentrales IAM + Admin IAM (inkl. Föderation ADs)	7,5
Virtualisierung/ Netzwerkanbindung (in JC)	7
Personalkosten Gesamt (gem. Tagessätzen)	57,1 M€
Sachkosten	
Infrastruktur (110 VMs)	4,3 M€
SD-WAN	1,7 M€
Lizenzen	9,6 M€
Sachkosten Gesamt	15,5 M€
Investitionskosten Gesamt (+ 20% Puffer)	72,6 M€ (87,1)

Kosten in Millionen € (M€); Anteil interner Mitarbeitender: 25%; Tagessätze pro Jahr: Intern = ~100.000€; Extern: ~260.000€; SIEM: Security Incident & Event Monitoring; SOC: Security Operations Center; Die im Zielbild vorgesehene Transformation der Entwicklungsverbünde zu Betriebsverbünden ist in der Investitionsschätzung nicht enthalten.

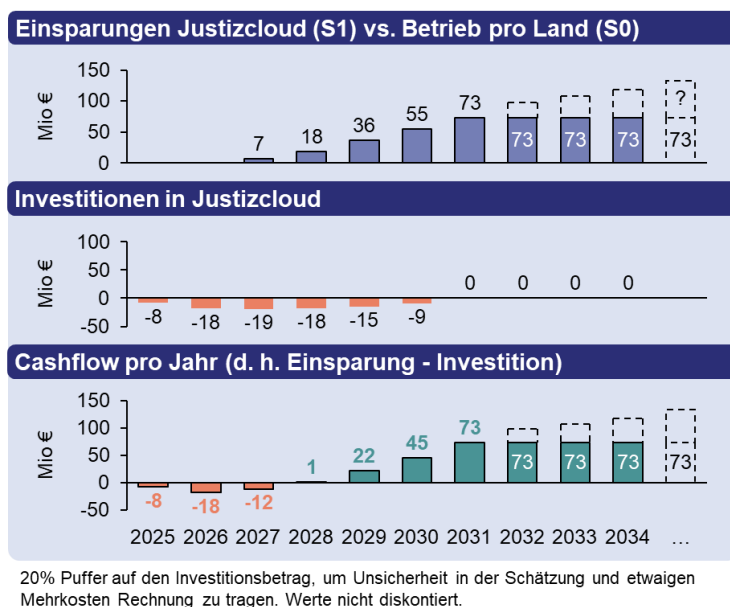
Die Service-Entwicklung verantwortet den Aufbau der technischen Plattform, d. h. der einzelnen Services sowie deren Integration und Provisionierung für die Leistungserbringung. Für jede der definierten Plattform-Komponenten sind dabei eigene Entwicklungsteams erforderlich. Insgesamt sind für die **Service-Entwicklung 137 VZÄ** vorgesehen.

Darüber hinaus sind auch während des Aufbaus bereits Sachkosten erforderlich. In der Spitze benötigt die Justizcloud 110 virtuelle Maschinen sowie Investitionen in das Justiznetz inkl. jährlicher Betriebskosten. Auch Lizenzkosten fallen bereits während der Aufbauphase an. Insgesamt werden **Sachaufwände von 15,5 M€** über sechs Jahre geschätzt.

Es wird angenommen, dass der Aufbau mit 25% internen und 75% externen Mitarbeitenden erfolgt. Insgesamt wird für den Aufbau der Justizcloud daher ein Investitionsaufwand von ca. 72,6 M€ erwartet. Zur Absicherung gegen Schätzunsicherheiten und unvorhergesehene Kostensteigerungen wurde ein Sicherheitszuschlag von 20% einkalkuliert, wodurch sich der geschätzte **Investitionsbetrag auf 87,1 M€** beläuft.

4.3 Ergebnisse und Bewertung

Abbildung 90 | Gesamtsicht Einsparungen und Investitionen (in Jahren)



Um den finanziellen Mehrwert der Justizcloud zu berechnen, wurde ein Zeithorizont von zehn Jahren (2025 – 2034) betrachtet. Dabei wird erwartet, dass der Aufbau der Justizcloud insgesamt sechs Jahre erfordert, aber bereits ab 2027 mit einem MVP erste produktive Anwendungen auf der Justizcloud betrieben werden können (vgl. **Kapitel 5.1**). Über einen Zeitraum von zehn Jahren wurden die geschätzten jährlichen Einsparungen im laufenden Betrieb sowie

Weiterentwicklung und Pflege aufsummiert und den notwendigen Investitionen für die Justizcloud gegenübergestellt. (vgl. **Abbildung 90**).

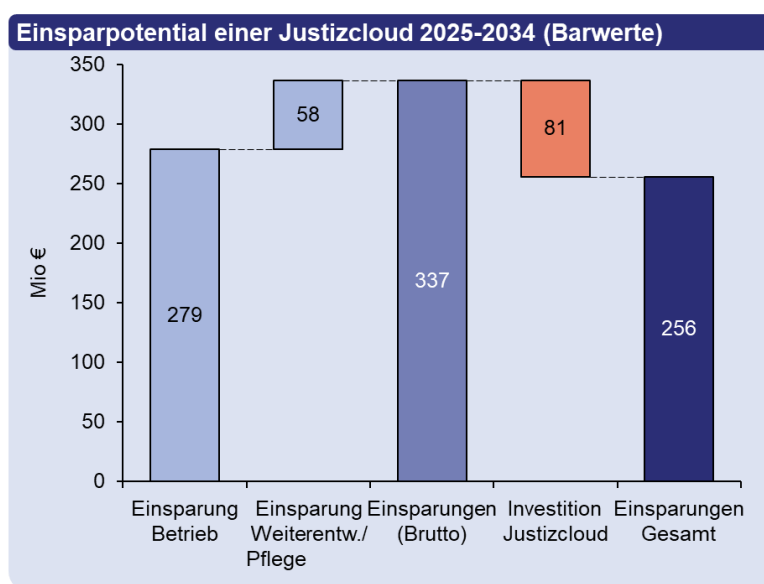
Die vollen Einsparungen von 6,6 M€ in Weiterentwicklung und Pflege sowie 63,3 M€ im laufenden Betrieb, d. h. 73 M€, ergeben sich dabei erst in der vollen Ausbaustufe der

Justizcloud. Es wurde geschätzt, dass mit dem MVP in 2027 und dem fortlaufenden Ausbau der Justizcloud diese Einsparungen jedes Jahr wachsen. Mit dem MVP ergeben sich zunächst 7 M€ Einsparungen, bis im Jahr 2031 die vollen 73 M€ realisiert werden können.

Der Investitionsbedarf wird im ersten Jahr mit 8 M€ bemessen und wächst mit der Gründung ab 2026 während des Aufbaus der Justizcloud-Einheit sowie Justizcloud-Plattform. Insgesamt sollen in Jahr 2030 die Investitionen vollständig getätigt sein.

Insgesamt ergibt sich damit, dass in den Jahren 2025 und 2026 zunächst nur in den Aufbau der Justizcloud investiert wird und dafür finanzielle Mittel von 26,5 M€ erforderlich sind. Mit dem MVP können erste Mehrwerte von 7M € gehoben werden, doch es muss weiter mit 19 M€ investiert werden. Ab 2028 entstehen weitere Mehrwerte durch die Produktivsetzung weitere Anwendungen auf der Justizcloud. Im Jahr 2028 ergeben sich dadurch erstmals Nettoeinsparungen von 1 M€. Diese wachsen anschließend sukzessive bis 2031 die vollen Nettoeinsparungen von 73 M€ realisiert werden.

Abbildung 91 | Barwertbetrachtung der Investition in Justizcloud (S1)



Eine Barwertbetrachtung mit einem Diskontierungssatz von 3% ergibt die erwarteten Nettoeinsparungen über zehn Jahre (vgl. **Abbildung 91**). Dabei werden Bruttoeinsparungen von 337 M€ erwartet, wovon 279 M€ im laufenden Betrieb und 58 M€ durch eine effizientere Weiterentwicklung und Pflege entstehen. Dem steht ein Barwert der Gesamtinvestitionen von 81 M€ gegenüber. In Summe sind daher über

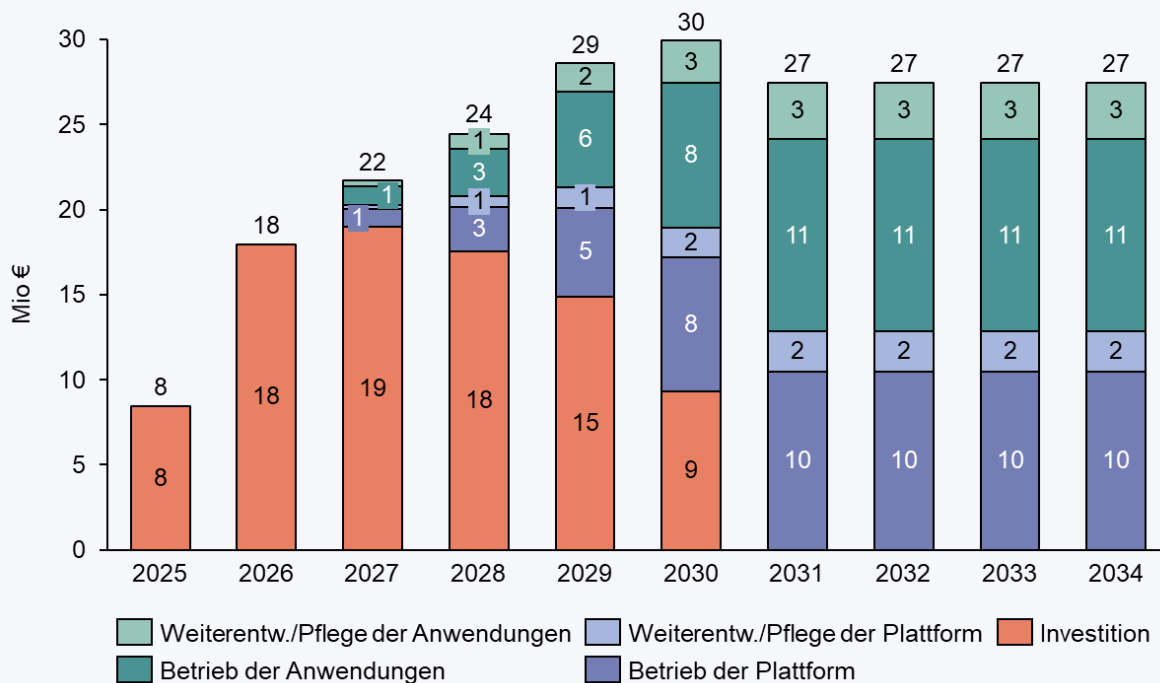
10 Jahre **Nettoeinsparungen von 256 M€ durch die Justizcloud** zu erwarten.

Aus der Wirtschaftlichkeitsbetrachtung ergeben sich zudem Schätzwerte für den erwarteten Finanzbedarf des Aufbaus sowie des laufenden Betriebs inkl. Weiterentwicklung und Pflege der Cloud-Anwendungslandschaft sowie der Justizcloud-Plattform (vgl. **Abbildung 92**).

In den Jahren 2025 und 2026 fallen nur Investitionskosten von 8 M€ bzw. 18,5 M€ an. Ab 2027 entstehen mit dem MVP erste Kosten für den Betrieb der Plattform sowie der

Anwendungen von je 1 M€. Die Betriebskosten wachsen sukzessive, während die erforderlichen Investitionen ab 2028 sinken und in 2030 abgeschlossen sind. Ab 2031 kostet der Betrieb der Cloud-Anwendungen die Justiz insgesamt 27 M€ pro Jahr. Davon entfallen 12 M€ auf den Betrieb der Plattform und 14 M€ für den Anwendungsbetrieb.

Abbildung 92 | Kostenentwicklung für die Justizcloud-Plattform und -Anwendungslandschaft



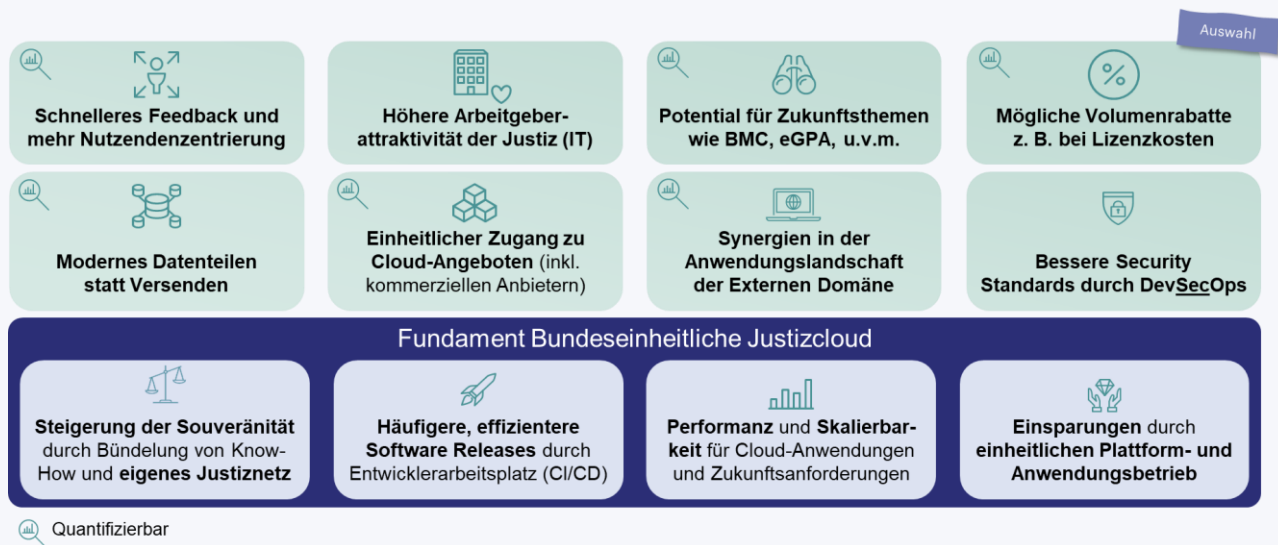
4.4 Zusatzmehrwerte einer Justizcloud

Die Justizcloud ermöglicht neben quantifizierbaren finanziellen Mehrwerten auch die Erschließung zusätzlicher Mehrwertpotenziale, die in einem Cloud-Betrieb pro Land (S0) nicht oder nur durch zusätzliche länder-spezifische Investitionen umgesetzt werden können. Einige dieser Mehrwerte könnten quantifiziert werden, eine Detailbetrachtung erfolgte während der vorliegenden Untersuchung aber nicht.

Die Übersicht der Mehrwertpotenziale (vgl. **Abbildung 93**) zeigt, dass einige Mehrwerte bereits in das Zielbild und die Wirtschaftlichkeitsbetrachtung eingeflossen sind. Bspw. ermöglicht der Aufbau der Justizcloud die Schaffung eines eigenen Justiznetzwerks, bündelt Cloud-Know-how der Justiz und stärkt somit die Souveränität und Unabhängigkeit. Auch die Möglichkeit häufigerer und effizienterer Software-Releases sowie besserer Performanz und Skalierbarkeit von Anwendungen wurde betrachtet, bspw. durch die geringeren Aufwände

für die Weiterentwicklung und Pflege von Anwendungen. Zudem waren die Einsparungspotenziale im Anwendungs- und Plattformbetrieb Kerngegenstand der Wirtschaftlichkeitsbetrachtung. Dazu ergeben sich viele weitere Mehrwerte, die nicht quantifiziert wurden.

Abbildung 93 | Zusätzliche Mehrwertpotenziale einer Justizcloud



Die Justizcloud ermöglicht durch moderne CI/CD Prozesse und die Entwicklung und den Betrieb auf einer Umgebung deutlich schnelleres Feedback, Testing und Ausbringung und somit eine nutzendenzentrierte, agile Anwendungsentwicklung. Darüber hinaus kann die Justizcloud durch ein modernes, innovatives Arbeitsumfeld die Arbeitgeberattraktivität fördern. Die Justizcloud ermöglicht auch modernes Teilen statt Versenden von Daten und bietet so umfassendes Potenzial für die Zukunftsthemen der Justiz, wie eine Cloud-basierte eGPA (vgl. **Kapitel 2.2.4**). Weiterhin eröffnet die Justizcloud die Möglichkeit für die Justiz, in Zukunft einheitlich auch Public Cloud Angebote zu erschließen, was erwartungsgemäß deutlich billiger und effizienter Zugang zu Innovationen für alle Länder bieten kann. Zudem wurde in der Wirtschaftlichkeitsbetrachtung nur die interne Domäne betrachtet, doch auch für die externe Domäne bieten sich viele Synergie- und Innovationspotenziale, wie im fachlichen Zielbild dargestellt. Abschließend ermöglicht die Justizcloud auch eine Vereinheitlichung von Sicherheitsstandards und die Bündelung von Investitionen in IT-Sicherheit (z. B. SIEM Tools, Know-how, etc.) und kann somit langfristig die IT-Sicherheit in der Justiz stärken.

5 Strategisch-planerisches Konzept



In der finalen Projektphase wurde ein umfassendes Konzept zur strategischen Planung der Justizcloud entwickelt, das eine strukturierte Roadmap und eine gezielte Kommunikationsstrategie zur Stakeholdereinbindung umfasst. Die Roadmap visualisiert die zeitliche Umsetzbarkeit, definiert die nächsten Schritte und Aktivitäten und ermöglicht durch die Identifizierung potenzieller Abhängigkeiten eine vorausschauende Risikominimierung. Sie fördert durch klare Darstellung der Handlungsschritte, ein gemeinsames Verständnis bei den Stakeholdern und unterstützt so fundierte und zielgerichtete Entscheidungen.

Die Roadmap ist in drei Phasen unterteilt und beschreibt konkrete Handlungsstränge, die zur vollständigen Realisierung des Justizcloud-Zielbildes erforderlich sind. Gleichzeitig hilft sie, die erforderlichen Ressourcen im zeitlichen Kontext präzise einzuordnen.

Im Verlauf der Untersuchung hat sich eine effektive Stakeholderkommunikation als zentral erwiesen. Durch die konzeptionelle Zusammenarbeit, Sparring-Sitzungen, Rückkopplungen und den aktiven Wissenstransfer, wurde eine kontinuierliche Einbindung der relevanten Stakeholder erreicht und ein gemeinsames Verständnis für die Justizcloud aufgebaut. Alle 16 Länder wurden durch Interviews, Workshops und Informationstermine einbezogen. Mehr als 130 Experten waren im Rahmen der Ist-Analyse eingebunden und brachten ihr Wissen in über 45 Auftakt-, Fach- und IT-Gesprächen ein. Zur Entwicklung des Zielbildes wurden über 200 Stakeholder in mehr als 36 fachlich, rechtlich-organisatorisch und technisch fokussierten Workshops eingebunden. Zusätzlich vermittelten zehn Cloud-Sprechstunden über 100 Justizmitarbeitenden grundlegendes Wissen zu den Möglichkeiten der Technologie.

Eine transparente Kommunikation und gezielte Einbindung relevanter Stakeholdergruppen stärken die Akzeptanz, kollaborative Ergebnisentwicklung und das Vertrauen in die Justizcloud, was essenziell für die erfolgreiche Umsetzung ist. Eine Kommunikationsstrategie wurde entwickelt, die die kontinuierliche Information und den Austausch mit allen relevanten Akteuren priorisiert. Dabei war vor allem das Ziel, alle relevanten Stakeholder vor der Entscheidung des EJR am 25. September 2024 und anschließend des *Bund-Länder-*

Digitalgipfels Ende November 2024 über die Ergebnisse der Justizcloud zu informieren und den Stakeholdern, die an der Entscheidungsvorbereitung unmittelbar beteiligt sind, Informationsmaterial für die Vorbereitung an die Hand zu geben. Hierfür wurden verschiedene Medien, z. B. ein Justizcloud-Video und Informationsunterlagen, vorbereitet.

5.1 Roadmap

Die Roadmap zum Aufbau des Justizcloud-Fundaments (Wertstrom A) wurde auf Basis des entwickelten fachlichen, technischen und rechtlich-organisatorischen Zielbilds erstellt. Dabei fokussiert die Roadmap den Aufbau der Cloud-Infrastruktur (IaaS und PaaS, Justizcloud-Netz) als Betriebsumgebung für neue Fachverfahren der Justiz, die Bereitstellung eines Entwicklerarbeitsplatz für Entwicklungsverbünde sowie den rechtlich-organisatorischen Aufbau der hierfür zuständigen Justizcloud-Einheit.

Entsprechend des „Greenfield“-Ansatzes schafft die Justizcloud initial eine technische Grundlage, die schrittweise mit Anwendungen bestückt werden kann. Der Wert und die Effizienzgewinne der Justizcloud entfalten sich erst dann umfassend, wenn Teile der Justizanwendungslandschaft auf der Justizcloud betrieben werden. Aus diesem Grund ist es wichtig, auch die geplanten Entwicklungszyklen der Fachverfahren *GeFa* und *AuRegis* in den Blick zu nehmen, die Cloud-Readiness und Modernisierung der Justizanwendungslandschaft (Wertstrom B) voranzutreiben und diese Aspekte zeitlich mit dem Aufbau des Justizcloud-Fundaments abzustimmen (vgl. **Kapitel 3.4.2**). Nur so kann sichergestellt werden, dass die Justizcloud durch die Endnutzenden genutzt und gestaltet werden kann. Mit dem Beginn der Cloud-nativen Entwicklung der neuen Fachverfahren ist die Justiz bereits erste Schritte in diese Richtung gegangen. Künftig gilt es fachlich, technisch und auch finanziell abzuwägen, welche weiteren Justizanwendungen für den Betrieb auf der Justizcloud auszubauen sind. Die Mehrwerte der Justizcloud steigen mit jedem Verfahren an, das Cloud-ready modernisiert oder von Beginn an Cloud-nativ entwickelt wird.

Dies setzt in Zukunft die vermehrte Entwicklung standardisierter Fachverfahren voraus, die idealerweise durch ein zentrales, strategisches Anforderungsmanagement (Wertstrom C) abgestimmt und koordiniert werden. Das Anforderungsmanagement bündelt und priorisiert zukünftige Anforderungen an die Justiz-IT und leitet sie zur Umsetzung an die zuständigen Stellen weiter, wobei es durch ein Architekturboard unterstützt wird, das für die Umsetzung des Justizanwendungszielbilds und die erforderliche Technologieharmonisierung sorgt (vgl. **Kapitel 3.3.3**).

Um diese Transformation der Justiz-IT-Landschaft effizient und nachhaltig zu gestalten, kann die Funktion einer strategischen Steuerung und Agilisierung (Wertstrom D) ganzheitlich steuern und wirken. Diese sorgt dafür, dass die Wertströme und Abhängigkeiten zentral koordiniert und orchestriert werden und die Transformation bspw. von Entwicklungs- zu Betriebsstrukturen in einem konsistenten Rahmen nach agilen Methoden erfolgt.

Im Fokus der Untersuchung steht die Entwicklung einer denkbaren Roadmap für das Justizcloud-Fundament. Eine ganzheitliche Perspektive ist jedoch entscheidend, um sicherzustellen, dass die verschiedenen Wertströme ineinandergreifen. Deshalb wurde im Rahmen der Untersuchung ebenfalls eine grobe Roadmap für die weiteren Wertströme skizziert, die als Impuls für die Transformation und Weiterentwicklung der Justiz-IT dienen kann. Dies erlaubt eine koordinierte, schrittweise Umsetzung des Justizcloud-Zielbildes und stellt die Weichen dafür, dass alle relevanten Stakeholder entlang einer gemeinsamen, klar strukturierten Roadmap zusammenarbeiten können.

Die Roadmap stellt dabei die folgenden vier strategischen Wertströme in den Fokus, die orchestriert und synchronisiert umgesetzt werden sollten, um das volle Potenzial der Justizcloud zu realisieren:

Wertstrom A – Justizcloud-Fundament: Entwicklung skalierbarer und leistungsfähiger Cloud-Infrastruktur (IaaS- und PaaS-Dienste), Umsetzung eines justizeigenen Netzwerks, eines Entwicklerarbeitsplatzes sowie Aufbau einer Justizcloud-Einheit.

Wertstrom B – Justizanwendungslandschaft: Strategische Ausrichtung anhand eines gemeinsamen und übergreifenden Designs der Justizanwendungslandschaft.

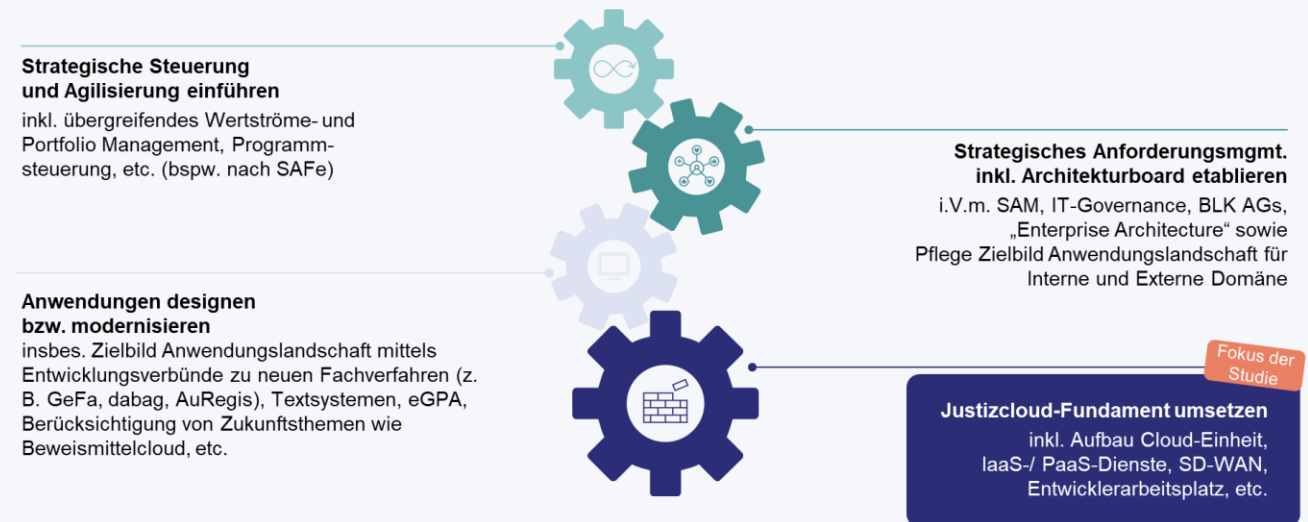
Wertstrom C – Strategisches Anforderungsmanagement inkl. Architekturboard: Einführung eines zentralen Management- und Steuerungsmechanismus inkl. eines Bund-Länder-übergreifenden Architekturboards, der eine konsistente, bedarfsorientierte Entwicklung sowie eine konforme Architekturausrichtung sowie die kontinuierliche Pflege des Zielbilds der Anwendungslandschaft für die interne und externe Domäne sicherstellt.

Wertstrom D – Strategische Steuerung und Agilisierung: Entwicklung eines agilen Steuerungsmodells, das die ganzheitliche Transformation der Justiz-IT-Landschaft flexibel begleitet und übergreifend das Wertströme- und Portfoliomanagement sowie die Programmsteuerung übernimmt.

Die Umsetzung der Modernisierung von Anwendungen, der Aufbau eines strategischen Anforderungsmanagements, eines Architekturboards sowie einer strategischen Steuerung und

Agilisierung ist als Ergebnis dieser Untersuchung zunächst als Impuls und Denkanstoß zu verstehen. **Abbildung 94** gibt einen Überblick über diese vier Wertströme.

Abbildung 94 | Übersicht vorgeschlagener Wertströme



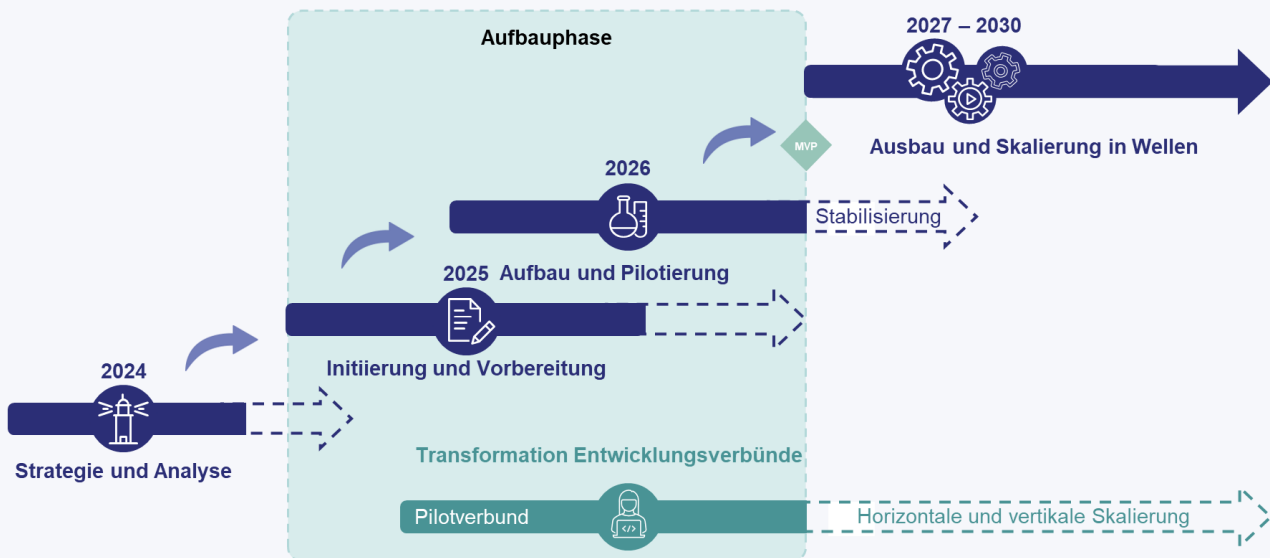
Bei einer positiven Entscheidung über den Übergang in die nächste Vorhabensphase (Vorbereitungsphase) könnte Anfang 2025 mit dem Aufbau der Justizcloud begonnen werden. In der Vorbereitungsphase steht das übergreifende Ziel im Fokus, Mitte 2026 einen Justizcloud-Pilot und bereits Ende 2026, also über einen Zeitraum von ca. zwei Jahren, ein produktives Justizcloud-MVP bereitstellen zu können.

Mit dem Piloten besteht erstmals die Möglichkeit zur Ausbringung und dem Test von Anwendungen auf der Cloud-Plattform. Die Plattform selbst ist dabei noch nicht produktiv und befindet sich weiterhin im sukzessiven Aufbau. Durch den Piloten können bereits wertvolle Erkenntnisse für den späteren produktiven Betrieb der Justizcloud gewonnen und entsprechend gezielt Optimierungen und Anpassungen vorgenommen werden. Der produktive Betrieb beginnt mit der Bereitstellung des Justizcloud-MVP bereits Ende 2026. Mit dem MVP sind die Kernfunktionen der Justizcloud, d. h. der Plattformbetrieb und Entwicklerarbeitsplatz für die Entwicklungs- bzw. transformierten Betriebsverbünde, nutzbar. Ab 2027 erfolgt dann der Justizcloud-Ausbau sowohl vertikal, durch die Einführung neuer Justizcloud-Funktionen, als auch horizontal, durch das Onboarding zusätzlicher Anwendungen und IT-Dienstleister. Diese Skalierung führt zu einem schrittweisen Übergang vom Justizcloud-MVP zu einem stabilen Regelbetrieb ab 2028.

Nachfolgend wird beleuchtet, welche konkreten Aktivitäten für den Aufbau des Justizcloud-Fundaments ergriffen werden müssten, bevor anschließend ein Ausblick auf die Modernisierung der Justizanwendungslandschaft, das strategische Anforderungsmanagement sowie die strategische Steuerung und Agilisierung gegeben wird.

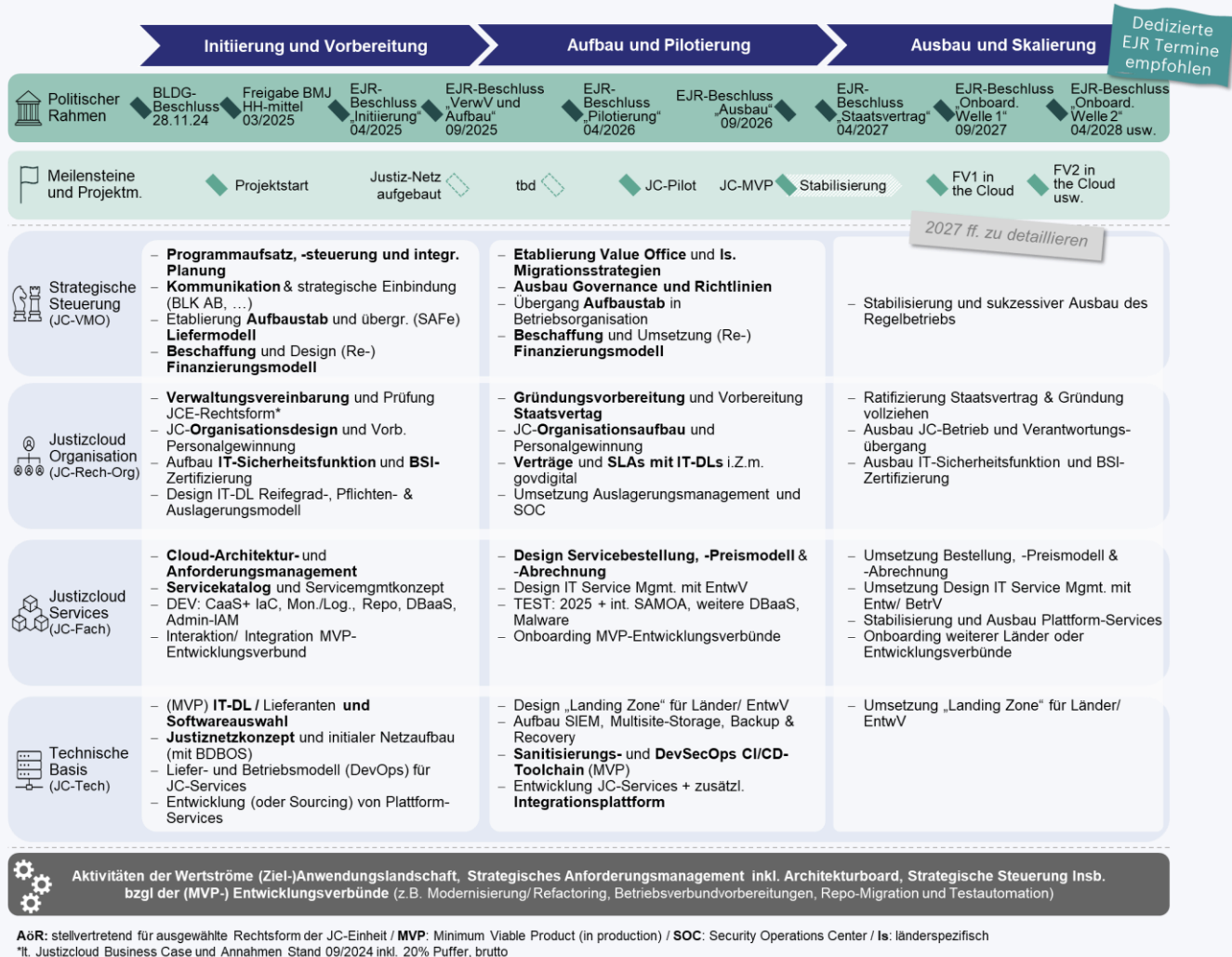
5.1.1 Justizcloud-Fundament

Abbildung 95 | Grobe Roadmap Justizcloud-Fundament



Im Rahmen der Untersuchung wurden die strategischen Grundlagen für das Justizcloud-Fundament gelegt. Damit endet auch die Phase „Strategie und Analyse“ im Jahr 2024. Vorausgesetzt, dass die Entscheidung zur Fortführung der Konzeption einer bundeseinheitlichen Justizcloud Ende 2024 getroffen wird und ab 2025 die finanziellen Mittel bereitstehen, könnte im Frühjahr 2025 eine Initiierungs- und Vorbereitungsphase starten. Diese würde 2026 in eine Aufbau- und Pilotierungsphase übergehen, bevor die Justizcloud zwischen 2027 und 2030 in mehreren Wellen durch das Onboarding weiterer Anwendungen und Länder ausgebaut und skaliert würde (indikative Planung). Entsprechend gliedert sich die Roadmap für das Justizcloud-Fundament in drei Phasen: (1) Initiierung und Vorbereitung, (2) schrittweiser Aufbau und Pilotierung und (3) Ausbau und Skalierungsphase.

Abbildung 96 | Indikative Roadmap für das Justizcloud-Fundament



In jeder der Phasen erfolgt der Aufbau des Fundaments schrittweise entlang von vier zentralen Handlungssträngen: einem übergreifenden Handlungsstrang zur „strategischen Steuerung“ und den drei weiteren: der „Justizcloud-Organisation“, den „Justizcloud-Services“ sowie der „Technischen Basis“. Der übergreifende Handlungsstrang Strategische Steuerung übernimmt den Programmaufsatz und die -steuerung sowie die integrierte Planung und Orchestrierung der weiteren Handlungsstränge. Dabei erarbeitet der Strang „Justizcloud-Organisation“ die rechtlichen und organisatorischen Grundlagen der Justizcloud-Einheit und setzt diese für den Aufbau der Einheit um (vgl. **Kapitel 3.6**). Der Handlungsstrang Justizcloud Services umfasst das Cloud-Architektur- und -Anforderungsmanagement, die Entwicklung des Servicekatalogs und das Design der Servicebereitstellung für zukünftige Kunden der Justizcloud und erstellt das entsprechende Preis- und Abrechnungsmodell (vgl. **Kapitel 3.4**). Die Umsetzung des technischen Zielbilds erfolgt im Rahmen des

Handlungsstrangs Technische Basis und umfasst den Aufbau des Justiznetzes, die technologische Entwicklung der Cloud-Plattform und der -Services sowie die benötigte Produktauswahl und ein entsprechendes Lieferantenmanagement (vgl. **Kapitel 3.5**).

Im Zuge der Entwicklung der Justizcloud-Roadmap wurden die Aktivitäten des jeweiligen Handlungsstrangs unter Einbezug bestehender Abhängigkeiten mit Fokus auf die kommenden zwei Jahre weiter detailliert und den jeweiligen Phasen zugeordnet.

Einzelne größere Umsetzungsentscheidungen, mit denen Weichenstellungen für das Vorhaben verbunden sind, werden jeweils dem E-Justice-Rat vorgelegt. So kann der Auf- und Ausbau der Justizcloud kontinuierlich evaluiert und zielgerichtet zwischen den Ländern und dem Bund abgestimmt werden. Im Folgenden werden zunächst indikativ mögliche Beschlussgegenstände der turnusmäßigen Sitzungen unterbreitet.

5.1.1.1 Initiierungs- und Vorbereitungsphase

Die Initiierungs- und Vorbereitungsphase würde mit einem Beschluss des E-Justice-Rats zur Initiierung voraussichtlich im April 2025 eingeleitet. Diese Phase dient dazu, die wesentlichen rechtlich-organisatorischen, fachlichen und technischen Vorbereitungen für den Aufbau des Justizcloud-MVP zu treffen.

Im Rahmen der Strategischen Steuerung würden der Aufbau und die Etablierung des Justizcloud-Aufbaustabs initiiert, welcher gemeinsam mit der strategischen Steuerung die drei Handlungsstränge übergreifend koordiniert und aufeinander abstimmt. Die Strategische Steuerung wäre außerdem dafür verantwortlich, den weiteren Projektverlauf kommunikativ zu begleiten und relevante Stakeholder der strategischen Ebene einzubinden. Zudem würden das (Re-)Finanzierungsmodell ausgearbeitet werden.

Im Handlungsstrang Justizcloud Organisation würde an der benötigten rechtlichen Grundlage für den Aufbau der Justizcloud gearbeitet. Die Einheit würde konzeptionell weiter detailliert, deren Personalgewinnung vorbereitet sowie IT-Sicherheitsfunktionen aufgebaut und das IT-Dienstleister Reifegrad-, Pflichten- und Auslagerungsmodell konzipiert werden.

Fachlicher Schwerpunkte der Initiierungs- und Vorbereitungsphase wären die Etablierung des Cloud-Architektur- und Anforderungsmanagements (vgl. **Kapitel 3.3.3**) sowie die Ausarbeitung des Justizcloud-Servicekatalogs inkl. eines Servicemanagement-Konzepts (vgl. **Kapitel 3.4.7**). Zudem müsste im Handlungsstrang Justizcloud Services die Einbindung eines ersten Entwicklungsverbunds für das Justizcloud-MVP sichergestellt werden.

Technisch würde das Justizcloud-MVP durch die Auswahl geeigneter IT-Dienstleister sowie der konzeptionellen Ausarbeitung und dem Aufbau eines Justiznetzes vorbereitet. Eine Lieferorganisation mit zwei bis drei IT-Dienstleistern und ein initiales NdB-Justiznetz sollen bis Ende 2025 entstehen. Außerdem würden die für das MVP notwendigen Plattform-Services sowie eine Container-Plattform entwickelt oder, wo möglich, nachgenutzt sowie ein Liefer- und Betriebsmodell (DevOps) für die Justizcloud-Services etabliert werden.

Die Initiierungs- und Vorbereitungsphase könnte Ende 2025 vom E-Justice Rat evaluiert und bei positivem Entscheid in die Phase „Aufbau und Pilotierung“ übergeleitet werden.

5.1.1.2 Aufbau und Pilotierung

In der Aufbau- und Pilotierungsphase stehen zwei zentrale Meilensteine im Fokus: der Aufbau des Justizcloud-Piloten sowie des Justizcloud-MVP.

In dieser Phase würde die Strategische Steuerung ein Value Management Office (VMO) etablieren und länderspezifische Migrationsstrategien für die Justizcloud ausarbeiten. Das VMO stellt dabei eine zentrale Einheit dar, die sicherstellt, dass Projekte und Investitionen den maximalen Wert für die Organisation schaffen, indem sie auf die strategischen Ziele ausgerichtet sind und kontinuierlich optimiert werden. Neben der Verantwortung für den Aufbau der Justizcloud-Organisation/ -Governance und die Weiterentwicklung von Richtlinien setzt sie auch das zuvor ausgearbeitete (Re-)Finanzierungsmodell um. Zudem koordiniert die strategische Steuerung den Übergang vom Aufbaustab zur Betriebsorganisation der Justizcloud-Einheit.

Parallel hierzu würde der Handlungsstrang Justizcloud-Organisation die Gründung der Justizcloud durch einen Staatsvertrag vorbereiten, die Justizcloud-Einheit weiter aufbauen und qualifiziertes Fachpersonal akquirieren. Im Rahmen des Handlungsstrangs würden außerdem SLAs mit den IT-Dienstleistern geschlossen und sowohl das Auslagerungsmanagement als auch das Security Operations Center (SOC) umgesetzt werden.

Der Handlungsstrang Justizcloud-Services würde die Servicebereitstellungs-, Preis- und Abrechnungsmodelle erarbeiten und den MVP-Entwicklungsverbund in der Initiierungs- und Vorbereitungsphase auf die Justizcloud zur Zusammenarbeit onboarden.

Technisch würde das Onboarding durch das Design von Landing Zones vorbereitet. Außerdem würden die Justizcloud Services weiterentwickelt und ein zentrales internes IAM (SAmOA) sowie eine Integrationsplattform entstehen. Auch das in der vorherigen Phase initiierte Justiznetz mit zwei bis drei IT-Dienstleistern könnte produktiv in den Betrieb

genommen werden. Die Grundlagen für die Pilotierung der Justizcloud Mitte 2026 wären gelegt. Auf der Pilotierungsphase aufbauend, soll Ende 2026 der Meilenstein des Justizcloud-MVP erreicht werden und damit bereits das erste MVP-Fachverfahren in der Justizcloud betrieben und von ein bis zwei Ländern produktiv genutzt werden können. Mit dem Justizcloud-MVP würde gleichzeitig der Start der Justizcloud-Stabilisierung eingeläutet.

Im Herbst 2026 könnte erneut der E-Justice-Rat bzgl. der Finanzierungsfreigaben zum weiteren Justizcloud-Aufbau entscheiden und hierfür die Beschlussvorlage zur Einleitung der Phase „Ausbau und Skalierung“ erhalten.

5.1.1.3 Ausbau und Skalierung

Sollte diese Umsetzungsentscheidung getroffen werden, würde in der ab 2027 stattfindenden Ausbau- und Skalierungsphase im Rahmen der Strategischen Steuerung die weitere Stabilisierung der Justizcloud und der Übergang in den Regelbetrieb vorangetrieben, während gleichzeitig der weitere Ausbau der Justizcloud stattfände.

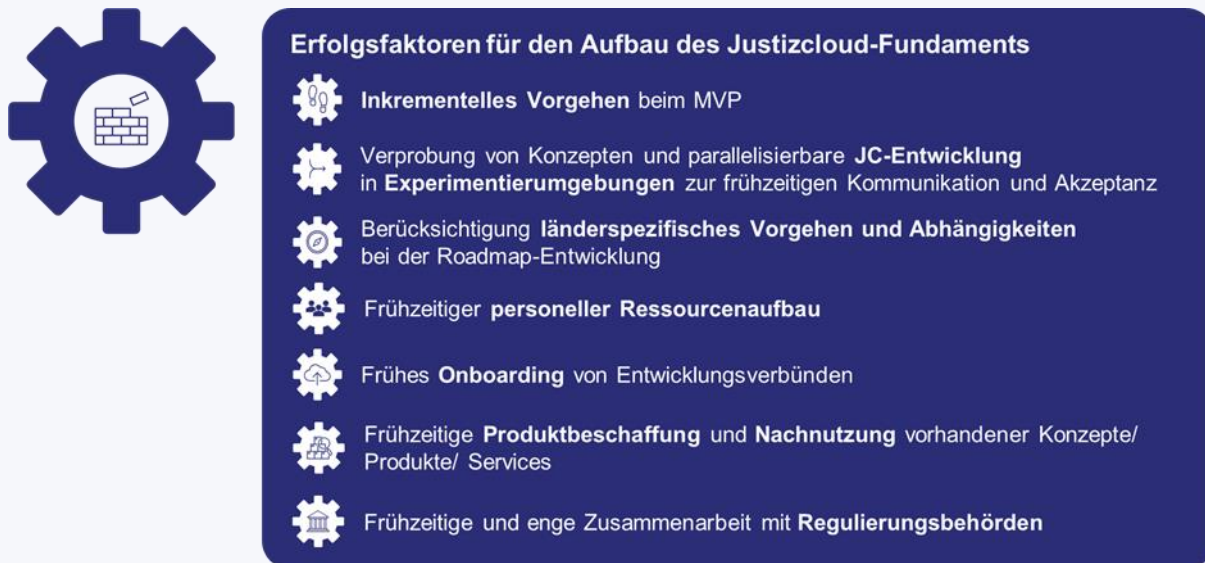
Parallel dazu würde die Gründung der Justizcloud-Einheit durch die Ratifizierung des Staatsvertrags abgeschlossen. Auf dieser Basis würde der weitere Ausbau des Justizcloud-Betriebs sowie die finale Verantwortungsübergabe vom Aufbaustab an die Justizcloud-Einheit erfolgen. Zusätzlich würde der Ausbau der IT-Sicherheitsfunktionen angestrebt, einschließlich relevanter BSI-Zertifizierungen.

Im Rahmen der Cloud-Services, würden das erarbeitete Bestellungs-, Preis- und Abrechnungsmodell sowie das IT-Service-Management mit den Entwicklungs- bzw. Betriebsverbünden implementiert und die Justizcloud-Platformservices weiter ausgebaut. Sukzessive würde das Onboarding zusätzlicher Länder und Entwicklungsverbünde (horizontale Skalierung) sowie Anwendungen (vertikale Skalierung) auf die Justizcloud voranschreiten.

Technisch läge der Fokus auf dem Ausbau der Justizcloud-Infrastruktur, u.a. der Umsetzung von Landing Zones für die Entwicklungsverbünde und Länder. Weitere Schritte würden kontinuierlich entlang der definierten Roadmap konkretisiert und umgesetzt werden.

Erfolgsfaktoren

Abbildung 97 | Erfolgsfaktoren für den Aufbau des Justizcloud-Fundaments



Für den erfolgreichen Aufbau eines bundeseinheitlichen Justizcloud-Fundaments sind verschiedene Erfolgsfaktoren entscheidend, die eine zügige, ressourceneffiziente und anforderungsgerechte Umsetzung ermöglichen.

Ein inkrementelles Vorgehen ist hierbei zentral. Durch ein iteratives Entwicklungsmodell (Programme/ Product Increments (PI)) können frühzeitig greifbare Ergebnisse bis zum MVP erzielt und weiterführend optimiert werden. Diese Herangehensweise schafft von Beginn an Mehrwerte sowie greifbare Ergebnisse und stellt sicher, dass alle relevanten Anforderungen praxisnah erfüllt werden.

Die Erprobung von Konzepten und die Entwicklung der Justizcloud sollten in parallelen Umgebungen stattfinden. So können Konzepte in Experimentierumgebungen frühzeitig getestet, Geschwindigkeit gewonnen und die Akzeptanz der Stakeholder gefördert werden.

Für eine nachhaltige Umsetzung sind länderspezifische Besonderheiten und mögliche Abhängigkeiten konsequent in die Roadmap-Planung zu integrieren, um ein koordiniertes Onboarding und eine reibungslose Zusammenarbeit zu gewährleisten.

Ein frühzeitiger Aufbau personeller Ressourcen ist entscheidend, um die erforderlichen Umsetzungskapazitäten zu sichern und die für das Projekt benötigten Kompetenzen rechtzeitig aufzubauen. Durch eine klar definierte Personalstrategie und eine vorausschauende

Planung können die benötigten Fachkräfte mit relevanten Stakeholdern abgestimmt und rechtzeitig an Bord geholt werden.

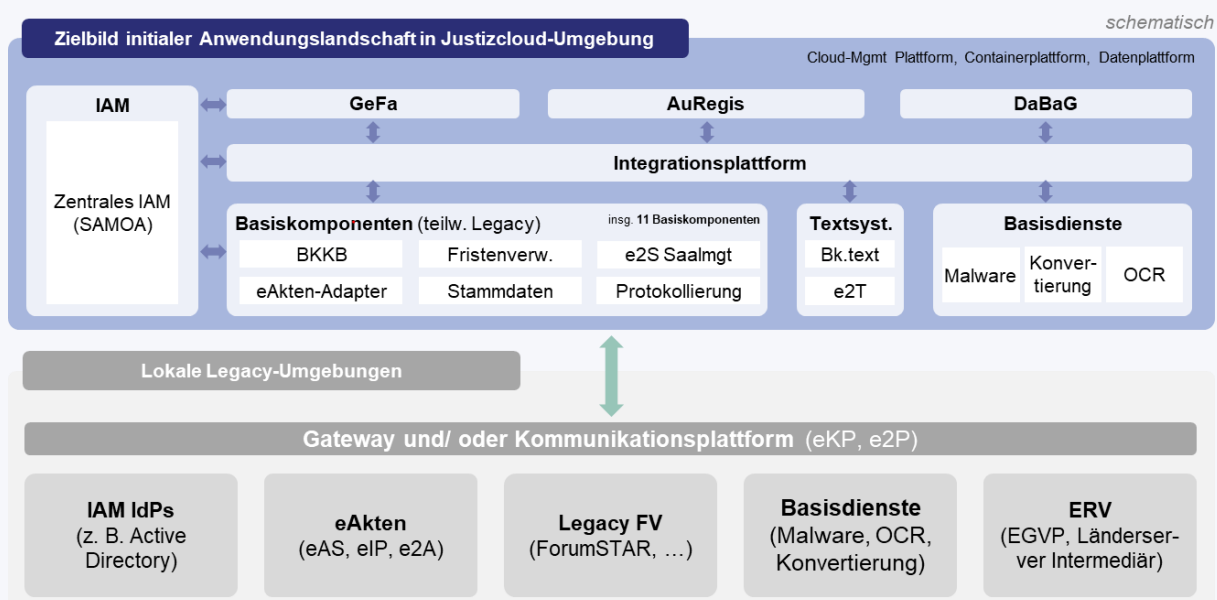
Das frühzeitige Onboarding von Entwicklungsverbünden auf die Justizcloud stellt einen weiteren wesentlichen Erfolgsfaktor dar. Es ermöglicht eine schnelle Erprobung der Entwicklungs- und Betriebsumgebung, ermöglicht frühzeitige Feedbackschleifen und Iterationen sowie schnelle greifbare Ergebnisse.

Ebenso ist eine proaktive Produktbeschaffung sowie die Nachnutzung vorhandener Konzepte, Produkte und Services essenziell, um Synergien zu nutzen, die Vereinheitlichung von Standards praktisch umzusetzen und eine hohe Umsetzungsgeschwindigkeit zu fördern.

Eine enge Zusammenarbeit mit Regulierungsbehörden (z. B. BSI) ermöglicht es, frühzeitig Sicherheitszertifizierungen zu erlangen und Compliance-Richtlinien von Anfang an vollumfänglich einzuhalten.

5.1.2 Justizanwendungslandschaft

Abbildung 98 | Zielbild initialer Anwendungslandschaft in Justizcloud-Umgebung



Der Fokus der Justizanwendungslandschaft liegt auf der internen Domäne und hier insb. auf der ersten wesentlichen Ausbaustufe des Justizcloud-Anwendungsgefüges mit drei modernen Fachverfahren (vgl. **Abbildung 98**).

Die Anwendungslandschaft der Justizcloud besteht aus modernen Fachverfahren, der Integrationsplattform, Basiskomponenten, Textsystemen, Basisdiensten und einem IAM. Die Kommunikation zwischen Cloud-Anwendungen erfolgt durch die Integrationsplattform. Die Kommunikation zwischen der Cloud-Umgebung und lokalen Legacy-Umgebungen erfolgt durch die Integrations- und Kommunikationsplattform (eKP, e2P).

Wie eingangs erläutert, entfaltet die Justizcloud ihre Mehrwerte erst, sobald Justizanwendungen auf ihr betrieben werden können. Um die Modernisierung der Justizanwendungslandschaft zeitlich auf den Aufbau des Justizcloud-Fundaments abstimmen zu können, wurde im Rahmen der Untersuchung der aktuelle Entwicklungsstand von Justizanwendungen betrachtet und eine initiale Einschätzung vorgenommen, bis zu welchem Zeitpunkt diese voraussichtlich Cloud-ready und auf einer Cloud-Infrastruktur lauffähig sind. Cloud-ready bedeutet in diesem Kontext, dass mindestens fünf wesentliche technische Konzepte umgesetzt sind: Containerisierung, Microservice-Architektur, Entkopplung, Webfähigkeit und Mandantenfähigkeit (vgl. **Kapitel 2.2.1**).

Dabei wurde herausgearbeitet, dass die Fachverfahren *AuRegis* und *GeFa* sowie das Benutzer- und Berechtigungsmangement *SAmOA public* und die Basiskomponenten bis voraussichtlich 2025 in der Cloud betriebsfähig sind. Die Anwendungen *bk.text* und *e2T* sowie die Basisdienste könnten voraussichtlich bis 2027 Cloud-ready sein (vgl. **Kapitel 2.2.1**). Abzustimmen bleibt noch, bis wann die Integrationsplattform sowie die Anwendung *dabag* auf der Cloud betrieben werden können.

Der mögliche Zeitpunkt der Anwendungsmigration in die Justizcloud richtet sich nach länderspezifischen Gegebenheiten. Jedes Land ist verantwortlich, eine länderspezifische Onboarding-Roadmap auf die Justizcloud zu entwerfen, in der z. B. detailliert wird, mit welchen Anwendungen und zu welchem Zeitpunkt das Onboarding durch die Entwicklungs- bzw. Betriebsverbünde sowie eine mögliche Datenmigration stattfinden können.

Neben der zeitlichen und länderspezifischen Komponente des Justizcloud-Onboardings gilt es außerdem zu beachten, dass Anwendungen nur in Bündeln funktionsfähig sind und entsprechend gemeinsam in die Cloud migriert werden müssen. Da *AuRegis* voraussichtlich bis 2025 Cloud-ready ist, besteht die Möglichkeit, das erste Justizcloud-Anwendungsbündel an dieser Anwendung auszurichten und sie, gemeinsam mit den Basiskomponenten und -diensten sowie der Integrationsplattform und *SAmOA*, in die Cloud zu heben. Entsprechend der zeitlichen Einordnung der Cloud-Readiness, könnten als zweites Bündel darauffolgend *GeFa* und *bk.text* migriert werden.

Für ein erfolgreiches Onboarding auf die Justizcloud ist eine länderspezifisch abgestimmte Herangehensweise erforderlich, die maßgeschneiderte Roadmaps für jedes Land umfasst. Diese Roadmaps definieren den Onboarding-Prozess sowie die Nutzung der spezifischen Anwendungen.

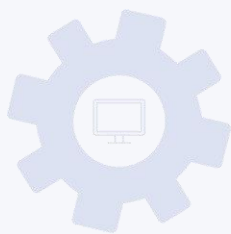
Die technischen Voraussetzungen für das Onboarding beinhalten mehrere kritische Schritte. Jedes Land muss an das Netzwerk und Admin-IAM-Dienste angebunden werden, einschließlich der Integration und Föderation von Usern über *SAMOA public*. Zusätzlich ist die Anlage von Gerichten in den Basiskomponenten notwendig, ebenso wie die Konfiguration der Justizcloud-Plattform, etwa durch die Zuweisung spezifischer Namespaces, sowie der Integrationsplattform und Anbindung an ein lokales eAkten-System.

Das rechtlich-organisatorische Onboarding umfasst die Ausarbeitung und Verhandlung von Verträgen, SLAs, IT-Service-Management-Prozessen sowie die Berücksichtigung bestehender Restlaufzeiten und anderer rechtlicher Verpflichtungen. Auch das fachliche Onboarding spielt eine entscheidende Rolle: Hier gilt es, den optimalen Zeitpunkt für den Umstieg jedes Gerichts festzulegen und bei Bedarf eine Datenmigration durchzuführen.

Durch das Prinzip Flexibility-by-Design kann der Zeitpunkt des Onboardings flexibel an die spezifischen Anforderungen der Länder angepasst werden, wodurch die Justizcloud auch bei künftigen Änderungen der Anforderungen reaktionsfähig bleibt.

Erfolgsfaktoren

Abbildung 99 | Erfolgsfaktoren für die Justizcloud Anwendungslandschaft



Erfolgsfaktoren für die Justizanwendungslandschaft

-  Aufbau und Nutzung der **Integrationsplattform**
-  **Flexibilität** bei **Auswahl der Anwendungen** für JC-Plattformbetrieb
-  Frühzeitige Definition von **Anwendungsbündeln** und **Bereitstellung** von **JC-Plattform-Grundfunktionen**
-  Konsequente **Anwendungsmodernisierung** in Kooperation mit Architekturboard
-  Sukzessive Transformation von **Entwicklungs- zu Betriebsverbünden** (DevOps, Service Desk, u.v.m.)

Für die Modernisierung der Justizanwendungslandschaft wird entscheidend sein, dass sie konsequent und in enger Abstimmung mit dem Architekturboard vorangetrieben wird, so dass sie einheitlichen Standards folgt und ein stimmiges Justizanwendungsgefüge entsteht. Dabei gilt es, Anwendungsbündel frühzeitig zu definieren, um die Modernisierung der jeweiligen Anwendungen zeitlich aufeinander abzustimmen und Grundfunktionen der Justizcloud-Plattform sowie die Integrationsplattform rechtzeitig bereitstellen zu können. Der Aufbau und die Nutzung der Integrationsplattform ermöglichen die flexible Einbindung und bedarfsgerechte Bereitstellung von Anwendungen für den Betrieb auf der Justizcloud. Eine frühzeitige Definition und Bündelung relevanter Anwendungen sowie die Bereitstellung wesentlicher Plattform-Grundfunktionen unterstützen die zügige Inbetriebnahme.

Für die Modernisierung der Anwendungslandschaft ist es außerdem essenziell, dass sie eng von der Transformation der Entwicklungsverbünde hin zu Entwicklungs- und Betriebsverbünden begleitet wird. Durch die Justizcloud wird die Möglichkeit geschaffen, Justizanwendungen künftig bundeseinheitlich zu entwickeln und zu betreiben. Im Gegensatz zur derzeitigen Trennung der Anwendungsentwicklung durch die Entwicklungsverbünde vom Anwendungsbetrieb durch die IT-Dienstleister der Länder können die Entwicklungsverbünde künftig ihre selbst entwickelten Anwendungen auf der Justizcloud auch betreiben. Um die Vorteile dieses DevOps-Prinzips umfänglich heben zu können, bedarf es jedoch einer Weiterentwicklung der Entwicklungsverbünde zu Entwicklungs- und Betriebsverbünden. Hierdurch erweitert sich deren Aufgabenspektrum um die Ausbringung von Anwendungen, die Bereitstellung des Second- und Third-Level-Anwendungssupports sowie der kontinuierlichen Beobachtung und Optimierung von Anwendungen.

Essenziell sind dabei die Abstimmung und Entscheidung über die Modernisierung bestehender und die Entwicklung neuer Anwendungen. Anzuregen wären zudem, dass möglichst für alle neuen bzw. modernisierten Anwendungen eine bundeseinheitliche Lösung gefunden wird, um die Potenziale der Justizcloud voll ausnutzen zu können.

5.1.3 Strategisches Anforderungsmanagement inkl. Architekturboard

An den Abhängigkeiten zwischen Justizcloud-Fundament und Anwendungslandschaft lässt sich die Notwendigkeit eines strategischen Anforderungsmanagements ableiten.

Mit dem Ziel, Anforderungen an die Justiz-IT künftig zentral zu bündeln, priorisieren und entsprechend deren Umsetzung initiieren zu können, könnte parallel zum Aufbau des Justizcloud-Fundaments in der ersten Hälfte 2025 ein strategisches Anforderungsmanagement

aufgebaut und etabliert werden. Es hat die Aufgabe, strategische Anforderungen der Justiz an die IT-Infrastruktur aufzunehmen, zu priorisieren und fachliche Schwerpunkte für die Weiterentwicklung der Justiz-IT zu setzen. Damit einhergehend könnte der Aufbau eines Architekturboards angestoßen werden. Dieses übergibt in Abstimmung mit dem strategischen Anforderungsmanagement die fachlichen und technischen Anforderungen zur operativen Umsetzung an die zuständigen Einheiten und wirkt auf die kontinuierliche Weiterentwicklung der Justizanwendungslandschaft hin (vgl. **Kapitel 3.3.3**).

Erfolgsfaktoren

Ein strategisches Anforderungsmanagement in Verbindung mit einem effektiven Architekturboard kann erheblich dazu beitragen, eine zukunftsfähige und konsistente Justizanwendungslandschaft zu gestalten. Die Etablierung eines strukturierten Anforderungsmanagements unter Einbeziehung der Entwicklungsverbünde und IT-Dienstleister stellt sicher, dass Anforderungen koordiniert aufgenommen, priorisiert und in Einklang mit der strategischen Ausrichtung effizient umgesetzt werden können. Die Etablierung eines solchen strategischen Anforderungsmanagement entspricht dabei marktüblichen Standards und wurde bereits im Rahmen der DVS und mit den Entwicklungsverbünden umgesetzt.

Das Architekturboard fungiert als zentrale Instanz der IT-Governance. Es arbeitet gezielt auf die Entwicklung einer harmonisierten Anwendungslandschaft hin. Durch die Definition und Durchsetzung einheitlicher Technologiestandards gewährleistet es eine kohärente und skalierbare Architektur, die die Integration und Nutzung unterschiedlicher Systeme erleichtert und langfristige Synergien innerhalb der Justiz schafft. Diese klaren Governance-Strukturen und die Durchsetzung technologischer Standards bilden gemeinsam die Grundlage für eine effektive und zukunftssichere IT-Architektur.

Abbildung 100 | Erfolgsfaktoren für das strategische Anforderungsmanagement und Architekturboard



Erfolgsfaktoren für das strategische Anforderungsmanagement inkl. Architekturboard



Etablierung **strategisches Anforderungsmanagements** mit Entwicklungsverbünden und IT-Dienstleistern



Gründung **Architekturboard** und **IT-Governance** zur Wirkung auf eine **Zielanwendungslandschaft**



Durchsetzung übergreifender **Technologiestandards**

5.1.4 Strategische Steuerung und Agilisierung

Eine strategische Steuerung und ganzheitliche Agilisierung sind entscheidend, um die umfassende Transformation der Justiz effektiv zu begleiten. Durch eine gemeinsame strategische Steuerung lassen sich übergreifende Wertströme gezielt orchestrieren und koordinieren sowie Abhängigkeiten frühzeitig identifizieren und transparent gestalten.

So könnte eine strategische Steuerung die Umsetzung eines standardisierten DevOps- und Service-Desk-Prinzips umfassen, bei dem Entwicklungsverbünde in Betriebsverbünde übergehen und gezielt Ressourcen aufgebaut werden. Ein effektives Wertstrom- und Abhängigkeitsmanagement, bspw. durch SAFe Program Increment Planning (PI), stellt sicher, dass alle Vorhaben effizient aufeinander abgestimmt sind. Darüber hinaus sind ein systematisches Wertstrom-Portfolio- und Budget-Management notwendig, um die Justiztransformation nachhaltig und finanziell konsistent umzusetzen.

Ergänzt wird dieser Ansatz durch ein umfassendes Changemanagement und gezielte Weiterbildungsinitiativen wie etwa eine Cloud Academy, die Mitarbeitenden relevante Kompetenzen und Fähigkeiten vermitteln, um den Wandel aktiv mitzugestalten.

Erfolgsfaktoren

Abbildung 101 | Erfolgsfaktoren für die strategische Steuerung und Agilisierung



Erfolgsfaktoren für die strategische Steuerung und Agilisierung

-  Ganzheitliche **Transformation** der **Justiz-Strukturen** (z. B. auf Entscheidungsebene)
-  Aufsatz **integriertes Wertstrom- und Portfoliomanagement**
-  Aufbau von **Agilitäts-Know-how** (z. B. SAFe, DevOps) und **Cloud-Know How**

Für die erfolgreiche strategische Steuerung und Agilisierung der Justiz-IT ist eine ganzheitliche Transformation bestehender Strukturen vorzusehen. Ein integriertes Wertstrom- und Portfolio-Management ermöglicht eine gezielte Priorisierung und Allokation der Ressourcen und schafft eine klare Ausrichtung auf die strategischen Ziele der Justiz.

Ebenso wichtig ist der systematische Aufbau von Agilitäts- und Cloud-Know-how. Die Anwendung agiler Frameworks wie *SAFe* (auf *Enterprise*-Ebene) fördert die Effizienz und Flexibilität innerhalb der Prozesse und befähigt die Justiz, auf dynamische Anforderungen schnell zu reagieren. Cloud-Know-how unterstützt die nachhaltige Implementierung und den reibungsloseren Betrieb von Anwendungen, wodurch langfristig eine nachhaltige IT-Infrastruktur geschaffen wird. Diese Erfolgsfaktoren bilden gemeinsam die Basis für eine resiliente und adaptierbare Justizorganisation.

5.2 Stakeholderkommunikation

5.2.1 Identifikation und Analyse der Stakeholder

Aufgrund der föderalen Struktur, dem Verantwortungsschnitt zwischen Anwendungsentwicklung und -betrieb sowie der Vielzahl digitalpolitischer Akteure, ergibt sich eine umfassende Stakeholderlandschaft. Für den Erfolg der Umsetzung der Justizcloud ist eine enge, koordinierte Einbindung relevanter Stakeholdergruppen im Justizumfeld und eine länderübergreifende Zusammenarbeit essenziell. Transparente wie zielgerichtete Kommunikation der Projektziele und -ergebnisse schafft die notwendige Unterstützung und befähigt Stakeholder, innerhalb ihrer Verantwortungsbereiche aktiv zum Erfolg der Justizcloud beizutragen.

Im Rahmen der Untersuchung wurde die Stakeholderlandschaft analysiert und in fünf zentrale Gruppen gegliedert: (1) Ministerien und Senatsverwaltungen (Justiz-, Finanz- und ggf. Digitalressorts) auf Bundes- und Landesebene, (2) justizrelevante IT-Dienstleister der Länder, (3) Projekte und Initiativen im Kontext der Justizcloud, (4) Digitalpolitische Akteure, (5) (Fach-)Gerichte sowie weitere Justizbehörden (z. B. Bundesamt für Justiz, Selbstverwaltungskörperschaften der Rechtsanwaltschaft- und der Notariate) und Rechtsberufe (z. B. Rechtspflegende, Gerichtsvollzieher).

Abbildung 102 | Übersicht der Stakeholdergruppen im engen und erweiterten Kontext



Die **Justizministerien und Senatsverwaltungen** der Länder und des Bundes sind zentrale Stakeholder im Justizcloud-Projekt und bereiten die Entscheidungsfindung im E-Justice-Rat und auf dem *Bund-Länder-Digitalgipfel* vor. Dafür ist Klarheit über die strategische Bedeutung und Funktionsweise der Justizcloud unerlässlich, ebenso wie die Beantwortung offener Fragen und Anliegen. Bereits in der Ist-Analyse, Zielbildentwicklung und strategischen Konzeptionsphase waren die Justizministerien durch ihre durchgehende Vertretung in Fachpanels und im Sounding Board intensiv eingebunden. Diese enge Zusammenarbeit hat das Projektverständnis und Akzeptanzniveau deutlich gestärkt. Für die anstehenden Entscheidungen ist die fortgesetzte Einbindung dieser Stakeholder von hoher Priorität. Zusätzlich zur Justiz ist es erforderlich, relevante Ministerien wie Finanz- oder Digitalressorts auf Länder und Bundesebene einzubeziehen. Hierbei sind die spezifischen Kommunikationsbedarfe zu berücksichtigen und die Justizministerien gezielt zu unterstützen.

Die **IT-Dienstleister** spielen eine zentrale Rolle im Zielbild der Justizcloud, da sie das technologische Fundament bereitstellen sollen und die technische Umsetzung maßgeblich vorantreiben müssten. Im Rahmen der Justizcloud würden sich ihre Verantwortungsbereiche und die Zusammenarbeit mit der Justiz verändern. Über vereinbarte SLAs würden sie direkt mit der Justizcloud zusammenarbeiten und potenziell neue Dienste einbringen, wodurch sie als Innovationstreiber agieren und Mehrwerte wie Innovationspotenziale, Ressourcenoptimierung und Synergieeffekte für sich erschließen könnten. Da die IT-Dienstleister unterschiedliche Leistungsportfolios und Kundensegmente bedienen, variieren ihre Bedürfnisse und Mehrwerte in Bezug auf die Justizcloud. Eine enge Einbindung der IT-Dienstleister, die durch die Zusammenarbeit in Fachpanels mit 13 IT-Dienstleistern im Projektverlauf bereits gefördert wurde, ist entscheidend, um die Implikationen und zukünftige Zusammenarbeit mit den Justizministerien transparent zu gestalten.

Während der Untersuchung wurden relevante **digitalpolitische Akteure** sowie **Projekte und Initiativen** im direkten und erweiterten Justizumfeld gezielt über Workshops, Interviews und Informationstermine eingebunden. Ziel war es, wertvollen Input zu gewinnen, Transparenz zu schaffen, mögliche Synergien frühzeitig zu identifizieren und einen kontinuierlichen Kommunikationsfluss sicherzustellen. So wurde bspw. ein enger Austausch mit der DVS aufgebaut, um existierende Konzepte wiederzuverwenden.

Die **(Fach-)Gerichte sowie weitere Justizbehörden und Rechtsberufe** bilden die Endnutzenden der Justizcloud. Hierzu zählen insb. Richter, Rechtsanwälte, Notare, Rechtspflegende und Gerichtsvollzieher. Eine gezielte Kommunikation ist entscheidend, um die

Mehrwerte klar aufzuzeigen, Fragen zu klären und mögliche Vorbehalte abzubauen. Im Rahmen der Untersuchung wurde dieser Ansatz bedarfsorientiert verfolgt. So wurden bspw. die *Bundesrechtsanwaltskammer (BRAK)* und die *Bundesnotarkammer (BNotK)* in Interviews eingebunden, um deren Anforderungen frühzeitig zu berücksichtigen.

5.2.2 Kommunikationsstrategie

Zur effektiven Kommunikation der Ergebnisse dieser Untersuchung und bedarfsorientierten Adressierung relevanter Stakeholder wurden auf Grundlage der Stakeholderanalyse elf Kernbotschaften entwickelt (**Abbildung 103**). Diese dienen als Grundlage für die Entwicklung maßgeschneiderter Kommunikationsmaterialien. Ein strategischer Kommunikationsplan wurde erarbeitet, der festlegt, wann und wie die Stakeholder eingebunden werden.

Abbildung 103 | Übersicht Kernbotschaften für die Justizcloud-Kommunikation



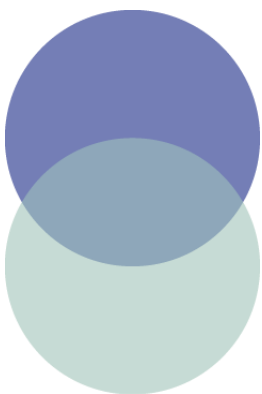
Dabei stützt sich die Kommunikation auf drei wesentliche Säulen:

1. **Fokussierte Ansprache von Entscheidungsträgern:** Bis zur geplanten Umsetzungsentscheidung auf dem *Bund-Länder-Digitalgipfel* im November 2024 wurde der kommunikative Schwerpunkt auf die Justizministerien und IT-Dienstleister der Länder gelegt, um eine fundierte Entscheidungsbasis zu schaffen. Dafür wurden Materialien

wie eine Executive Summary, Informationspakete mit Präsentationen, ein Konzeptvideo und der Abschlussbericht bereitgestellt.

2. **Kollaborative Einbindung digitalpolitischer Akteure:** Relevante Ressorts, digitalpolitische Akteure und Initiativen wie die *Deutsche Verwaltungscld (DVC)* und *govdigital eG* sowie Aufsichtsbehörden wie das *BSI* wurden frühzeitig in das Projekt einbezogen, um von deren Best Practices zu profitieren und Synergien für die Justizcloud zu schaffen. Hierzu wurden spezifische Präsentationen entwickelt, Workshops durchgeführt und Regeltermine für den Austausch aufgesetzt.
3. **Proaktive, breitflächige und landesspezifische Kommunikation:** In Vorbereitung auf den *Bund-Länder-Digitalgipfel* wurde neben dem Sounding Board ein Multiplikatoren-Netzwerk eingerichtet, um eine länderübergreifende Kommunikation sicherzustellen und Feedback aus den Ländern aufzunehmen. Justizministerien und IT-Dienstleister wurden eingeladen, an diesem Netzwerk mitzuwirken, um eine kohärente und zielgerichtete Informationsverbreitung zu gewährleisten. Die Multiplikatoren erhielten ein umfassendes, mit dem Sounding Board abgestimmtes, Informationspaket mit Präsentationen sowie einer Executive Summary zur gezielten Unterstützung ihrer Kommunikationsarbeit.

Im Falle einer positiven Umsetzungsentscheidung für die Justizcloud beim *Bund-Länder-Digitalgipfel* im November 2024 werden eine intensive Zusammenarbeit mit den bereits eingebundenen Stakeholdern sowie die verstärkte Einbindung von zusätzlichen Beteiligten in den Aufbau der Justizcloud (z. B. durch ein Multiplikatoren-Netzwerk) weiter vorangetrieben. Entsprechend würde eine zielgerichtete Kommunikationsstrategie entwickelt, die den spezifischen Anforderungen in der Aufbauphase Rechnung trägt.



6 Glossar

Begriff	Erläuterung
Akteneinsichtsportal (AEP)	Das Akteneinsichtsportal (AEP) ist eine digitale Plattform, die berechtigten Nutzenden den Zugriff auf Kopien elektronischer Akten zum Zwecke der Akteneinsicht ermöglicht.
Anstalt des öffentlichen Rechts (AöR)	Anstalten des öffentlichen Rechts sind öffentl.-rechtl. Verwaltungseinrichtungen, die einem bestimmten Nutzungszweck dienen und im Gegensatz zu den Körperschaften des öffentlichen Rechts nicht mitgliedschaftlich organisiert sind. Die Benutzer sind deshalb nicht Anstaltsmitglieder. Die Rechtsbeziehungen zwischen ihnen und der Anstalt des öffentlichen Rechts werden durch die Anstaltsordnung geregelt. Diese kann öffentlich-rechtlich oder privatrechtlich ausgestaltet sein. Juristische Personen des öffentlichen Rechts sind nur die vollrechtsfähigen Anstalten, die rechtlich selbständige Einheiten der mittelbaren Staatsverwaltung darstellen, insb. Satzungsgewalt und andere Selbstverwaltungsrechte haben.
Application Programming Interfaces (API)	APIs sind Schnittstellen, die den Austausch von Daten und Funktionen zwischen verschiedenen Softwareanwendungen ermöglichen. Sie nutzen standardisierte Protokolle, über die Programme miteinander kommunizieren und Informationen sicher und effizient ausgetauscht werden können.
Länderübergreifendes Registerfachverfahren (AuRegis)	Das einheitliche Registerfachverfahren (AuRegis) ist ein System zur zentralen Verwaltung von Registerdaten. Es ermöglicht den standardisierten Zugriff auf verschiedene behördliche Register wie Handels- oder Vereinsregister und unterstützt die effiziente Abwicklung von Verwaltungsprozessen.
Auslagerungsmanagement	Bezeichnet die systematische Planung, Steuerung und Überwachung von ausgelagerten Geschäftsprozessen oder IT-Dienstleistungen. Es stellt sicher, dass externe Anbieter effizient arbeiten und alle regulatorischen sowie vertraglichen Anforderungen erfüllt werden.
Berechtigungsmanagementsystem (IAM)	Berechtigungsmanagementsysteme (Identity and Access Management (IAMs)) verwalten und steuern den Zugriff von Nutzern auf IT-Ressourcen eines Unternehmens. Sie sorgen dafür, dass nur autorisierte Personen die passenden Rechte und Zugriffsberechtigungen erhalten, um Sicherheit und Compliance zu gewährleisten.
Bund-Länder-Kommission (BLK)	Die Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) ist die ständige Arbeitsgruppe des E-Justice-Rats. Sie beschäftigt sich mit strategischen und operativen Themen der Justizdigitalisierung und bereitet die Sitzungen des E-Justice-Rats vor.

Begriff	Erläuterung
Basiskomponente Kostenbearbeitung (BKKB)	Die Basiskomponente Kostenbearbeitung (BKKB) ist ein Kostenverfahren, zur Erfassung, Berechnung und Verteilung von Kosten in bestimmten Verwaltungsprozessen. Es dient der transparenten und rechtlich einheitlichen Abwicklung von Gebühren und Auslagen.
bk.text	Eine Softwarelösung zur Erstellung, Bearbeitung und Verwaltung von Textdokumenten in einem strukturierten Format. Sie unterstützt Benutzer bei der effizienten Texterstellung, z.B. durch Vorlagen und die automatische Befüllung von Textinhalten aus den Fachverfahren.
CI/CD-Pipeline (Continuous Integration/ Continuous Delivery)	Continuous Integration: Regelmäßige automatisierte Ausführung von Code Merges (Kompilierung) und Unit Tests (sog. Funktions-test) sowie Containerisierung. Continuous Delivery: Regelmäßige automatisierte Ausbringung der Container auf Umgebungen und Tests (z. B. System- und Abnahmetest) der containerisierten Anwendung.
Client	Ein Client ist ein Computerprogramm (z. B. Webbrowser, Anwendung), das auf einem Gerät (z. B. PC, Smartphone) ausgeführt wird und auf Dienste oder Ressourcen eines Servers zugreift. Er dient als Schnittstelle zum Benutzer und ermöglicht die Interaktion mit dem Server, um Daten abzurufen, zu senden oder zu bearbeiten.
Cloud-Computing	Cloud-Computing ist ein Modell zur Bereitstellung von IT-Ressourcen wie Rechenleistung, Speicher, Software und Netzwerk über das Internet ("die Cloud").
Cloud-nativ	Cloud-native bezeichnet einen Ansatz zur Softwareentwicklung, bei dem Anwendungen speziell für die Ausführung in Cloud-Umgebungen konzipiert werden. Cloud-native Anwendungen sind in der Regel modular aufgebaut, skalierbar und nutzen die Vorteile von Cloud-Diensten wie Computing, Storage und Netzwerk.
Customer Identity and Access Management (CIAM)	CIAM (Customer Identity and Access Management) ist ein System zur Verwaltung von Identitäten und Zugriffsrechten von <u>externen</u> Kunden z. B. im Kontext von Online-Diensten. Es ermöglicht eine sichere Authentisierung, Autorisierung und Verwaltung von Kundeninformationen, um personalisierte Benutzererfahrungen zu bieten und gleichzeitig Datenschutz- und Sicherheitsanforderungen zu erfüllen. CIAM unterstützt Funktionen wie Single-Sign-On (SSO), Multi-Faktor-Authentisierung (MFA) und Einwilligungsmanagement.
Container Images	Container Images sind ausführbare Softwarepakete, die alle notwendigen Komponenten wie Code, Laufzeitumgebungen, Bibliotheken und Abhängigkeiten enthalten, um eine Anwendung konsistent auf verschiedenen Container-Plattformen auszuführen. Sie dienen als Vorlage bzw. Basisbestandteil für die Erstellung von Containern, die isolierte und portable Anwendungen ermöglichen, und werden häufig in containerisierten Plattformen wie Docker und Kubernetes verwendet. Container Images fördern die Effizienz und Konsistenz in der Anwendungsbereitstellung.

Begriff	Erläuterung
Bundeseinheitliches Datenbankgrundbuch (dabag)	Das bundeseinheitliche Datenbankgrundbuch (dabag) ist ein elektronisches System zur digitalen Erfassung, Verwaltung und Einsichtnahme von Grundbuchdaten. Es soll künftig eine effiziente und transparente Dokumentation von Grundstücksrechten und -transaktionen ermöglichen.
DDoS Prevention	DDoS steht für Distributed Denial of Service. Es handelt sich um einen Cyberangriff, bei dem eine Vielzahl von Computern (oftmals Botnets) genutzt wird, um ein Zielsystem (z. B. einen Server) mit Anfragen zu überfluten. Dadurch werden die Ressourcen des Zielsystems erschöpft und es kann für legitime Benutzer nicht mehr erreichbar sein.
DevOps	DevOps ist eine Methodologie, die Entwicklung (Development) und IT-Betrieb (Operations) so miteinander integriert, dass die Zusammenarbeit zwischen diesen beiden Bereichen verbessert wird. Ziel ist es, Software schneller und zuverlässiger zu entwickeln, zu testen und bereitzustellen, indem automatisierte Prozesse, kontinuierliche Integration und kontinuierliche Bereitstellung (siehe CI/CD) gefördert werden.
DevSecOps	DevSecOps ist ein Ansatz, bei dem Sicherheitsaspekte von Anfang an in den Softwareentwicklungsprozess integriert werden. Es kombiniert die Bereiche Development (Entwicklung), Security (Sicherheit) und Operations (Betrieb). Ziel ist es, durch Automatisierung und Zusammenarbeit, Sicherheitsprobleme frühzeitig zu erkennen und zu beheben, um sichere und zuverlässige Software schneller bereitzustellen.
Domain-Driven Design (DDD)	Domain-Driven Design ist ein Ansatz zur Softwareentwicklung, der die Fachlichkeit (Domäne) in den Mittelpunkt stellt. Es geht darum, die Komplexität der Software durch eine enge Zusammenarbeit zwischen Entwicklern und Fachexperten zu beherrschen, ein gemeinsames Verständnis der fachlichen Domäne zu schaffen und dabei die Software entsprechend dem fachlichen Schnitt zuzuschneiden.
eAkten-System	Ein eAkten-System ist ein integriertes digitales System zur Verwaltung und Bearbeitung der Gerichtsakten. Es gibt verschiedene Lösungen in der Justiz: <u>eAs (elektronische Aktenlösung)</u> <u>e2A (elektronische Aktenverarbeitung)</u> <u>eIP (elektronisches Informationsportal)</u>
e-CODEX	e-CODEX ist das in der Verordnung 2022/850(EU) normierte, dezentrale und interoperable System für den sicheren, grenzüberschreitenden elektronischen Austausch von Daten zwischen Gerichten und anderen Justizbehörden untereinander sowie mit Bürgern und Unternehmen in der EU.
EfA-Prinzip (Einer-für-Alle)	Das EfA-Prinzip ist ein Konzept im deutschen E-Government, das die Zusammenarbeit und Effizienz bei der Digitalisierung von Verwaltungsleistungen fördern soll. Es besagt, dass eine digitale Verwaltungsleistung nur einmal entwickelt und dann von anderen Behörden und Kommunen nachgenutzt werden soll. Damit sollen Doppelarbeit vermieden und Kosten durch die gemeinsame Nutzung von digitalen Lösungen reduziert werden.

Begriff	Erläuterung
Elektronische Gefangenenpersonalakte (eGPA)	Die elektronische Gefangenenpersonalakte (eGPA) ist ein digitales System zur Erfassung und Verwaltung von Personalakten von Inhaftierten. Es ermöglicht die elektronische Dokumentation von Informationen zu Haftbedingungen, Verhaltensauffälligkeiten und Rehabilitationsmaßnahmen, um die Effizienz und Transparenz im Justizvollzug zu erhöhen.
Elektronisches Gerichts- und Verwaltungspostfach (EGVP)	Das elektronische Gerichts- und Verwaltungspostfach (EGVP) ist ein digitales Kommunikationssystem, das den sicheren Austausch von Dokumenten zwischen Gerichten, Behörden und Rechtsanwälten ermöglicht. Es dient der elektronischen Übermittlung von Schriftstücken im Rahmen von Verwaltungs- und Gerichtsverfahren und fördert die Effizienz und Rechtsverbindlichkeit der Kommunikation.
Elektronisches Saalmanagement (e2S)	Das elektronische Saalmanagement (e2S) ist ein digitales System zur Planung, Verwaltung und Organisation von Räumlichkeiten in öffentlichen Einrichtungen, wie z.B. Gerichten oder Verwaltungen. Es ermöglicht eine effiziente Raumnutzung durch die digitale Buchung, Zuweisung und Koordination von Besprechungs- und Veranstaltungsräumen, unterstützt die Ressourcentransparenz und verbessert die Logistik in der Raumplanung.
E-Justice Rat	Der E-Justice-Rat ist ein Gremium der Justiz in Deutschland, das sich mit der Digitalisierung der Justiz befasst. Ihm gehören die Staatssekretärinnen und Staatssekretäre bzw. Amtschefinnen und Amtschefs der Justizverwaltungen des Bundes und der Länder an. Ziele sind z. B. die Koordinierung und Steuerung von Digitalisierungsaktivitäten, Entwicklung gemeinsamer Standards und Schnittstellen, um den Datenaustausch zwischen den verschiedenen Justizbehörden zu verbessern und Unterstützung der Einführung neuer Technologien und der Modernisierung der Justiz.
Fachaufsicht vs. Rechtsaufsicht	Fachaufsicht: Die Fachaufsicht ist ein wichtiges Instrument zur Steuerung und Kontrolle der öffentlichen Verwaltung. Sie überprüft sowohl die Rechtmäßigkeit als auch die Zweckmäßigkeit des Verwaltungshandelns, um eine einheitliche Aufgabenerfüllung zu gewährleisten. Rechtsaufsicht: Die Rechtsaufsicht überprüft nur die Rechtmäßigkeit des Verwaltungshandelns, um sicherzustellen, dass die Verwaltung in ihrem Handeln die Gesetze und sonstige Rechtsvorschriften einhält.
Fat Clients	Fat Clients sind Computer, die einen Großteil der Anwendungslogik, Datenverarbeitung und Ressourcen lokal ausführen, anstatt auf einen Server oder die Cloud zuzugreifen. In dem Fall erfolgt der Zugriff auf die Justizaufwendungen der internen Domäne typischerweise über Fat Clients, d. h. in auf dem PC-Arbeitsplatz der Nutzenden installierten Anwendungen. Demnach erfordert eine Aktualisierung dieser Anwendung auch jeweils die Arbeit am jeweiligen Desktop.

Begriff	Erläuterung
Fein-granulare (fine-grained) vs. Grob-granulare (coarse-grained) Authorisierung	Diese Begriffe beschreiben zwei Ansätze zur Zugriffskontrolle, die sich in der Granularität der Berechtigungen unterscheiden: Coarse-grained Authorization (grobgranulare Berechtigung) • Prinzip: Vergabe von Berechtigungen auf einer hohen Ebene, z. B. basierend auf Rollen (z. B. "Administrator", "Benutzer"). • Beispiel: Alle Benutzer mit der Rolle "Redakteur" haben Zugriff auf alle Artikel im CMS. • Vorteile: Einfache Implementierung und Verwaltung. • Nachteile: Geringere Flexibilität und Sicherheit, da nicht auf individuelle Bedürfnisse eingegangen werden kann. Fine-grained Authorization (feingranulare Berechtigung) • Prinzip: Vergabe von Berechtigungen auf einer detaillierten Ebene, z. B. basierend auf Attributen, Kontext oder Daten. • Beispiel: Ein Benutzer darf nur Artikel in bestimmten Kategorien und zu bestimmten Zeiten bearbeiten, die er selbst erstellt hat. • Vorteile: Höhere Flexibilität und Sicherheit, da Berechtigungen präzise an individuelle Bedürfnisse angepasst werden können. • Nachteile: Komplexere Implementierung und Verwaltung.
FinOps	FinOps ist ein Ansatz für das Cloud Financial Management, der die Zusammenarbeit zwischen verschiedenen Teams wie IT, Finanzen und Business fördert, um die Cloud-Kosten zu verstehen, zu optimieren und zu kontrollieren.
Fördergesellschaft für IT-Kooperationen (FITKO)	Die Fördergesellschaft für IT-Kooperationen (FITKO) ist eine deutsche Institution, die die digitale Transformation in der öffentlichen Verwaltung unterstützt. Sie fördert die Zusammenarbeit zwischen Bund, Ländern und Kommunen, um innovative IT-Lösungen zu entwickeln und zu implementieren sowie die Effizienz und Benutzerfreundlichkeit öffentlicher Dienstleistungen verbessern.
Gemeinsames Fachverfahren (GeFa)	GeFa steht für Gemeinsames Fachverfahren und ist ein zentrales Digitalisierungsprojekt der deutschen Justiz. Es handelt sich um eine neue, einheitliche Software, die für alle Gerichte und Staatsanwaltschaften in Deutschland entwickelt wird. Ziel ist die Ablösung der veralteten und uneinheitlichen IT-Systeme in der Justiz durch eine moderne, benutzerfreundliche und zukunftsfähige Softwarelösung.
GitOps (sog. GitOperations)	GitOps ist ein Ansatz zur Automatisierung und Verwaltung von Cloud-nativen Anwendungen und Infrastrukturen, der Git als zentrale Quelle/Repository für die Konfiguration von Anwendungen und Infrastruktur verwendet. Die Kernidee ist, dass alle Konfigurationen, Deployments und Änderungen in Git-Repositories versioniert verwaltet werden. Ein automatisierter Prozess stellt sicher, dass der gewünschte, in Git definierte Zustand, mit dem tatsächlichen Zustand des Systems übereinstimmt.
GraphQL	GraphQL ist eine Abfragesprache für APIs und eine serverseitige Laufzeitumgebung, die 2015 als Open Source veröffentlicht wurde. Sie stellt eine moderne Alternative zu REST-APIs dar und bietet eine effizientere und flexiblere Möglichkeit, Daten zwischen Client und Server auszutauschen.

Begriff	Erläuterung
„Greenfield“-Ansatz	Der „Greenfield“-Ansatz beschreibt ein Vorgehen bei der Softwareentwicklung, bei dem ein Projekt von Grund auf neu begonnen wird, ohne dabei auf bestehende Systeme oder Codebasen zurückzugreifen.
gRPC	gRPC steht für Remote Procedure Calls. Es handelt sich um ein modernes, von Google entwickeltes, Open-Source-Framework für Remote Procedure Calls (RPCs), das in verschiedenen Umgebungen eingesetzt werden kann.
IAM	IAM steht für Identity and Access Management (Identitäts- und Zugriffsmanagement). Es umfasst die Richtlinien und Technologien, die verwendet werden, um den Zugriff von Benutzern und Geräten auf digitale Ressourcen zu verwalten und zu kontrollieren.
Identity Provider (IdP)	Der Identity Provider ist ein Dienst, der die Authentisierung von Nutzenden übernimmt und Identitätsinformationen über die Nutzenden hält und bereitstellt, welche für den Zugang zu verschiedenen Anwendungen oder Systemen benötigt werden. Der IdP verwaltet die Anmeldeinformationen der Nutzenden und stellt anderen Diensten vertrauenswürdige Informationen zur Identität bereit, oft im Zusammenhang mit Single-Sign-On (SSO) oder anderen Authentisierungsmechanismen.
Inferenz	KI-Inferenz ist der Prozess, bei dem ein trainiertes KI-Modell verwendet wird, um Vorhersagen oder Entscheidungen über neue, unbekannte Daten zu treffen. Nachdem ein KI-Modell gelernt hat (durch Training), wird es in der Inferenzphase angewendet, um "Schlussfolgerungen" aus neuen Daten zu ziehen.
Integrationstests	Ein Integrationstest ist ein Verfahren in der Softwareentwicklung, um das Zusammenspiel verschiedener Module oder Komponenten eines Systems zu überprüfen. Ziel ist es, sicherzustellen, dass die einzelnen Module, die unabhängig voneinander entwickelt wurden, korrekt miteinander interagieren und als Gesamtsystem funktionieren.
Intrusion Prevention System (IPS)	Ein Intrusion Prevention System (IPS), auch bekannt als Intrusion Detection and Prevention System (IDPS), ist eine Sicherheitstechnologie, die Netzwerke oder Systeme auf bössartige Aktivitäten überwacht und diese aktiv blockiert. Dabei wird der Netzwerkverkehr auf Muster analysiert, die auf Angriffe hindeuten.
IT-Kontrollkommission	Die IT-Kontrollkommission ist ein justizielles Gremium, dass die Unabhängigkeit der Justiz / dritten Gewalt in den IT-Systemen sicherstellen soll.
IT-Planungsrat	Der IT-Planungsrat ist ein wichtiges politisches Steuerungsgremium in Deutschland, das sich mit der Digitalisierung der öffentlichen Verwaltung befasst. Er wurde 1997 gegründet und setzt sich aus Vertretern des Bundes und der Länder zusammen.
JBoss	JBoss ist eine Sammlung von Open-Source-Softwareprodukten für Enterprise-Anwendungen, die von Red Hat entwickelt und vertrieben werden. Der Name "JBoss" bezieht sich hauptsächlich auf den JBoss Application Server, der in WildFly umbenannt wurde.

Begriff	Erläuterung
JEE	JEE steht für Jakarta Enterprise Edition, früher bekannt als Java Platform, Enterprise Edition (Java EE). Es handelt sich um eine Sammlung von Spezifikationen und APIs für die Entwicklung und Ausführung von Enterprise-Anwendungen in Java.
JSF	JSF steht für Jakarta Server Faces (früher JavaServer Faces) und ist ein komponentenbasiertes Framework zur Entwicklung von Benutzeroberflächen für Webanwendungen in Java. Es ist Teil der Jakarta EE (früher Java EE) Spezifikation.
Cloud Landing Zone	Eine Cloud Landing Zone ist ein grundlegendes Konstrukt für die Einrichtung und Verwaltung einer Cloud-Umgebung. Sie dient als Fundament für die Bereitstellung von Workloads und Anwendungen in der Cloud und stellt sicher, dass diese sicher, skalierbar sind und den Unternehmensrichtlinien entsprechen.
Large-Language-Modell (LLM)	Ein Large Language Model (LLM) ist ein fortschrittliches KI-System, das darauf trainiert wurde, menschliche Sprache zu verstehen und zu generieren. Es basiert auf Deep-Learning-Techniken und wird mit riesigen Mengen an Textdaten gefüttert, um Muster und Beziehungen in der Sprache zu erkennen.
Mandantenfähigkeit	In einer bundeseinheitlichen Justizcloud könnten Anwendungen aus einer Betriebsinfrastruktur und einer Instanz, d. h. einer Installation einer Anwendung, für verschiedene Mandanten (z. B. Länder, Gerichte etc.) betrieben und administriert werden (SaaS). Dafür müssen Anwendungen jedoch bspw. in der Lage sein, durch Anpassungen im Berechtigungsmanagement Nutzende verschiedener Mandanten zu unterscheiden und eine strikte, logische Trennung von Daten verschiedener Mandanten zu implementieren.
Microservice-Architektur	Eine Microservice-Architektur ist ein Software-Designansatz, der eine Anwendung als Sammlung kleinerer, unabhängiger Dienste strukturiert, die jeweils spezifische Funktionen erfüllen. Jeder Microservice kann unabhängig entwickelt, bereitgestellt und skaliert werden, was die Flexibilität, Wartbarkeit und Wiederverwendbarkeit erhöht. Diese Architektur ermöglicht eine bessere Anpassungsfähigkeit an Änderungen und fördert die Nutzung verschiedener Technologien innerhalb derselben Anwendung.
Application Monitoring	Application Monitoring ist ein Prozess zur Überwachung der Leistung und Verfügbarkeit von Softwareanwendungen. Er umfasst die Erfassung und Analyse verschiedener Metriken, um Probleme zu erkennen, die Performance zu optimieren und die Benutzererfahrung zu verbessern.
Multi-instanzierter Betrieb	Bezeichnet eine Architektur, bei der mehrere Instanzen einer Softwareanwendung oder eines Systems gleichzeitig auf einer gemeinsamen Infrastruktur betrieben werden. Jede Instanz ist unabhängig und kann unterschiedliche Konfigurationen oder Daten haben, was eine flexible Nutzung für verschiedene Kunden oder Geschäftsbereiche ermöglicht. Dieser Ansatz fördert die Ressourcennutzung, Effizienz und Skalierbarkeit in der Softwarebereitstellung.

Begriff	Erläuterung
Minimum Viable Product (MVP)	MVP steht für Minimum Viable Product. Es beschreibt eine Produktversion mit minimalen, aber dennoch funktionsfähigen Features, die <u>in der Produktion</u> veröffentlicht werden, um frühzeitig Feedback von Nutzenden zu erhalten und das Produkt iterativ weiterzuentwickeln. Anstatt ein Produkt vollständig zu entwickeln, bevor es auf den Markt kommt, wird beim MVP-Ansatz eine abgespeckte Version mit den wichtigsten Funktionen veröffentlicht. So können schnell erste Rückmeldungen von Nutzenden gesammelt und in die weitere Entwicklung integriert werden.
Mutual Transport Layer Security (mTLS)	mTLS steht für Mutual Transport Layer Security und ist eine Methode zur beidseitigen Authentifizierung in Netzwerkverbindungen. Im Gegensatz zum herkömmlichen TLS, bei dem nur der Server seine Identität gegenüber dem Client bestätigt, authentifizieren sich bei mTLS beide Seiten gegenseitig.
Netze des Bundes (NdB)	Die Netze des Bundes (NdB) sind alle Netze und Bundesnetze, die innerhalb des Rechtsrahmens von Artikel 91c GG sowie IT-NetzG fallen. Beispiele dafür sind Netze der Verfassungsschutzbehörden sowie des Auswärtigen Amts, das Verbindungsnetz uvm. Sie gewährleisten den Datenaustausch zwischen Behörden, bieten eine Plattform für digitale Verwaltungsprozesse und dienen bspw. auch als Integrationsplattform für Weitverkehrsnetze der Verwaltung.
Optical Character Recognition (OCR)	Optical Character Recognition (OCR) ist eine Technologie zur automatischen Erkennung und Umwandlung von gedrucktem oder handschriftlichem Text in maschinenlesbare, digitale Daten. Sie wird häufig verwendet, um gedruckte Dokumente, Bilder und PDFs zu digitalisieren, sodass der Text bearbeitet, durchsucht und gespeichert werden kann. OCR verbessert die Effizienz bei der Datenverarbeitung und erleichtert den Zugriff auf Informationen.
Penetration Test (Pentests)	Ein Penetrationstest (auch bekannt als Pentest) ist ein simulierter Cyberangriff auf ein Computersystem, um Schwachstellen zu identifizieren.
REST	REST steht für Representational State Transfer. Es ist ein Architekturstil für verteilte Systeme, der insb. für Webservices verwendet wird. REST hat sich zu einem der wichtigsten Paradigmen für die Entwicklung von Web-APIs entwickelt.
Proof-of-Concept (PoC)	Proof-of-Concept (PoC) (deutsch: "Machbarkeitsnachweis"), ist ein Verfahren, um die Realisierbarkeit einer Idee oder eines Konzepts zu demonstrieren, bevor in die vollständige Entwicklung investiert wird.
Scaled Agile Framework (SAFe)	SAFe ist ein umfassendes Rahmenwerk zur Skalierung agiler Praktiken in großen Organisationen. Es bietet strukturierte Ansätze und Best Practices für die Umsetzung von Agilen und Lean Methoden in verschiedenen Ebenen einer Organisation, einschließlich Team-, Programm- und Portfolio-Ebene. SAFe zielt darauf ab, die Zusammenarbeit, Effizienz und Produktivität zu verbessern, während es gleichzeitig eine agile Lieferkette und wertschöpfende Prozesse fördert.
SAFE mit OAuth (SAmOA)	Die Initiative SAmOA erweitert das bekannte SAFE-System zur Authentisierung von Nutzendenzugriffen, um moderne OAuth 2.0 Fähigkeiten (z. B. JWT-Token).

Begriff	Erläuterung
Software-defined Wide Area Network (SD-WAN)	SD-WAN ist ein moderner Ansatz für die Verwaltung von Unternehmensnetzwerken, der Software verwendet, um den Datenverkehr intelligent und effizient über verschiedene WAN-Verbindungen zu leiten.
Single-Sign-On (SSO)	SSO ist ein Authentisierungsverfahren, das es Nutzern ermöglicht, sich mit einer Anmeldung bei mehreren Anwendungen oder Systemen anzumelden. Dadurch entfällt die Notwendigkeit, sich für jeden Dienst separat zu authentifizieren und verschiedene Passwörter zu verwenden, was die Benutzerfreundlichkeit erhöht und die Sicherheit verbessert, indem zentrale Multifaktor-Zugangskontrollen genutzt werden.
Step-up-Authentication	Step-up-Authentication (deutsch: gestufte Authentifizierung) ist ein Sicherheitskonzept, bei dem je nach Risikostufe einer Aktion oder eines Zugriffs auf bestimmte Ressourcen zusätzliche Authentisierungsfaktoren angefordert werden.
SQL	SQL steht für Structured Query Language (deutsch: strukturierte Abfragesprache). Es ist die Standardsprache für die Kommunikation mit relationalen Datenbanken. Mit SQL können Daten in Datenbanken definiert und abgefragt werden.
Technologie-Stack (Tech-Stack)	Technologie-Stack bezeichnet die Gesamtheit der Technologien, Programmiersprachen, Frameworks und Tools, die zur Entwicklung und Bereitstellung einer Softwareanwendung oder eines Systems verwendet werden. Der Technologie-Stack kann in verschiedene Schichten unterteilt werden: <u>Frontend</u>: umfasst alle Technologien, die für die Gestaltung und Entwicklung der Benutzeroberfläche verantwortlich sind. <u>Backend</u>: umfasst die serverseitigen Technologien, die für die Verarbeitung von Anfragen, die Verwaltung von Daten und die Geschäftslogik verantwortlich sind. <u>Middleware</u>: fungiert als Vermittler zwischen dem Frontend und dem Backend, indem sie Daten und Befehle zwischen den beiden Schichten austauscht. Middleware kann Dienste wie APIs, Authentisierung, Datenverarbeitung und Integration von Drittanbieterdiensten umfassen.
Virtual Private Cloud (VPC)	VPC ist ein virtualisierter, isolierter Bereich innerhalb einer öffentlichen Cloud, der benutzerdefinierte Ressourcen wie Rechenleistung, Speicher und Netzwerk zur Verfügung stellt.
Virtual Private Network (VPN)	Ein VPN ist eine Technologie, die eine sichere und verschlüsselte Verbindung über ein öffentliches Netzwerk wie das Internet herstellt.

7 Anhang

7.1 Standardisierter Fragebogen Justizanwendungen

#	Fragen Fragebogen Justizanwendungen
1.	Allgemeine Fragen zur Anwendung
1.1	Welche fachlichen Funktionen bietet die Anwendung?
1.2	Welche justizinternen und/ oder -externen Nutzenden(-gruppen) hat die Anwendung? (z. B. Justizverwaltung, Gerichte, Anwälte, Bürger)
1.3	Wo steht die Anwendung in ihrem Lebenszyklus? Wird die Anwendung noch aktiv weiterentwickelt oder wird eine Ablösung vorbereitet?
1.4	Handelt es sich bei der Anwendung um eine Kaufsoftware oder Eigenentwicklung?
1.5	Ist die Anwendung multi-mandantenfähig?
1.6	Wird die Anwendung landesübergreifend entwickelt? Wenn ja, von wem? Gibt es relevante organisatorische Besonderheiten?
1.7	Wird die Anwendung landesübergreifend genutzt und betrieben? Wenn ja, von wem? Gibt es relevante organisatorische Besonderheiten?
1.8	Bestehen länderspezifische Unterschiede in den Anforderungen an die Anwendung? Gibt es Potenzial für ein bundeseinheitliches Vorgehen?
1.9	Bestehen derzeit besondere fachliche Herausforderungen bei Nutzung der Anwendungen (z. B. Ausfälle, Performanz, Innovationspotenzial etc.)
1.10	Welches Konsolidierungspotenzial besteht aus Nutzendenperspektive mit anderen Anwendungen?
1.11	Bestehen wesentliche Abhängigkeiten und/ oder Schnittstellen mit anderen Fachverfahren, Querschnitts-/ Basisdiensten oder zu Desktop-Anwendungen?
1.12	Ist die Anwendung eine Client-Serverapplikation mit Zugriff über Web-UI oder eine Desktop-Applikation?
1.13	Welche Nutzer-/ Berechtigungsmanagement-Lösung verwendet die Anwendung?
1.14	Welche Datenklassifizierung haben die Daten der Anwendung (unkritisch, normal, hoch, sehr hoch)?
1.15	Welche Verfügbarkeitsanforderungen bestehen an die Anwendung (z. B. "hoch verfügbar"; 24x7 etc.)?
1.16	Welche länderspezifischen Anforderungen an IT-Sicherheit und Datenschutz bestehen?
1.17	Bestehen fachliche/ technische Bedarfe und wesentliche künftige Anforderungen an die Anwendung, die derzeit nicht bedient werden?
2.	Fragen zur Entwicklung der Anwendung
2.1	Exponiert die Anwendung moderne Schnittstellen (z. B. API, X-Austausch)?

#	Fragen Fragebogen Justizanwendungen
2.2	Inwieweit stellen Schnittstellen in der Anwendungsentwicklung eine Herausforderung dar?
2.3	Wird die Anwendung bereits Cloud-ready, d. h. "containerisiert", entwickelt?
2.4	Nutzt die Anwendung eine automatisierte Continuous Integration/ Continuous Delivery (CI/CD) Pipeline?
2.5	Kann die Infrastruktur für die Anwendung durch den Entwicklungsverbund/ Hersteller der Anwendung automatisch aufgesetzt werden? (Infrastructure as Code)
2.6	Wie oft findet eine Übergabe von neuen Anwendungsversionen in den Betrieb statt und wie lange dauert diese?
2.7	Wie groß ist das Entwicklungs-Team in etwa?
2.8	Wo findet die Entwicklung der Anwendung statt (z. B. beim IT-Dienstleister des Landes oder in einer kommerziellen Cloud-Entwicklungsumgebung)?
2.9	Wo findet der Test der Anwendung statt (z. B. beim IT-Dienstleister des Landes oder in einer kommerziellen Cloud-Entwicklungsumgebung)?
2.10	Wie lange dauert die Bereitstellung eines Entwicklerarbeitsplatzes (z. B. Entwicklungs-Desktop mit Tooling, Berechtigungen, Zugang zu Entwicklungsumgebungen)?
2.11	Bestehen derzeit besondere Herausforderungen bei der Entwicklung der Anwendung?
3.	Fragen zum Betrieb der Anwendung
3.1	Wie groß und in welcher Organisation ist das Team für die fachliche Anwendungsbetreuung (Fachverfahrenspflegestelle) verortet?
3.2	Wie groß und in welcher Organisation ist das Team für die technische Anwendungsbetreuung verortet?
3.3	Wie groß und in welcher Organisation ist das Team für die Betreuung der Infrastruktur im Rechenzentrum verortet?
3.4	Sind verschiedene Versionen gleichzeitig im Betrieb? Wenn ja, wie viele Versionen?
3.5	Wo findet der Betrieb der Anwendung statt (z. B. einmal beim IT-Dienstleister oder mehrere Male pro Gericht)?
3.6	Bestehen derzeit besondere Herausforderungen beim Betrieb der Anwendung?
3.7	Bestehen wesentliche Auslagerungen? (z. B. Auslagerung bei Betriebstätigkeiten oder Infrastruktur an Dritte)

7.2 Standardisierter Fragebogen IT-Dienstleister

#	Fragen Fragebogen IT-Dienstleister
1.	Allgemeine Fragen zur Justiz als Kunde
1.1	Ist die Justiz alleinige Kundin/ Nutzerin des Rechenzentrums/ IT-Dienstleisters? Wenn nein, wie viel Prozent der Leistungen bezieht die Justiz in etwa?
1.2	Gibt es ein zentrales Portfoliomanagement zu Anforderungsaufnahmen (der Justiz)?
1.3	Welche Anwendungen der Justiz werden beim IT-Dienstleister betrieben (siehe Liste der Fachapplikationen des <i>BLK-Architekturbüros</i>)?
1.4	Für welche dieser Anwendungen übernimmt der IT-Dienstleister Infrastrukturbetrieb, technischen Anwendungsbetrieb und/ oder Entwicklungsleistungen für die Justiz?
1.5	Werden Justizanwendungen anderer Länder oder des Bundes neben dem eigenen Träger-Land betrieben? Wenn ja, für wen und welche?
1.6	Gibt es Schmerzpunkte beim Betrieb der Justizanwendungen (z. B. Ausfälle, häufige Änderungen, Besonderheiten der Justiz)?
1.7	Gibt es aktuelle IT-Bedarfe der Justiz, die als herausfordernd empfunden werden (z. B. Speichertechnologien)?
1.8	Gibt es einen fest definierten Landesarbeitsplatz (z.B. Windows, Office)? Gibt es einen Arbeitsplatz spezifisch für die Justiz?
1.9	Wie stark ist das Rechenzentrum ausgelastet (bzgl. physischer und personeller Kapazitäten)?
1.10	Werden Services nur innerhalb des Landesverwaltungsnetzwerks oder auch über andere Netze angeboten?
1.11	Ist die Netzstrategie 2030 (Beschluss IT-Rat) im Land umgesetzt? Gibt es eine landesübergreifende Anbindung über <i>BDBOS</i> ?
1.12	Wie ist die Verantwortungstrennung bzgl. IT Sicherheit zwischen IT-Dienstleister, Justizministerium und Anwendungsbetrieb geregelt?
2.	Fragen zu Cloud-Initiativen und Cloud-Service-Portfolio des IT-Dienstleisters
2.1	Hat der IT-Dienstleister eine Cloudstrategie? Wenn ja, welche (Hybrid/ Community/ Multi cloud, etc.)?
2.2	Stellt der IT-Dienstleister der <i>Deutsche VerwaltungscLOUD (DVC)</i> oder einer anderer Cloud-Initiative Dienste zu Verfügung? Wenn ja, welche?
2.3	Welche Clouddienste von anderen Providern (z. B. Hyperscalern oder <i>DVC</i>) nutzt der IT-Dienstleister selbst? Wenn ja, welche?
2.4	Welche IaaS- und PaaS-Dienstangebote sind aktuell durch Kunden (z. B. Justizministerien, Gerichte) bestellbar und gibt es einen Servicekatalog mit Gebühren?
2.5	Unterstützen die PaaS-Dienstangebote Mandantentrennung?
2.6	Wer trägt die Betriebsverantwortung für die IaaS- und PaaS-Dienste?
2.7	Sind verschiedene Dienste in Kombination bestellbar und automatisch miteinander verzahnt (z.B. PaaS auf IaaS)?
2.8	Gibt es ein Bestell-Serviceportal oder APIs, um Dienste vom IT-Dienstleister automatisiert bestellen zu können? Wenn ja, welche?
2.9	Wie lange dauert die Bereitstellung von virtueller Infrastruktur? Ist IaC (Automatische Provisionierung) möglich oder sind manuelle Eingriffe nötig?
2.10	Sind die IaaS- und PaaS-Dienstangebote skalierbar?

#	Fragen Fragebogen IT-Dienstleister
2.11	Werden Dienste redundant an mehr als einem Rechenzentrumsstandort betrieben?
2.12	Sind vorgehaltenen Überkapazitäten fest einem Kunden/ Mandanten zugewiesen oder werden sie über alle Kunden gepoolt?
2.13	Gibt es einen automatisierten verbrauchsbasierten Abrechnungsprozess? Kann der Kunde seine Kosten zeitnah selbst pro Dienst auswerten und kontrollieren?
2.14	Bestehen Service Level Agreements (SLAs) auf Infrastrukturebene (IaaS) sowie auf Anwendungsebene (PaaS)?
2.15	Gibt es Herausforderungen beim Aufbau von Cloud-Kompetenzen bzw. Cloud-Wissensaufbau?
3.	Fragen zu IT-Organisation
3.1	Untersteht der IT-Dienstleister der Justiz? Wenn nein, wem?
3.2	Welche Rechtsform hat der IT-Dienstleister?
3.3	Unterliegt Ihre Organisation anderen rechtlichen Beschränkungen bspw. durch Festschreibung in Ihrem Gründungserlass?
3.4	Wie ist die Organisationsform des IT-Dienstleisters strukturiert (z.B. nach Services, nach Produkten, nach Kundensegmenten, Fachkompetenzen)?
3.5	Wie werden Dienstleistungen für die Justiz abgerechnet?
3.6	Bestehen Kontrahierungszwänge mit der Justiz? Wenn ja, welche?
3.7	Gibt es IT-Investitionen des Landes und der Justiz, die geschützt werden müssen? (z.B. Rechenzentrumsmodernisierung)?
3.8	In welchen Justizcloud relevanten Projekten oder Initiativen arbeitet der IT-Dienstleister aktuell (bund-)länderübergreifend?
3.9	Wie tauscht sich der IT-Dienstleister mit anderen IT-Dienstleistern der Justiz aus?
3.10	Wer übernimmt Vertragsverhandlungen und Auslagerungsmanagement (z.B. kommerziellen Herstellern)? Welchen Anteil übernimmt der IT-Dienstleister und welchen die Justiz?

Rechtliche Hinweise

Haftungsausschluss

Dieses Dokument wurde mit größtmöglicher Sorgfalt erstellt. Das Material in diesem Dokument spiegelt Informationen wider, die zum Zeitpunkt der Erstellung dieses Dokuments verfügbar waren, wie durch das auf der Titelseite angegebene Datum angegeben, jedoch entwickelt sich die globale Situation schnell und die Position kann sich ändern. Diese Inhalte werden nur zu allgemeinen Informationszwecken zur Verfügung gestellt, berücksichtigen nicht die spezifischen Umstände des Lesers und sind nicht als Ersatz für die Beratung mit professionellen Beratern gedacht. Insb. übernimmt Accenture keine Haftung für die Nutzung der Untersuchung oder daraus abgeleitete Entscheidungen, insb. nicht für finanzielle Verluste oder andere Schäden, soweit dies rechtlich zulässig ist. Accenture übernimmt ebenso keine Haftung für die Richtigkeit und Vollständigkeit der Informationen in diesem Dokument. Accenture bietet keine rechtliche, regulatorische, Prüfungs- oder Steuerberatung an. Die Inhalte dieser Untersuchung sind nicht als rechtliches Gutachten zu verstehen. Die Inhalte dieses Dokuments sind urheberrechtlich geschützt.

Über Accenture

Accenture ist ein weltweit tätiges Beratungsunternehmen, führend in Digitalisierung, Cloud und Security. Wir bringen unsere umfassende Erfahrung und spezialisierten Fähigkeiten in mehr als 40 Branchen ein und bieten Dienstleistungen aus den Bereichen Strategy & Consulting, Interactive, Technology und Operations, gestützt auf das weltweit größte Netzwerk aus Zentren für Advanced Technology und Intelligent Operations. Unsere über 700.000 Mitarbeitenden arbeiten jeden Tag für Kunden in über 120 Ländern daran, Technologie und menschliche Kreativität zu vereinen. Wir setzen auf Veränderung, um Mehrwert und gemeinsamen Erfolg zu schaffen, für Kunden, Mitarbeitende, Aktionäre, Partner und für die Gemeinschaft. Besuchen Sie uns unter www.accenture.com.

Copyright © 2025 Accenture.

Alle Rechte vorbehalten. Accenture und das dazugehörige Logo sind Marken oder eingetragene Marken der Accenture Plc in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.