euritas
European Association of Public IT Service Providers

WE MAKE **IT** POSSIBLE. **TOGETHER.**

EURITAS POSITION PAPER:

FOUNDATIONS OF CLOUD SERVICES FOR PUBLIC ADMINISTRATIONS

Version 2.0

TABLE OF CONTENTS

Management Summary

The key takeaways from the document are:

- **Cloud offers great advantages for public administrations; however, applications, infrastructure and processes need to be adapted to this technology. The public IT service providers are supporting administrations in these challenges.**

- **Euritas proposes a network of cloud infrastructures for public administrations in Europe, built and maintained by the public IT service providers, who can ensure the secure and confidential handling of data moving through it. Correspondingly standards for interoperability and a framework for cooperation of public IT service providers have to be agreed between member states.**

- **Cloud services provided to the public administration need to adhere to a set of minimum requirements to guarantee the privacy of European citizen's data. These requirements should be codified in common European standards. Lock-in effects have to be prevented by reducing the dependency from single providers. The "high assurance" level of the ENISA's Cloud Certification scheme should exclude any transfer of data outside of the EU jurisdiction.**

Introduction

Euritas, as the voice of public IT service providers, supports the European Commission's efforts to digitally transform the European Union by 2030 (see Commission communication "2030 Digital compass: the European way for the Digital Decade", March 8, 2021).

Based on the prerequisite of digital sovereignty, which was described in detail in the position paper Digital Sovereignty, Euritas now addresses the topic of sovereign cloud solutions in particular in this position paper.

Cloud computing is an area that public administrations cannot and should not ignore, since it offers great potential for efficient digital processes and convenient services for citizens (Accenture Research, 2021). Therefore, from Euritas' point of view, it is of utmost importance to identify the necessary framework conditions and requirements that need to be put in place for public entities to use these services securely, sovereign and in compliance with all data protection requirements.

As a basis for its position paper, Euritas has examined national as well as EU cloud strategy documents and derived from them structures of cloud environments and essential provisions.

For the purpose of this paper cloud technology is understood as shared computing and storage resources, which can be rapidly scaled depending on the user's demand. Depending on specific use cases different service models and delivery models can be chosen.
Service models include Infrastructure as a Service (IaaS), where only server and network capacities are provided, Platform as a Service, which also includes underlying software on which users can run their applications, and Software as a Services, where users directly access applications from the cloud.

In terms of delivery models, the following can be considered: A Private Cloud can only be accessed by a single organisation and is often run in the organisations own data centre. In contrast, Public Clouds are run by a provider, who gives public access to its resources separating the user's environments only virtually. Hybrid clouds are a mix of the two, where an organisation has a private cloud, which is also connected to a public cloud, e.g. for load balancing when additional resources are needed quickly. Another variation is a Community Cloud, which works similarly to a Public Cloud, but can only be accessed by a fixed group of organisations or persons.

Especially larger organisations often use more than one cloud with different delivery models, which is summarized under the term Multi Cloud.

1. Shift into the cloud

Cloud technology offers substantial advantages in terms of efficiency and scalability. More and more organisations move capacities for storage and computing into cloud environments, since it allows them to streamline their own IT infrastructure and become more agile in developing new services. It also gives them the potential to scale up quickly and cost-effectively, when more IT resources are needed.

All examined strategy documents put emphasis on harnessing these advantages for future IT projects in the public administration. For example, cloud solutions are to be preferred over other solutions, when they are the most cost-effective option and as long as they fulfil certain requirements toward security and data protection.
In some documents, it is also suggested that new applications – developed in-house or external – should first and foremost be built for deployment in the cloud.

Euritas Position:
In the view of Euritas, cloud computing offers great opportunities for services of general interest in Europe. Administrations often work with large amounts of data. To offer convenient services to citizens and businesses, they need to make these data exchangeable between different departments of administrations. To fully realise the Once-Only-Principle, government agencies need to exchange data points and certifications, so that citizens do not have to input their data again and again, when interacting with different agencies. Being able to connect data points from different branches, also enables public administrations to develop new innovative services.

Cloud technology offers the basis for this by providing great agility in the modification of applications and processes. By being able to quickly move applications to new resources, also offers organisations higher resilience and strengthens the availability of their services. Last but not least the cost-efficiency of cloud technology is also an important factor. However, the use of cloud services can only be cost-effective, if the use of resources is actively managed. Public administrations need the awareness to continuously adapt the capacities they pay for to what is currently needed.

Public administrations have already begun using these advantages, while more and more processes are being transferred into the cloud (Deloitte, 2022). However, it should be kept in mind that building services on cloud platforms requires a different approach than providing other IT infrastructure. To fully harness the potential of the technology, applications have to be developed for the deployment in so called containers, which include not only the application itself, but also all the underlying software, necessary to run it. Containers can quickly be deployed in different cloud environments with little integration effort. Only then can public administrations really benefit from the agility and large scale of the cloud and

make their services for people and businesses more resilient. The public IT service providers in Euritas are supporting them with their competencies and experience on the way to a fully digitalised administration in the cloud.

Cloud offers great advantages for public administrations; however, applications, infrastructure and processes need to be adapted to this technology. The public ICT service providers are supporting administrations in these challenges.

2. Necessity for multiple cloud resources

For complex organisations, like public administrations, it is often more practical to have not just one public or private cloud. Instead, a mix of cloud models is used. The examined strategies reflect that. Most envision a multi cloud model with a mix of selfhosted capacities and external services as well as hybrid clouds. Which type of computing or storage resource is supposed to be used, depends on specific use cases. Therefore, the documents require the relevant administration bodies to conduct an assessment before deciding on a particular solution. The most important factor to consider is the type of applications used and especially the type of data, which will be processed. This aspect is discussed in detail in the next chapter.

Member states and also the European Union have pushed for stronger cooperation in the area of cloud technology, but the analysed strategy documents make no reference to these initiatives. However, a combined effort is needed to build cloud services and capacities for the requirements of public administrations in Europe.

Euritas Position:
Euritas endorses the principle of providing different cloud resources to public sector entities and enable them to choose the right solution for their use cases. At the same time, they are also able to quickly add more capacity, when workloads rise suddenly.

Having public cloud capacities available can also significantly increase the resilience of public administrations as data and workloads can be shifted to other servers, e.g. in case of natural disasters or large scale cyberattacks. However, the public administrations in Europe need to have a common position and a set of standards in regards to the use of large hyperscaler's services to gain the leverage necessary to assert compliance with the GDPR.

As an alternative model Euritas proposes a network of cloud infrastructures shared between public administrations in Europe. Such a network would allow for fast exchanges of

capacities in situations that force the shift of applications or data, while maintaining a high level of security and trust between the involved partners and insuring the digital sovereignty of public administrations at all times. The public IT service providers in the ownership of EU member states' governments are in a unique position to host such a network, as they run highly secure data centers and can build on the trust between the member states, to ensure that no data leave the European Union. Even in the event that personal data or certain sensitive data would have to be moved from a private cloud server of one member state to another node, a high level of security, encryption technology and trust between public ICT service providers can ensure that these data stay safe and confidential. To underpin such a network the European member states should agree to a set of standards for interoperability of digital public services and a framework, which enables such a cooperation between public IT service providers.

Euritas proposes a network of cloud infrastructures for public administrations in Europe, built and maintained by the public ICT service providers, who can ensure the secure and confidential handling of data moving through it. Correspondingly standards for interoperability and a framework for cooperation of public ICT service providers have to be agreed between member states.

3. Conditions for the use of public cloud services

Which type of cloud services can be used depends largely on the type of data that are supposed to be uploaded according to the analysed strategies. While the risks for data without any reference to personal data and without any security classification is minimal, especially personal data of citizens must be handled with a high level of security and privacy protection.

However, even after this assessment has been made and a strictly private cloud is not deemed necessary, there are still aspects to be considered in the procurement process of cloud services. Although some aspects differ in the documents, all put emphasis on complying with relevant regulations, especially with the General Data Protection Regulation (GDPR) and other privacy laws.

Euritas Position:
Euritas as well sees compliance with the GDPR as crucial requirement that must be met by providers of public cloud services to the public administration. This includes that those providers in their role as processors must support the controller in all necessary ways to help them comply with all provisions of the GDPR.

Furthermore, personal data cannot be transferred to third countries without the controller's knowledge and the data subject's consent. If no adequacy decision by the European Commission exists for that third country, no personal data should be transferred at all.

Additionally, any economic or technical dependencies from cloud providers must be avoided to secure the sovereignty of public administrations. Such lock-in effects must be prevented by the possibility to quickly migrate data and workloads to other services if necessary. This requires a certain level of interoperability between the different providers.

Since government data and often citizens data are involved, cloud providers must adhere to internationally recognised cyber security standards. The European Union Agency for Cybersecurity is developing a cybersecurity certification scheme for cloud services, which in the view of Euritas, should become a central pillar in this area after its release. Therefore, Euritas calls for the exclusion of access to as well as the transfer of any data outside the European Union on the assurance level "high" of the certification scheme currently discussed.

The NIS2 directive (EU 2022/2555) clearly states that the organisations using a cloud provider service have the responsibility to ensure that the provider adheres to the NIS2-requirements, covering much of the above mentioned.

Further, the NIS2 directive implements a number of additional requirements concerning risk management, security, documentation, reporting on incidents and the specific need for an exit strategy, in the form of an actual plan for moving systems and data, in case the cloud provider becomes unavailable or non-compliant.

Euritas suggests that these requirements should also be reflected in the planned "EU cloud rule book", which is currently being developed as a workstream of the European Alliance on Industrial Data, Edge and Cloud launched by the European Commission.

Cloud services provided to the public administration need to adhere to a set of minimum requirements to guarantee the privacy of European citizen's data. These requirements should be codified in common European standards. Lock-in effects have to be prevented by reducing the dependency from single providers. The "high assurance" level of the ENISA's Cloud Certification scheme should excluded any transfer of data outside of the EU jurisdiction.

EURITAS Head Office Vienna
M: euritas@brz.gv.at
Web: www.euritas.eu
Linkedin: https://www.linkedin.com/company/euritas