

## DESCRIPTION OF THE AVAILABLE CLOUD-BASED DATA STORAGE NETWORK SOLUTIONS

Regarding question 15) “description of the available solutions for cloud-based data storage and management”, an overview of the cloud storage and data sharing models that can be implemented is provided below, in order to provide a complete picture of the operational possibilities.

For EUCA, a hybrid cloud architecture is planned, with: primary storage and critical services hosted on a private cloud infrastructure/localized in data centres located exclusively within the European Union, with ISO/IEC 27001 certifications and, where applicable, EN 50600; potential use of IaaS/PaaS services from public cloud providers only in 'EU-only' mode, with data residency guaranteed in EU regions and encryption keys managed in HSMs located within the EU; prohibition of unnecessary transfers of personal or sensitive data to third countries, in compliance with the GDPR and European jurisprudence on international data transfers.

Cloud-based data storage network solutions are already used by the Agency, including through its State technology partner, for document sharing and secure data storage. Currently, the most widely used platform is the *Microsoft 365* ecosystem, which guarantees that archived data is stored exclusively within the European Union, in accordance with Regulation (EU) 2016/679 (GDPR).

For EUCA, these tools will be configured with a dedicated tenant, specific data retention and protection policies, and integration with the encryption and key management systems described in the response to question 23.

From a more general perspective, the cloud storage and data sharing models that could be implemented are as follows: public cloud, private cloud, hybrid cloud and multi-cloud. The public cloud, offered by global providers such as *Amazon Web Services (AWS)*, *Microsoft Azure* and *Google Cloud Platform (GCP)*, allows data to be stored on shared infrastructure, ensuring high scalability and variable costs according to a *pay-as-you-go* model. AWS, for example, offers Amazon S3, an object storage service with versioning, encryption and integration with advanced analytics tools. Azure offers Blob Storage, ideal for unstructured data, while Google Cloud offers Cloud Storage, with different classes (*Standard, Nearline, Coldline*) to optimise costs and performance.

The private cloud is suitable for contexts that require maximum security and control, such as regulated sectors. Solutions such as *IBM Storage Scale System* and *Oracle Cloud Infrastructure* allow you to implement dedicated architectures, with support for data-intensive workloads and integration with on-premises environments. The Customs and Monopolies Agency, for example, already operates in this way for tax data on an infrastructure managed by its state technology partner.

The hybrid cloud, combining public and private resources, is now the preferred choice for ensuring flexibility and regulatory compliance, facilitating the gradual migration of

workloads. In this context, platforms such as *Azure Arc* and *AWS Outposts* allow cloud services to be extended to local data centres, ensuring centralised governance.

Finally, the multi-cloud approach allows data to be distributed across multiple providers, reducing the risk of vendor lock-in and improving resilience. All these solutions integrate end-to-end encryption, geographic replication, disaster recovery and advanced monitoring capabilities, in accordance with Regulation (EU) 2016/679 (GDPR) and international security standards such as ISO/IEC 27001 and CSA STAR. The adoption of these technologies is a strategic factor in the modernisation of processes and the protection of sensitive data in the public administration.