




# Föderale Digitalstrategie



**Digitale  
Transformation**




**Digitale  
Infrastruktur**



**Digitale  
Anwendungen**



**Datennutzung**



**Informations-  
sicherheit**

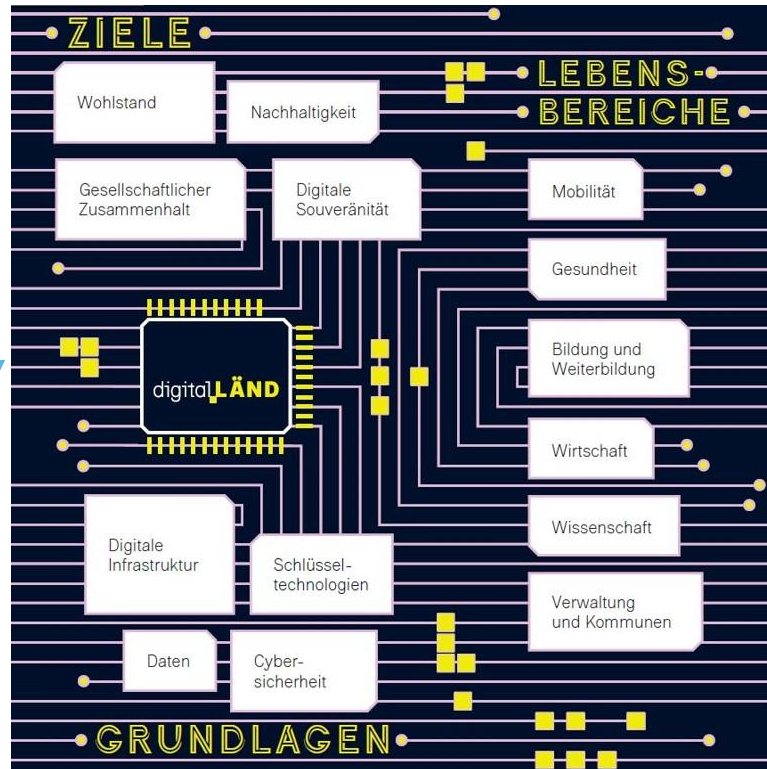
# Agenda

1. Digitalisierungsstrategie digital.LÄND
2. Digitale Verwaltung und KI
3. Cybersicherheit
4. Bundeseinheitliche Justizcloud



# 1. Digitalisierungsstrategie digital.LÄND

# Digitalisierungsstrategie digital.LÄND



Hier geht's zur Website



und hier direkt zu [www.daten-bw.de](http://www.daten-bw.de)

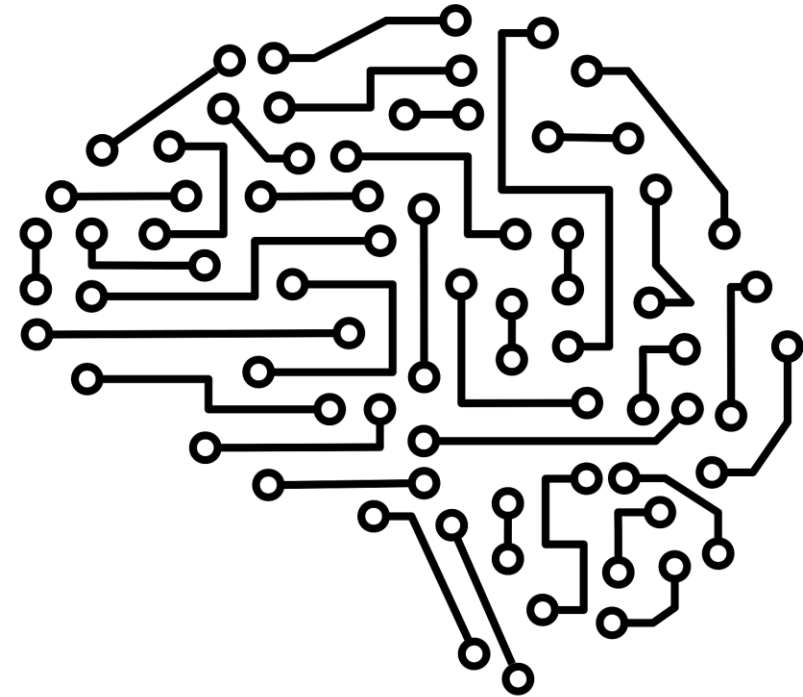




## 2. Digitale Verwaltung und KI

# KI für die Landesverwaltung

- Bedarf an KI-Anwendungen bzw. Integration in bestehende Anwendungen steigt.
- Die KI-Assistenz „F13“ steht der gesamten Landesverwaltung Baden-Württemberg zur Verfügung, ist Open Source und wird bereits nachgenutzt.
- Baden-Württemberg baut eine ressortübergreifend nutzbare, modulare Plattform für KI-Anwendungen auf, deren grundlegende Architektur „KIVA.arc“ bereits auf OpenCode veröffentlicht wurde
- Ziel ist es, gemeinsame KI-Standards zu erarbeiten und KI-Entwicklungen gemeinsam, bund-/länderübergreifend zu gestalten.




# „i-Kfz 4“: Die Fokusleistung aus Baden-Württemberg

- Projektstart: September 2021
- Fertigstellung i-Kfz 4: September 2023 (Inkrafttreten der Fahrzeugzulassungsverordnung)
- „in time and budget“
- Vorteile:
  - **„kein Gang zur Behörde mehr“**
  - **„sofortiges Losfahren“**
  - **„geringere Gebühren“**
- Aktuell nutzen bereits 141 Zulassungsbehörden (von bundesweit 411) in 12 Ländern den Onlinedienst aus Baden-Württemberg.

Meine Onlineanträge → Kraftfahrzeug zulassen oder ummelden

## Kraftfahrzeug zulassen oder ummelden

Amt für öffentliche Ordnung, Kfz-Zulassungsstelle  
Krailenshaldenstraße 32 | 70469 Stuttgart  
[Impressum](#), [Datenschutzerklärung](#), [Hilfe](#) und [Feedback](#) für diesen Onlineantrag | Version 2.4.1

STUTTGART 

1 Persönliche Angaben  \* Pflichtfeld  
2 Fahrzeugdaten   
3 Kennzeichen  
4 Antragsbearbeitung  
5 Zusammenfassung  
6 Bezahlung  
7 Bescheid

### Fahrzeugdaten

Bitte geben Sie Ihre Fahrzeug-Identifizierungsnummer (FIN) ein\*

Die FIN finden Sie in Ihrer Zulassungsbescheinigung

Handelt es sich um ein fabrikanes Fahrzeug?\*

Ja  
 Nein



# 3. Cybersicherheit

# Cybersicherheit – aktuelle Lage

Busse fahren - Service eingeschränkt

**Cyberangriff: Hacker legen Verkehrsgesellschaft Main-Tauber lahm**

Internet - Karlsruhe

**Cyberattacke auf Karlsruher Schulen: Hacker fordern Bitcoin**

Hackerangriff in Baden-Württemberg

**Cyberangriff: Fernwartungssoftware-Anbieter Teamviewer**



Bundesweite Attacken auf Städte

**Bestätigt: Prorussische Hacker für Cyberangriff auf Stadt Stuttgart verantwortlich**

IT-Sicherheit

**Cyberangriff bei Varta – Produktion heruntergefahren**

Bitkom Umfrage: Cybercrime verursacht Schaden von 179 Mrd. €

# KI-Assistent SIEM im landeseigenen Rechenzentrum BITBW

## Der KI-Assistent...

- läuft On-Premises mit europäischen LLM.
- bietet kontextsensitive Unterstützung durch natürliche Sprache und liefert umsetzbare Ratschläge in Bereichen wie Security, Observabilität und Datenanalyse.
- automatisiert repetitive Aufgaben wie Alert-Triage und Incident-Response-Vorbereitung, reduziert den manuellen Aufwand und beschleunigt Reaktionszeiten.
- unterstützt durch Integration von Expertenwissen und KI-gestützter Analyse bei der Erkennung von Anomalien und Bedrohungsmustern, reduziert False Positives und verkürzt die Verweildauer potentieller Angreifer.

# Leistungsportfolio der Cybersicherheitsagentur (CSBW)

## Prävention

- Themen- und anlassbezogene Sensibilisierungsaktionen
- In 2025 Schulungen mit mehr als 3.000 Teilnehmenden

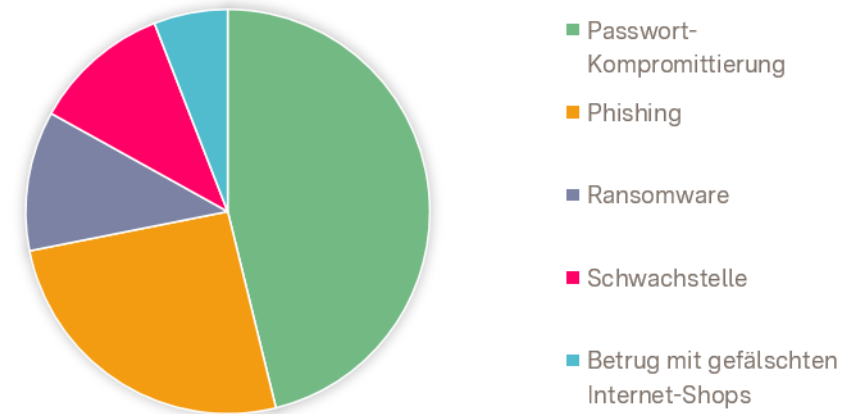
## Detektion

- mehr als 900 untersuchte Fälle im Jahr 2025, z. B.
  - in Landkreisen, Städten und Gemeinden
  - in der Landesverwaltung
  - bei Hochschulen und Universitäten
  - bei Unternehmen

## Reaktion

- Mobile Incident Response Team (MIRT)
- Cyber-Ersthilfe BW rund um die Uhr erreichbar
- Seit Ende 2024 Schwachstellenscans für öffentliche Stellen

TOP 5 DER ERFASSTEN ANGRIFFSARTEN 2025



# CyberSicherheitsCheck für KMU

Sicherheitslücken schließen

Netzübergänge absichern

Benutzerzugänge absichern

Schadprogramme abwehren

Datensicherung durchführen

Notfallplan erstellen

Gefahrenbewusstsein schaffen

Inventarisieren & Dokumentieren



## 1 SICHERHEITSLÜCKEN SCHLIESSEN

### SOFTWAREAKTUALISIERUNGEN (UPDATES UND PATCHES)

- Legen Sie einen Update-Prozess fest und benennen Sie eine verantwortliche Person.
- Aktualisieren Sie alle Anwendungen sobald ein Update oder Patch verfügbar ist.
- Aktivieren Sie möglichst die automatischen Aktualisierungsfunktionen.
- Ermitteln Sie Hard- und Software, die manuell zu aktualisieren sind.
- Aktualisieren Sie Betriebssysteme und Anwendungssoftware, sobald Sicherheitsupdates vom Hersteller zur Verfügung stehen.
- Ersetzen Sie Systeme, die nicht mehr vom Hersteller unterstützt werden (d. h. keine Sicherheitsupdates mehr erhältlich), durch neue Produkte.
- Können Sie das System nicht ersetzen, dann isolieren Sie es (z. B. mittels Firewall).

CyberSicherheitsCheck-Basismaßnahmen:  
 1 | Sicherheitslücken schließen  
 2 | Benutzerzugänge absichern  
 3 | Datensicherung durchführen  
 4 | Gefahrenbewusstsein schaffen  
 5 | Netzübergänge absichern  
 6 | Schadprogramme abwehren  
 7 | Notfallplan erstellen  
 8 | Inventarisieren und Dokumentieren

### NOTFALLKONTAKT CYBER-ERSTHILFE BW

0711-137-99999  
 @ cyberersthilfe@cybersicherheit.bwl.de  
 Online-Formular auf [www.cybersicherheit-bw.de/cyber-ersthilfe-bw](http://www.cybersicherheit-bw.de/cyber-ersthilfe-bw)



## 1 SICHERHEITSLÜCKEN SCHLIESSEN

### AUTHENTISIERUNGSDATEN TRENNEN

Software-Updates und -Patches sind ein Grundpfeiler der Cyber-sicherheit und ein Erfolgsrezept gegen Cyberangriffe. Zu spät oder nicht installierte Updates sind ein häufiger Grund für gelungene Cyberangriffe auf kleine und mittlere Unternehmen.

### WEITERFÜHRENDE INFORMATIONEN

Verschaffen Sie sich einen vollständigen Überblick der gesamten im Unternehmen eingesetzten Software (Inventarisierung siehe Basismaßnahme 8). Prüfen Sie, ob neue Softwareversionen mehr Schutz bieten. Updates und Patches dürfen sich nicht nur auf das Betriebssystem beschränken. Sie sollten alle Anwendungssoftware umfassen, also auch Office-Anwendungen, ERP, Controlling, Webbrowser, Rechnungsprogramme u. a. Hierfür ist vorab eine grundlegende Erhebung erforderlich.

Falls Sie einen Dienstleister beauftragt haben, stellen Sie vertraglich sicher, dass er auch tatsächlich alle in Ihrem Unternehmen verwendeten IT-Systeme aktualisiert. Haben Sie keinen Dienstleister beauftragt, dann weisen Sie jemandem die Aufgabe eindeutig zu.  
**BSI - Cybersicherheit für KMU - Die TOP 14 Fragen, Frage 4**  
<https://si.csc-kmu.de/b1-01.html>

Kann eine Schwachstelle nicht durch Softwareupdates geschlossen werden, sind weitergehende Maßnahmen notwendig.  
**BSI - Management von Schwachstellen und Sicherheitsupdates, siehe Punkt 4**  
<https://si.csc-kmu.de/b1-02.html>

Management von Schwachstellen und Sicherheitsupdates, Empfehlungen für kleine Unternehmen und Selbstständige.  
**BSI - Veröffentlichungen zur Cybersicherheit**  
<https://si.csc-kmu.de/b1-03.html>

Prüfen Sie, ob auf Ihren Geräten automatische Updates aktiviert sind.  
**BSI - Softwareupdates - ein Grundpfeiler der IT-Sicherheit**  
<https://si.csc-kmu.de/b1-04.html>

### FALLBEISPIEL

Ein Unternehmen erfährt von einer kritischen Sicherheitslücke in Microsoft Exchange, spielt aber das Sicherheitsupdate nicht zeitnah ein. Die Täter nutzen die Sicherheitslücke bereits nach zwei Tagen aus und verschlüsseln alle Dateien auf Servern und Arbeitsplatzrechnern. Die Lösegeldforderung beträgt 250.000 € in Bitcoin.

### FOLGEN

Verlust aller digital gespeicherten Unterlagen inklusive der Sicherungen.  
 Massive Beeinträchtigung des Geschäftsbetriebs ggf. inklusive finanziellen Schaden, Rückgriff auf Papierunterlagen erforderlich. Erheblicher personeller Aufwand: manueller Notbetrieb, Neuaufsetzen der internen IT-Infrastruktur.



## Geschätzte Kosteneinsparungen durch Monitoring (Q3 2024 bis Q3 2025): 21 Mio € (!)

Kategorie	Geschätzte Gesamtkosten
Domain-Missbrauch	102.040,00 €
DDoS-Angriffe	510.000,00 €
Leaks	11.011.000,00 €
Sicherheitswarnungen	9.450.000,00 €
<b>Gesamtsumme</b>	<b>21.073.040,00 €</b>

# Cybercrime-Bekämpfung: Beispiel „Operation Dawnbreaker“

- „HIVE“: Ransomware-as-a-Service Anbieter
  - Zahlreiche Angriffe gegen Unternehmen und Kritische Infrastruktur, Gefährdung von Menschenleben und Schäden in Milliardenhöhe
  - Gemeinsame Ermittlungen der Kriminalpolizei Esslingen mit ausländischen Dienststellen
- Zerschlagung der Infrastruktur der Gruppierung Anfang 2023, Festnahme mehrerer Tatverdächtiger Ende 2023 im Ausland
- Aktueller Erfolg: Bundesweiter Schlag gegen Underground Economy Szene durch Cybercrime-Zentrum BW und PPen Offenburg/Reutlingen





# 4. Bundeseinheitliche Justizcloud

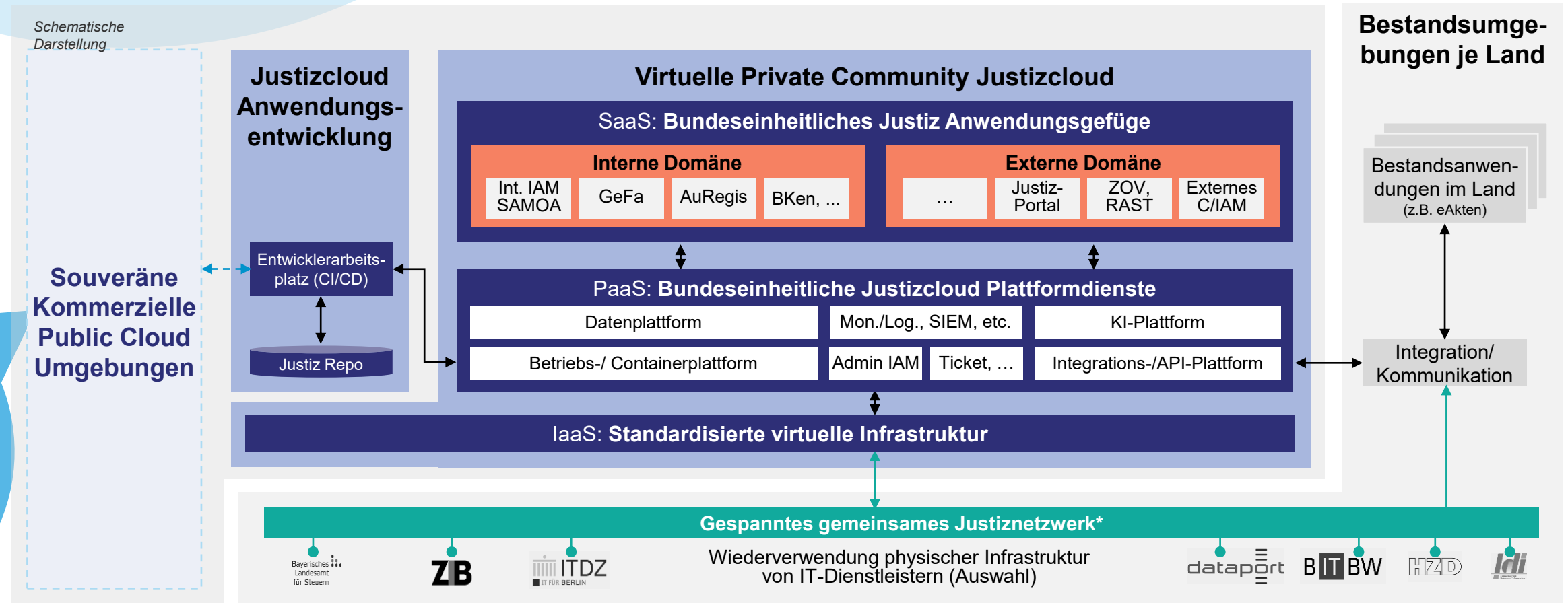


# Justizcloud-Zielbild

Die Justiz befindet sich mitten im **digitalen Transformationsprozess**, und die **Justizcloud** bildet eine **wesentliche Säule** der Digitalisierung



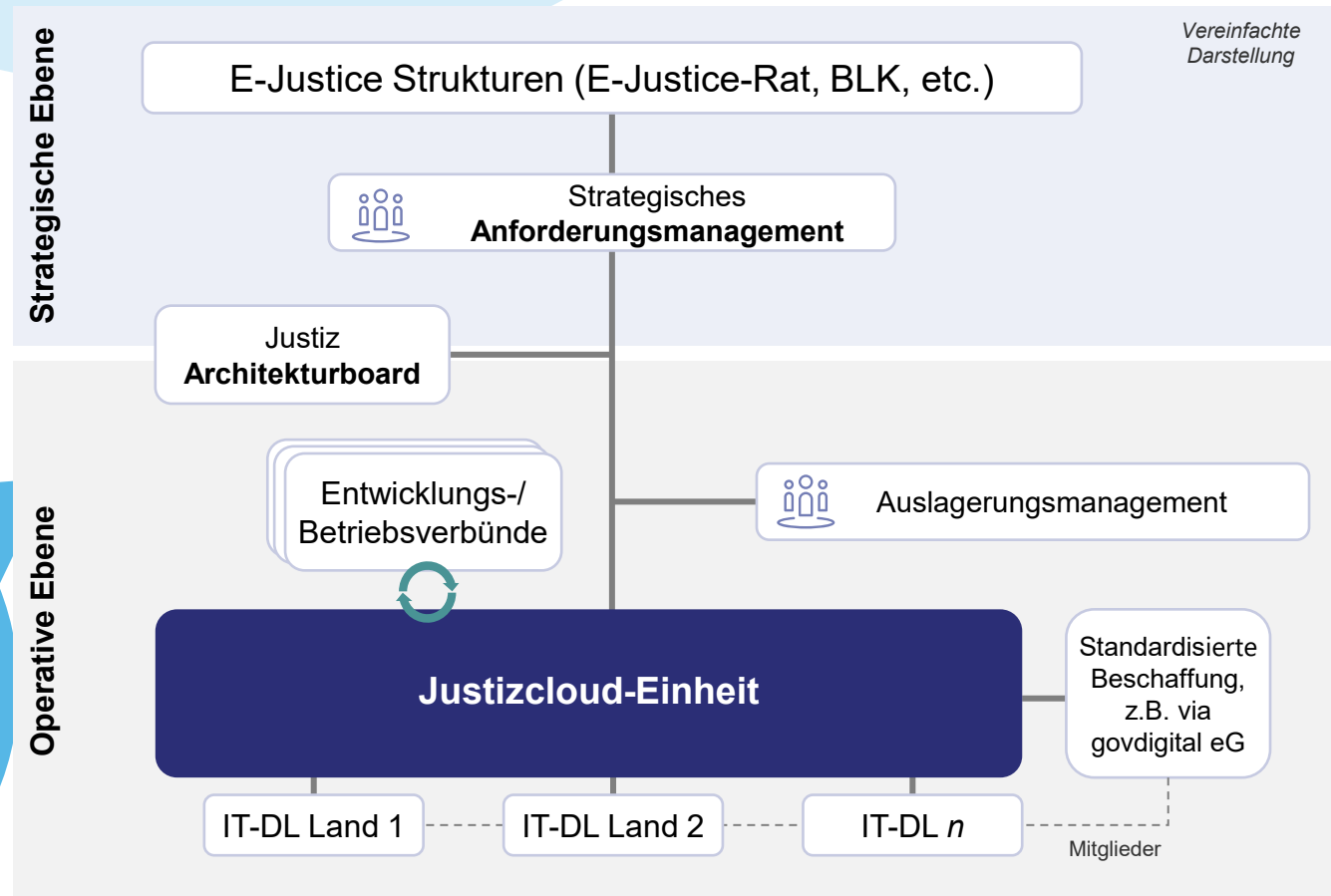
# Die Justizcloud-Plattform wird als **souveräne Private Community Cloud** auf Basis bestehender physischer Infrastruktur aufgespannt



↔ Justiz-eigenes Netzwerk   ← Zugriff über API   □ Zukünftige Ausbaustufe IAM: Benutzer- & Berechtigungssystem z.B. SAMOA   \*Justiznetz SD-WAN in den Netzen des Bundes

# Die **Justizcloud-Einheit** übernimmt **Verantwortung** für die Plattform und **bündelt** technische sowie personelle und finanzielle **Ressourcen**

Auszug



Gremium

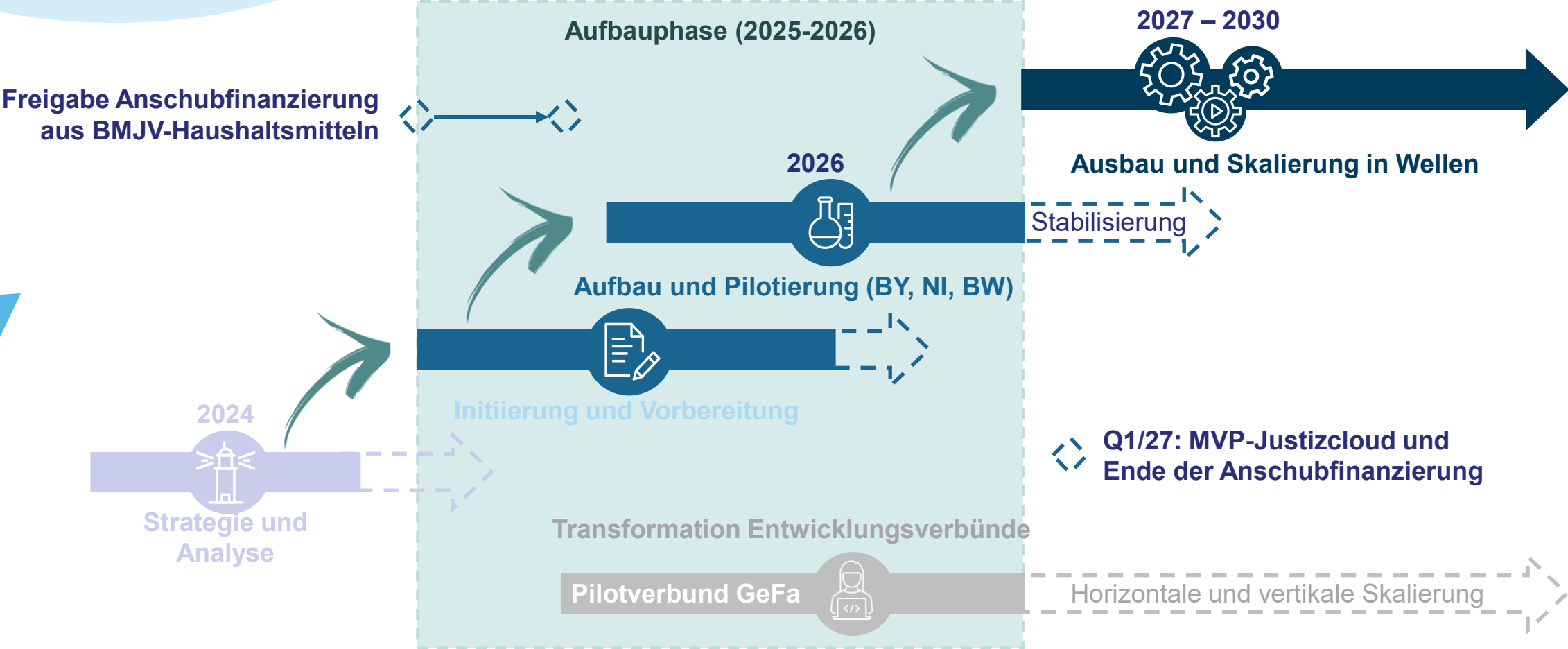
## Aufgaben der Justizcloud-Einheit

- Übernimmt **hoheitliche Aufgaben**
- **Stimmt sich** mit der BLK und deren AGs **strategisch** ab
- **Bündelt** das Cloud-Know-How
- **Normiert Plattformtechnologien** und **betreibt Plattformdienste** für die Justiz
- **Betreibt das Justiznetz** und **koordiniert Infrastrukturbedarfe** mit IT-Dienstleistern
- **Realisiert Volumenrabatte** durch einheitliche Beschaffung
- Bedarf eines **Staatsvertrags**



# Projekt & Netzausbau

In der **Aufbauphase** wird **das Justizcloud-MVP** aufgebaut, danach kann horizontal und vertikal **skaliert** werden



# Der Justizcloud-PLA hat für die ersten MVP-relevanten Leistungspakete Angebote öffentlicher IT-Dienstleister für die Justiz ausgewählt

**dataport**

- Logging & Monitoring
- SIEM / SOC
- Informationssicherheits-Tool (GRC)

**ZIB**

- Entwicklungsplattform
- Infrastrukturknoten (Dataport-Housing)

**HZD**

- Infrastrukturknoten
- PostgreSQL-Datenbank

**BIT BW**

- Betriebsplattform
- Infrastrukturknoten

**d-trust.**

- Zertifikatsdienst

 Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben

- Netzbereitstellung

**Justizcloud**

- **Gemeinsame Technologien** ausgewählt
- **Virtuelles Team** über ganz Deutschland
- **“Best of Breed”-Lösungsansatz** für die Justiz
- **Weitere Leistungspakete** im Projektverlauf

**Bayerisches Landesamt für Steuern**

- Infrastrukturknoten

SIEM/SOC: Security Information & Event Management / Security-Operations-Center | GRC: Governance, Risk, Compliance

# Mit GeFa, Openshift, GitLab und Elastic hat der PLA **standardisierende Produktentscheidungen** für das Justizcloud-MVP getroffen



**GeFa** als Pilotfachverfahren für das Justizcloud-MVP bestimmt.



**GitLab Self-Managed** als standardisierte Entwicklungsplattform



**ZIB** Entwicklungsplattformanbieter



**d-trust** Anbieter für den bundeseinheitlichen **Zertifikatsdienst**



**HZD** Anbieter für den bundeseinheitlichen **PostgreSQL-Datenbankservice**



**Initialer Aufbau des Justiz-Netzes** in BW, BY, NI wg. GeFa-Roadmap.

## Justizcloud-Vision Gemeinsame Technologien für eine unabhängige und zukunftsfähige Justiz

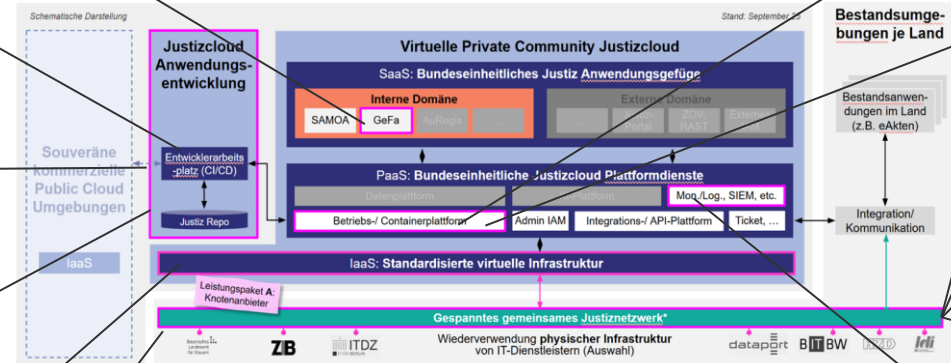


Abb.: Justizcloud-Zielbild



**Red Hat OpenShift** als **Kubernetes-Distribution** für **Betriebsplattform**



**Betriebsplattformanbieter** und damit auch als **1. Infrastrukturknotenanbieter**



**2. Infrastrukturknotenanbieter**



**3. Infrastrukturknotenanbieter**



**4. Infrastrukturknotenanbieter**



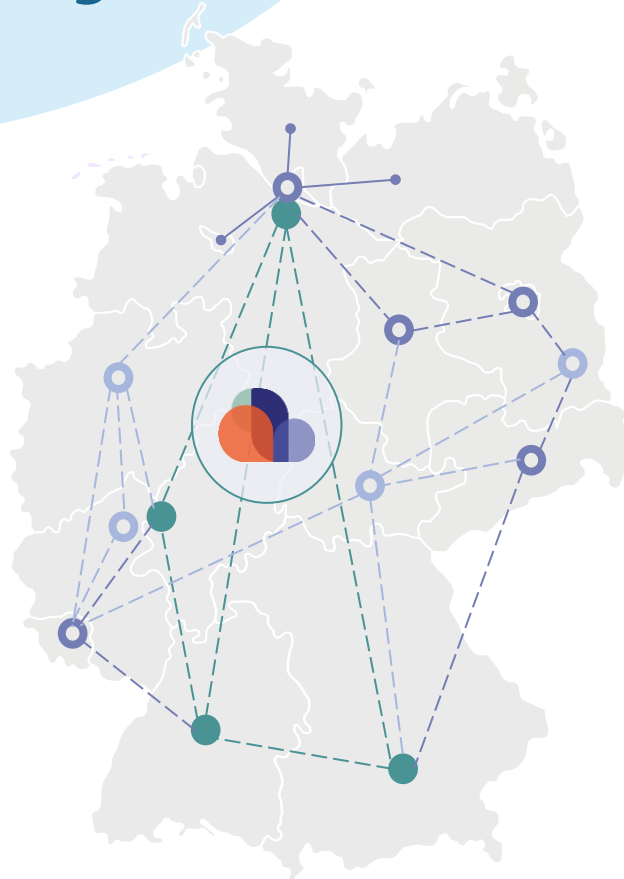
Anbieter für **betriebskritische Services** (SIEM/SOC, Logging & Monitoring, GRC) v.a. **Elastic-Stack**



**Produktentscheidungen Deutschland-Stack konform**

BY: Bayern, NI: Niedersachsen, BW: Baden-Wuerttemberg | SIEM/SOC: Security Information & Event Management / Security-Operations-Center | GRC: Governance, Risk, Compliance

Das Zielbild sieht den **stufenweisen Netzausbau** vor, um die **gleichberechtigte Teilhabe** aller Länder und Resilienz sicherzustellen



**Kreuz-vermaschtes, resilientes, skalierbares SD-WAN**

**Aufbau mit BDBOS** – Übergabe an Justizcloud-Einheit mit Staatsvertrag

Stufenweise **Anbindung aller Justiz-IT-Dienstleister** an das **Justiz(cloud)netz**:

- voraussichtlich im MVP
- mögliche Ausbaustufe 1
- mögliche Ausbaustufe 2



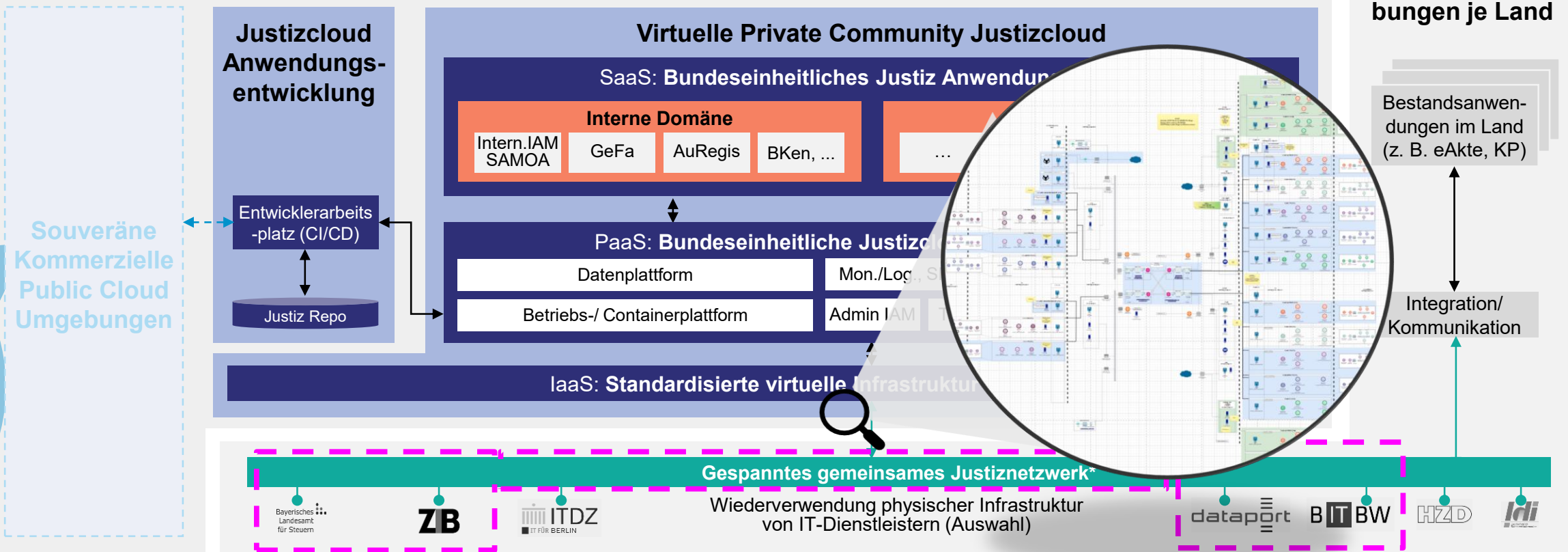
**Im Ausbauzustand hat jedes Land einen Justiznetzanschluss, einige sind Knotenanbieter.**

● Bisher festgelegte Infrastrukturknoten inkl. Netzanschluss

○ Netzanschlüsse

# Detaillierung des **Justiznetzes** und der dafür notwendigen **dezentralen Infrastruktur** hat begonnen - u.a. **Austausch mit DVC im TK6**

Schematische Darstellung



↔ Justiz-eigenes Netzwerk   
 ↔ Zugriff über API   
    Zukünftige Ausbaustufe   
 IAM: Benutzer- & Berechtigungssystem z.B. SAMOA   
 \*Justiznetz SD-WAN in den Netzen des Bundes

# Beim Aufbau des JC-MVPs haben wir den **ersten gemeinsamen Schlüsselmoment** erreicht – weitere sind bis zum Go-Live geplant





## Stefan Krebs

CIO/CDO – Beauftragter der Landesregierung  
für Informationstechnologie

[Stefan.Krebs@im.bwl.de](mailto:Stefan.Krebs@im.bwl.de)

+49 (0) 711 231-5200

[www.digital-laend.de](http://www.digital-laend.de)



## Jan Spoenle

Richter am Oberlandesgericht  
Leiter des Aufbaustabs der Justizcloud-Einheit

[Jan.Spoenle@cloud.justiz.de](mailto:Jan.Spoenle@cloud.justiz.de)

+49 (0) 711 33501-930

# Danke!



## Noch Fragen ?