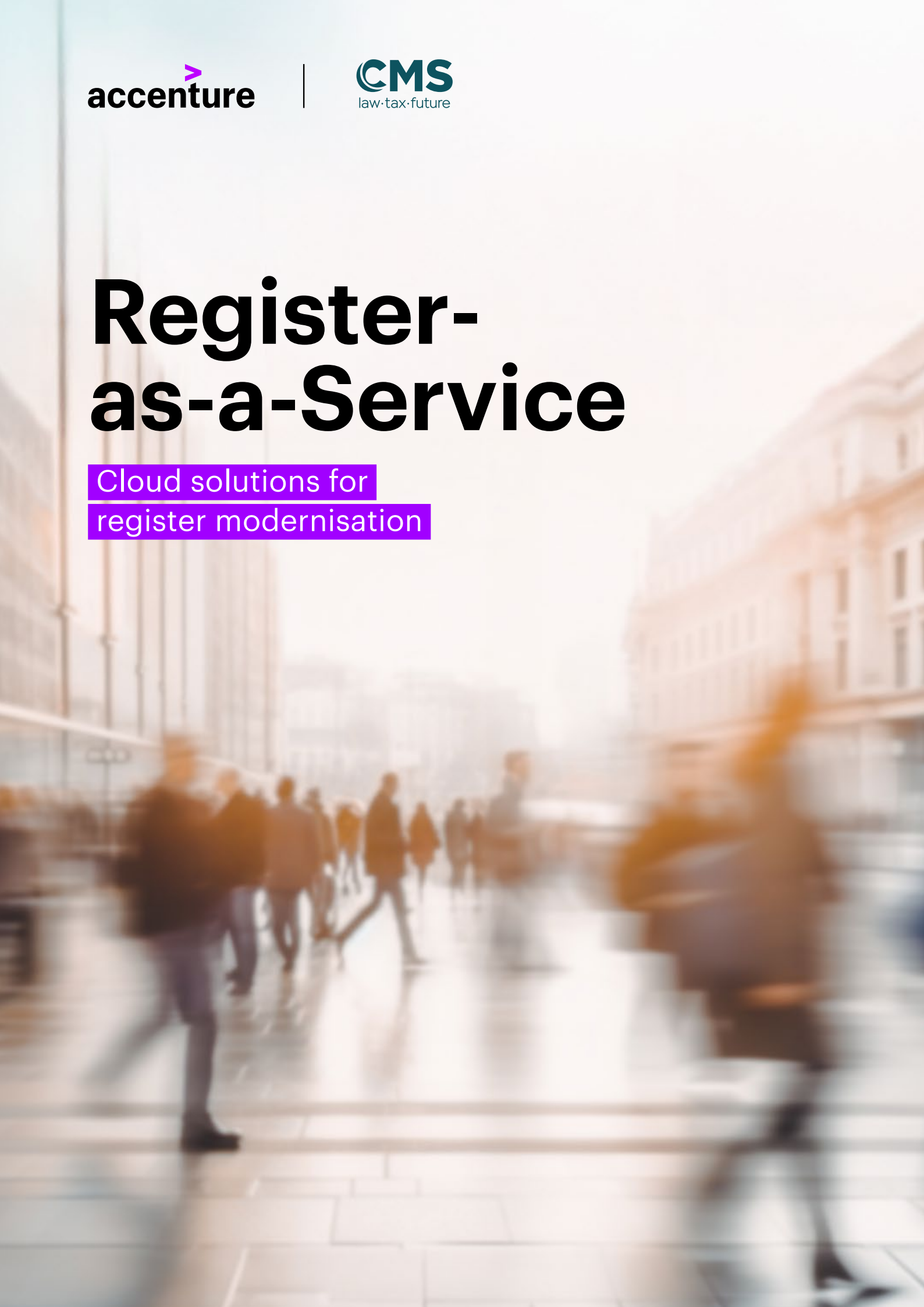
accenture | CMS law·tax·future

Register-as-a-Service

Cloud solutions for register modernisation



Management summary

Cloud-based registration solutions, so-called “Register-as-a-Service“ solutions, are at the centre of current considerations for modernising government data infrastructures. Against the backdrop of the German government‘s digital policy objectives and growing demands for sovereignty, data protection and efficiency, the question arises as to the conditions under which register data can be operated in cloud environments in a legally compliant, secure and future-proof way. This white paper provides a structured answer to this question – legally sound, technically well thought-out and set out in a practical way. The following eight core results summarise the key findings and show how a cloud-based register model can be successfully implemented.

1. Using a cloud for decentralised registers is possible from a legal perspective

The use of a shared cloud infrastructure for register data is permitted at all administrative levels. As such, it does not raise any constitutional or data protection concerns. This also applies if databases that have previously been physically separate are transferred to a uniform technical service platform. A prerequisite for using a cloud infrastructure is that the data remain logically separated from each other and that the registration authority retains full control over “its” data.

2. Cloud solution does not change the legal responsibility for collected data

The question of who “owns” the data, i.e. who is responsible for data storage, is not influenced by the administrative level (federal, state, municipal) or the way in which they are technically operated and managed. Registration authorities do not have free access to data, but may only collect, store and use them within the scope of their legal responsibility. The use of a cloud solution does not change this. In this case, responsibility for data management remains fully with the respective competent authority.

3. Encryption is a central pillar of Register-as-a-Service

Data encryption is a key element in achieving the necessary logical separation of register data from different areas of responsibility, i.e. according to who is responsible for their storage. Only the registration authority must be able to access "its" data. Unauthorised access by "third parties", including other registration authorities or the operators of the cloud infrastructure, must be prevented. The latter requires technical, contractual and organisational measures in accordance with the GDPR and the requirements of the German Federal Office for Information Security (BSI), and confidential computing may offer solutions. It should be noted that a shared storage environment could be an attractive target for attacks ("honeypot"). This risk can also be minimised by end-to-end encryption with the respective registration authority having exclusive responsibility for the key.

4. Linking of specialised procedures requires technical interfaces and standardised data preparation

a) The data available in specialised procedures are usually collected and stored in a process-orientated format. They must be converted into structured formats suitable for registers. Register data must be subject or object-orientated. The preparation of the data (e.g. aggregation, conversion, status generation) requires central specifications.

b) The specialised procedures must be technically capable of triggering CRUD operations (create, read, update, delete) in the cloud register via interfaces. "API only" applies. Register data can only be accessed via dedicated interfaces.

Ideally, these points should be standardised for the respective register. Specialised procedures and, if necessary, data preparation must be adapted accordingly.

5. Sector-based law is key

The operation of a register in the cloud and its connection to the NOOTS does not require express legal authorisation. Sector-based law may contain specific provisions in individual cases. This applies in particular to the issues of data access, the preparation of the data collected for provision in the registers and responsibility for these data, as well as the issue of the permissibility of making them available for other administrative procedures. Where subject-specific provisions exist, these must be observed when implementing Register-as-a-Service.

6. Data protection law is not an obstacle – as long as requirements are met

The report makes it clear that there are no fundamental data protection concerns with regard to cloud solutions, even when personal data are involved. The key aspects to consider to ensure data protection are the implementation of suitable technical and organisational measures in accordance with Article 32 GDPR and a clearly regulated relationship between the registration authority and the cloud provider (incl. data processing agreement in accordance with Article 28 GDPR).

7. Be careful when choosing the cloud operator

Choosing a cloud infrastructure operator presents a number of challenges. For digital sovereignty, solutions that make it easy to switch to another operator are preferable. For highly sensitive register data, it is advisable to secure operations in an EU-based or sovereign cloud region. Data residency, exclusive key control and contractually verifiable exit capability are crucial, regardless of whether the cloud provider is based in the EU or a third country.

8. Requirements for the cloud transformation of a register – separation of data, administrative procedures and software systems

Transferring existing data to the cloud requires preliminary clarification and structuring as well as quality assurance. Without this preparatory work, there is a risk that deficiencies in the infrastructure used to date will persist even after a cloud transformation ("from the town hall basement to the cloud"). This would significantly reduce the benefits of digitalisation and prevent a real shift towards digitalisation. In future, software systems, data storage and administrative procedures must be thought out and planned in an integrated way.

1 Technical reasons for Register-as-a-Service

Register modernisation ("RegMo")[1] is one of the largest digitalisation projects in Germany. It is establishing the National-Once-Only-Technical-System ("NOOTS") – the administrative "data highway". The aim is to provide uniform online access that makes administrative services easily accessible regardless of jurisdiction.

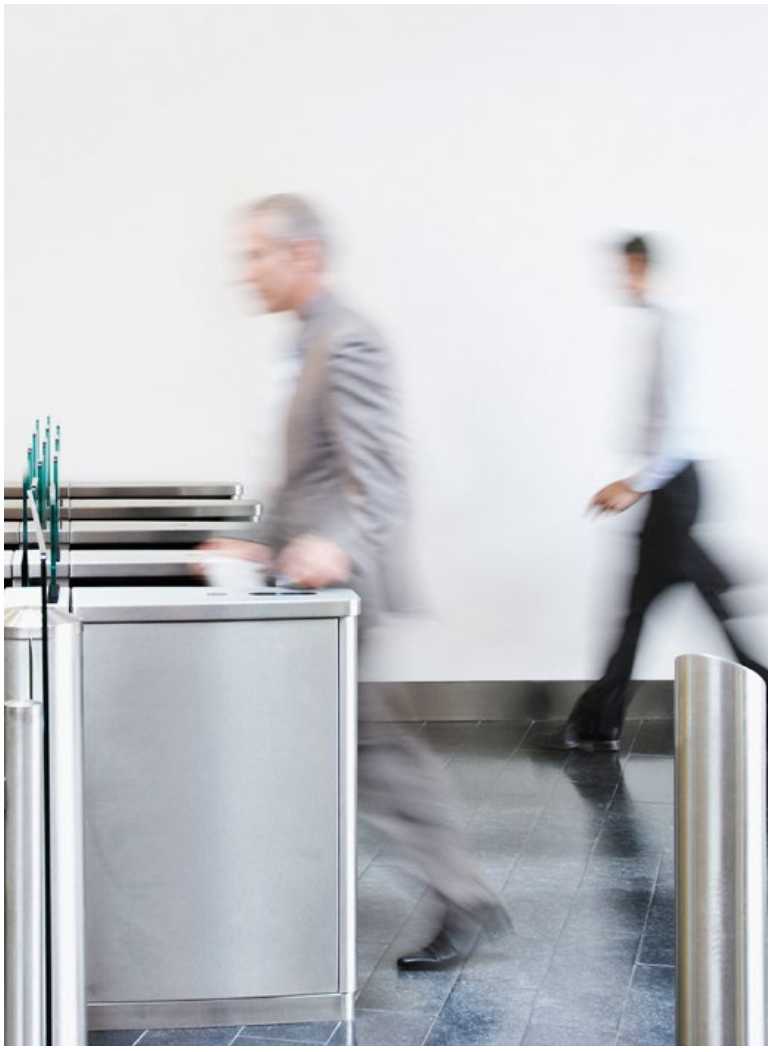
The NOOTS enables the flow of evidence data between registers and authorities in order to implement the "once-only principle": Data only need to be collected once and can then be retrieved and processed electronically. This reduces the burden on citizens, cuts administrative costs and creates a central technical basis for automated administrative procedures. An interface also enables data to be exchanged between the national system and the EU system ("EU-OOTS").

High-quality and readily available register data are essential for success. The challenge lies in the heterogeneity of the data: Even the term "register" is not clearly defined everywhere, and the distinction between registers and other administrative data is sometimes unclear. Registers exist at all federal levels and are kept by a wide range of different bodies, including authorities, courts, and self-governing bodies.[2] The register map of the German Federal Office of Administration lists 290 registers (May 2025), 50 of which are municipal. The term covers all data-based structures that are necessary for the provision of services.

Data quality and availability vary greatly due to a lack of standards. Municipal register data in particular are often available in decentralised specialised procedures that are tailored to specific administrative tasks and difficult to integrate. Data are stored there in a process-orientated format and can usually only be used within one administrative level – cross-administrative exchange is the exception, but a central goal of administrative digitalisation.

In future, data storage and management must be comprehensive, binding and standardised. Data are to be provided in an object or subject-orientated way and technological standards established across the board. The aim is to improve accessibility, scalability and availability – 24/7, in real time and with the flexibility to respond to changing needs.

One solution lies in the cloud: Register-as-a-Service enables the integration of heterogeneous data while complying with central standards, architectural guidelines and security requirements. The advantages of decentralised data security are retained while digital connectivity is improved. Registers can be connected more easily to the NOOTS – secure, available and in compliance with legal requirements.



Transferring decentralised register data to a cloud (“Register-as-a-Service”) could improve data security, maintenance and quality, and simplify connection to the NOOTS. Decentralised registers in particular could benefit from this. This requires a suitable technical solution. However, cloud use must not be viewed in isolation – it requires organisational integration: Administrative staff must be able to access the cloud infrastructure, and data delivery, preparation and quality assurance must be regulated at an organisational level.

Three key questions arise:

1. How do data get into the registers and the cloud? What needs to be considered when standardising data preparation?

2. How are data stored, processed and administered?

3. How are they made available via the NOOTS? How is the connection established from a technical and organisational perspective?

In technical terms, the aim is to create a robust, secure and flexible infrastructure based on open source technologies without vendor lock-in. At its core is a “decentralised-centralised cloud” that leaves clear data responsibility with the relevant administrative units but leverages centralised provisioning advantages. There are technical challenges in terms of transport routes and data storage during idle periods. The infrastructure of the NOOTS must be taken into account.

In addition to technical and organisational feasibility – especially with register data that are currently stored in a decentralised form – questions arise regarding the legal permissibility of cloud use. The use of a uniform technical system (“Register-as-a-Service”) while maintaining the logical responsibility of the register controllers (e.g. municipalities) has not yet been tested. This white paper outlines technical options and the legal framework. It is not a final legal opinion, but a basis for a framework architecture and initial prototypes.

2 | Legal basis for Register-as-a-Service

2.1 Background

Union law level

The Regulation on the "Single Digital Gateway" (Regulation 2018/1724, or "SDG Regulation" for short) creates a digital gateway to the public administration of the Member States at EU level. Access is via the "Your Europe" portal[3], which is linked with the German Federal Portal[4] and provides online access to administrative services at all levels. The SDG Regulation requires Member States to provide certain information and services digitally across borders (Article 14). It also requires a technical system for the automated exchange of evidence in order to implement the once-only principle throughout Europe. The specifications are set out in the Implementing Regulation (Regulation 2022/1463). At national level, implementation is carried out via the NOOTS with a link to the EU-OOTS.

National level

The national counterpart to the SDG Regulation is the German Online Access Act (OZG) of 2017, which was recently amended. The central object of the amendment, "OZG 2.0", is the efficient and targeted implementation of the once-only principle. The German Online Access Act (OZG) now contains a general clause for the retrieval of evidence data (sections 5, 5a German E-Government Act (EGovG)), amendments to the provisions on data collection (section 8 German Online Access Act (OZG)) and an obligation on the federal states to ensure that the municipalities are connected to the portal network (section 1a (3) sentence 2 German Online Access Act (OZG)).

The constitutional basis for cooperation between the federal and state governments with regard to IT systems is Article 91c German Basic Law (GG). This is the basis for the German IT Network Act (IT-NetzG), which defines the operation of the network and the connection provisions for all administrative levels. Details are regulated by the IT Planning Council (section 4 (3) German IT Network Act (IT-NetzG)).

Register modernisation is both a central and challenging component of the once-only principle. Its basis is the Register Modernisation Act of 28 March 2021, which, together with the German Identification Number Act (IDNrG), introduces the use of the tax ID (section 139b German Tax Code (AO)) as a reference code. The Annex to the German Identification Number Act (IDNrG) lists 50 priority registers to which an identification number must be assigned as a reference code by the end of 2028.

The heterogeneity of the register landscape makes implementation particularly complex. The federal and state governments have set up the IT Planning Council to coordinate their IT cooperation. Its tasks also include the necessary guidance for implementing the NOOTS. In December 2024, the federal and state governments agreed on a separate NOOTS treaty to regulate the guidelines for establishing the NOOTS and integrating the register data, although this has not yet been fully ratified.[5] The IT Planning Council published a target vision with an implementation plan back in January 2021. This prioritises 18 of the registers listed in the German Identification Number Act (IDNrG)[6]. Binding requirements for full connection to the NOOTS are still pending.

2.2 Constitutional requirements

2.2.1 Permissibility of federal requirements for register modernisation

Federal regulatory competence

As part of the municipal integration into the German Online Access Act (OZG), there was discussion as to whether Article 91c (5) German Basic Law (GG) is sufficient as a legislative competence. Even though it only refers to the federal and state governments, municipalities are organisationally assigned to them. The explanatory memorandum on the legislation makes it clear that the legislature expressly wanted to include municipalities – especially as many services are provided by municipalities.

There is no impermissible transfer of tasks: It is not about new tasks, but about the digital fulfilment of existing obligations.

Guarantee of local self-government

Article 28 (2) German Basic Law (GG) guarantees municipalities the right to regulate their own affairs ("guarantee of local self-government"). However, this only applies to matters relating to the local community. Tasks in the delegated sphere of activity, in which the municipalities implement federal or state laws (such as passport and registration matters), are not covered by the guarantee of local self-government. Federal requirements for administrative and register modernisation can therefore only influence the protected area of self-government if they would place an excessive financial burden on municipalities and thus restrict their scope for action in the area of self-government. The connexity principle in the state constitutions, i.e. the need for provisions to cover costs when transferring state tasks to municipalities, takes this into account. The German Federal Constitutional Court also recognises the functionality of the administration as a matter of public interest that can justify certain interventions in the area of self-government.[7] As such, neither the German Online Access Act (OZG) nor the Register Modernisation Act have yet been challenged in court.

2.2.2 Informational self-determination

According to the case law of the German Federal Constitutional Court[8], the general right of personality protected by Article 1 (1) and Article 2 (1) German Basic Law (GG) also guarantees the right to informational self-determination. This means that each and every individual has the fundamental right to decide for themselves how their personal data are disclosed and used.

Existing database

Register modernisation only concerns the digital availability of existing data. The permissibility of data collection is governed by the relevant sector-based law. Data retrieval via the NOOTS is also subject to existing legal bases. Data are only used at the instigation of the data subject (section 8 German Online Access Act (OZG)).

Constitutionality of the German Identification Number Act (IDNrG)

The constitutionality of register modernisation does not depend on the constitutional assessment of the reference code (tax number) used in the German Identification Number Act (IDNrG). With reference to an older decision of the German Federal Constitutional Court[9] as well as Article 1 (1) German Basic Law (GG), isolated concerns were expressed that a personal identification number could lead to impermissible cataloguing. However, storage for "once only" data exchange does not allow for unconstitutional personality profiling. No constitutional complaints against the German Identification Number Act (IDNrG) are currently pending.

Data sovereignty

Data sovereignty is not affected by register modernisation. In the concept of decentralised cloud data storage, the data-collecting authority's access and thus its legal responsibility remain unrestricted.

Adequate protection against unauthorised data access

The right to informational self-determination requires adequate protection by the collecting authority. The following considerations show that this can be adequately protected in decentralised cloud data storage by the measures provided for in the NOOTS.

2.3 Data protection, data security and choice of operator

Data storage in a third-party system ("Register-as-a-Service") involves outsourcing to an entity other than the registration authority. This is not prohibited under data protection law. Technical support activities such as data centre operation or IT services can generally be outsourced and provided by private entities.[10]

2.3.1 Cloud use per se

From a legal perspective, the term "cloud operation" refers to the replacement of self-operated systems with the use of (parts of) high-performance and scalable third-party data centres.

2.3.2 Fundamental permissibility of cloud service use

There are limits to cloud use if sovereign activities are transferred to third parties – such as the processing of applications or the issuing of administrative acts. Such functions may only be transferred to authorised private entities in exceptional cases. These restrictions do not apply to technical support functions. In this case, private entities act as administrative assistants and perform tasks on behalf of and in accordance with the instructions of the authorities.[11] The decisive factor is that the details as to whether and how data are processed are determined by the administration and the legislature. When outsourcing to the cloud, the public administration remains responsible for the permissibility and lawfulness of the processing of personal data.

2.3.3 Use of a service provider for several register controllers

Insofar as personal data are processed by third parties on behalf of the authorities, the provisions on commissioned data processing pursuant to Article 28 GDPR apply. No dedicated hardware owned by the authorities is required under data protection law; the use of shared resources is permitted, provided that the body responsible for the register retains control over data and their processing in the cloud. This is ensured by a data processing agreement in accordance with Article 28 GDPR. The cloud operator must exclusively follow the instructions of the principal. These obligations correspond to the constitutional and administrative law requirements for technical assistance on behalf of the authorities.

2.3.4 Restrictions on the use of non-European providers

The GDPR generally permits the transfer of data to providers outside the EU if the same level of data protection is ensured at the place of processing as in the EU. For some countries, the EU Commission has formalised this in an adequacy decision. For other countries, this can be achieved through other protective measures, such as the conclusion of standard contractual clauses. However, in view of the political situation, particularly in the US, it is important to critically examine whether these requirements can be met in the long term. It is currently unclear whether the adequacy decision for the US remains applicable or whether EU standard contractual clauses will suffice. Against this background, European cloud providers should be used.

2.3.5 Restrictions on cloud use in individual cases

In individual cases, sector-specific provisions may restrict the use of cloud service providers – for example in German Social Code X (SGB X) for social data or in sections 45 ff. German Federal Data Protection Act (BDSG) for law enforcement data. There are also exceptions for register data: Serial numbers of identity cards may only be stored at the German Federal Printing Office, the Bundesdruckerei (section 16 (3) German Passport Act (PassG), section 26 (3) German Act on Identity Cards and Electronic Identification (PAuswG)). Other restrictions that were in place until recently, for example in the Brandenburg or Saxony Registration Acts, have been lifted. Before moving a register to the cloud, it is therefore necessary to check whether there are any restrictions for the specific register in individual cases. However, there is no general ban on the Register-as-a-Service approach.

2.3.6 Security requirements

The data protection security requirements for cloud outsourcing are set out in Article 32 GDPR: Appropriate technical and organisational measures must be taken to ensure confidentiality, integrity, availability and resilience. Physical separation ("air gap") of the registers is not prescribed. The use of shared computer resources is permissible if suitable logical separation mechanisms – such as role and authorisation concepts or virtual instances – are used.

3 Technical diagram for Register-as-a-Service

The use of a cloud-based infrastructure for register data marks a technical reorientation: The aim is to transform heterogeneous, historically evolved register structures into a modern, federally-linked platform architecture. Register data should be provided in such a way that they meet the requirements of administrative digitalisation – particularly with regard to the NOOTS and the once-only principle – without undermining register sovereignty or responsibilities.

3.1 Basic principles of the architecture

At the system's core is a multi-client-capable platform architecture that processes data jointly from a technical perspective but separately from a legal and logical perspective. It follows the principles of modern cloud-native systems, but integrates federal lines of responsibility: Each registration authority remains responsible for the data and controls access – even when operating within a shared platform environment.

The client model is based on a containerised infrastructure with dynamic orchestration. Each client (each register) is operated in isolation in a dedicated namespace – technically shielded, clearly assigned organisationally and secured via a role and attribute-based access concept. Control over access, configurations and data catalogues remains with the competent authority. Key material is also managed on a client-specific basis – without centralised bundling.

The platform is not a central register instance, but a standardised operating framework – a kind of "digital parcel". Registers use shared services such as status monitoring or certificate management, but remain strictly separate. There is no higher-level instance with access to register data. Data are exchanged exclusively via defined interfaces, such as the NOOTS or the EU-OOTS.

This creates an infrastructure with a common technical basis and strict federal separation. Its strength lies not in centralisation, but in standardised decentralisation – without sacrificing legal or technical independence.

3.2 Security, quality and sovereignty as drivers of architecture

The quality of a cloud-based register architecture depends not only on scalability or elegance, but also to a large extent on security, stability and trustworthiness. Since register data contain sensitive information, their protection is paramount.

All platform components follow "security by design". Internal communication is fully TLS-encrypted, certificates are automatically managed on a client-specific basis, and key material is only accessible via separate storage instances. Data are stored and transmitted in encrypted form (mTLS). Every API access is logged, versioned and traced back to the responsible role. Confidentiality, integrity and traceability are technically embedded.

The platform is designed for high availability, fault tolerance and reliability. Automated orchestration, self-healing, rollback mechanisms and dynamic load management ensure round-the-clock operation – not as a goal, but as standard. Maintainability and expandability are integral components. Changes to configurations or clients are described declaratively, tested and rolled out automatically – versioned, traceable and reversible. New register clients, data models or guidelines can be added during operation. Security updates are carried out continuously. The platform scales horizontally and vertically and adapts dynamically to registers and specialised procedures. Critical components such as gateways, databases or authentication services can be configured on a client-specific basis. The system remains stable and compliant even if there are mass retrievals – for example via the NOOTS. Security, availability, expandability, performance and scalability are not abstract goals, but fundamental design principles – technically feasible and legally viable.

3.3 Not just secure, but smart: API access model and connection to the NOOTS

Based on this architecture, it is clear that the platform is not only an operating environment, but also a control room for digital evidence. Controlled, traceable access to register data creates the conditions for a reliable connection to the NOOTS.

The platform uses an API-based access model: All access – through specialised procedures, portals or the NOOTS – is via clearly defined, versioned interfaces. These APIs are part of a governance model and are linked to a role and attribute-based authorisation system. Access is authorised on a context-sensitive basis – depending on role, purpose and legal basis.

The platform provides standardised adapters for the NOOTS that process XNachweis messages, check signatures and validate access in real time. Register retrieval thus becomes an integrated process – with automated control, connectable to national and EU infrastructures, without each register having to develop its own connectors.

This standardisation does not restrict flexibility: Register controllers use configurations to define which data formats are provided, which request limits apply and which authentication requirements must be met. Even complex rules, such as those for data combinations or filtering, can be implemented without central intervention – for uniformly orchestrated, legally compliant data access.

The platform takes the burden off the NOOTS connection and creates a new understanding of data access: not as an exception, but as a rule-based, machine-readable authorisation process. It paves the way for automated administrative procedures – not centralised, but federally standardised.

3.4 Client separation: technical enforcement of federal responsibility

Client separation is a key security feature. It ensures that each registration authority can only access its data.

The first level is operational isolation, e.g. through Kubernetes namespaces. Each client operates in a dedicated area with its own configuration, key management and operating metrics – separated in terms of logic and network. Requests are only forwarded after successful authentication and clear client assignment.

Protection begins right at the entry point: Each request requires certificate or token authentication, the identity of which is included in the request context – manipulation is technically impossible.

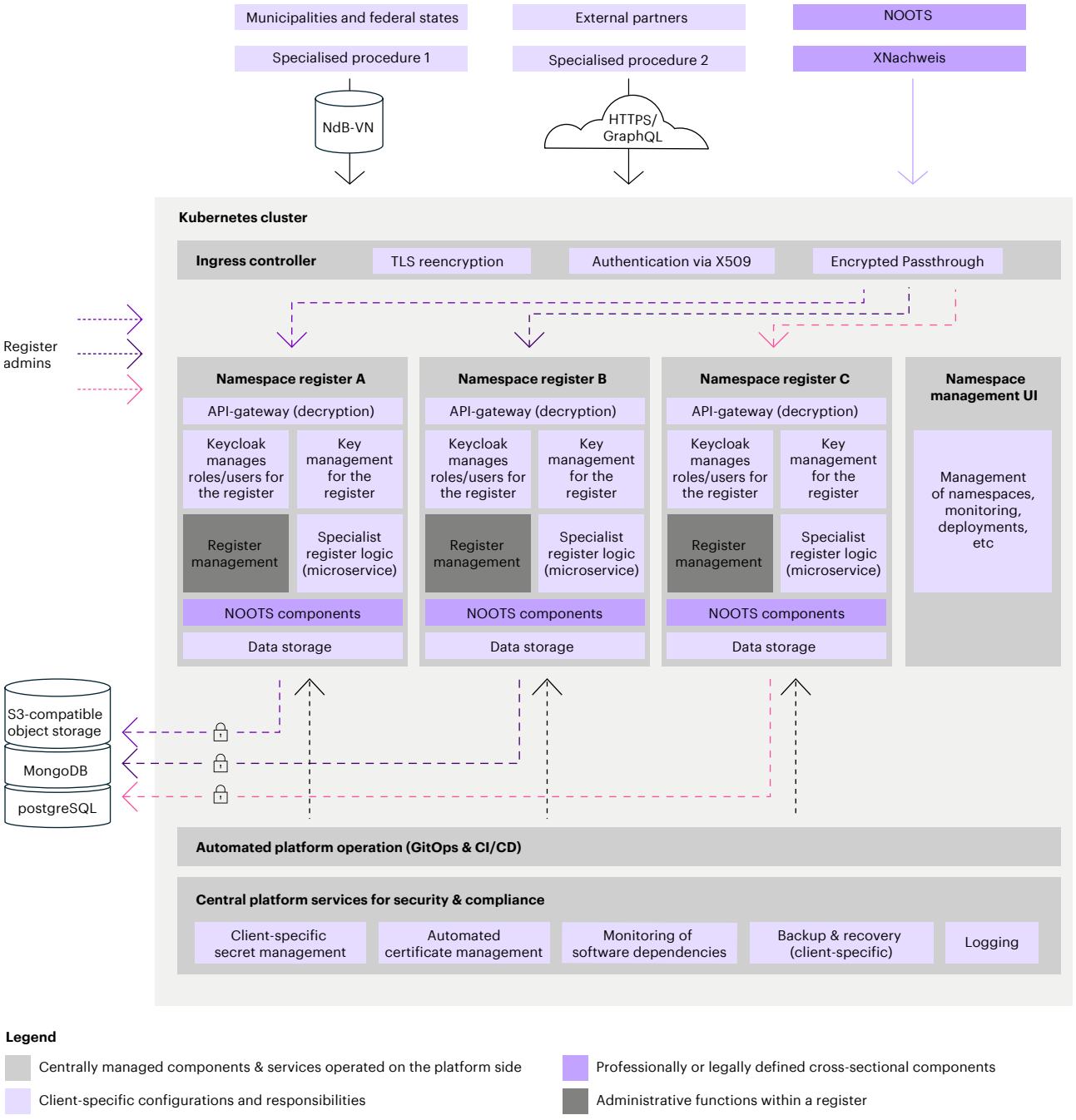
A fine-grained authorisation model regulates who can access which resources – depending on the client, role, source or purpose. Management portals and admin interfaces are also strictly segmented by client. Each register administrator only has access to “their” register – both from a technical perspective and an operational perspective.

Operational services such as monitoring, deployment or logging are organised on a client-specific basis. Audit data are stored separately and technical guidelines are enforced decentrally – without a centralised collective audit.

The combination of network segmentation, access control, identity binding and isolated services ensures that nobody can access third-party data – not even the platform itself – unless explicitly delegated. Logical separation is at the heart of the security architecture and reflects the federal trust model of register management in Germany.

3.5 Architectural diagram

Register-as-a-Service



Legend

- Centrally managed components & services operated on the platform side
- Client-specific configurations and responsibilities
- Professionally or legally defined cross-sectional components
- Administrative functions within a register

The proposed architecture is not only a technical platform, but above all an organisational structure for trust in federal contexts: trust that data are available but not withdrawn; that infrastructure is modern but not centralised; that scalability is achievable but not synonymous with loss of control.

3.6 Connecting a municipal specialised procedure to the platform

A typical working day for a clerk at the Residents' Registration Office begins with logging on to the workplace computer. They then launch the municipal specialised procedure for the residents' register – a specialised application for handling processes such as changes of address, deregistration or requests for information.

To start with, they log in with their personal access data – usually via the centrally managed user administration system of their municipality (e.g. City of Düsseldorf), which is connected to the platform's identity service. Authentication is carried out using a standardised protocol that checks identity, role and organisational affiliation and secures them using cryptography.

After successful authentication, the specialised procedure is assigned an access token that contains the identity, role (e.g. "registration clerk"), organisational affiliation (e.g. "Düsseldorf Residents' Registration Office") and the permitted client context (e.g. "Düsseldorf Residents' Register"). This token is included with every request to the platform – for example when retrieving data or generating evidence.

Access is only possible via an authorised administrative network, such as a state network or the federal network.

When a connection is established, the platform uses certificate exchange (mutual TLS) to check whether a valid, trustworthy client certificate is available. Only then will the request be accepted.

Only after this verification does the platform use the token to check whether the request is validly signed and corresponds to the intended client context. If a specialised procedure attempts to access another residents' register (e.g. Cologne) – for example, due to an error or misuse – the platform immediately blocks access.

A fine-grained authorisation check is performed within the permitted client area. The platform transfers the request to the interface of the Düsseldorf Residents' Register, where the role, context and purpose are checked – e.g. whether a clerk is permitted to view a data set but not export it. These rules can be customised for each register client.

All access attempts – whether successful or rejected – are logged in an audit-proof manner. This means that it is always possible to see who requested what and when – and how the platform responded.

The platform does not act as a specialist system in its own right, but provides information as a secure data provider. The infrastructure remains invisible to the clerk, who works as usual in their application. However, all access takes place via a secure, client-specific environment.

Conclusion

This white paper has examined the provision of registers in cloud infrastructures from a legal and technical perspective.

The legal analysis shows that Register-as-a-Service is not compatible with constitutional and data protection law as a solution for providing register data. However, it is legally required that the register data be technically and organisationally protected against the creation of personality profiles and unauthorised data access.

The responsibility of the competent authority for data collection and for the substantive decision remains unaffected by the outsourcing of data storage to a technically uniform cloud platform. This does not affect the relevant competences. In order to comply with EU law (SDG Regulation including implementing legislation) and the goal of harmonisation through the once-only availability of register data, it is essential that the municipal level also takes the necessary technical precautions to be able to feed the register data it holds into the NOOTS.

The technical assessment was based on a Register-as-a-Service framework architecture that takes into account the legal requirements and enables legally compliant implementation. However, it is also clear that a simple lift-and-shift to cloud infrastructure may not be sufficient for the use of Register-as-a-Service. It is not only the lack of standardisation of data formats and interfaces that needs to be addressed. Regardless of the Register-as-a-Service approach, challenges arise in order to use the new register architecture. These relate specifically to the collection of data in administrative processes, their transformation from process data in the administrative procedure to subject or object data in the register, their storage and maintenance and finally the provision and transfer of the register data to other procedures.

The specialised procedures need to be modernised, as many of the systems currently in use are not sufficiently designed to meet the requirements of modern, digital administrative processes and do not always offer sufficient options for data analysis and evaluation. The different administrative networks also play a major role in the transfer of register data. Since decentralised register infrastructures are likely to occur primarily under municipal responsibility, the role of OSCI and XTA2 as standards for municipal transport routes must also be considered. The Register-as-a-Service system must take appropriate precautions to deal with the standards or implement the standards appropriately[12].

Important: As we have seen, the use of the Register-as-a-Service architecture and the associated further development of the registers does not lead to centralised super registers. However, data are no longer stored physically, but logically separated using technical parameters. This provision and processing of data in state-of-the-art IT infrastructures complies with the legal requirements that apply in other areas. At the same time, data can be provided centrally in such a way that the connection to the NOOTS is easy to implement.

References

1 This refers to the overall register modernisation programme commissioned by the IT Planning Council.

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/EN

5 For more information, see https://bmds.bund.de/fileadmin/BMDS/Dokumente/5-Anlage_GE_NOOTS-StV.pdf and https://bmds.bund.de/aktuelles/pressemitteilungen/pressemitteilung-5/2025-28052025

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

7 See German Federal Constitutional Court, decision of 19 November 2002 – 2 BvR 329/97, municipal administrative communities in Saxony-Anhalt.

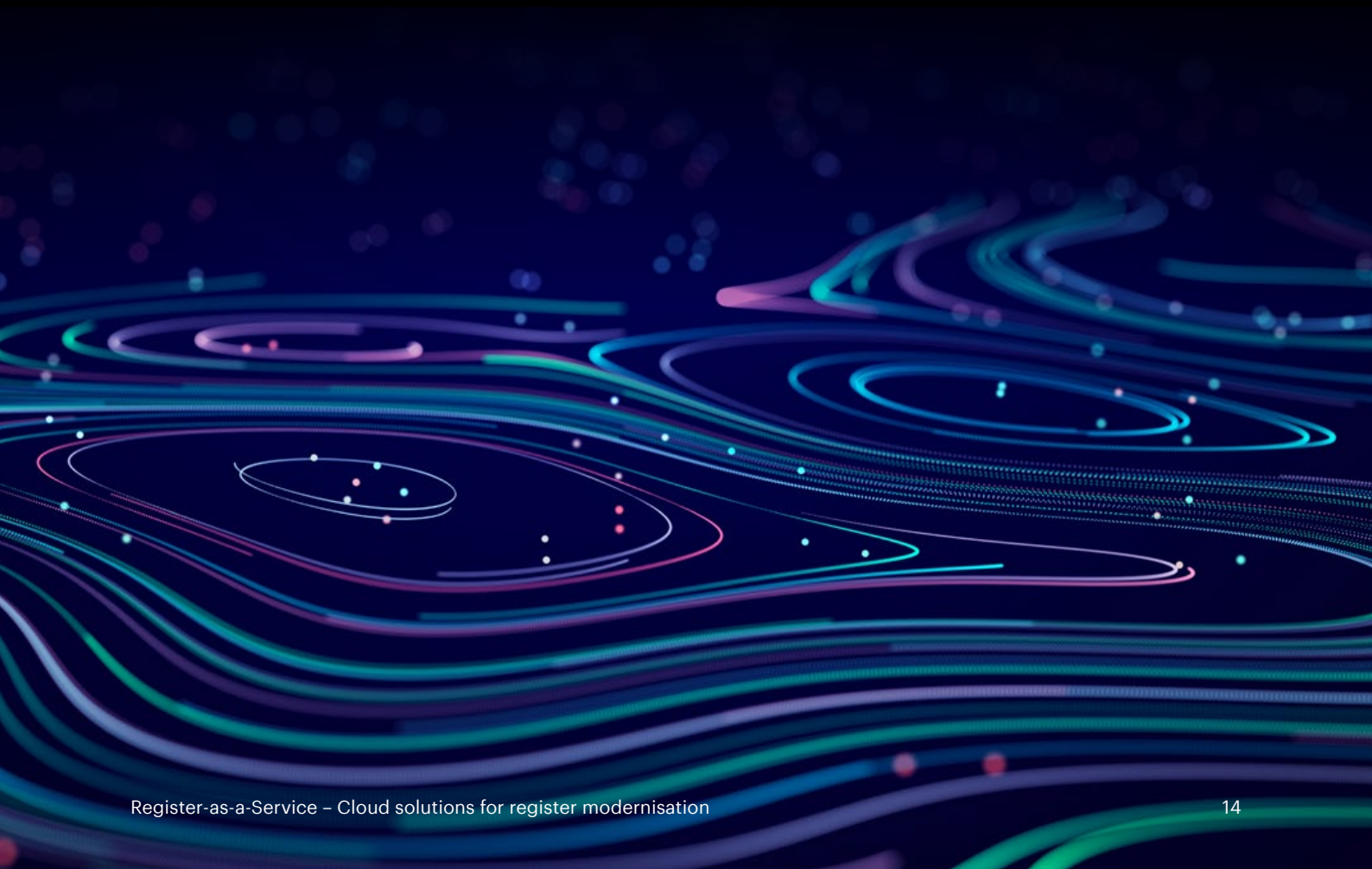
8 Fundamental decision of the German Federal Constitutional Court, judgment of 15 December 1983 –, 1 BvR 209/83 and others, „Volkszählung". (census)

9 German Federal Constitutional Court, decision of 16 July 1969 – 1 BvL 19/67, „Mikrozensus" (microcensus)

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

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

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



Authors

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

Contributors

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

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 791,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. Our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at accenture.com.

About CMS

CMS is one of the leading corporate law firms in Germany. More than 750 lawyers, tax advisors and notaries advise clients from major corporations to SMEs and start-ups on all aspects of national and international corporate law. CMS has offices in the eight major business centres in Germany: Berlin, Düsseldorf, Frankfurt, Hamburg, Cologne, Leipzig, Munich and Stuttgart. CMS is represented by more than 6,800 lawyers in over 45 offices worldwide. Further information can be found at cms.law.