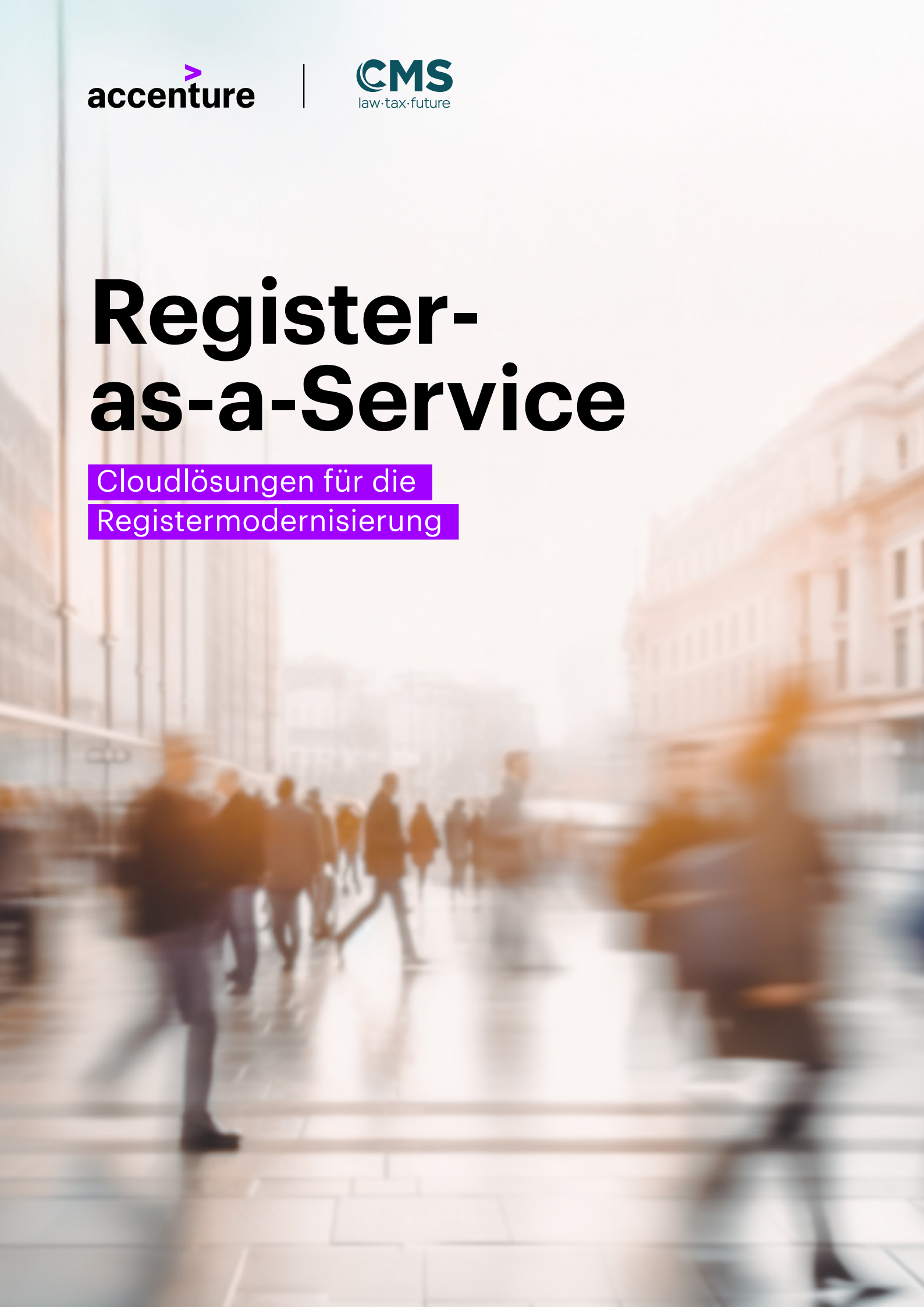
accenture | CMS law·tax·future

Register-as-a-Service

Cloudlösungen für die Registermodernisierung



Management Summary

Cloudbasierte Registerlösungen, sog. „Register-as-a-Service“ stehen im Zentrum aktueller Überlegungen zur Modernisierung staatlicher Dateninfrastrukturen. Vor dem Hintergrund digitalpolitischer Zielsetzungen der Bundesregierung und wachsender Anforderungen an Souveränität, Datenschutz und Effizienz stellt sich die Frage, unter welchen Bedingungen Registerdaten rechtskonform, sicher und zukunftsfähig in Cloudumgebungen betrieben werden können. Das vorliegende Whitepaper gibt darauf eine strukturierte Antwort – juristisch fundiert, technisch durchdacht und praxisnah formuliert.
Die folgenden acht Kernergebnisse fassen die zentralen Erkenntnisse zusammen und zeigen, wie ein cloudbasiertes Registermodell erfolgreich umgesetzt werden kann.

1. Cloudnutzung für dezentrale Register ist rechtlich möglich

Die Nutzung einer gemeinsamen Cloudinfrastruktur für Registerdaten ist auf allen Verwaltungsebenen zulässig. Sie begegnet als solche weder verfassungs- noch datenschutzrechtlichen Bedenken. Dies gilt auch dann, wenn bislang physisch getrennte Datenbestände in eine einheitliche technische Serviceplattform überführt werden. Voraussetzung für die Nutzung einer Cloudinfrastruktur ist, dass die Daten logisch voneinander getrennt bleiben und die registerführende Stelle die volle Kontrolle über “ihre” Daten behält.

2. Cloudlösung verändert nicht die gesetzliche Verantwortung für erhobene Daten

Die Frage, wem die Daten „gehören“, d.h. wer für die Datenhaltung verantwortlich ist, wird nicht dadurch beeinflusst, auf welcher Verwaltungsebene (Bund, Länder, Kommunen) und auf welche Art sie technisch betrieben und verantwortet wird. Registerführende Stellen verfügen nicht frei über Daten, sondern dürfen sie nur im Rahmen ihrer gesetzlichen Zuständigkeit erheben, speichern und nutzen. Die Verwendung einer Cloudlösung verändert daran nichts. Die Verantwortung für die Datenverwaltung verbleibt auch in diesem Fall uneingeschränkt bei der jeweils zuständigen Behörde.

3. Verschlüsselung ist zentraler Pfeiler der Register-as-a-Service

Die Verschlüsselung der Daten ist ein wesentlicher Baustein, um die erforderliche logische Trennung der Registerdaten aus unterschiedlichen Verantwortungsbereichen, d.h. entsprechend der Zuständigkeit für ihre Haltung, zu erreichen. Nur die registerführende Stelle darf in der Lage sein, auf "ihre" Daten zuzugreifen. Ein unbefugter Zugriff „Dritter", auch anderer registerführender Stellen oder der Betreiber der Cloudinfrastruktur, muss ausgeschlossen sein. Letzteres erfordert technische, vertragliche und organisatorische Maßnahmen gemäß DSGVO und BSI-Vorgaben, ggf. bietet confidential computing Lösungen. Dabei ist zu berücksichtigen, dass eine gemeinsam genutzte Speicherumgebung ein attraktives Ziel für Angriffe darstellen könnte („honey pot"). Auch dieses Risiko lässt sich durch Ende-zu-Ende-Verschlüsselung mit ausschließlicher Schlüsselverantwortung der jeweils registerführenden Stelle minimieren.

4. Anbindung der Fachverfahren erfordert technische Schnittstellen und standardisierte Datenaufbereitung

a) Die in Fachverfahren vorliegenden Daten sind meist prozessual erhoben und prozessorientiert gespeichert. Sie müssen in registertaugliche, strukturierte Formate überführt werden. Registerdaten müssen subjekt- oder objektorientiert sein. Die Aufbereitung der Daten (z. B. Aggregation, Umrechnung, Statusbildung) erfordert zentrale Vorgaben.

b) Die Fachverfahren müssen technisch befähigt werden, über Schnittstellen CRUD-Operationen (Create, Read, Update, Delete) im Cloudregister auszulösen. Es gilt „API-Only". Registerdaten sind nur über dedizierte Schnittstellen erreichbar. Diese Punkte müssen idealerweise für das jeweilige Register einheitlich vorgegeben werden. Fachverfahren und ggf. Datenaufbereitung sind entsprechend anzupassen.

5. Fachrecht ist entscheidend

Der Betrieb eines Registers in der Cloud und dessen Anbindung an das NOOTS bedarf keiner ausdrücklichen gesetzlichen Gestattung. Das Fachrecht kann im Einzelfall spezifische Regelungen enthalten. Dies betrifft insbesondere die Fragen des Datenzugriffs, der Datenaufbereitung aus dem Erhebungsprozess in die Register und die Frage der Verantwortlichkeit für diese Daten sowie der Zulässigkeit ihrer Bereitstellung für andere Verwaltungsverfahren. Soweit fachspezifische Regelungen bestehen, sind diese bei der Umsetzung des Registers-as-a-Service zu beachten.

6. Datenschutzrecht ist kein Hindernis – sofern Vorgaben eingehalten werden

Das Gutachten stellt klar: Datenschutzrechtlich bestehen keine grundsätzlichen Bedenken gegen eine Cloudlösung – auch nicht bei personenbezogenen Daten. Entscheidend ist die Umsetzung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO sowie ein klar geregeltes Verhältnis zwischen der registerführenden Stelle und dem Cloudanbieter (inkl. AV-Vertrag nach Art. 28 DSGVO).

7. Augen auf bei der Auswahl des Cloudbetreibers

Die Wahl des Betreibers der Cloudinfrastruktur birgt einige Herausforderungen. Für die digital Souveränität sind Lösungen vorzugswürdig, die einen Wechsel zu einem anderen Betreiber niederschwellig ermöglichen. Mit Blick auf außereuropäische Anbieter sollten die aktuellen Entwicklungen in den Drittstaaten beobachtet und die politischen und judikativen Konsequenzen verfolgt werden. Um Zweifel gar nicht erst aufkommen zu lassen, ist der Rückgriff auf Cloudangebote europäischer Provider dringend zu empfehlen.

8. Voraussetzungen für die Cloudtransformation eines Registers – Trennung von Daten, Verwaltungsverfahren und Softwaresystemen

Der Transfer bestehender Daten in die Cloud erfordert ihre Vorklärung und Strukturierung sowie eine Qualitätssicherung. Ohne diese Vorarbeiten besteht die Gefahr, dass Defizite der bislang genutzten Infrastruktur auch nach einer Cloudtransformation fortbestehen („vom Rathauskeller in die Cloud"). Die Vorteile der Digitalisierung würden dadurch wesentlich geschmälert und ein echter Digitalisierungsschub bliebe aus. Softwaresysteme, Datenhaltung und Verwaltungsverfahren müssen künftig integriert gedacht und geplant werden.

1 Fachliche Gründe für Register-as-a-Service

Die Registermodernisierung („RegMo“)[1] zählt zu den größten Digitalisierungsprojekten Deutschlands. Sie baut das National-Once-Only-Technical-System („NOOTS“) – die „Datenautobahn“ der Verwaltung – auf. Ziel ist ein einheitlicher Onlinezugang, über den Verwaltungsleistungen unabhängig von der Zuständigkeit einfach erreichbar sind.

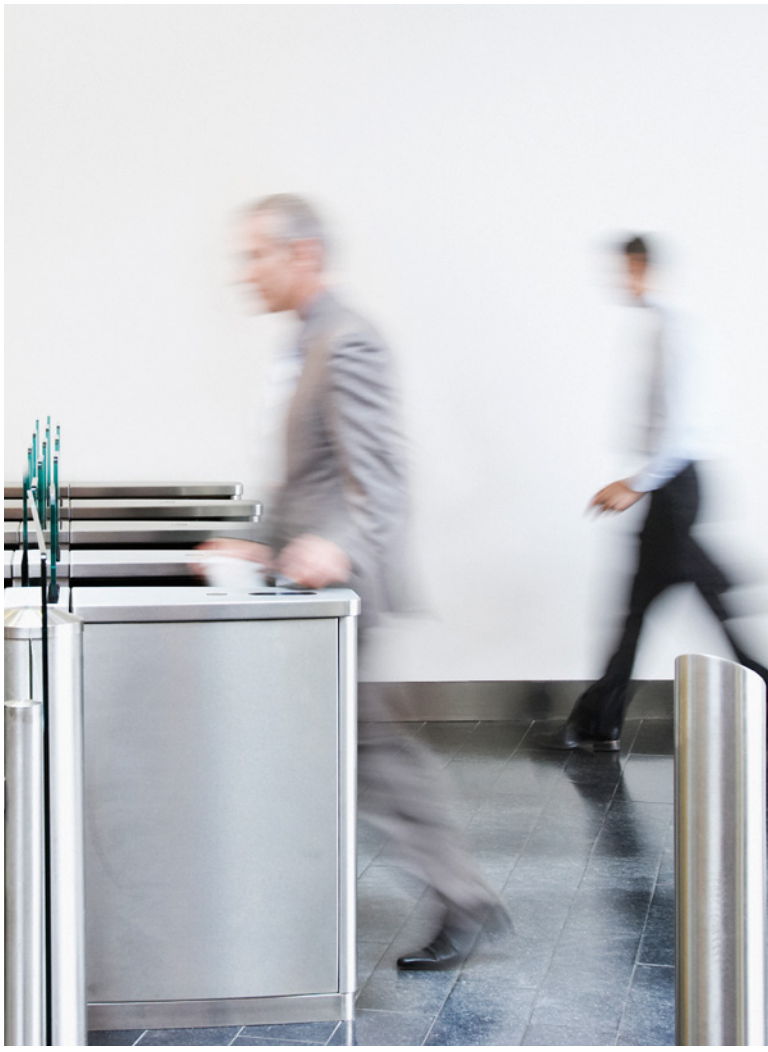
Das NOOTS ermöglicht den Nachweisdatenfluss zwischen Registern und Behörden, um das „Once-Only-Prinzip“ umzusetzen: Daten müssen nur einmal erfasst werden und können danach elektronisch abgerufen und verarbeitet werden. Dies entlastet Bürgerinnen und Bürger, reduziert Verwaltungsaufwand und schafft eine zentrale technische Grundlage für automatisiert prozessierte Verwaltungsverfahren. Über eine Schnittstelle ist auch der Austausch mit dem EU-System („EU-OOTS“) möglich.

Für den Erfolg braucht es Registerdaten in hoher Qualität und Verfügbarkeit. Die Herausforderung liegt in der Heterogenität der Daten: Selbst der Registerbegriff ist nicht überall klar definiert, die Abgrenzung zu sonstigen Verwaltungsdaten teils unklar. Register existieren auf allen föderalen Ebenen und werden von unterschiedlichsten Stellen geführt – Behörden, Gerichten, Selbstverwaltungskörperschaften.[2] Die Registerlandkarte des Bundesverwaltungsamts listet 290 Register (Mai 2025), davon 50 kommunal. Der Begriff umfasst alle datenbasierten Strukturen, die zur Leistungserbringung nötig sind.

Die Datenqualität und Verfügbarkeit sind wegen fehlender Standards stark unterschiedlich. Besonders kommunale Registerdaten liegen oft dezentral in Fachverfahren vor, die auf spezifische Verwaltungsaufgaben zugeschnitten und schwer integrierbar sind. Daten werden dort prozessorientiert gespeichert und sind meist nur innerhalb einer Verwaltungsebene nutzbar – übergreifender Austausch ist die Ausnahme, aber zentrales Ziel der Verwaltungsdigitalisierung.

Zukünftig müssen Datenhaltung und -management übergreifend, verbindlich und standardisiert erfolgen. Daten sollen objekt- oder subjektorientiert bereitgestellt, technologische Standards flächendeckend etabliert werden. Ziel sind bessere Erreichbarkeit, Skalierbarkeit und Verfügbarkeit – 24/7, in Echtzeit, flexibel auf wechselnde Bedarfe reagierend.

Eine Lösung liegt in der Cloud: Register-as-a-Service ermöglicht unter Einhaltung zentraler Standards, Architekturleitlinien und Sicherheitsvorgaben die Integration heterogener Daten. Die Vorteile dezentraler Datensicherheit bleiben erhalten, während digitale Konnektivität verbessert wird.



Register lassen sich einfacher an das NOOTS anbinden – sicher, verfügbar, rechtskonform. Die Überführung dezentraler Registerdaten in eine Cloud („Register-as-a-Service“) könnte Datensicherheit, Pflege und Qualität verbessern und den Anschluss an das NOOTS vereinfachen. Besonders dezentrale Register könnten davon profitieren. Es braucht dafür eine geeignete technische Lösung. Die Cloudnutzung darf jedoch nicht isoliert betrachtet werden – sie erfordert eine organisatorische Einbettung: Verwaltungspersonal muss auf die Cloudinfrastruktur zugreifen können, und Datenlieferung, Aufbereitung und Qualitätssicherung sind organisatorisch zu regeln.

Es stellen sich drei zentrale Fragen:

1. Wie gelangen Daten in die Register und in die Cloud? Was ist bei einheitlicher Aufbereitung zu beachten?

2. Wie werden Daten gespeichert, verarbeitet und administriert?

3. Wie werden sie über das NOOTS bereitgestellt? Wie erfolgt die Anbindung technisch und organisatorisch?

Technisch wird eine robuste, sichere und flexible Infrastruktur angestrebt, basierend auf Open-Source-Technologien ohne Vendor-Lock-in. Herzstück ist eine „dezentral-zentrale Cloud“, die klare Datenverantwortung bei den zuständigen Verwaltungseinheiten belässt, aber zentrale Bereitstellungsvorteile nutzt. Technisch bestehen Herausforderungen bei Transportwegen und der Datenspeicherung in Ruhe. Die Infrastruktur des NOOTS muss berücksichtigt werden.

Neben technischer und organisatorischer Umsetzbarkeit – insbesondere bei heute dezentral gehaltenen Registerdaten – stellen sich Fragen der rechtlichen Zulässigkeit der Cloudnutzung. Die Nutzung eines einheitlichen technischen Systems („Register-as-a-Service“) bei fortbestehender logischer Zuständigkeit der Registerverantwortlichen (z.B. Kommunen) wurde bislang nicht erprobt. Dieses Whitepaper skizziert technische Optionen und den rechtlichen Rahmen. Es handelt sich nicht um ein abschließendes Rechtsgutachten, sondern eine Grundlage für eine Rahmenarchitektur und erste Prototypen.

2 | Rechtliche Basis für Register-as-a-Service

2.1 Hintergrund

Unionsrechtliche Ebene

Die Verordnung zum „Single Digital Gateway“ (Verordnung 2018/1724, kurz: „SDG-Verordnung“) schafft auf EU-Ebene ein digitales Zugangstor zur öffentlichen Verwaltung der Mitgliedstaaten. Der Zugang erfolgt über das Portal „Your Europe“[3], das mit dem deutschen Bundesportal[4] vernetzt ist und einen Online-Zugang zu Verwaltungsleistungen aller Ebenen eröffnet.
Die SDG-Verordnung verpflichtet die Mitgliedstaaten, bestimmte Informationen und Dienste grenzüberschreitend digital bereitzustellen (Art. 14). Sie verlangt zudem ein technisches System für den automatisierten Nachweisaustausch, um das Once-Only-Prinzip europaweit umzusetzen. Die Spezifikationen sind in der Durchführungsverordnung (Verordnung 2022/1463) geregelt. National erfolgt die Umsetzung über das NOOTS mit Anbindung an das EU-OOTS.

Nationale Ebene

Das nationale Pendant zur SDG-Verordnung ist das Onlinezugangsgesetz („OZG“) von 2017, das zuletzt novelliert wurde . Zentraler Gegenstand der Novellierung, des „OZG 2.0“, ist die effiziente und zielgerichtete Umsetzung des Once-Only-Prinzips. Das OZG enthält nun eine Generalklausel für den Nachweisdatenabruf (§§ 5, 5a EGovG), Anpassungen der Regelungen zur Datenerhebung (§ 8 OZG) sowie eine Verpflichtung der Länder, die Anbindung der Kommunen an den Portalverbund sicherzustellen (§ 1a Abs. 3 S. 2 OZG).
Verfassungsrechtliche Grundlage für die Zusammenarbeit von Bund und Ländern bei IT-Systemen ist Art. 91c GG. Hierauf basiert das IT-Netzgesetz (IT-NetzG), das den Betrieb des Netzes und die Anschlussregelungen aller Verwaltungsebenen definiert. Einzelheiten regelt der IT-Planungsrat (§ 4 Abs. 3 IT-NetzG).
Ein zentraler und zugleich anspruchsvoller Baustein des Once-Only-Prinzips ist die Registermodernisierung.

Grundlage ist das Registermodernisierungsgesetz vom 28.03.2021, das mit dem Identifikationsnummerngesetz (IDNrG) die Nutzung der Steuer-ID (§ 139b AO) als Ordnungsmerkmal einführt. In der Anlage zum IDNrG werden 50 prioritäre Register benannt, denen bis Ende 2028 eine Identifikationsnummer als Ordnungsmerkmal zugespeichert werden muss.
Die Heterogenität der Registerlandschaft macht die Umsetzung besonders komplex. Für die fachliche Koordination ihrer IT-Zusammenarbeit haben Bund und Ländern den IT-Planungsrat eingerichtet. Zu dessen Aufgaben gehört auch die notwendige Steuerung zur Umsetzung des NOOTS.
Zur Regelung von Leitplanken für den Aufbau des NOOTS und die Integration der Registerdaten haben sich Bund und Länder im Dezember 2024 auf einen eigenen NOOTS-Staatsvertrag verständigt, der allerdings noch nicht vollständig ratifiziert ist.[5]
Ein Zielbild mit Umsetzungsplan hat der IT-Planungsrat bereits im Januar 2021 veröffentlicht. Darin sind 18 der im IDNrG genannten Register besonders priorisiert[6]. Verbindliche Vorgaben für die vollständige Anbindung an das NOOTS stehen noch aus.

2.2 Verfassungsrechtliche Anforderungen

2.2.1 Zulässigkeit bundesrechtlicher Vorgaben zur Registermodernisierung Bundesrechtliche Regelungskompetenz

Im Rahmen der kommunalen Einbindung in das OZG wurde diskutiert, ob Art. 91c Abs. 5 GG als Gesetzgebungskompetenz genügt. Auch wenn dort nur von Bund und Ländern die Rede ist, sind Kommunen diesen organisatorisch zugeordnet. Die Gesetzesbegründung macht klar, dass der Gesetzgeber die Kommunen ausdrücklich einbeziehen wollte – zumal viele Leistungen kommunal erbracht werden.

Eine unzulässige Aufgabenübertragung liegt nicht vor: Es geht nicht um neue Aufgaben, sondern um die digitale Erfüllung bestehender Pflichten. Kommunale Selbstverwaltungsgarantie Art. 28 Abs. 2 GG garantiert den Kommunen das Recht, ihre eigenen Angelegenheiten selbst zu regeln („kommunale Selbstverwaltungsgarantie"). Dies betrifft jedoch nur die Angelegenheiten der örtlichen Gemeinschaft. Aufgaben im übertragenen Wirkungskreis, in dem die Kommunen Bundes- oder Landesgesetze umsetzen (wie z.B. im Pass- und Meldewesen), nehmen nicht am Schutz der kommunalen Selbstverwaltungsgarantie teil. In den geschützten Selbstverwaltungsbereich können bundesrechtliche Vorgaben zur Verwaltungs- und Registermodernisierung daher nur eingreifen, wenn die Kommunen dadurch finanziell überfordert und damit ihre Gestaltungsmöglichkeiten im Selbstverwaltungsbereich eingeschränkt würden. Das Konnexitätsprinzip der Landesverfassungen, d.h. die Notwendigkeit von Regelungen zur Kostendeckung bei der Übertragung staatlicher Aufgaben an die Kommunen, trägt dem Rechnung. Das Bundesverfassungsgericht erkennt zudem die Funktionsfähigkeit der Verwaltung als Gemeinwohlgrund an, der auch bestimmte Eingriffe in den Selbstverwaltungsbereich rechtfertigen kann.[7] Entsprechend wurden bisher weder OZG noch Registermodernisierungsgesetz gerichtlich angefochten.

2.2.2 Informationelle Selbstbestimmung

Das durch Art. 1 Abs. 1 und Art. 2 Abs. 1 GG grundrechtlich geschützte allgemeine Persönlichkeitsrecht gewährleistet nach der Rechtsprechung des Bundesverfassungsgerichts[8] auch das Recht auf informationelle Selbstbestimmung. Damit ist gemeint, dass jede und jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten bestimmen darf.

Vorhandener Datenbestand

Die Registermodernisierung betrifft ausschließlich die digitale Verfügbarkeit vorhandener Daten. Die Zulässigkeit der Erhebung richtet sich nach dem jeweiligen Fachgesetz. Auch der Datenabruf über NOOTS unterliegt bestehenden Rechtsgrundlagen. Eine Nutzung erfolgt nur auf Veranlassung der betroffenen Person (§ 8 OZG).

Verfassungsmäßigkeit des IDNrG

Die Verfassungskonformität der Registermodernisierung hängt nicht von der verfassungsrechtlichen Bewertung des im IDNrG verwendeten Ordnungsmerkmals (Steuernummer) ab. Unter Bezug auf eine ältere Entscheidung des Bundesverfassungsgerichts[9] sowie Art. 1 Abs. 1 GG wurden vereinzelt Bedenken geäußert, da ein Personenkennzeichen eine unzulässige Katalogisierung bewirken könne. Die Speicherung für den „once only"-Datenaustausch erlaubt jedoch keine verfassungswidrige Persönlichkeitsprofilierung. Verfassungsbeschwerden gegen das IDNrG sind bislang nicht anhängig.

Datensouveränität

Die Datensouveränität wird durch die Registermodernisierung nicht angetastet. Im Konzept einer dezentralen Clouddatenhaltung bleibt der Zugriff der datenerhebenden Behörde und damit deren rechtliche Verantwortung vielmehr uneingeschränkt erhalten.

Ausreichender Schutz gegen unbefugten Datenzugriff

Das Recht auf informationelle Selbstbestimmung verlangt angemessenen Schutz durch die erhebende Behörde. Dass dieser bei einer dezentraler Clouddatenhaltung durch die im NOOTS vorgesehenen Maßnahmen ausreichend geschützt werden kann, zeigen die nachfolgenden Betrachtungen.

2.3 Datenschutz, Datensicherheit und Betreiberauswahl

Der Datenhaltung in einem Drittsystem („Register-as-a-Service“) liegt die Auslagerung an eine von der registerführende Stelle verschiedene Einheit zugrunde. Datenschutzrechtlich ist dies nicht grundsätzlich verboten. Technische Hilfstätigkeiten wie Rechenzentrumsbetrieb oder EDV-Dienstleistungen sind in der Regel outsourcingfähig und können von Privaten erbracht werden.[10]

2.3.1 Cloudnutzung an sich

Der Begriff des „Cloudbetriebs“ entspricht aus rechtlicher Sicht dem Ersatz selbst betriebener Systeme durch die Nutzung von (Teilen von) leistungsfähigen und skalierbaren Rechenzentren Dritter.

2.3.2 Grundsätzliche Zulässigkeit der Nutzung von Clouddiensten

Grenzen der Cloudnutzung bestehen, wenn hoheitliche Tätigkeiten an Dritte übertragen würden – etwa die Bearbeitung von Anträgen oder der Erlass von Verwaltungsakten. Solche Funktionen dürfen nur ausnahmsweise an beliehene Private übertragen werden. Für technische Hilfsfunktionen gelten diese Einschränkungen nicht. Hier handeln Private als Verwaltungshelfer und nehmen Aufgaben im Auftrag und nach Weisung der Behörden wahr[11]. Maßgeblich ist, dass das Ob und Wie der Datenverarbeitung durch Verwaltung und Gesetzgeber bestimmt wird. Bei Auslagerung in die Cloud bleibt die öffentliche Verwaltung für Zulässigkeit und Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich.

2.3.3 Nutzung eines Dienstleisters für mehrere Registerverantwortliche

Soweit personenbezogene Daten durch Dritte im Auftrag verarbeitet werden, gelten die Regelungen der Auftragsdatenverarbeitung nach Art. 28 DSGVO. Datenschutzrechtlich ist keine dedizierte Hardware im Eigentum der Verwaltung erforderlich; die Nutzung geteilter Ressourcen ist zulässig, sofern die registerverantwortliche Stelle auch in der Cloud die Kontrolle über Daten und deren Verarbeitung behält. Dies wird durch eine Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO sichergestellt. Der Cloudbetreiber ist verpflichtet, ausschließlich den Weisungen des Auftraggebers zu folgen. Diese Verpflichtungen entsprechen den verfassungs- und verwaltungsrechtlichen Anforderungen an technische Hilfstätigkeit im Auftrag der Behörden.

2.3.4 Einschränkungen hinsichtlich des Einsatzes außereuropäischer Anbieter

Die DSGVO erlaubt grundsätzlich die Datenübermittlung an Anbieter außerhalb der EU, wenn am Ort der Verarbeitung das gleiche Datenschutzniveau wie in der EU sichergestellt ist. Für einige Länder hat die EU-Kommission dies durch einen Angemessenheitsbeschluss festgestellt. Für andere Länder kann dies durch andere Schutzmaßnahmen, wie z.B. den Abschluss von Standardvertragsklauseln, erreicht werden. Angesichts der politischen Lage, insbesondere in den USA, ist jedoch kritisch zu prüfen, ob diese Vorgaben nachhaltig erfüllt werden. Aktuell ist unklar, ob der Angemessenheitsbeschluss für die USA Bestand hat oder EU-Standardvertragsklauseln ausreichen. Vor diesem Hintergrund sollte auf europäische Cloudanbieter zurückgegriffen werden.

2.3.5 Einschränkungen der Cloudnutzung im Einzelfall

Im Einzelfall können bereichsspezifische Regelungen den Einsatz von Clouddienstleistern einschränken – etwa im SGB X für Sozialdaten oder in §§ 45 ff. BDSG für Strafverfolgungsdaten. Auch bei Registerdaten bestehen Ausnahmen: Seriennummern von Ausweisen dürfen nur bei der Bundesdruckerei gespeichert werden (§ 16 Abs. 3 PassG, § 26 Abs. 3 PAuswG). Weitere, bis vor kurzem bestehende Einschränkungen, etwa im brandenburgischen oder sächsischen Meldegesetz, wurden aufgehoben. Vor Umzug eines Registers in die Cloud ist daher zu prüfen, ob im Einzelfall Einschränkungen für das konkrete Register bestehen. Ein grundsätzliches Verbot für den Register-as-a-Service Ansatz besteht allerdings nicht.

2.3.6 Sicherheitsanforderungen

Die datenschutzrechtlichen Sicherheitsanforderungen bei Cloud-Auslagerung ergeben sich aus Art. 32 DSGVO: Es sind angemessene technische und organisatorische Maßnahmen zu treffen, um Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit zu gewährleisten. Eine physische Trennung („air gap“) der Register ist nicht vorgeschrieben. Die Nutzung gemeinsamer Rechnerressourcen ist zulässig, wenn geeignete logische Trennmechanismen – etwa Rollen- und Berechtigungskonzepte oder virtuelle Instanzen – eingesetzt werden.

3 Technische Skizze für Register-as-a-Service

Die Nutzung einer Cloud-basierten Infrastruktur für Registerdaten markiert eine technische Neuausrichtung: Ziel ist die Transformation heterogener, historisch gewachsener Registerstrukturen in eine moderne, föderal anschlussfähige Plattformarchitektur. Registerdaten sollen so bereitgestellt werden, dass sie die Anforderungen der Verwaltungsdigitalisierung – insbesondere im Hinblick auf NOOTS und das Once-Only-Prinzip – erfüllen, ohne Registerhoheit oder Zuständigkeiten zu unterlaufen.

3.1 Grundprinzipien der Architektur

Im Zentrum steht eine mandantenfähige Plattformarchitektur, die Daten technisch gemeinsam, aber rechtlich und logisch getrennt verarbeitet. Sie folgt den Prinzipien moderner Cloud-native-Systeme, integriert jedoch föderale Verantwortungslinien: Jede registerführende Stelle bleibt datenverantwortlich und zugriffssteuernd – auch beim Betrieb innerhalb einer gemeinsamen Plattformumgebung.
Das Mandantenmodell basiert auf einer containerisierten Infrastruktur mit dynamischer Orchestrierung.

Jeder Mandant (jedes Register) wird isoliert in einem dedizierten Namespace betrieben – technisch abgeschirmt, organisatorisch klar zugeordnet und über ein rollen- und attributbasiertes Zugriffskonzept gesichert. Die Kontrolle über Zugriffe, Konfigurationen und Datenkataloge verbleibt bei der zuständigen Behörde.
Auch Schlüsselmaterial wird mandantenspezifisch verwaltet – ohne zentrale Bündelung.
Die Plattform stellt keine zentrale Registerinstanz dar, sondern ein standardisiertes Betriebsgerüst – eine Art „digitale Parzelle".

Register nutzen gemeinsame Dienste wie Zustandsüberwachung oder Zertifikatsverwaltung, bleiben aber strikt getrennt. Eine übergeordnete Instanz mit Zugriff auf Registerdaten existiert nicht. Der Datenaustausch erfolgt ausschließlich über definierte Schnittstellen, etwa über NOOTS oder EU-OOTS.

So entsteht eine Infrastruktur mit gemeinsamer technischer Basis und strikter föderaler Trennung. Ihre Stärke liegt nicht in Zentralisierung, sondern in standardisierter Dezentralität – ohne Aufgabe juristischer oder technischer Eigenständigkeit.

3.2 Sicherheit, Qualität und Souveränität als Architekturtreiber

Die Qualität einer Cloud-basierten Registerarchitektur hängt nicht allein von Skalierbarkeit oder Eleganz ab, sondern maßgeblich von Sicherheit, Stabilität und Vertrauenswürdigkeit. Da Registerdaten sensible Informationen enthalten, stehen deren Schutzgüter im Mittelpunkt. Alle Plattformkomponenten folgen „Security by Design". Interne Kommunikation ist vollständig TLS-verschlüsselt, Zertifikate werden automatisiert mandantenspezifisch verwaltet, Schlüsselmaterial ist nur über getrennte Speicherinstanzen zugänglich. Daten werden verschlüsselt gespeichert und übertragen (mTLS). Jeder API-Zugriff wird protokolliert, versioniert und zur verantwortlichen Rolle zurückverfolgt. Vertraulichkeit, Integrität und Nachvollziehbarkeit sind technisch verankert.

Die Plattform ist auf Hochverfügbarkeit, Fehlertoleranz und Ausfallsicherheit ausgelegt. Automatisierte Orchestrierung, Self-Healing, Rollback-Mechanismen und dynamisches Lastmanagement sichern den Betrieb rund um die Uhr – kein Ziel, sondern Standard. Wartbarkeit und Erweiterbarkeit sind integrale Bestandteile. Änderungen an Konfigurationen oder Mandanten werden deklarativ beschrieben, getestet und automatisiert ausgerollt – versioniert, nachvollziehbar und reversibel. Neue Registermandanten, Datenmodelle oder Richtlinien lassen sich im laufenden Betrieb ergänzen. Sicherheitsupdates erfolgen kontinuierlich. Die Plattform skaliert horizontal wie vertikal, passt sich dynamisch an Register und Fachverfahren an. Kritische Komponenten wie Gateways, Datenbanken oder Authentifizierungsdienste sind mandantenspezifisch konfigurierbar. Auch bei Massenabrufen – etwa über NOOTS – bleibt as System stabil und regelkonform. Sicherheit, Verfügbarkeit, Erweiterbarkeit, Performance und Skalierbarkeit sind keine abstrakten Ziele, sondern tragende Designprinzipien – technisch realisierbar, rechtlich tragfähig.

3.3 Nicht nur sicher, sondern smart: API-Zugriffsmodell und Anbindung an das NOOTS

Auf dieser Architektur aufbauend zeigt sich: Die Plattform ist nicht nur Betriebs-, sondern auch Steuerungsraum für digitale Nachweise. Kontrollierte, rückverfolgbare Zugriffe auf Registerdaten schaffen die Voraussetzung für eine belastbare Anbindung an NOOTS.

Die Plattform nutzt ein API-basiertes Zugriffsmodell: Alle Zugriffe – durch Fachverfahren, Portale oder NOOTS – erfolgen über klar definierte, versionierte Schnittstellen. Diese APIs sind Bestandteil eines Governance-Modells und binden sich an ein rollen- und attributbasiertes Berechtigungssystem. Zugriff wird kontextsensitiv autorisiert – abhängig von Rolle, Zweck und Rechtsgrundlage.

Für NOOTS stellt die Plattform standardisierte Adapter bereit, die XNachweis-Nachrichten verarbeiten, Signaturen prüfen und Zugriffe in Echtzeit validieren. Der Registerabruf wird so ein integrierter Vorgang – mit automatisierter Kontrolle, anschlussfähig an nationale und EU-Infrastrukturen, ohne dass jedes Register eigene Konnektoren entwickeln muss.

Diese Standardisierung schränkt die Flexibilität nicht ein: Registerverantwortliche definieren über Konfigurationen selbst, welche Datenformate bereitgestellt, welche Abrufgrenzen und Authentifizierungsanforderungen gelten. Auch komplexe Regeln, etwa bei Datenkombinationen oder Filterungen, lassen sich ohne zentrale Eingriffe umsetzen – für einen einheitlich orchestrierten, rechtlich belastbaren Datenzugang. Die Plattform entlastet bei der NOOTS-Anbindung und schafft ein neues Verständnis von Datenzugriff: nicht als Ausnahme, sondern als regelbasierter, maschinenlesbarer Berechtigungsprozess. Sie ebnet den Weg für automatisierte Verwaltungsverfahren – nicht zentralisiert, sondern föderal standardisiert.

3.4 Die Mandantentrennung: technische Durchsetzung föderaler Verantwortung

Die Mandantentrennung ist zentrales Sicherheitsmerkmal. Sie gewährleistet, dass jede registerführende Stelle ausschließlich auf ihre Daten zugreifen kann. Die erste Ebene ist die Betriebsisolation, z. B. durch Kubernetes-Namespaces. Jeder Mandant läuft in einem dedizierten Bereich mit eigener Konfiguration, Schlüsselverwaltung und Betriebsmetriken – logisch und netzwerktechnisch getrennt. Anfragen werden nur bei erfolgreicher Authentifizierung und eindeutiger Mandantenzuordnung weitergeleitet. Bereits am Einstiegspunkt beginnt die Absicherung: Jeder Request erfordert Zertifikats- oder Tokenauthentifizierung, deren Identität im Request-Kontext mitgeführt wird – Manipulation ist technisch ausgeschlossen.

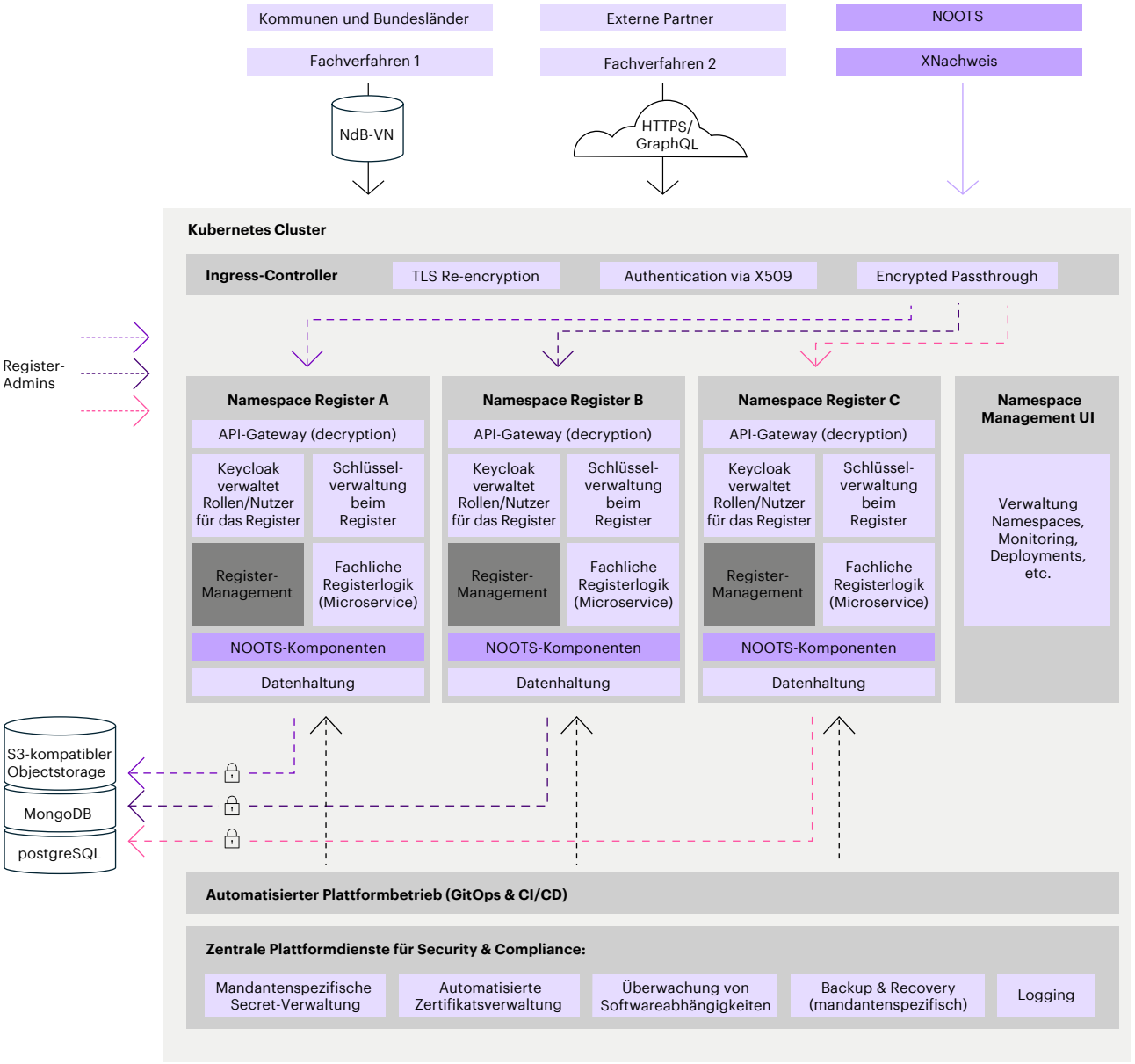
Ein feingranulares Berechtigungsmodell regelt, wer auf welche Ressourcen zugreifen darf – je nach Mandant, Rolle, Quelle oder Zweck. Auch Managementportale und Adminschnittstellen sind strikt mandantenspezifisch segmentiert. Jeder Registeradministrator hat ausschließlich Zugriff auf „sein“ Register – technisch und betrieblich. Betriebliche Dienste wie Monitoring, Deployment oder Logging sind mandantenspezifisch organisiert.

Auditdaten werden getrennt gespeichert, technische Richtlinien dezentral durchgesetzt – ohne zentrale Sammelprüfung.
Die Kombination aus Netzwerksegmentierung, Zugriffskontrolle, Identitätsbindung und isolierten Diensten stellt sicher: Kein Zugriff auf fremde Daten – auch nicht durch die Plattform selbst – außer bei explizit delegierter Freigabe.

Die logische Trennung ist Kern der Sicherheitsarchitektur – und Ausdruck des föderalen Vertrauensmodells der Registerführung in Deutschland.

3.5 Architekturskizze

Register-as-a-Service



Legende

- Plattformseitig betriebene, zentral verantwortete Komponenten & Dienste
- Mandantenspezifische Konfigurationen und Zuständigkeiten
- Fachlich oder gesetzlich definierte Querschnittskomponenten
- Verwaltungsfunktionen innerhalb eines Registers

Die vorgeschlagene Architektur ist nicht nur eine technische Plattform, sondern vor allem eine Organisationsstruktur für Vertrauen in föderalen Kontexten: Vertrauen darauf, dass Daten verfügbar, aber nicht entzogen sind; dass Infrastruktur modern, aber nicht zentralistisch ist; dass Skalierbarkeit erreichbar, aber nicht gleichbedeutend mit Kontrollverlust ist.

3.6 Anschluss eines kommunalen Fachverfahrens an die Plattform

Ein typischer Arbeitstag beginnt für eine Sachbearbeiterin im Einwohnermeldeamt mit der Anmeldung am Arbeitsplatzrechner. Anschließend startet sie das kommunale Fachverfahren für das Melderegister – eine spezialisierte Anwendung zur Bearbeitung von Vorgängen wie Umzügen, Abmeldungen oder Auskunftsersuchen.

Beim Start meldet sie sich mit ihren persönlichen Zugangsdaten an – in der Regel über die zentral verwaltete Nutzerverwaltung ihrer Kommune (z. B. Stadt Düsseldorf), die mit dem Identitätsdienst der Plattform verbunden ist. Die Authentifizierung erfolgt über ein standardisiertes Protokoll, das Identität, Rolle und organisatorische Zugehörigkeit prüft und kryptografisch absichert.

Nach erfolgreicher Authentifizierung erhält das Fachverfahren ein Zugriffstoken, das Identität, Rolle (z. B. „Melde-SB“), organisatorische Zugehörigkeit (z. B. „Einwohnermeldeamt Düsseldorf“) und den zulässigen Mandantenkontext (z. B. „Melderegister Düsseldorf“) eindeutig festlegt. Dieses Token wird bei jeder Anfrage an die Plattform mitgeführt – etwa bei Datenabrufen oder Nachweiserstellung.

Der Zugriff erfolgt ausschließlich über ein zugelassenes Verwaltungsnetz, etwa ein Landesnetz oder das Netz des Bundes.

Beim Verbindungsaufbau prüft die Plattform per Zertifikatsaustausch (mutual TLS), ob ein gültiges, vertrauenswürdiges Client-Zertifikat vorliegt. Nur dann wird die Anfrage akzeptiert.

Erst nach dieser Absicherung prüft die Plattform anhand des Tokens, ob die Anfrage gültig signiert ist und dem vorgesehenen Mandantenkontext entspricht. Versucht ein Fachverfahren – etwa fehlerhaft oder missbräuchlich – auf ein anderes Melderegister zuzugreifen (z. B. Köln), blockiert die Plattform den Zugriff unmittelbar.

Innerhalb des erlaubten Mandantenbereichs greift eine fein granulare Berechtigungsprüfung. Die Plattform übergibt die Anfrage an die Schnittstelle des Melderegisters Düsseldorf, wo Rolle, Kontext und Zweck geprüft werden – z. B., ob eine Sachbearbeiterin einen Datensatz einsehen, aber nicht exportieren darf. Diese Regeln sind je Registermandant anpassbar.

Alle Zugriffe – ob erfolgreich oder abgelehnt – werden revisionssicher protokolliert. So ist jederzeit nachvollziehbar, wer wann was angefragt hat – und wie die Plattform reagierte. Die Plattform tritt nicht als eigenes Fachsystem auf, sondern stellt als sicherer Datenbereitsteller Informationen bereit. Für die Sachbearbeiterin bleibt die Infrastruktur unsichtbar – sie arbeitet wie gewohnt in ihrer Anwendung. Doch jeder Zugriff erfolgt über eine abgesicherte, mandantenscharfe Umgebung.

Fazit

Das vorliegende Whitepaper betrachtete die Bereitstellung von Registern in Cloudinfrastrukturen in einer rechtlichen und technischen Perspektive.

Die rechtliche Betrachtung hat ergeben, dass Register-as-a-Service als Lösung für die Bereitstellung von Registerdaten keine dem Verfassungs- und Datenschutzrecht vereinbar ist. Rechtlich ist es allerdings erforderlich, dass die Registerdaten technisch und organisatorisch gegen die Erstellung von Persönlichkeitsprofilen sowie vor unbefugtem Datenzugriff geschützt werden.

Die Verantwortlichkeit der zuständigen Behörde für die Datenerhebung und für die Sachentscheidung bleibt durch die Auslagerung der Datenhaltung auf eine technisch einheitliche Cloud-Plattform unangetastet. Die entsprechenden Kompetenzen werden hierdurch nicht berührt. Um die unionsrechtlichen Vorgaben (SDG-VO einschließlich Umsetzungsrechtsetzung) und das Ziel einer Harmonisierung durch eine Once-Only-Verfügbarkeit von Registerdaten zu erreichen, ist es unerlässlich, dass auch die kommunale Ebene die notwendigen technischen Vorkehrungen trifft, um die bei ihr gehaltenen Registerdaten in das NOOTS einspeisen zu können.
Die technische Betrachtung basierte auf einer Register-as-a-Service Rahmenarchitektur, die die rechtlichen Anforderungen berücksichtigt und eine rechtskonforme Umsetzung ermöglicht.

Es wird aber auch deutlich, dass für die Nutzung von Register-as-a-Service ein reines lift-and-shift in Cloudinfrastruktur nicht ausreichen könnte. Denn es muss nicht nur die mangelnde Standardisierung der Datenformate und Schnittstellen angegangen werden. Um die neue Registerarchitektur nutzen zu können, stellen sich unabhängig vom Register-as-a-Service-Ansatz Herausforderungen, die im Detail die Erhebung von Daten in Verwaltungsprozessen, deren Transformation von Prozessdaten im Verwaltungsverfahren zu Subjekt- oder Objektdaten im Register, deren Speicherung und Pflege und schließlich die Bereitstellung und Übergabe der Registerdaten in andere Verfahren betreffen.

Es gilt die Fachverfahren zu modernisieren, denn viele der aktuell genutzten Systeme sind nicht ausreichend auf die Anforderungen moderner, digitaler Verwaltungsprozesse ausgelegt und bieten nicht immer ausreichende Möglichkeiten zur Datenanalyse und -auswertung. Zudem spielen die unterschiedlichen Verwaltungsnetze für die Übertragung der Registerdaten eine große Rolle. Da dezentrale Registerinfrastruktur v.a. in kommunaler Zuständigkeit auftreten dürften, muss nicht zuletzt die Rolle von OSCI und XTA2 als Standards der kommunalen Transportwege betrachtet werden. Das Register-as-a-Service-System muss entsprechende Vorkehrungen treffen, um mit den Standards umzugehen, bzw. die Standards in geeigneter Weise implementieren[12].

Wichtig: Wie gesehen, führt die Nutzung der Register-as-a-Service-Architektur und die damit einhergehende Weiterentwicklung der Register nicht zu zentralen Superregistern. Die Datenspeicherung erfolgt allerdings nicht mehr physisch, sondern logisch getrennt anhand fachlicher Parameter. Diese Datenbereitstellung und -verarbeitung in hochmodernen IT-Infrastrukturen entspricht den auch sonst geltenden rechtlichen Anforderungen.Gleichzeitig können Daten so zentral bereitgestellt werden, dass die Anbindung an das NOOTS einfach realisiert wird.

Referenzen

1 Gemeint ist hier das Gesamtprogramm Registermodernisierung im Auftrag des IT-Planungsrats.

2 https://www.normenkontrollrat.bund.de/Webs/NKR/SharedDocs/Downloads/DE/Gutachten/2017-ergänzendes-gutachten-staba-beistellung-registerlandschaft.pdf?__blob=publicationFile&v=2

3 https://europa.eu/youreurope

4 https://verwaltung.bund.de/portal/DE/

5 Siehe näher hierzu https://bmds.bund.de/fileadmin/BMDS/Dokumente/5-Anlage_GE_NOOTS-StV.pdf und https://bmds.bund.de/aktuelles/pressemitteilungen/pressemitteilung-5/2025-28052025

6 Siehe https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-05_Registermodernisierung.pdf

7 Vgl. BVerfG, Beschluss vom 19.11.2002 – 2 BvR 329/97, kommunale Verwaltungsgemeinschaften in Sachsen-Anhalt.

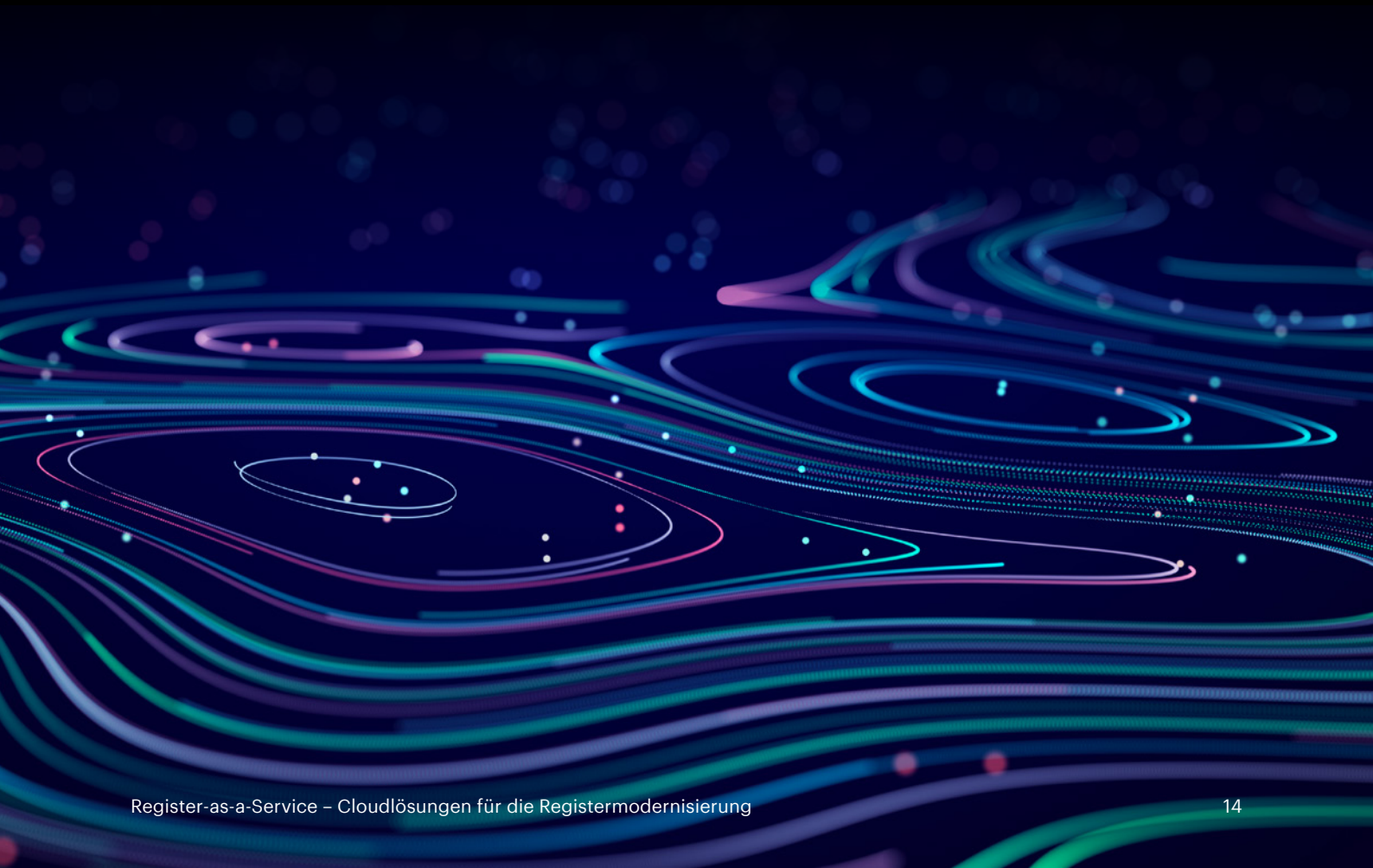
8 Grundlegend BVerfG, Urteil vom 15.12.1983 –, 1 BvR 209/83 u. a., „Volkszählung“.

9 BVerfG, Beschluss vom 16.07.1969 – 1 BvL 19/67, „Mikrozensus“.

10 Büllesbach/Rieß, Outsourcing in der öffentlichen Verwaltung NVwZ 1995, 444.

11 Büllesbach/Rieß, Outsourcing in der öffentlichen Verwaltung NVwZ 1995, 444, 445.

12 Siehe https://www.it-planungsrat.de/beschluss/beschluss-2025-18



Autoren

Benedikt Matthes
benedikt.matthes@accenture.com

Dr. Stefan Bauer
stefan.bauer@cms-hs.com

Kai Sattler
kai.sattler@accenture.com

Martin Kilgus
martin.kilgus@cms-hs.com

Na-Hyeon Shin
na-hyeon.shin@accenture.com

Mitwirkung

Dr. Markus Häuser, Dr. Ursula Steinkemper, Lars Grajewski, Laurence Greeb, Judith Michels, Sven Hellmich, Nikolaj Bøggild, Marco Lechner, Marcus Rumler, Michael Pfleger

Über Accenture

Accenture ist ein weltweit tätiges Beratungsunternehmen, das führende Unternehmen, Regierungen und andere Organisationen dabei unterstützt, einen digitalen Geschäftskern aufzubauen, ihren Betrieb zu optimieren, das Umsatzwachstum zu beschleunigen und Bürgerdienste zu verbessern. So schaffen wir für unsere Kunden in mehr als 120 Ländern Mehrwert. Technologie steht dabei im Mittelpunkt des Wandels, den wir mit starken Partnerschaften in unserem Ökosystem vorantreiben. Unsere 801.000 Mitarbeitenden verfügen über umfassende technologische Kompetenz, insbesondere auf den Gebieten Cloud, Data und Künstliche Intelligenz, sowie über tiefgehende Branchenkenntnis und funktionale Expertise. Damit setzen sie ein breites Spektrum an Dienstleistungen, Lösungen und Ressourcen in den Bereichen Strategy & Consulting, Technology, Operations, Industry X sowie Song um. Unser Erfolg misst sich dabei am Mehrwert für Kunden, Mitarbeitende, Aktionäre, Partner und für die Gemeinschaft. Besuchen Sie uns unter www.accenture.de.

Über CMS

CMS ist in Deutschland eine der führenden Anwaltssozietäten auf dem Gebiet des Wirtschaftsrechts. Mehr als 750 Rechtsanwält:innen, Steuerberater:innen und Notar:innen beraten Großunternehmen ebenso wie mittelständische Unternehmen und Start-ups in allen Fragen des nationalen und internationalen Wirtschaftsrechts. CMS verfügt in Deutschland über Büros an den acht großen Wirtschaftsstandorten Berlin, Düsseldorf, Frankfurt, Hamburg, Köln, Leipzig, München und Stuttgart. Weltweit ist CMS mit mehr als 6.800 Anwält:innen in über 45 Ländern vertreten. Weitere Informationen finden Sie unter cms.law.