The public cloud in the public sector

Open Telekom Cloud

FOREWORD

The public sector is currently carrying out a comprehensive modernization and digitalization of its services and processes. Public cloud solutions are an important component that supplement the sector’s own capacities in order to create a flexible IT infrastructure. However, due to its special position and for reasons of security and data protection, the public sector can only use these solutions to a limited extent and under specific conditions.

This whitepaper provides guidance on the requirements that public cloud services and providers must meet for use by federal, state, and municipal authorities. Deutsche Telekom AG ("Telekom" for short) can contribute its many years of experience in working with the sector and in implementing IT projects in the public sector. Nevertheless, this paper can only cover the topic of public cloud solutions in the public sector to a limited extent. It, therefore, by no means deals with this issue definitively and, in particular, only depicts the situation at the time of publication (January 2022). It does not replace any security-related, data protection-related, or other legal advice in individual cases. Despite the utmost care in its preparation, the publishers accept no liability.

Content

1. Summary

To offer employees and citizens better services in the future, the public sector is currently modernizing its processes and services with a broad range of measures. A flexible IT infrastructure is essential in order to reach quickly to changing needs. Public cloud solutions offer many advantages and opportunities to supplement in-house capacities in an uncomplicated manner. However, due to its special position, the public sector can only take advantage of public cloud offerings to a very limited extent. For example, for security and data protection reasons alone, many providers are not even considered. As federal, state, and municipal public administrations have to regularly retender their contracts, they are also not allowed to make a firm commitment to a single provider. However, because many cloud providers operate proprietary interfaces and file formats that make it difficult to transfer data in the event of a change of provider, in many cases public sector clients cannot rule out a vendor lock-in.

Public administrations, therefore, have to choose a public cloud solution that is as open as possible, subject exclusively to European law, and meets all the requirements of the GDPR. Services such as dedicated resources and advanced encryption methods increase the level of security. Ideally, providers can prove this with meaningful certificates. The Open Telekom Cloud's numerous projects, for example, show how federal, state, and municipal authorities benefit from the flexible services of a secure public cloud. From infrastructure for citizen apps and the digitalization of administrative services to concentrated computing power for research, the solution has proven itself in a wide range of public sector scenarios.

2. Introduction: Driving digitalization forward with flexible IT infrastructures

Digitalization in the public sector is picking up speed: With the Online Access Act (OZG), by the end of 2022 at the latest, Germany's federal, state, and municipal authorities will also offer their administrative services digitally. Citizens will then be able to apply for documents such as their ID card, passport, and birth certificate entirely online. More than 500 services will be made available digitally as part of the roll-out, including processes such as vehicle registrations and change of address notifications. In addition, the law provides for the previously independent portals of the states and municipalities to be merged into a uniform portal network.

To give digitalization measures a stable foundation, the authorities are also increasingly modernizing the processes behind the application submission process. Based on the Register Modernization Act passed by Germany's upper legislative body, the Bundesrat, in spring 2021, for example, public sector bodies are reducing redundant data processing and creating a uniform means of identification for the OZG services. In the future, citizens will only need their tax identification number when they go to the (digital) authorities, instead of having to provide their data over and over again when contacting the various state registers.

New technologies improve day-to-day working life

The digitalization of public administration services benefits not only citizens, but also public sector employees: Modern IT solutions relieve the administrative staff of tedious routine tasks, make paper-based processes superfluous, and enable more flexible and remote work with cloud-based technologies. In public institutions with a high level of digitalization and automation, civil servants and employees have more time for the citizen:

They work through approval processes faster, can access important information more quickly, and are easier to reach. The fact that digitalization is having a positive impact on employees' day-to-day work is also shown by recent surveys on the subject: According to Price Waterhouse Coopers (PwC), 64 percent of employees in German companies are convinced that new technologies are improving their day-to-day working life. Meanwhile, a survey conducted by the Deutsche Angestellten Krankenkasse (DAK) health insurance fund illustrates the extent to which the coronavirus pandemic has affected positive attitudes toward digitalization in the workplace. According to the survey, the proportion of employees who perceive new technologies as making their working life easier increased by 39 percent during the pandemic.[2]

Flexible IT infrastructures help public sector bodies to respond quickly to the needs of employees and citizens. In this context, the public cloud in particular opens up many opportunities for planners and managers as a supplement to their own data centers. Whether it is the uncomplicated scaling of applications for hybrid work models, the rapid provision of new services, or the development of innovative technologies based on AI – the advantages are clear. However, because the public administration has to look particularly critically at aspects such as security and data protection, public cloud solutions are only an option for public sector bodies under certain conditions.

The following chapters show how public authorities can meet the various requirements of digitalization with the right cloud technology and, on this basis, develop innovative solutions that bring real added value to both the administration's employees and citizens.

Sustainable digitalization
In order to promote sustainable digitalization, public sector institutions must start with their own IT infrastructures. The linchpin of this approach is energy consumption in data centers. As data traffic grows globally, energy requirements are also rising steadily. According to research by the Uptime Institute, data centers were responsible for between 0.8 and 2 percent of global electricity consumption in 2018.[3] Those who obtain their resources from the cloud instead of operating their own data center benefit from the significantly more efficient capacity utilization, cooling, and energy distribution of the large cloud data centers. The result is a smaller carbon footprint. According to the Eco Association, companies can reduce their energy requirements by up to 84 percent in this way.[4]

3. The cloud in the public sector: Hurdles and challenges

For cloud solutions in the public sector to reach their full potential, it is important to define the boundaries for any projects. These are defined by a set of specifications, guidelines, and laws to which public sector organizations are obliged to adhere. The strategy for the sustainable and value-added use of technology must work within these set coordinates. To better understand the resulting framework, we look here at three essential cornerstones for a functioning cloud strategy: data protection, procurement law, and vendor independence.

3.1 Data protection: GDPR, Schrems II, Cloud Act

Data protection is a key challenge for public sector clients when using public cloud solutions. These organizations typically process a high level of personal information and must adhere to strict regulations when transferring this data in terms of so-called commissioned data processing. Accordingly, they are obliged to take responsibility for controlling all the data protection aspects of a potential cloud solution and also remain responsible for requirements throughout the entire duration of the business relationship.

If the federal, state, or municipal authorities have to assess a public cloud provider based on these criteria, then the location of the data processing as well as the location of the provider's headquarters are decisive factors. The first question that arises is where the cloud service provider's servers are located on which the data is processed. According to Art. 45 of the GDPR, organizations may only transfer personal data to a third country if it provides an equivalent level of protection. With the ruling of the European Court of Justice, which invalidated the EU-US Privacy Shield (so-called Schrems II ruling), it was made clear that these conditions are not fulfilled in the United States.[5]

58 %

of companies have adjusted their cloud strategy as a result of the Schrems II ruling.[6]

To cushion the impact of the ruling, many US service providers were discussing storing data from European customers only in the European Union. But even then, public sector institutions would be exposed to a great risk, as US authorities could obtain access to the data on the basis of the Cloud Act, provided the cloud service provider’s corporate headquarters are located in the US. Public administration should therefore concentrate on purely European providers in addition to data storage in Germany.

3.2. Tendering and award procedures: More flexibility required

With the economy and society changing at an ever-increasing pace, the long-term planning certainty for all involved will be significantly reduced in the future. Unpredictable events are becoming the exception rather than the rule. For this reason, IT managers in the public administration must also be far quicker at adapting to new needs and requirements. However, because the procurement of IT solutions is linked to strict tendering and award procedures, they quickly reach their limits when it comes to providing additional resources or new services at short notice. For example, bottlenecks can occur during unexpected surges in IT utilization.

If such load peaks are not absorbed by additional capacity, the performance of applications, networks, and databases can suffer noticeably. Ultimately, this also restricts the staff in their work, causing entire process chains to come to a standstill. To make up for their speed disadvantage when adding IT resources, ministries and public administrations can avail of cloud solutions with services that can be scaled spontaneously and flexibly. In order to set up an appropriate contract structure for this, IT managers should already set the framework for such usage scenarios during the tendering phase. This makes it possible, for example, to call up services at short notice via specially designed framework agreements. This enables IT managers to quickly ramp up capacities in demanding situations and scale them down again as needed. Lengthy tendering procedures for new servers in the company's own data center become superfluous for such scenarios. This also allows for the minimization of investment risks.

3.3. Dependence on individual suppliers due to lack of portability

Experts are constantly debating the dangers of vendor dependency in public cloud environments, also known as vendor lock-in. As a rule, it is not possible to make a blanket statement regarding the risk since the effect is directly related to the way in which the resources are used. For example, when ministries and public administrations develop and deploy their own applications in the cloud, many proprietary cloud platforms create a lock-in effect.

68 %

of CIOs are concerned about potential vendor lock-in in the public cloud.[7]

Some public cloud providers work with their own standards, which then complicates the transfer of applications and data in the event of a change of provider. In certain cases, this also applies when users want to migrate virtual machines. Therefore ministries and public administrations face the challenge of having to always take these aspects into account in their cloud strategy.

4. Solution approaches for the path to the public cloud

In order to implement cloud projects legally and securely within the specified framework, public sector clients can combine special operating models and functionalities. Coordinated constellations of dedicated resources, effective security and encryption technologies, and open standards based on open source enable ministries and public administrations to implement a wide range of application scenarios.

4.1 Virtual private cloud: Protection against unauthorized access

In order to also meet the high requirements for data protection and security in the public cloud, public sector organizations have to deploy a virtual private cloud (VPC). VPCs isolate networks within and between clients with their own IP addresses. They ensure that there is no unauthorized access to third-party resources. With this network isolation, each client gets its own range of IP addresses. VPCs can span one or several data centers (availability zones). Additional subnets can then be added to the VPC.

When setting up the VPCs, the IT staff can assign access controls via firewalls and security groups. Later, they decide which ports are used to make which resources accessible to which user groups. For example, IP-VPN can be used to set up a secure tunnel connection to their own IT resources in their data center.

4.2 Dedicated resources: Dedicated host and bare metal server

Public sector organizations can use so-called dedicated hosts for sensitive applications and workloads. In this case, the server hardware is available exclusively for one customer. The usual distribution of virtual machines for different customers is no longer necessary. In contrast to these shared hosts, this allows the user to be sure that no performance-intensive applications from third parties are operated on the hardware used, which could have a negative impact on the user's own services. The IT staff configure and run only their own virtual machines on these dedicated hosts.

For more specialized requirements, organizations can also book bare metal servers without virtualization via the public cloud in order to freely configure the hardware according to their ideas and needs. This type of server is ideal for applications that cannot be virtualized or have special licensing conditions.

4.3 Encryption: Reliable protection of data traffic

Since data security is a decisive issue for public administration bodies when choosing a cloud provider, the encryption of all data is an important factor in the decision-making process. When it comes to personal data, the GDPR requires the processor to take the appropriate technical and organizational measures to protect that data. Encryption is not only an obvious means but is also explicitly mentioned in Art. 32 of the GDPR. If personal data is transferred to the cloud, the supervisory authorities require end-to-end encryption. An appropriate level of security is provided, for example, if the cloud provider offers encryption for block and object storage based on the AES-256 standard in order to provide the data with the best possible level of protection.

4.4 Certificates: Identifying meaningful evidence

To gain a comprehensive impression of a public cloud provider's security capabilities, decision-makers and public sector IT professionals should consult a number of certificates for guidance. Since there are now a large number of certificates, it is worth taking a closer look. First of all, compliance with the C5 criteria catalog (Cloud Computing Compliance Criteria Catalogue) of the German Federal Office for Information Security (BSI) is mandatory. This formulates strict minimum requirements for secure cloud solutions and is aimed directly at professional cloud providers, their auditors, and customers. Cloud providers independently commission auditors to demonstrate their compliance with the criteria to customers.

Another indicator of a high level of security is the DIN ISO 27001. With this certificate, service providers demonstrate that they meet all the requirements for implementing, optimizing, and operating a documented information security management system. This proves to clients that there is a high level of IT security and data protection. Other meaningful cloud certifications such as ISO 27017, ISO 27018, TCDP 1.0 (Trusted Cloud Data Profile), CSA Star Level as well as the SOC reports and BSI C5 criteria catalogue have also become established as market standards. In addition, the listing as a Trusted Cloud by the Federal Ministry for Energy and Economic Affairs provides good orientation for secure cloud use in the public sector.

In addition, depending on the area that the cloud solution is being used, government agencies and authorities require additional safeguards such as the obligation to protect secrets as defined in Section 203 of the German Criminal Code (StGB). On the basis of this, a cloud provider may also process the data of professional secrecy holders, which requires special protection. Social service authorities and their service providers are also obliged to maintain social service data secrecy in accordance with Section 35 of the German Social Security Code I (SGB I) if they wish to host data in the cloud that is covered by social service data secrecy.

4.5 Open source: More options through open standards

To avoid too much dependency on individual cloud providers, public sector organizations should stick to public cloud solutions based on open source. With their open and recognized standards, these offerings ensure the greatest possible independence. Users choose different providers for their respective needs without being subjected to the product policy of a single provider. Developers also have the opportunity to participate in the further development of the software and make changes to the code independently. This achieves the maximum level of freedom.

Although popular open-source frameworks function independently of manufacturers, users can benefit from the experience of large IT companies. For example, companies such as HP, IBM, SAP, and Deutsche Telekom are participating in the OpenStack initiative. Other industry sectors, such as automotive manufacturing within Germany, are also driving the issue forward.

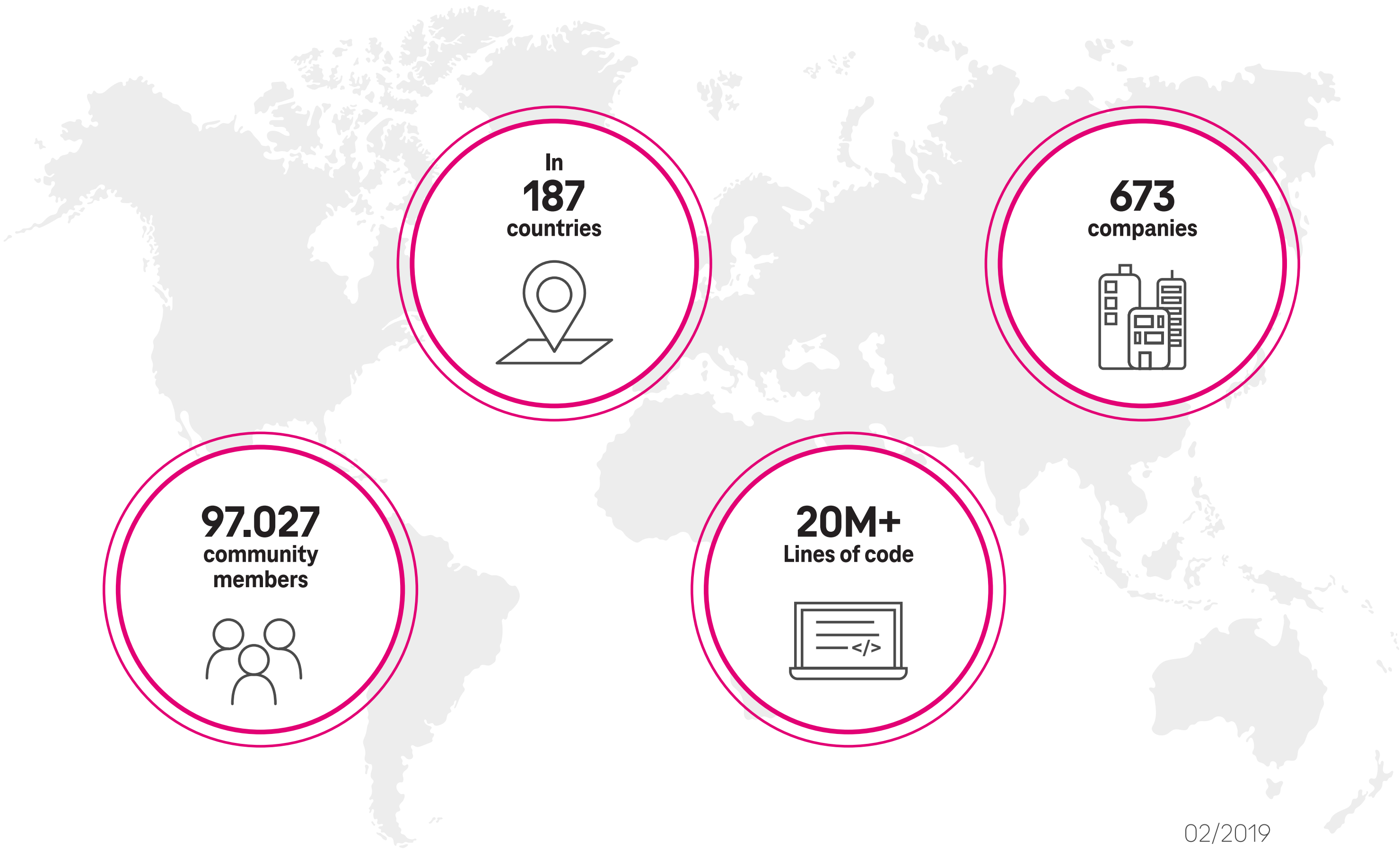


Figure: A large community is constantly driving forward the development of the OpenStack cloud operating system.

4.6 Data protection-compliant open-source solution from European data centers

The Open Telekom Cloud has repeatedly proven itself to be suitable for public sector projects. Federal, state, and municipal authorities as well as educational and research institutions rely on the solution. Telekom provides the cloud via two highly available, interconnected (twin core) data centers with locations in Magdeburg and Biere (around 25 kilometers apart). There is also the option of operating in Amsterdam with the same technical capabilities. This location is also GDPR-compliant. In addition, the coupling of all the sites is possible in order to achieve "true" geo-redundancy.

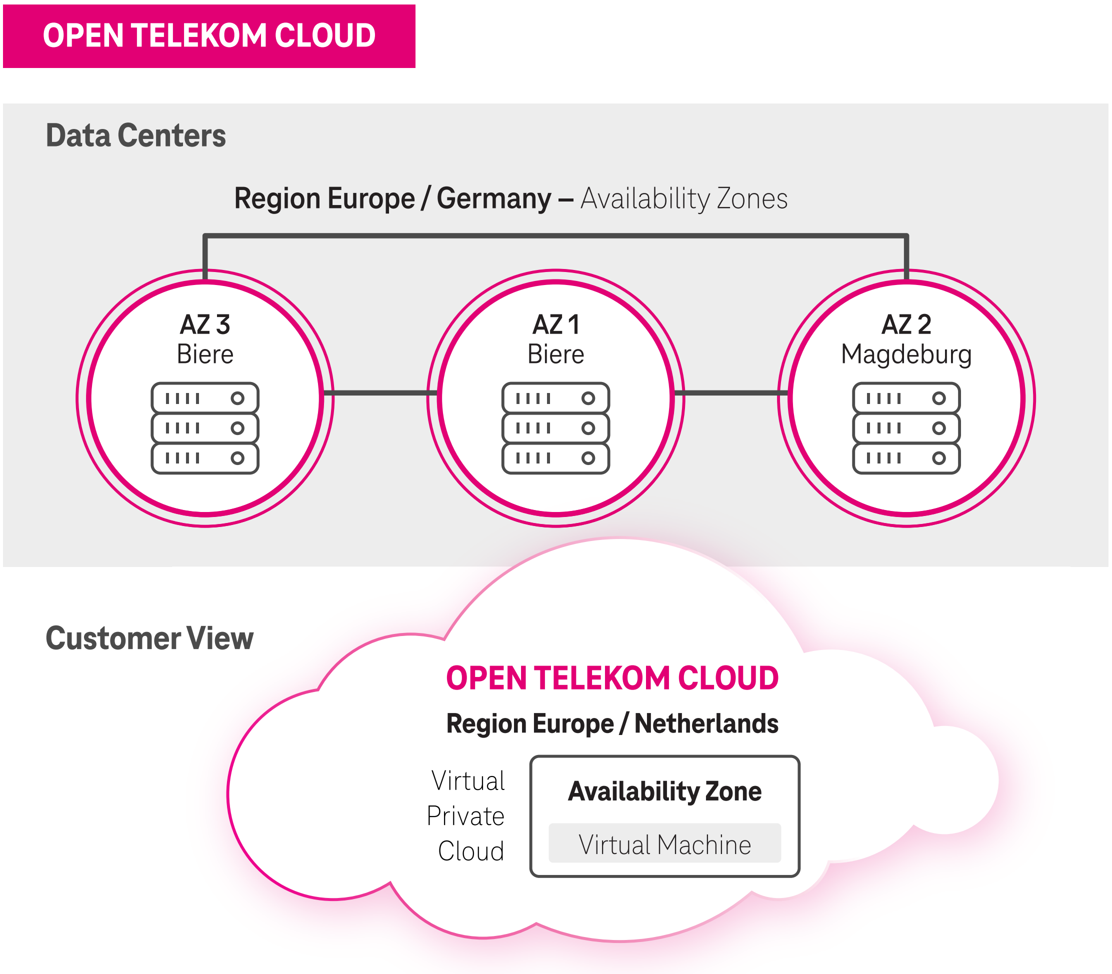


Figure: Telekom provides the cloud via two highly-available, interconnected data centers located in Magdeburg and Biere.

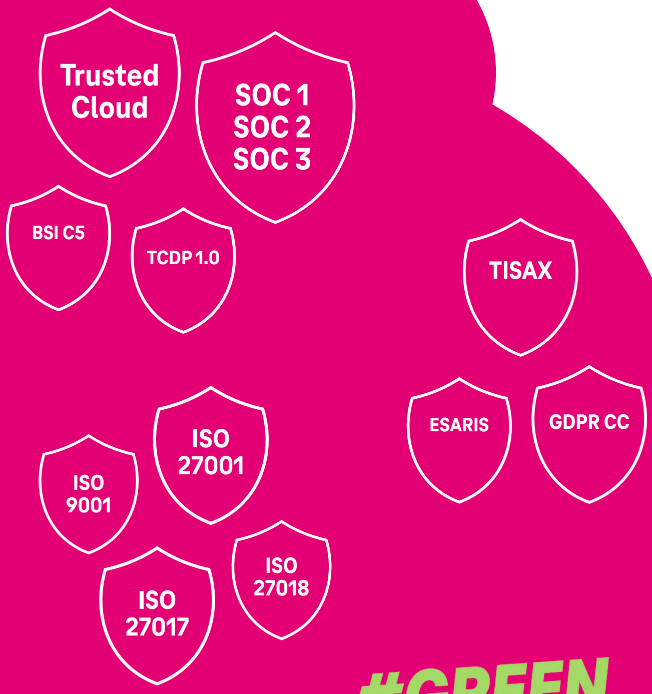
Since many IT users cannot implement pure public or private cloud scenarios, they are faced with the challenge of bringing both worlds together coherently. If companies combine both models, this can create great advantages, but at the same time it also entails certain hurdles. It is, therefore, of central importance that there are no breaks at the interfaces and that IT users can manage all the instances homogeneously. To this end, to complement the Open Telekom Cloud, the Open Telekom Cloud Hybrid was developed, which can also be used as a private cloud. The private and public variants of the Open Telekom Cloud are based on the same technology. This means that IT systems and their data can be migrated between the two models with minimal effort. The offering is also based on the OpenStack standard and, as an open-source solution, ensures maximum independence. In fact, the solution is already part of the GAIA-X initiative, which is working on a sovereign, European data infrastructure.

With the Open Telekom Cloud, public sector organizations are able to scale up server and storage capacities within minutes and also scale them down again if required. This allows organizations to flexibly expand their IT capacities when workloads increase. Users can also reschedule mass storage in various speed classes at short notice.

Due to the ownership structure of Deutsche Telekom AG, the Open Telekom Cloud is not subject to the US Cloud Act. All processes and technologies are 100 percent GDPR-compliant and designed for maximum data protection. This is evidenced by numerous verifications: It offers the common ISO certificates such as ISO 27001 and ISO 27017, specific data protection certificates such as ISO 27018 and TCDP 1.0, as well as a range of other certificates and reports including SOC 1, SOC 2, SOC 3 and BSI C5.

It is also listed by the Federal Ministry for Economic Affairs and Energy and complies with industry-specific regulations for the secure provisions for the secure processing of data from professional secrecy holders (in the sense of § 203 StGB) and social service providers (according to § 35 SGB I).
Telekom's public cloud is designed for the highest possible level of security and offers a range of features that ensure the optimum protection of infrastructures. This means that users' resources are secured against unauthorized access at all times. Clients assign individual rights and roles to their employees via a modern access management system, so that everyone can only access the application areas that are intended for them. Additional encryption and monitoring services as well as effective defense solutions guarantee a worry-free operation of the cloud.

Hybrid cloud
To take full advantage of a hybrid cloud environment, companies need to be able to move their workloads and applications easily between public and private clouds. Unified APIs and management tools that allow IT users to manage all instances across the board are one of the ways to do this. For ministries and public authorities this model is suitable, for example, for using the public cloud resources for the development and then operation of the applications in the private cloud in compliance with data protection requirements. With the appropriate contractual arrangements, public sector institutions can also easily use additional resources from the public cloud.



#GREEN MAGENTA
GREEN NETWORK.
ELECTRICAL POWER FROM 100% RENEWABLE ENERGY.

- ✓ **Made in Germany**
- ✓ **GDPR compliant**
- ✓ **Protection of professional secrets** in accordance with § 203 StGB
- ✓ **Protection of social service data secrecy** according to § 35 SGB I

5. The sustainable path to digital sovereignty for Germany

Those who want to benefit from digital solutions to a significant degree will sooner or later be faced with the question of how to make them as sustainable and future-proof as possible. For ministries and public administrations, this provides the opportunity to set an important example and to advance the public discourse around a climate-friendly digitalization. The public cloud can be an active contributor to this: When public sector institutions run their applications in the Open Telekom Cloud, they share the energy-intensive resources in the data centers with many other parties.

Due to the fact that Telekom is continuously working on an energy-efficient interaction between all the components in its data centers, it uses up to 30 percent less energy there than in comparable data centers. The electricity for the computing power comes 100 percent from renewable energy sources. In order to further improve the future carbon footprint of its infrastructures, Telekom is working with the Fraunhofer IFF on technologies for an even more efficient interplay of renewable energy generation, storage, and flexible consumer components. The long-term goal is a data center that is completely self-sufficient.

59 Mil.

CO_2

tons of CO_2 emissions per year could be saved by migrating to the public cloud.[8]

5.1 Smart city: Shaping green living spaces with the cloud

With the Open Telekom Cloud, the federal, state and local authorities are not only reducing the carbon footprint of their IT infrastructures but can also promote a more sustainable future through smart city projects. Intelligent traffic guidance systems, modern e-mobility concepts, and smart lighting solutions for public spaces are already increasing sustainability and improving the quality of life for many citizens thanks to their emissions-reducing effects. There is already a trend toward networking public spaces and this will become significantly more important in the future, thus gradually bringing to life the concept of a city's "digital twin." As a result of this dynamic, managers in public sector institutions are constantly faced with the enormous challenge of having to adapt their IT infrastructures to the requirements in each case at short notice. For this reason, demand-oriented and quickly scalable resources from the public cloud are the right choice for the implementation of smart city projects.

84 %

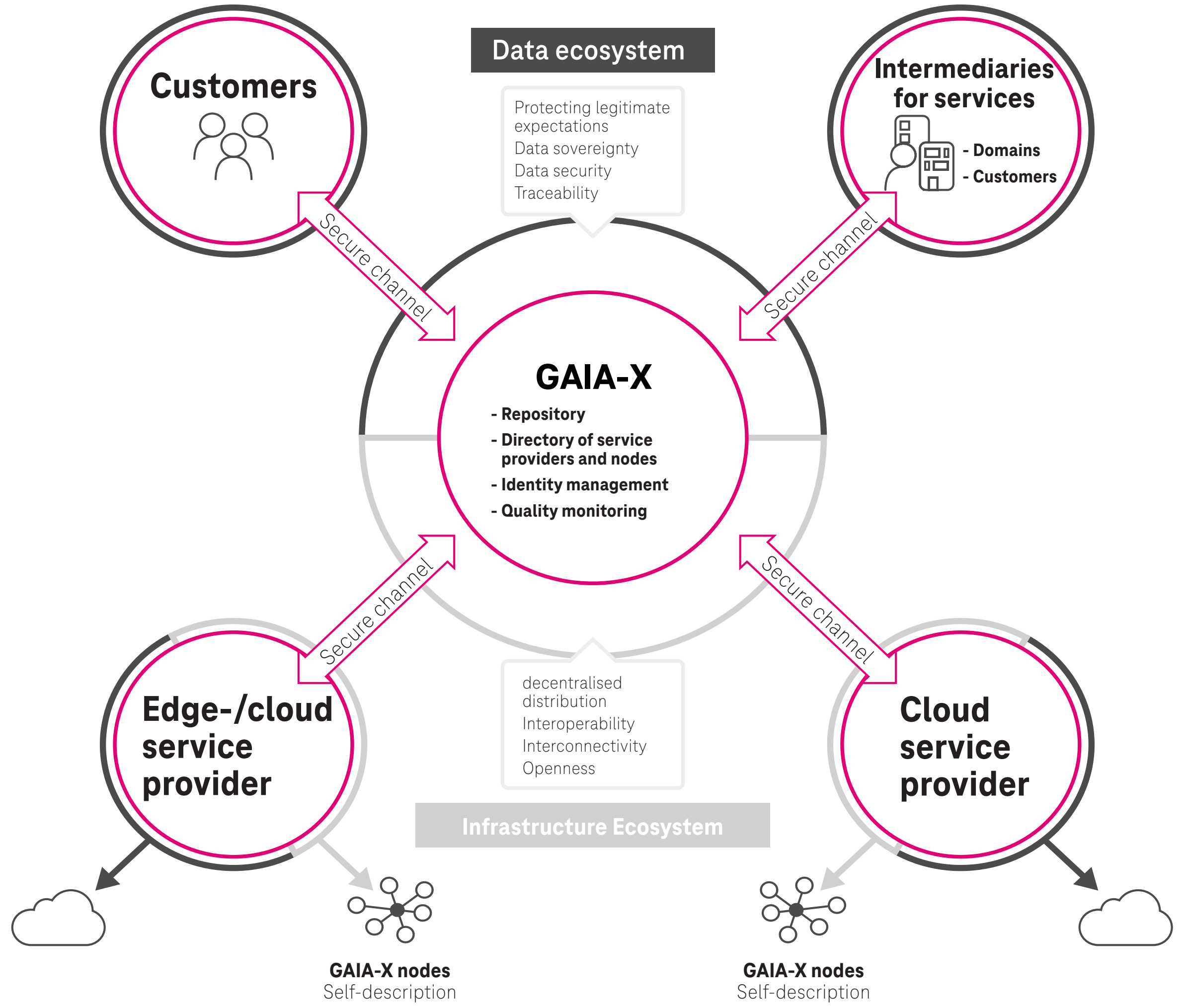
of all IoT applications are already contributing to the achievement of sustainability goals or have the potential to do so.[9]

As the intelligent networking of public spaces is largely based on the Internet of Things (IoT), the handling of this data is also a key success factor for the digital city. It's only when the planners in charge centrally collate, analyze, and evaluate all the information from the public IoT infrastructure that they can view the networking in a larger context and manage it efficiently – thus a digital twin of the city is created. To meet these requirements, users of the Open Telekom Cloud have access to an Urban Data Platform. This is where all the information about the digital city is brought together. It is only with this SaaS solution that cities and regions can make all the data available via a secure end-to-end platform – from aggregation, harmonization, and analysis to the creation of digital services for citizens. In short, the solution forms the backbone of the smart city infrastructure. Another advantage is that municipalities can record their fulfillment of sustainability targets, for example the United Nations' Sustainable Development Goals (SDG) and make them visible to the public via a dashboard. In this way, regions not only fulfill a role model function, but also make themselves more attractive.

5.2 GAIA-X: Basis for future-proof investments

For companies and public sector clients, the sustainability of a cloud solution is important not only from an environmental perspective, but also from a strategic one. Clients often need to align new IT infrastructures with many, small-scale processes and, therefore, want to benefit as much as possible from their investments in the public cloud over the long term, once the right configuration is in place. Those who do not take this aspect into account in their strategy will likely have to deal with disruptive factors such as changing business conditions, problematic dependencies, and legal ambiguities. Factors which, in the worst-case scenario, mean a short-term retender instead of a long-term planned investment – the opposite of sustainable planning.

As a founding member of the GAIA-X initiative, Telekom, with its Open Telekom Cloud, already meets all the requirements for providing a long-term, independent, and secure cloud infrastructure that is 100 percent compliant with European data protection regulations. The aim of the initiative is to strengthen the EU's digital sovereignty by creating its own data infrastructure. This is accompanied by binding standards and principles to which Deutsche Telekom actively contributes – and which already apply to the Open Telekom Cloud. Anyone who opts for the solution can, therefore, be sure that they are investing in a sustainable and future-proof infrastructure.



GAIA-X-Tasks

Creating framework conditions
- **Architecture**
- **Interfaces**
- **Data classification**
- **Processes between those involved**
- **Interoperability and interconnectivity**

Making arrangements for governance
- **Conditions of participation**
- **List of participants**
- **Rules and "data contract"**
- **Certification**

Coordinating operations
- **Necessary central services**

Figure: Operating principle of the GAIA-X initiative

Source:iBMW

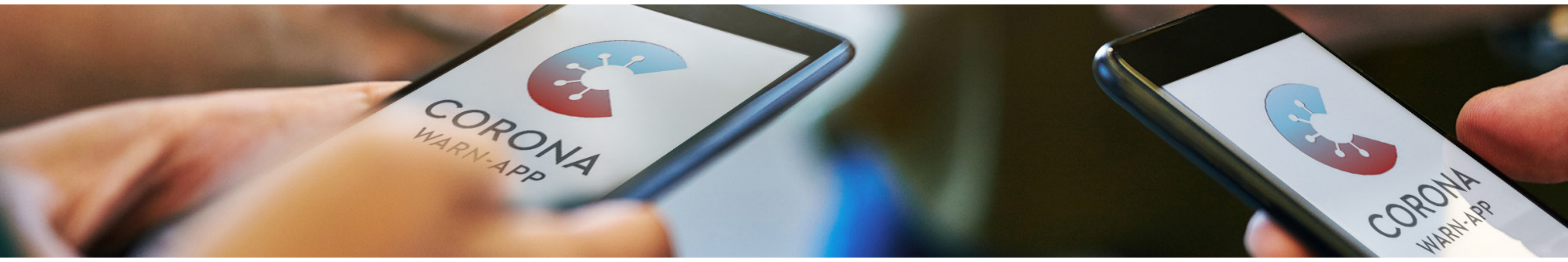
6. References: Open Telekom Cloud in practice

Once public sector institutions have defined and deployed their individual cloud set-up, the possibilities are endless. Digital administrative services, automated processes, or even the rapid provision of new applications – in practice, there's an almost infinite range of application scenarios. This is reason enough to take another look at a few selected success stories.

6.1 Corona-Warn-App for Germany and Europe

To support contact tracing in the fight against the COVID-19 pandemic, the German Federal Ministry of Health commissioned the Corona-Warn-App last year. T-Systems worked with SAP and various institutions and working groups to develop a GDPR-compliant solution. The protection of personal data and compliance with the GDPR were top priorities for both the Federal Ministry of Health as the client and the Robert Koch Institute as the operator of the Corona-Warn-App.

The rest of the catalog of requirements was also demanding. The most important specifications were that the technology used had to be based on open standards, the data centers had to be in Germany, and they had to have important security certifications. As a result, the Open Telekom Cloud, the public cloud solution from app development partner Telekom, was the obvious choice for the technical infrastructure. Provided from highly secure data centers in Magdeburg and Biere, the Open Telekom Cloud is based on the open standard OpenStack. It also meets the German Federal Office for Information Security (BSI)'s C5 catalog of requirements, which certifies that cloud providers offer the highest level of security.



6.2 Coronavirus emergency aid Bavaria

The Bavarian Ministry of Economic Affairs implemented a special online application solution to make it easier and faster for the self-employed, farmers, and companies to apply for coronavirus emergency aid. It replaces the previous application process that used PDF documents, some of which were filled out by hand, scanned, and sent to the application offices by e-mail. With the new online form, all the data is available digitally from the start of the application process and flows into the public administration's review and approval process.

The Bavarian Ministry of Economic Affairs developed the application and process platform for coronavirus emergency aid together with Pegasystems and was able to complete it in just five days together with T-Systems. It runs on Pegasystems' highly configurable low-code platform and is operated by T-Systems on a secure, highly available, and scalable infrastructure in its own data centers in Germany. The new online process is already being used extremely actively by Bavarian businesses. Shortly after it went live, more than 108,500 of them submitted applications for emergency assistance. In accordance with Germany's so-called Kiel resolutions, the solution can also be made available for use in other German states, municipalities, and the federal government – in a sense, serving as a blueprint for the specific requirements, administrative processes, and infrastructures of the respective bodies.

6.3 Digital citizen card: Digital administrative services from the cloud.

For a German municipality, T-Systems implemented and operated a digital citizen card with extensive administrative services (library services, news and events, free public transport). The solution, which processes personal data among other things, is operated in the Open Telekom Cloud.

The various services of the cloud-native architecture (microservice architecture) are implemented as Docker containers running in a highly available target environment in the Open Telekom Cloud. A container orchestration is used to manage the containers. Further cloud services from the Open Telekom Cloud such as server infrastructure, load balancing, anti-DDoS, and database services are integrated into the system.

DevOps-as-a-Service running on the Open Telekom Cloud was used for development, executing an end-to-end CI/CD process with integrated and automated tests and security checks. On this basis, it was possible to implement the essential DevOps principles such as fast delivery, high quality, and traceability.

6.4 Mundi Web Services: Scalable computing power for sophisticated analyses

With the Copernicus program, the European Space Agency (ESA) is fulfilling the European Union's mandate to observe the Earth from space. To this end, a series of Sentinel Earth Observation satellites transmit around 20 terabytes of images back to Earth every day. Meanwhile, the available satellites have provided several hundred petabytes of data to users inside and outside the EU, providing new views of the environment and climate change. This data is made available in a cloud-based manner via Mundi Web Services. The goal of this is to promote new geo-based business models.

Mundi Web Services is a platform that allows users to directly use preconfigured geoservices. But it also offers new geoservice providers the option of offering their services on the market. The great strength of Mundi Web Services? All the components required to put new geo-based business ideas into action are already integrated. These include constantly updated data from the Sentinel satellites as well as historical data from the US Landsat program, geoservice applications, and flexibly deployable IT resources from the Open Telekom Cloud. Since the computing capacity for the evaluations and the data are on the same technical platform, lengthy copying processes are eliminated. In addition, Mundi allows the specific selection of data relevant for the respective analysis.

With the Open Telekom Cloud, Mundi has the right infrastructure foundation: The resources from the cloud are optimal for temporary high-load calculations and adapt to the user's requirements. If they want faster results, they can speed up the evaluation with additional capacity. Depending on the speed – the following always applies: Costs are only incurred for resources actually used.

Which project can we support you with?

Do you want to add powerful resources to your IT infrastructure or provide your own applications and services via the cloud without having to make significant investments in hardware? Then please get in touch with us. We will develop tried-and-tested solutions based on the Open Telekom Cloud for your individual application scenario. Thanks to our extensive experience with projects in the public sector, we know its needs and hurdles first-hand. For this reason, data protection, IT security, and compliance are top priorities for us. With the Open Telekom Cloud, you can implement your digitalization projects on a state-of-the-art infrastructure that is operated exclusively in European data centers.

We can answer your questions about test options, booking, and use – free of charge and individually. We are there for you 24 hours a day, 7 days a week.

Get in contact today!
+800 33 04477

References

1 PwC: Upskilling hopes and fears 2021

2 DAK: Digitalisierung und Homeoffice in der Corona-Pandemie

3 Uptime Institute: Renewable energy for data centers

4 Eco-Studie: Rechenzentren sind Garant für nachhaltige Digitalisierung in Europa

5 EuGH: Rechtssache C-311/18

6 KPMG/Bitkom: Cloud Monitor 2021

7 The Flexera 2020 CIO Priorities Report

8 IDC: Cloud Computing Could Eliminate a Billion Metric Tons of CO_2 Emission Over the Next Four Years

9 WEF: Internet of Things Guidelines for Sustainability

Contact:
open-telekom-cloud.com/en/contact

Internet:
open-telekom-cloud.com/en

Publisher:
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany