

**Digital Government:**  
How the EU cannot miss  
the cloud opportunity

NOVEMBER 2021



# Cloud Computing should be a key technology for a successful post-pandemic recovery across the European Union

From the immense strain on the public healthcare systems to the impossibility of delivering primary public services in-person, COVID-19 left most public services stranded and at the mercy of citizens' distrust. Governments everywhere felt the hit of the pandemic and the urgency to respond appropriately.

Now, with post-pandemic times at bay, **long-term strategic investment on digital transformation is a way to ensure economies emerge stronger, more resilient and prepared for what's coming next.**

In fact, digital is part of the vision of the European, which claimed for a fair, green and digital recovery in the aftermath of the pandemic.

In this critical moment, digital modernization and connectivity in the public sector play a decisive role, and **Cloud computing is a key enabler in this digital agenda.**

This is the reason why we have conducted a research to help Governments and public officials in understanding the benefits of Cloud and the key steps to take in the transition.

Today, Migrating to Cloud **carries benefits that go well beyond effective data storage.** In fact, Cloud Computing has the potential to be the bridge across and between an ecosystem of diverse technologies, binding together different capabilities and tools in an accessible manner. Thus, Cloud-enabled transformation has earned its place as an established **high-potential accelerator of digital modernization for Governments and other Public Services.**

At Deloitte, we hold the experience and expertise to lead and deliver this kind of transformation in Governments and other public institutions globally. On top of that, we are committed to be a crucial player in the digital revolution of the European Union on the verge of facing.

**Debbie Sills**

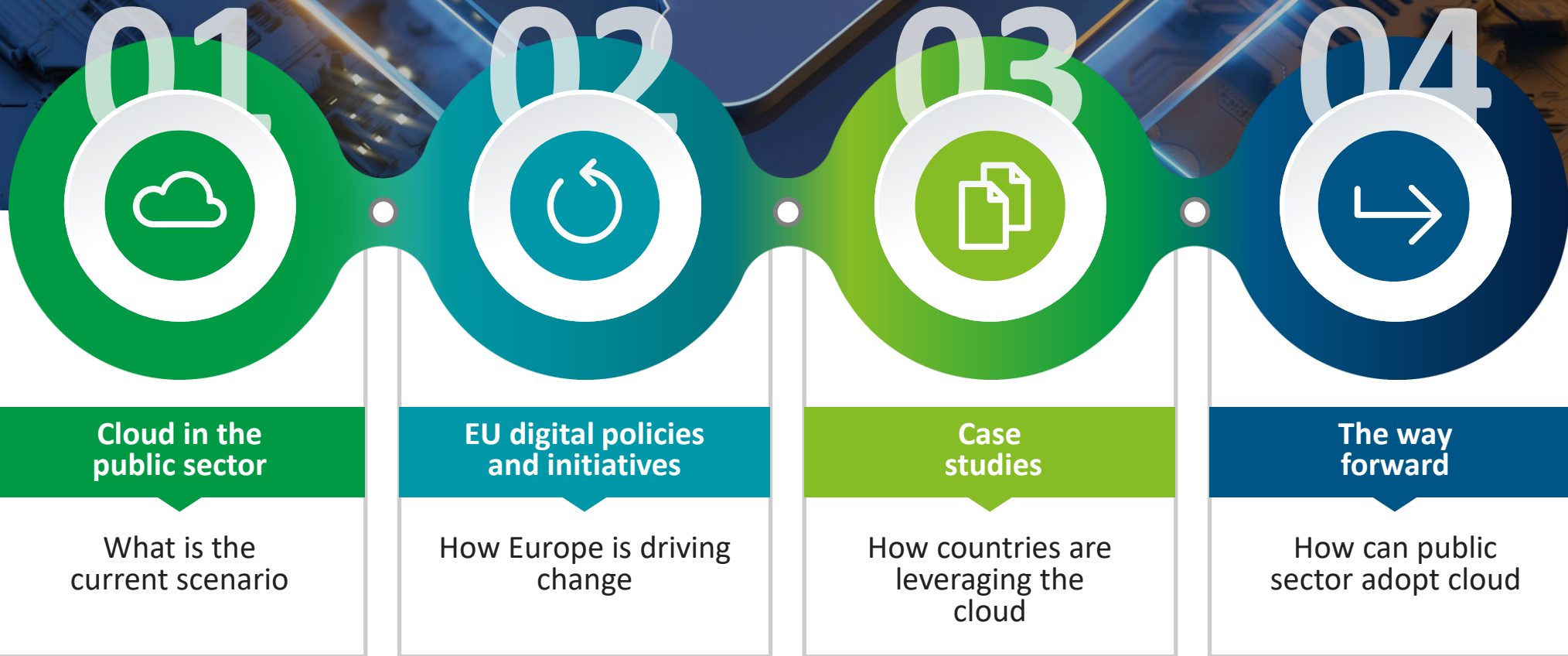
*Global Public Sector Consulting Leader*

**Jean Barroca**

*Global Public Sector Digital Modernization Leader*



# TABLE OF Contents



01



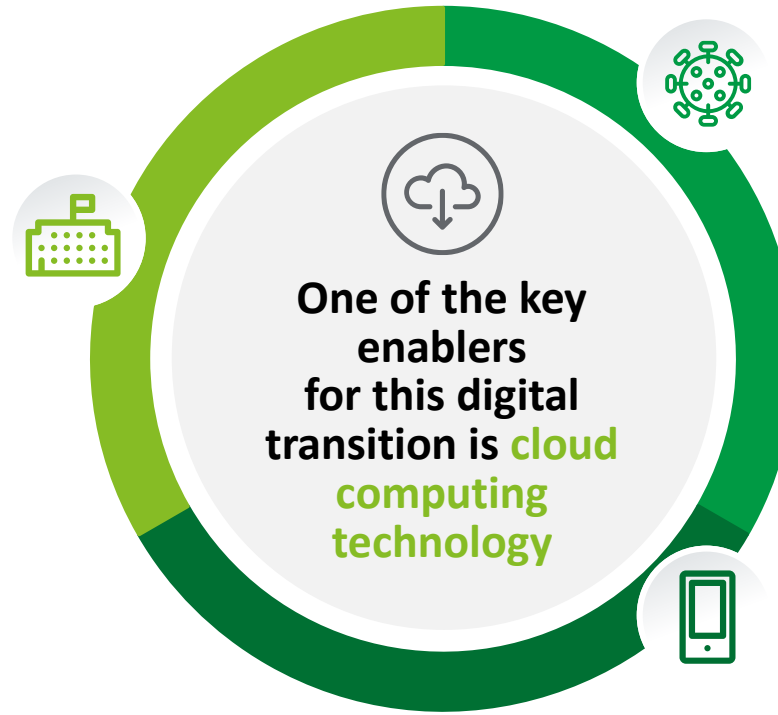
# Cloud in the public sector

What is the current scenario

# Digital transformation in the public sector

Across the globe, the public sector is implementing digital transformation projects and initiatives for many reasons

Governments aim to **adapt to the rapid changes** in digital usage and consumption patterns, and to **improve** their 'e-government' efforts, at the same time **promoting savings in cost** and time.



The **COVID-19** crisis has brought about years of change in the way the **Public Sector performs**.

**People** and **businesses** are consuming **more digital content** and becoming increasingly **reliant on digital sources** for information and services.



# Cloud computing

Cloud computing enables digital transformation projects and offers the scale and speed that are needed for the public sector to focus on this transformation.

Cloud computing is a model for ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or Cloud Services Provider (CSP) interaction.



## ELASTIC

Adjusted to needs, so that data storage and other resources aren't wasted.

01



## SHARED

Delivered by a common pool of **technology resources**.

02



## METERED

Users pay as they go and only for what they use. This **optimises infrastructure while keeping costs low**.

03



## SECURE

**Data is protected and backed up** so nothing is lost.

04



## AGILE

**'Out of the box'** solutions that help faster innovation and the development of new products and services.

05

# Cloud computing: What does it mean



There are different cloud deployment and service models, which provide differing levels of control, flexibility and management, and define who has access and where the servers are located.



## DEPLOYMENT MODELS

### PUBLIC CLOUD

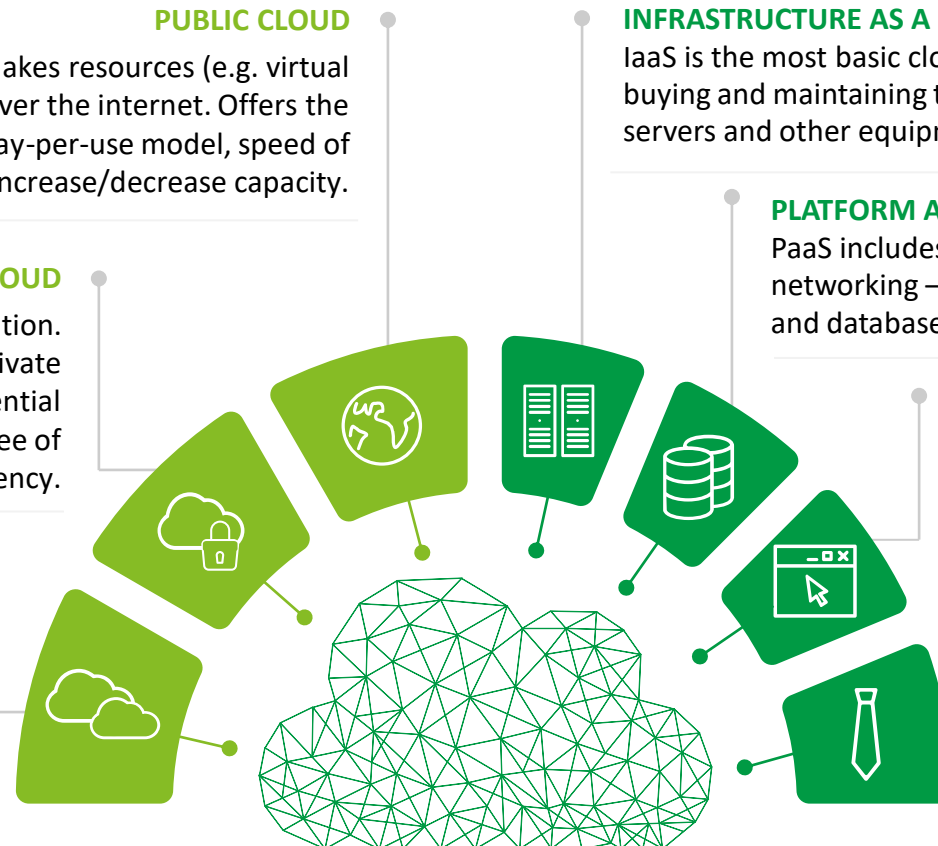
Hosted by the CSP, where the provider makes resources (e.g. virtual machines, applications, data storage) available over the internet. Offers the ability to consume IT and related services on a pay-per-use model, speed of access to resources, and the flexibility to increase/decrease capacity.

### PRIVATE CLOUD

A private cloud is dedicated to a single organisation. Serving as the organisation's data centre, a private cloud is suitable for processing confidential information that requires a very high degree of security and very low latency.

### HYBRID CLOUD

Hybrid cloud is a mix of on-premises private cloud and third-party public cloud that work together. It allows partitioned use so that sensitive data can be kept secure while shared data is easily accessible.



## SERVICE MODELS

### INFRASTRUCTURE AS A SERVICE

IaaS is the most basic cloud service model: Instead of buying and maintaining their own infrastructure (e.g. servers and other equipment) organisations use a CSP.

### PLATFORM AS A SERVICE

PaaS includes infrastructure – servers, data storage and networking – but also middleware, development tools, and database management systems.

### SOFTWARE AS A SERVICE

With an SaaS model software applications are hosted by the CSP and consumed by customers on a 'pay-as-you-go' basis.

### BUSINESS PROCESS AS A SERVICE

Use of cloud tools to outsource processes like payroll or supply chain planning to specialist vendor or advisor teams.

# Benefits of cloud migration in the public sector

Cloud computing can be a connective tissue that brings together several technology capabilities and tools in an easy-to-consume way.

## FLEXIBILITY

The cloud facilitates flexible and immediate use of resources, allowing the public sector to have the flexibility to use demand-oriented services, achieve better technological and analytical capabilities, and adopt advanced technologies [e.g. artificial intelligence (AI), virtual reality].

## EFFICIENCY

Using the cloud reduces the need for procurement, installation, configuration and maintenance of hardware and software, and improves efficiency, particularly reflected in the time it takes to process transactions with citizens and data in general.

## RESILIENCE

The cloud improves government resilience by providing protection against business disruption caused by a natural disaster or other adverse event. Also, the cloud increases resilience against cybersecurity threats, due its stronger protections.

## COST-EFFECTIVENESS

The need to invest in IT infrastructure is reduced: IT resources are used on an as-needed and temporary basis, reducing technology costs.

01

02

03

04

## AGILITY & SCALABILITY

Cloud resources are available at any time and to any extent, allowing spikes in demand to be handled without service interruptions, as the provision of IT support is scaled up as required (e.g. in periods for filing online tax returns just before a deadline).

## SUSTAINABILITY

There is a contribution to a sustainable public sector IT infrastructure by using service providers with low- or zero-emission data centres.

## CUSTOMER EXPERIENCE & SKILLS DEVELOPMENT

Cloud adoption improves customer experience, shortening response times, speeding up product development, generating deeper insights, powering dynamic decision-making, and allowing the effective and efficient engagement. Also, cloud helps facilitate human resource development in the public sector, as all technology professionals must keep up to date with developments in IT.

05

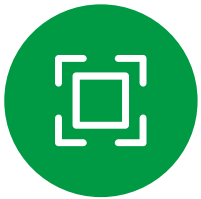
06

07



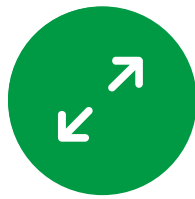
# Cloud innovation is not really about “the Cloud”

It's about turning the status quo of today into market-leading business innovations for tomorrow



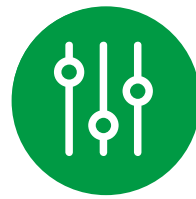
## APPLICATION HOSTING AND INFRASTRUCTURE

*Driving cheaper and  
faster delivery and ops*



## PRODUCT DEVELOPMENT AND CAPABILITIES

*Building market relevant  
products quickly*



## INNOVATIVE SERVICES AND ACCELERATORS

*Leveraging differentiated  
capabilities*



## NEW BUSINESS SERVICES AND MODELS

*Altogether new revenue  
and business models*



## ECO-SYSTEM PLAYS AND FORCE MULTIPLIERS

*Shared economy,  
utilities and alliances*

# Migration to the cloud: Challenges in the public sector

Cloud computing is now more than a decade old, but the adoption rate in the public sector still does not follow the pace of other industries. Governments have invested heavily in on-premises data centres as well as their operation and maintenance.



Cloud Service Providers have been responding to the specific **challenges** and **resistances** raised by Public Sector clients.



## POLICY & REGULATION ISSUES

▶ The cloud offers a secure way to house applications and their associated data and provides a transformation path that governments can accelerate and control.

Some actions can be taken to **ensure data sovereignty and privacy**: robust authentication and access controls; encryption technologies and advanced key management; and adoption of hybrid cloud models.



## TALENT ISSUES

▶ Existing staff may not be ready for migration to a new system, particularly in terms of their knowledge (capabilities and skills).

There may possibly be a need to **reorganise headcount, and/or retrain staff to use the new systems**. However, some agencies may consider that it is too expensive to retrain staff.



## STRUCTURAL ISSUES

▶ Policies may need to be **overhauled in order to move to cloud computing**. Some of these actions may require time and possibly legislative changes to be put in place: they include redesigning database systems, instituting technical interoperability policies, and developing cloud governance mechanisms.

**Leaders must understand the full capabilities of the cloud.**



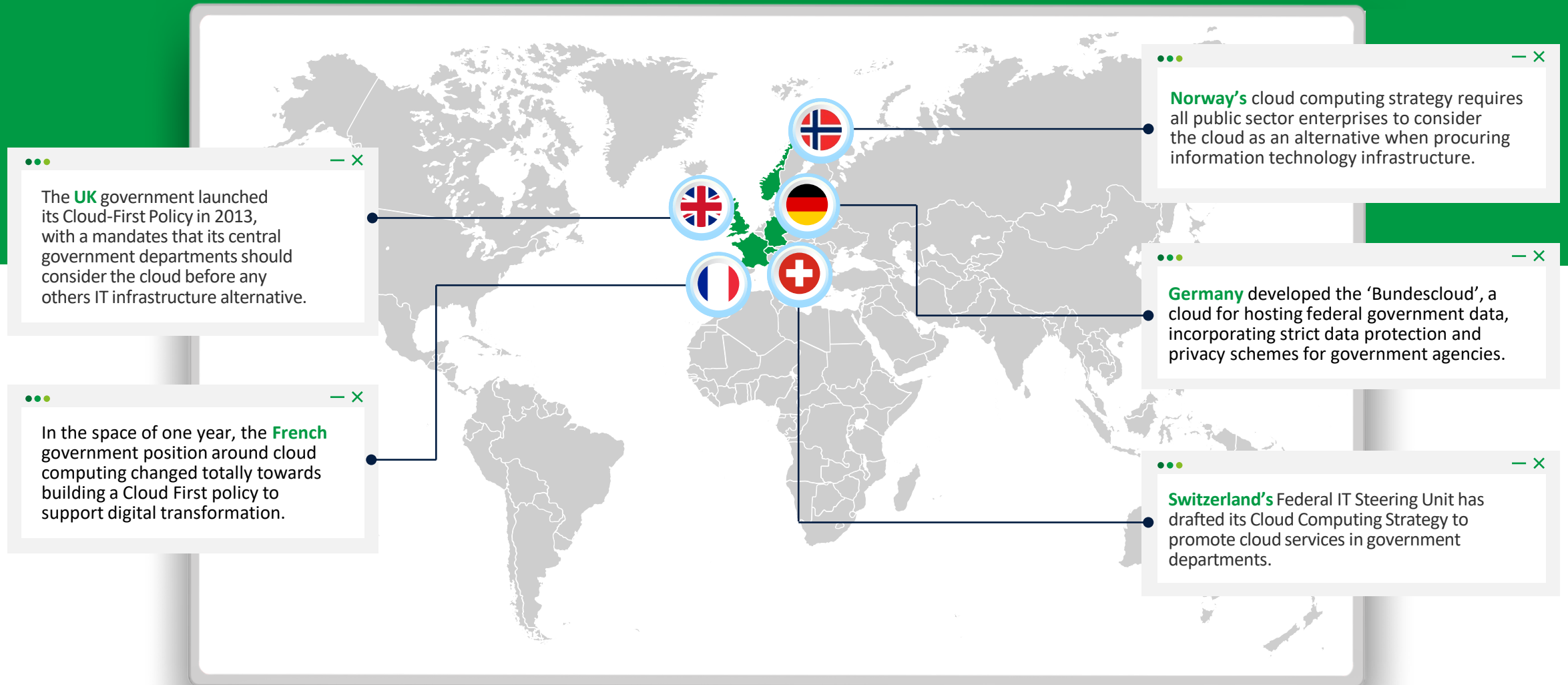
## PROCUREMENT (& OTHERS) ISSUES

▶ Some agencies are **locked in to an existing contract and face constraints in searching for an appropriate vendor**. Existing infrastructure investment may not yet have reached its financial accounting 'end of life', due to amortisation. Also, some agencies consider that the cloud is too expensive.

It is crucial to adjust **public sector procurement policies**.

# Cloud adoption in the public sector

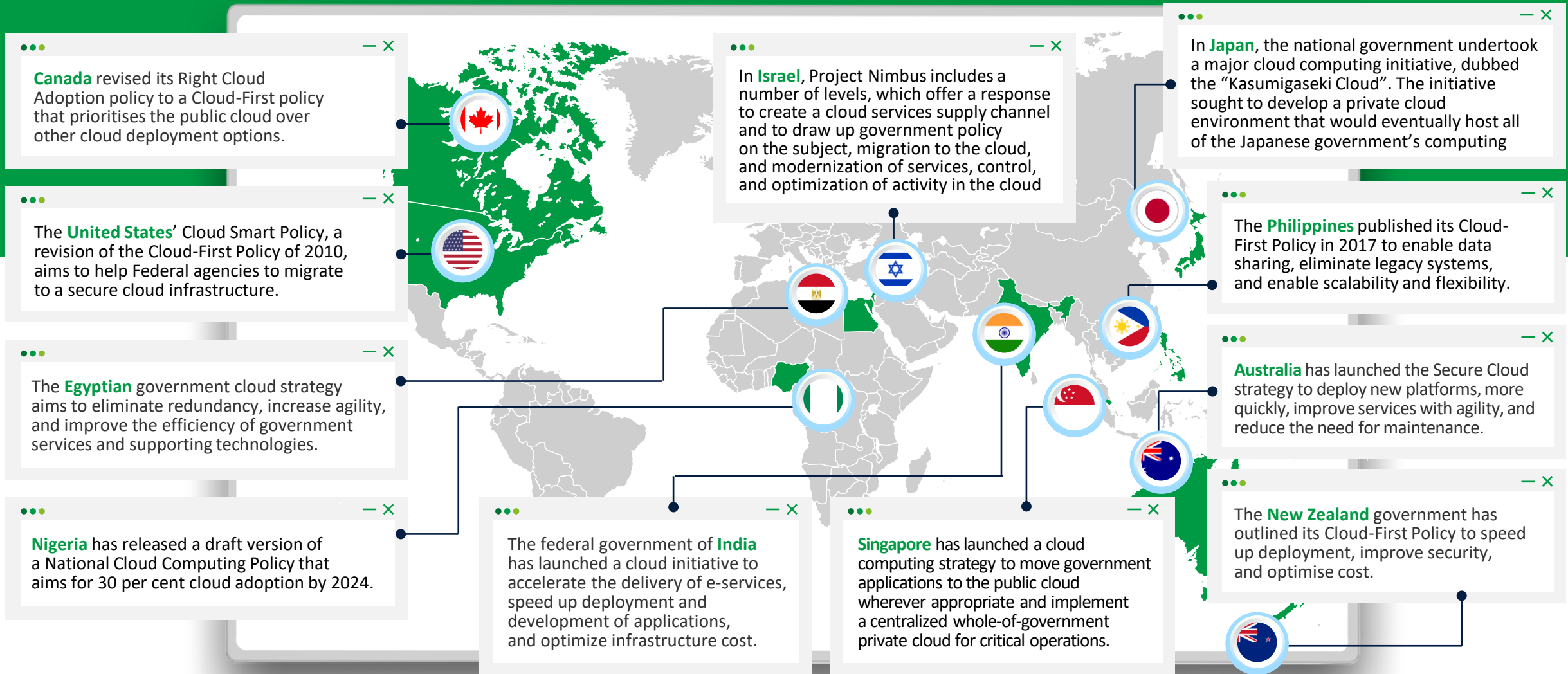
There are cases of successful cloud adoption at a global level:  
Governments are adopting differing strategies according to their digital maturity and business needs





# Cloud adoption in the public sector

There are cases of successful cloud adoption at a global level:  
Governments are adopting differing strategies according to their digital maturity and business needs



# Cloud adoption in the public sector

The cloud has been a successful driver of innovation in government

## Breaking down data silos



Cloud adoption can create new opportunities for innovation in many government domains:

- Reducing congestion;
- Anticipating crime;
- Analysing data for space experiments;
- Reducing fraud and waste, and power abuse.

The cloud offers more than just a **link to different sources of data**: it also offers flexibility in setting up complex and innovative environments (e.g. deep learning).



### SAFE ROADS

Transportation agencies in Nevada deployed a cloud-based AI platform to gather data from connected cars, road cameras and apps such as Waze, about road conditions and weather patterns to predict high-risk corridors where accidents are likely to happen. Results from this pilot programme included a 17% reduction in the number of crashes and, because agencies were able to clear accident sites faster, a 23% reduction in secondary collisions.

## Offering customised solutions to drive AI



Growth in SaaS has been immense. A government agency no longer has to create its own solutions, because **viable solutions are already on the cloud**.

SaaS applications, where cognitive technologies are built into the software, have the **potential to increase the uptake in government of AI and other emerging technologies**.



### REDUCTION IN NUMBER OF TICKETS (GERMANY)

Due to the increasing use of digital services, helpdesk services are increasingly in demand, leading to a high number of tickets. The use of chatbots arises which makes it possible to solve a large number of tickets in a dialogue-based way. Each chatbot should be programmed and filled with the knowledge to respond to questions with appropriate answers, freeing up staff time for reallocation to other work.

## Connecting stakeholders across the ecosystem



At the heart of the cloud's ability to drive innovation is its ability to **connect a wider ecosystem of partners** such as developers, designers, researchers, and other government agencies.

In the past, these stakeholders may have created solutions that benefited just themselves. Now, housed in the cloud, innovations can be available to all, and participants enjoy new opportunities for collaboration. **The cloud can also connect different organisations**.



### CONNECTION BETWEEN DIFFERENT PARTS

The cloud can also connect different players. Organizations in the USA ranging from the Federal Bureau of Investigation to the State of Delaware have found that the cloud can connect them to a rich environment of external developers. This allows users to find existing solutions to their problems that have already been developed in the cloud rather than having to build their own tools from scratch.

02



# EU digital policies and initiatives

How Europe is driving change



# European Digital Compass

It is important to define a set of digital principles across Europe, in order to launch important multi-country projects rapidly, prepare legislative proposals for a robust governance framework, and to monitor progress.

The **European Digital Compass** translates the EU's digital ambitions into clear targets, setting out a European pathway for the digital decade.

## DIGITALISATION OF PUBLIC SERVICES

### GOVERNMENT AS A PLATFORM:

**100%** online provision of key public services

**100%** of European citizens have access to medical records (e-records)

**80%** of citizens will use a digital ID solution

## DIGITAL TRANSFORMATION OF BUSINESSES

**Scale ups:** Europe will double the number of unicorn businesses

**Digital 'late adopters':** More than 90% of European Small and Medium-sized Enterprises (SMEs) reach at least a basic level of digital maturity

**Take-up of technologies:** 75% of European enterprises have taken up cloud computing services, big data and AI



# 2030 DIGITAL TARGETS

## DIGITALLY-SKILLED POPULATION AND HIGHLY SKILLED DIGITAL PROFESSIONALS

**Information and Communications Technology (ICT) specialists:** 20 million employed ICT specialists, with convergence between women and men

**Citizens:** 80% of citizens aged 16-79 have at least basic digital skills

## SECURE, PERFORMANT AND SUSTAINABLE DIGITAL INFRASTRUCTURES

**Connectivity:** All populated areas in Europe will be covered by 5G

**Semiconductors:** At least 20% (of the world total by value) of the production of cutting-edge and sustainable semiconductors in Europe

**Edge/Cloud:** 10,000 climate-neutral highly secure edge nodes are deployed in the EU

**Quantum computing:** By 2025, Europe will have its first computer with quantum acceleration

# European Alliance for Industrial Data, Edge & Cloud

The European Alliance for Industrial Data, Edge and Cloud aims to foster the development and deployment of next generation edge and cloud technologies



## WHAT IS THE AIM OF THE ALLIANCE?

Strengthen the **position of EU industry in cloud and edge technologies** and industrial data, serving the **needs of EU businesses and public administrations** that process sensitive categories of data, and providing the **infrastructure for highly innovative use cases**.

Bring together **businesses, representatives of Member States and relevant experts** from the private and public sectors, to jointly **define strategic investment roadmaps** to the next generation of highly secure, distributed, interoperable and resource-efficient **computing technologies**.

**Serve as a platform for exchanges on issues of cloud governance**, for example relating to the public procurement of cloud services.



## WHAT WILL BE THE ROLE OF THE ALLIANCE?

Bringing together relevant actors to **prepare and** update horizontal and technology-specific **investment roadmaps for cloud and edge**.

Providing **recommendations** to ensure the **coherent integration** of **investments** for the deployment of European Data Spaces in relevant areas. Common European Data Spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control.

Advising the European Commission on **requirements and standards for cloud services**, including for public procurement.



## WHO CAN JOIN THE ALLIANCE AND HOW?

Any **organisation** that has a **legal representative in the EU** and with activities of significant relevance to the **provision of highly secure cloud and data processing** can join the Alliance at **any time** by signing up to the **Alliance Declaration**.

Entities which are subject to control by a **third country**, acting either directly or by way of measures addressed to a third country entity, will have to submit **additional proof of the legal, organisational and technical measures** they have taken to ensure full **compliance with the EU's data protection framework**.

Eligible organisations can express their interest in joining the Alliance by responding to the **continuously open call**.



**European Alliance for Industrial Data, Edge and Cloud**

The Alliance will contribute to **shaping the next generation of secure, low-carbon and interoperable cloud and edge services and infrastructure for Europe** as envisaged in the **European Data Strategy**. It will also contribute to the **EU's digital compass targets for 2030**.

# GAIA-X

Gaia-X is a European initiative to create a networked and secure data infrastructure to the highest European standards in terms of digital sovereignty and innovation.

## WHAT IS GAIA-X? ▼

**GAIA-X** builds on existing initiatives for the development of new business models and data spaces in the EU and its Member States. Its main objective is to establish a **European ecosystem** that brings together national initiatives and serves as the central point of contact for interested parties in different countries, enabling the presentation of services and providers on a single platform.

GAIA-X is based on the idea of **open-source** and supports everything that contributes to it. All individuals and organisations involved in GAIA-X work together on a **common platform**, from the perspective of both user and provider.

## GAIA-X DRIVERS ▼



### DATA SOVEREIGNTY

Europe aims to secure and maintain permanent digital sovereignty, accepting the fact that the major cloud players are non-European providers.



### DATA AVAILABILITY

Europe needs a reliable, secure and transparent data infrastructure that allows data exchange while guaranteeing European standards.



### INNOVATION

Europe needs a digital ecosystem that allows the development of innovative products and helps European companies and business models to scale up and be globally competitive.



# EU digital policies

Despite encouragement to achieve digital transformation, security and data protection in the EU are still major barriers to cloud adoption. Policies, regulations and protection laws are constantly being created:

GDPR

## GENERAL DATA PROTECTION REGULATION

This imposes obligations on organisations everywhere regarding the processing of personal data of EU citizens.

ESMA

## EUROPEAN SECURITIES AND MARKETS AUTHORITY

ESMA created guidelines to help firms and competent authorities identify, address and monitor the risks and challenges arising from cloud outsourcing arrangements, such as making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities and providing for exit strategies.

ENISA

## EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA produced several reports to guide public bodies in different contexts, such as security and resilience in governmental clouds, and indirectly supporting EU Member States in the definition of their cloud strategy.

EU-U.S.  
PSF

## EU-U.S. PRIVACY SHIELD FRAMEWORKS

It ensures the secure transfer of data between EU and the US. Also, through a set of defined requirements, it governs the use and handling of personal data transferred from the EU, as well as access and dispute resolution mechanisms that participating companies must provide for EU citizens.

EU MC

## EUROPEAN UNION MODEL CLAUSES

The EU Model Clauses are standardised contractual clauses used in agreements between service providers and their customers to ensure that any personal data leaving the European Economic Area will be transferred in compliance with EU data protection laws and meet the requirements of the EU Data Protection Directive 95/46/EC.



## GERMANY

### German policy Act (BDSG-new) 2017

Restricts data transfers to third countries. Companies that process national citizens' data must fulfill requirements even if located outside the national borders. CSP are required to have a Trusted Cloud Data Protection Profile (TCDP).



## BELGIUM

### Belgian Data Protection Act 2018

Establishes that organisations based or operating outside Belgium may be subject to the Act to the extent that they process personal data in Belgium. Data processed by foreign persons in Belgium is still subject to the protection law.



## FRANCE

### Data Protection Act

Even if data is processed outside the country's borders, it must comply with French law. There are no specific rules relating to cloud storage, although there are strict rules for processing health data.



## FINLAND

### Finnish Data Protection Act 2019

Finland has a law on processing health data, an act to regulate the collection and use of personal data online, and another act establishing rules for the processing of employees' personal data.

## EU MEMBERS STATES PROTECTION LAWS



# EU Cloud Code of Conduct

A Code of Conduct specifically for the cloud.



## WHAT IS THE EU CLOUD CODE OF CONDUCT?

It consists of requirements for CSP that wish to adhere to the Code, plus a governance section designed to support the effective and transparent implementation, management, and evolution of the Code.

The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements, either through self-evaluation and self-declaration of compliance and/or through third-party certification.



## WHY WAS THE EU CLOUD CODE OF CONDUCT DEVELOPED?

The intention of the EU Cloud Code of Conduct is to **cover GDPR requirements and make it easier for cloud customers** (particularly SMEs and public entities) to determine whether certain cloud services are appropriate for their designated purpose.

In addition, the transparency created by the Code will **contribute to an environment of trust** and create a high level of data protection in the European cloud computing market.

# EU Cloud Code of Conduct

## WIDE-RANGING

Covers the full spectrum of **cloud services**: SaaS and PaaS as well as IaaS.

## INDEPENDENT

Has an independent **governance structure** to deal with **compliance**, as well as an independent monitoring body, SCOPE Europe, which scrutinises cloud service providers which sign up to the Code and monitors services that are certified in the Code – a requirement of the **GDPR**.



## INCLUSIVE

Invites **CSP** of all sizes and from all **cloud sectors** to join: there are different membership options, depending on the CSP's interests. Once a member, a CSP can declare itself adherent to the Code, and committed to rigorous **data protection safeguards**.

## COMPREHENSIVE

The Code was developed by the Cloud Select Industry Group (Data Protection Code of Conduct Subgroup) convened by the European Commission under the auspices of the **Directorate-General for Communications Networks, Content and Technology (DG Connect)** and with the involvement and advice of **DG Justice**.



# EU digital investment funds

To implement different policies for digital transformation, many investments should be made using the various EU funds.

## NEXT GENERATION EU

The **Recovery and Resilience Facility** is the key instrument at the heart of the **Next Generation EU** funding programme to mitigate the economic and social impact of the coronavirus pandemic and make European economies and societies better prepared for green and digital transition.

€672.5  
BILLION

► Financial support to public investments and reforms

(up to)  
**€312.5 billion**  
in grants



(up to)  
**€360 billion**  
in loans

The expenditure of each **Recovery and Resilience Plan** should include:



**Climate** investments and reforms (**≥ 37%**)



**Digital** transition investments (**≥ 20%**)

## DIGITAL EUROPE PROGRAMME

The **Digital Europe Programme** (2021-2027) is a new EU funding programme focused on bringing digital technology to businesses, citizens and public administration.

€7.6  
BILLION

► What are the Digital Europe Programme priorities?



Ensuring the wide use of digital technologies across the economy and society (**€1.1 billion**)



Supercomputing (**€2.2 billion**)



Artificial Intelligence (**€2.1 billion**)



Cybersecurity (**€1.6 billion**)



Advanced digital skills (**€580 million**)



# EU digital investment funds

To implement different policies for digital transformation, many investments should be made using the various EU funds.



## CONNECTING EUROPE FACILITY: DIGITAL

The **Connecting Europe Facility (CEF): Digital** programme supports investments in trans-European networks and infrastructure, promoting digital connectivity during the period 2021-2027.

€2.1  
BILLION

► What is funded by the digital segment of the CEF?

**Connectivity projects** of common EU interest that contribute to the deployment **Gigabit and 5G networks**.

**Actions  
foreseen  
under the  
programme**



Developing and making available **high-capacity networks** across Europe, including 5G systems.



Supporting **increased security, resilience** and **capacity** of the digital backbone networks in the EU.



Boosting the **digitalisation** of transport and energy networks.

## EUROPEAN DEFENCE FUND

The **European Defence Fund (EDF)** aims at fostering the competitiveness and innovativeness of the European defence technological and industrial base, thereby contributing to the EU's strategic autonomy.

€8.0  
BILLION

► How does the EDF work?

Around **1/3** is finance for **competitive and collaborative defence research** projects (through **grants**).

About **2/3** to complement Member States' investment by co-financing the costs of **developing defence capabilities** following the research stage.

► The EDF aims to **trigger cooperative programmes** that would not happen without an EU contribution and, by supporting R&D activities, **to provide the necessary incentives** to boost **cooperation** at **each stage** of the **industrial cycle**.

# EU digital investment funds

In particular, EU member states have made the digitalization of public administration a priority, and some have included components of cloud computing in their recovery plans.



France

## Pillar:

### Item name:

- ▶ Plan to support the French cloud sector

### Budget:

(over four years)

€1.8  
BILLION



Greece

## Pillar:

### Item name:

- ▶ Supply of Central Cloud Computing Infrastructure and Service
- ▶ Upgrade of Cloud-computing infrastructure and services of the National Infrastructures for Research and Technology (GRNET)

### Budget:

€95  
MILLION

€63  
MILLION



Italy

## Pillar:

### Item name:

- ▶ Enabling and facilitating Cloud migration

### Budget:

€1  
BILLION

# Europe is driving change:

## EU digital policies and initiatives

- ▶ The main CSP are responding to pressures for change, especially in terms of data, since EU Data are sensitive assets

### Development of specific resources



- ▶ CSP are providing **online resources** to **help customers** more easily complete data transfer assessments and comply with the GDPR, taking into account the **European Data Protection Board** recommendations. These resources also assist customers in other countries to understand whether their use of services involves a data transfer.

### Certification and adoption of EU CCoC



- ▶ CSP are starting to **adopt EU CCoC** to demonstrate how they offer guarantees to **implement appropriate technical and organisational measures** as data processors under the **GDPR**. CSP are also obtaining **certification of compliance with internationally-recognised privacy standards** (e.g. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701), which provide **independent validation** of dedication to **world-class security and privacy**.

### Investment in European data centre infrastructure



- ▶ CSP will **not transfer data outside** a **customer's selected region** without the **customer's agreement**. CSP customers control **where** their data is stored, **how it's stored**, and **who has access to it**. CSP have a range of tools at their disposal to **enhance security**.

### Comply with or exceed EU guidelines



- ▶ CSP use **world-class encryption** and **robust lockbox solutions** that meet **current regulatory guidance**. In fact, CSP **strengthened efforts** to **protect customer data**, such as **challenging law enforcement** requests for customer data that conflict with EU law.

03



## Case studies

How countries are  
leveraging the cloud



# Governments: Cloud strategies and policies

Understanding cloud strategies and policies around the world can provide insights into how the public sector in the EU should adopt the cloud.



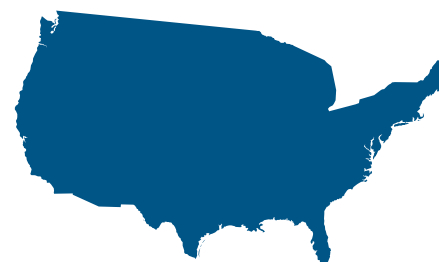
**UNITED KINGDOM**

CLOUD FIRST POLICY



**AUSTRALIA**

SECURE CLOUD STRATEGY



**UNITED STATES**

CLOUD SMART




**CANADA**

CLOUD FIRST  
ADOPTION STRATEGY

# CASE STUDY 1

# UK

## UNITED KINGDOM GOVERNMENT

-  The UK Government has developed a **'One Government Cloud Strategy'** (OGCS) to encourage agencies to move to the cloud through a clear vision of how they can benefit by using the cloud and other hosting solutions.
-  This guidance also enables organisations to address **security, business, digital, technology, skills** and **cultural considerations** and **requirements** from across government and public sector bodies to provide a clear vision for cloud adoption.
-  It is expected that the UK government will promote the adoption of the public cloud policy and subsequently the exploitation of alternatives that meet the right levels of **security, flexibility** and **value for money**.



## CURRENTLY

The UK government was an early adopter of a **Cloud First Policy**. However, after COVID-19 accelerated cloud adoption, many agencies started to **review their policies** on **data protection** and **cloud services**, and some agencies are moving forward with **hybrid** and **multi-cloud approaches**.

At the same time, the UK government provides **controls, funding** and **frameworks** to help agencies **adopt cloud** in the first instance. Some **initiatives** that drive cloud adoption are shown below:

### 01 ▼

#### LOCAL DIGITAL DECLARATION

Enhances and leverages the development of local public services from any public sector or not-for-profit organisation, which can join the movement by signing the Declaration.

### 02 ▼

#### TECHNOLOGY CODE OF PRACTICE

Provides guidance to help organisations design, build and buy technology developed under the Local Digital Declaration and Transformation Strategy.

### 03 ▼

#### CLOUD FIRST POLICY

This requires public sector organisations to consider and evaluate potential cloud solutions first before any other option during the search for new or existing services.

### 04 ▼

#### DIGITAL MARKETPLACE

This is an online tool for public sector organisations to find people, technology, services and frameworks for digital projects developed by the UK government.



# CASE STUDY 1

# UK

## THE UK ONE GOVERNMENT CLOUD STRATEGY (OGCS)

TWO PATHS TO PURSUE THE UK OGCS:

01 ▼

### CONSIDER CLOUD SOLUTIONS BEFORE ALTERNATIVES

When procuring **new or existing services**, public sector organisations should consider and fully evaluate potential cloud solutions first before considering any other option. This approach is **mandatory for central government** and strongly recommended to the wider public sector. Departments remain free to **choose an alternative to the cloud** but will need to demonstrate that it offers better value for money.

02 ▼

### PUBLIC CLOUD FIRST

Cloud First means “**public cloud rather than a community, hybrid or private deployment model**”. There are circumstances where other deployment models are appropriate but the primary benefits for government come from embracing the public cloud. Departments are encouraged to **replace legacy applications** with SaaS and build new ones applying PaaS solutions.



## GOVERNMENT ARRANGEMENTS



- ▶ The **Government Digital Service (GDS)** supports agencies with the delivery of **new services** and ensures the quality as well as the efficiency of cloud services. The GDS carries out a **Spend Control** process which requires agencies to explain value for money if the first choice is a non-cloud alternative. This process allows agencies (i) to work with the Her Majesty's Treasury to outline the cloud project and how funds will be spent, and (ii) to identify legacy spending and reduce the risk of failure.
- ▶ Buyers and suppliers on **Digital Marketplace** operate through the use of a **G-Cloud framework**, which allows agreements between the government and vendors to supply certain types of services under specific terms. The UK Government also have **Memorandums of Understanding** with CSP, to establish discounts on services and streamline the contract negotiation time between the government and suppliers.
- ▶ **Cloud Security Guidance** has been developed by the **National Cyber Security Centre (NCSC)** to support agencies in the configuration, implementation and secure use of cloud services. In addition, the NCSC contemplates the **Zero Trust Architecture Design Principles** to help organisations design and build their own Zero Trust Architecture.
- ▶ The **Digital, Data and Technology Capability Framework** has been created to improve **recruitment** and support strategic **workforce planning** by describing the skills required to work at each level in government.
- ▶ All government departments have to **make risk-based decisions** about their **data residency** in a CSP when storing government data. **Data protection requirements** vary between agencies. There are **six cloud compliance controls**: (i) ENISA, (ii) EU-U.S. Privacy Shield Framework, (iii) EU Model Clauses, (iv) GDPR, (v) Cyber Essentials Plus, and (vi) PASF.

## CASE STUDY 2

# AUSTRALIA

### AUSTRALIAN GOVERNMENT



- ▶ The **Digital Transformation Agency (DTA)** has developed a **Secure Cloud Strategy (SCS)** to promote cloud adoption across **Australian Public Service (APS)** agencies and to assist them in this transition.



- ▶ The Australian Government is reshaping digital transformation: the cloud is an option that offers **low cost reusable digital platforms** as well as a **fast and reliable digital channel** for service delivery. Thus, the Australian Government can become more **agile, convenient, available** and **user-centric** through cloud services.



- ▶ Therefore, the **DTA** is now beginning to **update** its **strategy** to continue to support the Australian government's **cloud transformation initiatives**.



## CURRENTLY

### n1 ▼

Since the introduction of the **Secure Cloud Strategy**, the use of cloud services has increased, together with **investment in cloud adoption**. Most APS agencies and organisations have already adopted the cloud and their main spending is no longer on cloud adoption costs.

### n2 ▼

Progress in the adoption and use of cloud services is well advanced across most APS agencies and commercial entities. However, the pace of **innovation** and level of maturity vary, highlighting the need for more **policy guidance** and **support**, enabled by an up-to-date and established cloud maturity assessment framework. Specifically, APS agencies continue to drive a **Cloud First policy** and information and technology departments address **security concerns**.

### n3 ▼

The DTA has launched a new **Cloud Marketplace** that replaces the Cloud Services Panel: this portal enables easy access to **cloud technology** and capabilities. Its catalogue of offerings includes services for SME and start-ups, as well as national and global providers. In addition, the offerings in the Cloud Marketplace are grouped into procurement categories: (i) Cloud Consulting and (ii) Cloud Services. Selected cloud vendors will be able to showcase their capabilities and update their service offerings by keeping pace with the evolution of cloud technology.





# CASE STUDY 2

# AUSTRALIA

## SECURE CLOUD STRATEGY

The Secure Cloud Strategy was developed in 2017 to help government agencies **use cloud services**. It provides the **framework for cloud transition** so that all agencies can prepare themselves to embrace what the cloud offers. Australian agencies use the **SCS** as a starting point to develop and implement their **own cloud policies**:

| JURISDICTION                | POLICY  |
|-----------------------------|---|
| Commonwealth                | <b>Secure Cloud Strategy</b> (2017)                             |
| NSW                         | <b>NSW Government Cloud Policy</b> (2018)                       |
| Victoria                    | <b>Cloud Computing Policy</b> (2013)                            |
| Queensland                  | <b>Cloud Computing Strategy and Implementation Model</b> (2014) |
| South Australia             | <b>Cloud Services Policy</b> (2015)                             |
| Western Australia           | <b>Cloud Policy</b> (2016)                                      |
| Tasmania                    | <b>Tasmania Cloud Policy</b> (2015)                             |
| Northern Territory          | <b>Cloud Computing Policy</b> (2017)                            |
| Australia Capital Territory | <b>ACT Government Digital Strategy</b> (2016)                   |



## GOVERNMENT ARRANGEMENTS

To promote an efficient cloud transition, the Australian government has defined and implemented a set of initiatives:

- Require agencies to develop their **own cloud strategies**, with the Secure Cloud Strategy as a starting point.
- Apply **cloud principles** to guide cloud implementation.
- Promote ICT systems certification across agencies through layered **Cloud Certification Model**.
- Promote **better cloud procurement** through the alignment between service procurement and ICT Procurement Review recommendations.
- Establish and clarify the necessary cloud requirements through a **baseline and assessment framework** for cloud service quality.
- Clarify responsibilities and accountabilities, through the development of a **Cloud Accountability Model**, supported by contracts.
- Enable **secure sharing of cloud service** assessments, technical blueprints and other agency cloud expertise through the creation of a cloud knowledge collaboration platform.
- Increase **government skills and competencies for the cloud**, through the design of cloud skills uplift programmes.
- Improve common **shared platforms and capabilities**.



# CASE STUDY 3

## US

### UNITED STATES GOVERNMENT

- ▶  The US Cloud Strategy has moved from **Cloud First Policy** to the Federal Cloud Computing Strategy, also known as **Cloud Smart**.
- ▶  **Cloud Smart** has accelerated the adoption of cloud services and promoted the creation of policies to manage **government data** in the cloud. When government data is involved in cloud services, agencies are required to comply with policies released by **The Office of Management and Budget** and follow **Federal Risk and Authorisation Management Program** (FedRAMP) guidelines.
- ▶  Thus, Cloud Smart has been providing **tools, expertise** and **flexibility** for agencies to reach **the potential of cloud-based technologies**.



## CURRENTLY

01 ▼

Cloud Smart strategy is focused on **security, procurement** and **workforce** and its main objective is to deliver greater return on investment, improved security, and better services.

02 ▼

The US government is developing initiatives to drive the adoption of cloud services. Involving the **evaluation of investments in cloud services** across agencies as well as **updating policies** that prevent **agency-owned data centres** from starting up or expanding without approval.

03 ▼

The Cloud Smart strategy promotes **multi-cloud environments** which provide **flexibility and cost efficiency**. Multi-cloud approaches are now the new normal for Federal agencies, **avoiding cloud vendor lock-in** and **promoting access to the latest services** from different CSP. This strategy helps organisations understand the **benefits** of moving to the **cloud**, as well as **when** and **how** they should do so.



# CASE STUDY 3

# US

## CLOUD SMART STRATEGY

01 ▼

**Cloud Smart Strategy** is a long-term strategy for the adoption of the cloud by Federal agencies in order to build a path for migrating to a safe and secure cloud infrastructure.

02 ▼

This strategy aims to achieve additional **savings, security, and faster services** through the adoption of cloud.

02 ▼

Specifically, the **Cloud Smart Strategy** requires agencies to analyse their existing service and mission needs, technical requirements, and policy constraints in order to prepare for migration to the cloud. Their **technology decisions** consider customer/ citizen impact, **cost risk management** and **cybersecurity** criteria, as well as the **long-term impact** of migrating the application.



## GOVERNMENT ARRANGEMENTS

- Agencies should follow client needs and invest in popular technology areas, as well as streamline and regularly update their applications to ensure three key pillars of successful cloud adoption – **security, procurement** and **human resources**.

**Security:** Upgrade security policies to improve risk-based decision making, automation and data protection. The following programmes are major elements of the Federal security strategy, allowing agencies to take a holistic and outcome-driven approach:



**Trusted Internet Connections;**



**Continuous Data Protection and Awareness;**



**FedRAMP:** Government -wide programme that provides a standardised approach to the certification and authorisation of cloud services.

**Procurement:** Guide agencies on **category management, risk management, Security Requirements for Contracts** and **SLA management**, about common practices for ensuring the cost-effective, safeguarded procurement of cloud-based solutions.

**Workforce:** Improve and develop key skills and recruit key talent for cybersecurity and cloud engineering. The Cloud Smart approach considers workforce reskilling and staff retraining crucial for promoting cloud adoption.

- The US government approved the **Clarifying Overseas Use of Data Act**, which allows CSP to ensure **data privacy**, but allows US officials to **access data held in a foreign country** without the need for a mutual legal assistance treaty, promoting data security and privacy.



# CASE STUDY 4

# CANADA

## CANADA GOVERNMENT



- ▶ Cloud transition by the Canadian government started initially with a strategy called the '**right cloud strategy**' which then progressed to a '**cloud first**' strategy.



- ▶ The cloud adoption strategy pursued by the Canadian government has **three broad goals**:
  - To help **balance** the **supply** of and **demand** for IT services;
  - To **manage** the **risks** of cloud adoption in a consistent way;
  - To **prepare** the **IT workforce** for the cloud.



## CURRENTLY

### 01 ▼

Government departments in Canada consider **COVID-19** to be the **main driver** for the **growth in cloud spending** and for **digital transformation**, accelerating the need to modernise the government's core infrastructure.

### 02 ▼

It is essential that government agencies continue to **explore new ways** to use the cloud as an **enabler of digital services**, at the same time promoting the definition and implementation of **policies for protected data processing and storage** in the cloud. However, different departments use different approaches, which leads to variations in the pace of cloud adoption across departments.

### 03 ▼

In addition, **Shared Services Canada** (an agency responsible for IT service delivery across government departments) provides a lightweight **cloud-brokering service** to government departments, where the **sourcing and consumption of cloud services is centralised**. Shared Services Canada also provides **security monitoring services** and uses the Security Operations Centre to centralise security operations, reducing the cost of security operations and promoting the dissemination of best practice.





# CASE STUDY 4

# CANADA

## CLOUD FIRST STRATEGY

The **Cloud First Strategy** sets out an order of preference when selecting a cloud deployment model but recognises that no one deployment model meets all the government's needs.

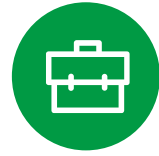
The **benefits** of the **Canadian public sector community cloud** include the following:

01 ▼  
"Procure once,  
buy many times"

03 ▼  
Collaboration

02 ▼  
Economies  
of scale

04 ▼  
Control of  
cloud sprawl



## GOVERNMENT ARRANGEMENTS

To promote an efficient cloud transition, the Canadian government defined and implemented the following initiatives:

- ▶ **Cloud services are identified and evaluated as the principal delivery option when initiating IT investments, initiatives, strategies and projects.**
- ▶ Manage security risk, by following the **Government of Canada Cloud Security Risk Management Approach and Procedures** and the **Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice**.
- ▶ Develop an **exit strategy**, to ensure **business continuity** and to **mitigate** and **manage risks**.
- ▶ Select **cloud service models**, in a specific order of priority.
- ▶ Create the **Government of Canada Right Cloud Selection Guidance**, which helps to select deployment models in a specific order of priority.
- ▶ Comply with the **Electronic Data Residency Directorate** for continuous access to **sensitive data**.
- ▶ Take into account **service portability** and **interoperability** when designing **cloud-based solutions**.
- ▶ Take **cloud services** as the **top priority** option when initiating IT investments, initiatives, strategies and projects.

**Canada's data sovereignty control** is governed by a policy that sensitive data under government control will be stored in **Canada Government-approved facilities**. Each department or agency must assess the **risk against data sensitivity parameters** and appropriate **security controls** must be applied to cloud services.

The **Cloud Center of Excellence (CCoE)** fosters the development of cloud talent, streamlining **demand forecasting**, **monitoring** and **optimising** of **cloud services consumption**, as well as **designing cloud-native solutions**. The Treasury Board of Canada Secretariat aims to **create a multi-departmental working group** focused on collaboration with other government departments and industry to **guide cloud adoption**.



04



## The way forward

How can public sector adopt cloud

# Recommendations for moving to the cloud

To promote and increase cloud adoption in the public sector, Governments should implement a set of actions.



## Governance, policies & regulations

Review, define and/or implement **policies for operating in the public cloud**, especially around risk sharing arrangements.



## Innovation & data-driven decision-making

Use the public cloud as a **platform for innovation**, and leverage for better outcomes for agencies and citizens.



## Skills & capabilities

Prepare the public sector for the public cloud by considering required **skills and competencies**.



## Resources & budgets

Bring forward proposals to **shift capital budgets** to operating budgets in sustainable ways and promote the optimisation of cloud resources.

**Develop data accountability tools** to promote cross-border data transfers.

Develop and update **cloud-relevant regulations**.

Reconcile **conflicting regulations** at central and local government levels.

Centralize **cloud governance**.

**Ensure that the cloud** is a key component of digital strategies and a driver for the economy.

Align **business context to data**.

**Integrate cloud** and organizational KPIs.

**Absorb know-how** about cloud migration.

Develop a **collaborative platform**.

**Create a CCoE** to coordinate cloud issues in government.

Optimize **resources cost and utilization**.

**Implement funding** and procurement initiatives.

# Recommendations for moving to the cloud

To promote and increase cloud adoption in the public sector, Governments should implement a set of actions.




## GOVERNANCE, POLICIES & REGULATIONS

### 01 | Develop tools for data accountability to promote cross-border data transfers

Create and put in place **legal mechanisms for data accountability** by businesses and governments, to enable data transfers between jurisdictions with different data protection and/or privacy regimes.

Leverage multilateral frameworks to **help government agencies easily identify interoperable or equivalent data protection standards** without having to prescribe specific requirements for each vendor or contract.

 **France creates a security certificate to achieve “clouds of trust”**

The creation of the ‘Cloud de Confiance’ certificate is the cornerstone of the strategy for having secure data and away from ‘extraterritorial’ eyes. This trusted data certificate will be awarded to data service providers who meet a long list of criteria validated by the French Agence Nationale de la Sécurité des Systèmes d’Information. Recipients of the trusted cloud seal must guarantee the maximum protection of data to companies and administrations that choose it and the certificate will have a security level among the highest in the world for fighting against cyberattacks.

### 02 | Develop and update cloud-relevant regulations

Assess bottlenecks in terms of data management, data classification, and interoperability between government service platforms, in order to **develop and implement frameworks**, such as a framework for data classification.

Define and share **regulatory approaches to data protection** and security that do not reflect the perception that in order to have oversight and access to data, it must be stored within the country. This way, there will be a reduction of the number of proposed data localisation measures, reducing costs, complexity, and constraints in transferring data between countries.



**UK and Australia developed and implement data classification frameworks**

The United Kingdom government established a risk-based assessment of cloud use to identify situations where it may not be appropriate to use cloud services for specific systems or data. The government of Australia defined a framework based on risk assessment and matching appropriate security controls, rather than checking off compliance requirements. This framework also considers moving high and low value information into different environments to increase flexibility and focus resources.

**Develop and update cloud-relevant data privacy regulations**, and raise awareness among relevant staff of its importance, since data privacy was one of the top barriers to cloud adoption in the public sector.

**Develop and update cloud-relevant cybersecurity regulations**, improve staff awareness (including basic and advanced cyber training), and establish or bolster computer emergency response teams and enforcement. These measures will increase government resilience against cybersecurity threats.

### 03 | Reconcile conflicting regulations at central and local government levels

Assess conflicting regulations at the central and local government levels to create interoperable cloud systems and promote regulation as a driver towards cloud adoption.

Leverage internationally-recognised standards and best practices and support regional initiatives to enable data portability and establish consistency across regulatory regimes.

### 04 | Centralise cloud governance

Define cloud **governance policies that provide alerts about any irregularities**, such as cost spikes, tagging compliance issues, security vulnerabilities, across the different business units and departments that use cloud resources.

Define **(i) the expected sophistication of policies**, which can range from an email notification to automated actions such as terminating an unused infrastructure, and **(ii) the team responsible for authorisations** within a cloud environment. Implementing cloud governance policies will free up staff for more mission-critical projects and can yield immediate cost savings.



# Recommendations for moving to the cloud

To promote and increase cloud adoption in the public sector, Governments should implement a set of actions.



## INNOVATION AND DATA-DRIVEN DECISION-MAKING

### 01 | Ensure that the cloud is a key component of digital strategies and a driver for the economy

Ensure **that strategies and roadmaps for advanced technologies** (such as AI) acknowledge the foundational role of the cloud, to guarantee an articulated and concerted process for migrating to the cloud.

Consider **adopting a cloud-first or cloud-by-default approach** as a whole-of-government approach, to benefit from secure, reliable, and cost-effective cloud computing options.

**Define, clearly, and manage the scope and timeline of projects** to prioritize use cases that are likely to have the highest impact, and build internal capacity.

Focus on innovation capabilities enabled by cloud, and promote and maintain alliances with different CSP (**multi-cloud approach**), in order for agencies to be constantly up-to-date with state-of-the-art technologies and **eliminate the barriers associated with data sovereignty** (e.g. through the creation by CSP of exclusive data centres for government).

**Promote technological spillover across other industries**, through the recognition of the government as a driver for the adoption of edge technologies.

Break data silos by **making data more organized, standardized, and accessible** across the agency, promoting data-driven decision-making

### 02 | Align business context to data

**Maintain control over cloud spend, due to the growing consumption of cloud resources**; and modernise operations and deliver improved services to constituents.

Ensure visibility into Cloud data: (i) develop a **consistent tagging strategy** in order to better identify and allocate spend and usage, (ii) **group resources in a way that's meaningful to the organisation**, such as building dynamic business groups by environment, department, or owner, and (iii) **drive accountability across the organisation** to show each group exactly how much they are spending and what they are spending it on, promoting the establishment of an accurate budget.

### 03 | Integrate cloud and organisational KPIs

**Align cloud and operational KPIs with the organisation's business KPIs, to measure the impact of cloud consumption.** KPIs may include for example time to bring new services to market, compliance issues, and customer satisfaction. Agencies should ensure the integration with existing business systems such as a governance risk and compliance solution or the accounting software. Also, it is important to ensure that the integration goes beyond the technical components and extends to driving a cultural change across the organization.



#### The Australian government includes the cloud in its digital transformation strategy

As part of its digital transformation initiative, it has recognised the cloud as a foundational platform for leveraging emerging technologies such as AI, blockchain, and quantum computing. It intends to provide all agencies with access to cloud systems.

# Recommendations for moving to the cloud

To promote and increase cloud adoption in the public sector, Governments should implement a set of actions.



## SKILLS AND CAPABILITIES

### 01 | Absorb know-how about cloud migration

**Build on existing solutions created by others.** To speed up the cloud implementation process, governments can encourage agencies to build applications using common resources or tried-and-tested open solutions.

**Pilot the migration with services that are simpler to migrate to the cloud,** and where a quick success encourages and emboldens the government agency to tackle larger cloud migrations projects with increasing confidence, familiarity, and skills.

Define an end goal and a targeted completion date to **provide government agencies with an impetus to move forward** and indicators to gauge the success of their cloud strategy.

### 02 | Develop a collaborative platform

**Support the sharing of common products to keep all agencies connected,** facilitating access to resources and information crucial for cloud services adoption/use.

**Promote the adoption of more homogenous and improved solutions,** instead of having a proliferation of different individual solutions.

**Provide agencies with training tools and environments for developing their own applications,** supporting the use of standard approaches to cloud development and allowing free experimentation in a safe and controlled environment.

### 03 | Create a CCoE to coordinate cloud issues in government

Retrain IT professionals and **give them clear career paths, focusing on new skills,** specifically best practices, architectural standards, and guidance across three areas of excellence: cloud financial management; cloud operations; and cloud security and compliance.

Create internal **support teams to provide advisory services** and support to agencies with integrating or building new cloud services.



#### Government Data Center and Cloud Service project in Thailand

Thailand implemented this project to create a central government cloud system, that included extensive training for 2,500 employees. This has been further built out into a certification programme with three levels of certification: Essential, Advanced and Expert.

# Recommendations for moving to the cloud

To promote and increase cloud adoption in the public sector, Governments should implement a set of actions.



## RESOURCES AND BUDGETS

### 01 | Optimise resources cost and utilisation

**Decommission idle or unused infrastructure** to avoid resistance, due to legacy infrastructure, against moving to cloud computing.

**Analyse performance metrics** (e.g. for CPU, memory, network, disk) **to right-size assets and optimise costs:** identify and make adjustments to these assets, and reclaim funds that can be reallocated to other mission-critical projects or initiatives. This is especially critical with the growing use of cloud services and the adoption of a multi-cloud strategy.

**Identify opportunities to take advantage of pricing discounts offered by CSP**, for instance by using a cloud management platform that helps with identifying purchase opportunities and managing discounts.

### 02 | Implement funding and procurement initiatives

**Update procurement rules and processes** to shift IT expenditures from capital to operating costs, since the cloud payment model (pay-as-you-go) differs from the traditional ICT payment model (pay-once).

**Create agile funding models to ensure effective use of IT funds** and, consequently, improve operational efficiency which help agencies make more frequent and accurate spending decisions.

Ensure that chief financial officers and finance departments **understand the importance of the rules**, processes and models for cloud adoption to keep abreast of cloud service updates to estimate and manage costs more efficiently.



#### Germany created a new platform for public tenders and established new rules for CSP

The German government requires that public tenders are published via the Bund.DE platform if they fall below EU-mandated price thresholds. Companies submitting tenders must respond via the eVergabe platform. In addition, CSP wishing to sell services to the federal government must sign a non-disclosure agreement to protect and prohibit access to German data in foreign jurisdictions ;and sensitive government information is stored on servers in Germany. The German government's IT security office, the BSI, only permits the use of certified CSP that are included in the Cloud Computing Compliance Controls Catalogue.



# References



Deloitte, Tech Trends 2021: A government perspective (December 2020)  
Deloitte, Seven pivots for government's digital transformation (May 2021)  
Gaia-X, [www.gaia-x.eu](http://www.gaia-x.eu) (accessed on October 2021)  
ESMA, Guidelines on outsourcing to cloud service providers (May 2021)  
BMW, [Using the intelligent Chatbot to reduce Helpdesk Tickets](#) (accessed on October 2021)  
European Commission, [Data Protection](#) (accessed on October 2021)  
ENISA, [ENISA Topics](#) (accessed on October 2021)  
European Commission, [EU-US data transfers](#) (accessed on October 2021)  
European Commission, [Standard Contractual Clauses](#) (accessed on October 2021)  
EU Cloud CoC, [Your path to trusted cloud services in Europe](#) (accessed on October 2021)  
European Commission, [A European Strategy for data](#) (accessed on October 2021)  
European Commission, [The Digital Europe Programme](#) (accessed on October 2021)  
European Commission, [NextGenerationEU](#) (accessed on October 2021)  
European Commission, [The Recovery and Resilience Facility](#) (accessed on October 2021)  
European Commission, [European Alliance for Industrial Data, Edge and Cloud](#) (accessed on October 2021)  
European Commission, [European data strategy](#) (accessed on October 2021)  
European Commission, [The Connecting Europe Facility regulation](#) (accessed on October 2021)  
European Commission, [Connecting Europe Facility — CEF Digital](#) (accessed on October 2021)  
European Commission, [European Defence Fund \(EDF\)](#) (accessed on October 2021)  
Microsoft, [Answering Europe's Call: Storing and Processing EU Data in the EU](#) (accessed on October 2021)  
Microsoft, [EU Data Boundary for the Microsoft Cloud](#) (accessed on October 2021)  
Microsoft, [EU Data Boundary for the Microsoft Cloud](#) (accessed on October 2021)  
AWS, [AWS and EU data transfers](#) (accessed on October 2021)  
AWS, [How AWS is helping EU customers with data protection](#) (accessed on October 2021)  
UK Government, [Cloud Native Development Services](#) (accessed on October 2021)  
UK Government, [Cloud guide for the public sector](#) (accessed on October 2021)  
UK Government, [Zero Trust Principles](#) (accessed on October 2021)  
UK Government, [Cloud Security Guidance](#) (accessed on October 2021)  
Australian Government, [Digital Transformation Agency](#) (accessed on October 2021)  
Australian Government, [Secure Cloud Strategy](#) (accessed on October 2021)  
US Government, [Federal Cloud Computing Strategy](#) (accessed on October 2021)  
Canada Government, [Right Cloud Selection Guidance](#) (accessed on October 2021)  
Canada Government, [Security Control Profile for Cloud-based GC Services](#) (accessed on October 2021)  
Canada Government, [Cloud Adoption Strategy](#) (accessed on October 2021)





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.