H-CLOUD

Cloud Computing in Europe

Appendix 4

Public Administration

15 July 2020

h-cloud.eu

Title	Cloud Computing in Europe. Appendix 4: Public Administration
Lead Editor	Massimiliano Claps
Contributors (in alphabetical order)	Massimiliano Claps
Version	0.7
Date	15 July 2020
Confidentiality Notice	**Confidential** - The information contained in this document and any attachments are confidential. It is governed according to the terms of the project consortium agreement

Important Notice: Working Document

This briefing is an annex to the Green Paper v 0.7. The Green Paper is an outcome of the H-CLOUD project, a Coordination and Support Action that has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement n. 871920.

1. CONTENTS

1 INTRODUCTION

Governments have experienced various waves of reform over the past 25 years. The application of market-oriented mechanisms and enterprise management principles and the usage of digital technologies transformed public service delivery and operating models. The public sector has made significant progress in terms of moving away from bureaucracy as an end in itself. Nowadays, governments strive to combine the transparency and repeatability of bureaucratic processes, with the agility to collaborate across agencies and departments, re-organize workflows around the needs of the citizen (or groups of citizens), draw insights from data for evidence based policymaking, service planning and management and operational efficiency.

Governments continuously improve their ability to deliver efficient, trusted, responsive, inclusive and convenient services for all. Digital technologies, such as mobile computing, analytics and artificial intelligence, the Internet of Things, and cloud computing are empowering public sector executives to accelerate this transformation. In particular, cloud computing is an enabler of many other capabilities, rather than an end in itself. It accelerates testing, developing and deploying services that are natively designed for consumption across multiple channels (online, mobile apps, chatbots). It enhances the elasticity to accommodate peak usage for high-volume services, like intake of tax declarations, student applications, farm subsidies applications, and emergency event management. It helps scale the ability to ingest data and process events coming from new sources, such as Internet of Things device feeds in smart cities.

European governments, with support from European Commission strategic policies, such as the Digital Single Market eGovernment Action Plan, and funding programs, such as Horizon 2020, have piloted, adopted and scaled the usage of cloud computing to accelerate digital transformation. However, challenges remain in terms of realizing the full potential of cloud in the public sector. Data sovereignty concerns, system migration and data portability constraints, skill gaps are some of the hurdles for the public sector, when it comes to embracing the cloud.

2 CONTEXT

Citizens expect governments to be good stewards of their taxpayer money. They want governments to act transparently, while protecting their privacy. They want their requests to be resolved rapidly. They expect to access high-quality service regardless of their income, ethnicity, physical and mental abilities. And they want to access those services, when, where and how they prefer, just like they are used to when dealing with private companies. Digital technologies are enabling European governments to bring together those strategic goals.

The EU eGovernment Action Plan 2016-2020 states that "*eGovernment supports administrative processes, improves the quality of the services and increases internal public sector efficiency. Digital public services reduce administrative burden on businesses and citizens by making their interactions with public administrations faster and efficient, more convenient and transparent, and less costly. In addition, using digital technologies as an integrated part of governments' modernization strategies can unlock further economic and social benefits for society as a whole. The digital transformation of government is a key element to the success of the Single Market.*" The plan further recommends that: "*public administrations and public institutions in the European Union should be open, efficient and inclusive, providing borderless, personalized, user-friendly, end-to-end digital public services to all citizens and businesses in the EU.*" Confirming the commitments of the Action Plan, the 2017 Tallin Ministerial Declaration on eGovernment states that "the *overall vision remains to strive to be open, efficient and inclusive, providing borderless, interoperable, personalised, user-friendly, end-to-end digital public services to all citizens and businesses – at all levels of public administration*". The key goals of the Tallin declaration are:

- Digital by default, inclusiveness and accessibility
- The once only principle
- Trustworthiness and security
- Openness and transparency
- Interoperability by default

Fostered by European Union policy guidelines and by international best practices, European public administrations are embracing a future where efficiency, agility, civil servant empowerment, cross agency and cross border collaboration augment the value of transparent and accountable government bureaucracies with the end goal of improving the citizen experience. A 2019 IDC survey of European government executives confirms that improving citizen experience, ensuring openness and transparency is the top priority.

62% of European executives consider "Improving citizen experience, ensuring openness and transparency" the top business priority for their organization, in 2020. The list of top three priorities includes "Reducing operational and/or capital expenditure, streamlining processes", at 61% and "Creating new services and channels" at 60%.

Source: IDC European Tech and Industry Pulse Survey - conducted in Q3 2019 and including 291 central and local government IT and non-IT executives, across Europe

The transformation of European governments is underpinned by the adoption of online services, mobile applications and social media that are enabling an omni-channel service delivery strategy that improves convenience for citizens. They are combining omni-channel platforms with advanced analytics and artificial intelligence to gain insights into citizen needs that enable them to proactively orchestrate services to make them relevant to groups of constituents and make processes more responsive. Furthermore, European public administrations will play a key role in the data economy, not just because of the opportunity to share and use more intelligently data within the public sector, but also because of:

- The opportunity to use privately-held data to improve evidence-driven policy-making and public services

- The opportunity to make public sector information available to businesses and civil society.

In fact, the EU Strategy for Data (EUSD) identifies the public sector as a cornerstone of this future scenario[1] and proposes both cross-sector data spaces as well as common European **data spaces for public administrations. Specific support is contemplated for** public procurement data covering both national and EU dimensions, as well as common standards and interoperable frameworks for legal information.

European member states' initiatives are also supporting the policy drive towards strategic use of data in public administrations. For example the French 'LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique', allowing the public sector to access certain (private sector) data of general interest or the Finnish Forest Act obliging forest owners to share information related to the management of the forest with the public sector. To realize the benefits of those opportunities, the implementation of the EUSD will have to take into account the role that open data spaces can play and the architectural capabilities that are necessary (see figure 1).

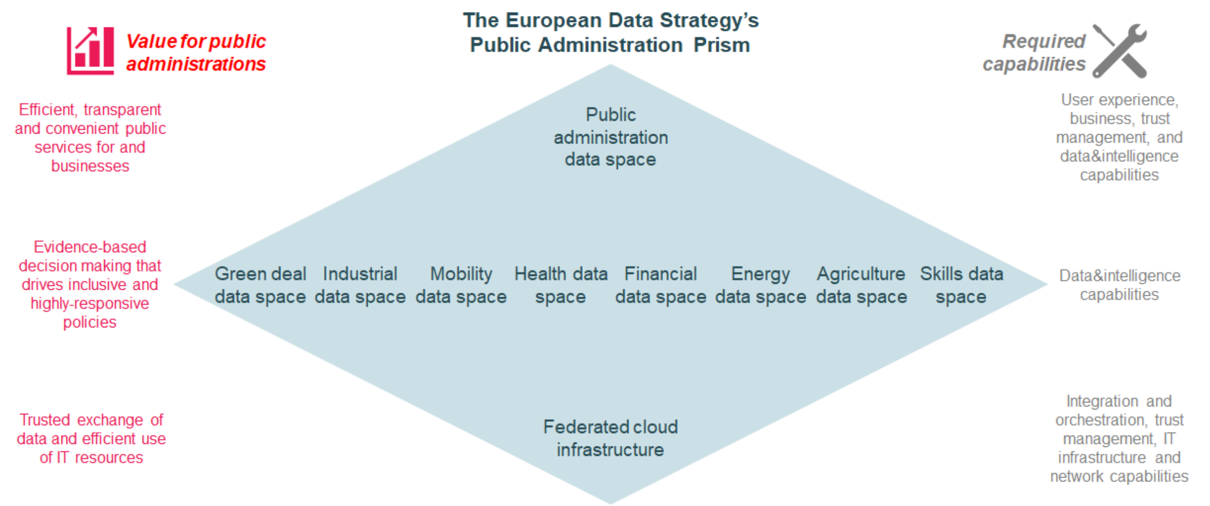
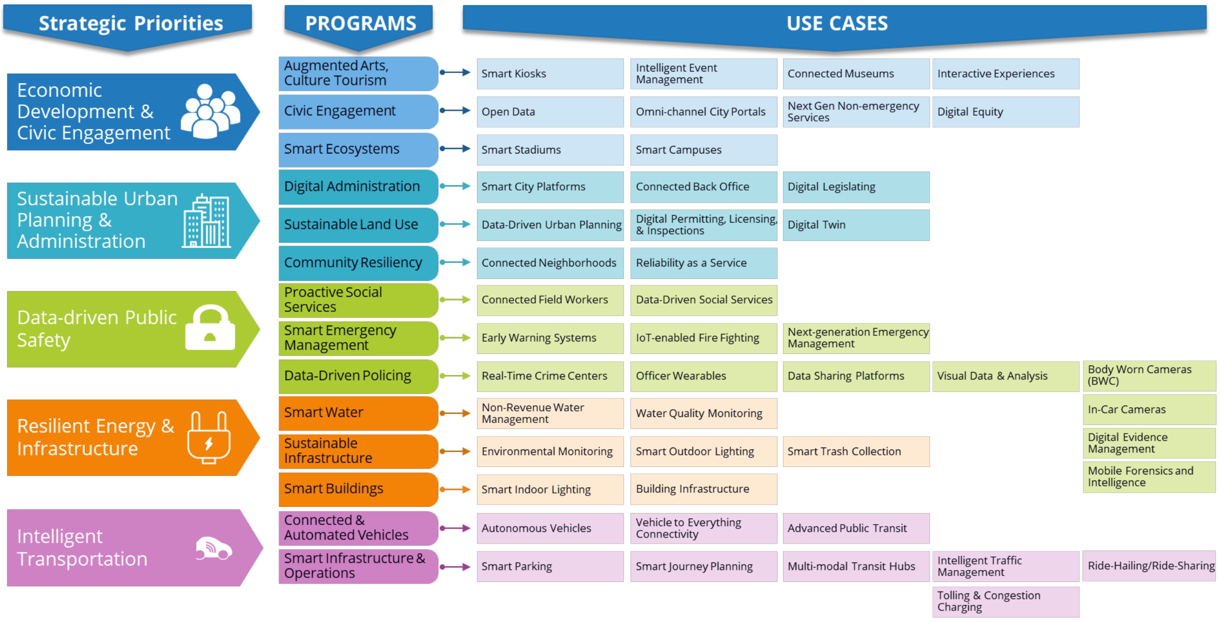

Value for public administrations
The European Data Strategy's Public Administration Prism
Required capabilities
Efficient, transparent and convenient public services for and businesses
Evidence-based decision making that drives inclusive and highly-responsive policies
Trusted exchange of data and efficient use of IT resources
Public administration data space
Green deal data space
Industrial data space
Mobility data space
Health data space
Financial data space
Energy data space
Agriculture data space
Skills data space
Federated cloud infrastructure
User experience, business, trust management, and data&intelligence capabilities
Data&intelligence capabilities
Integration and orchestration, trust management, IT infrastructure and network capabilities

Figure 1. The value of federated data spaces for the European public administration

Governments, in particular local and regional governments, are also taking a leading role in the context of smart cities. They are orchestrating the ecosystem of utilities, transportation companies, real-estate developers to connect applications with IoT devices to embed intelligent event processing in core business processes, such as economic development & civic engagement, sustainable urban planning & administration, data-driven public safety, resilient energy & infrastructure, intelligent transportation (see figure 2). This leadership role includes appropriating the budget for the duration of the project. Whether the source of funding was the municipality itself, a European Commission research and innovation program, or a national government innovation program; city officials must set a clear financial anchor for two or three years. Without that anchor funding, the ecosystem does not commit their own resources to some vague public-private partnership.

[1] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy



Strategic Priorities	PROGRAMS	USE CASES				
Economic Development & Civic Engagement	Augmented Arts, Culture Tourism	Smart Kiosks	Intelligent Event Management	Connected Museums	Interactive Experiences	
	Civic Engagement	Open Data	Omni-channel City Portals	Next Gen Non-emergency Services	Digital Equity	
	Smart Ecosystems	Smart Stadiums	Smart Campuses			
Sustainable Urban Planning & Administration	Digital Administration	Smart City Platforms	Connected Back Office	Digital Legislating		
	Sustainable Land Use	Data-Driven Urban Planning	Digital Permitting, Licensing, & Inspections	Digital Twin		
	Community Resiliency	Connected Neighborhoods	Reliability as a Service			
Data-driven Public Safety	Proactive Social Services	Connected Field Workers	Data-Driven Social Services			
	Smart Emergency Management	Early Warning Systems	IoT-enabled Fire Fighting	Next-generation Emergency Management		
	Data-Driven Policing	Real-Time Crime Centers	Officer Wearables	Data Sharing Platforms	Visual Data & Analysis	Body Worn Cameras (BWC)
Resilient Energy & Infrastructure	Smart Water	Non-Revenue Water Management	Water Quality Monitoring			In-Car Cameras
	Sustainable Infrastructure	Environmental Monitoring	Smart Outdoor Lighting	Smart Trash Collection		Digital Evidence Management
	Smart Buildings	Smart Indoor Lighting	Building Infrastructure			Mobile Forensics and Intelligence
Intelligent Transportation	Connected & Automated Vehicles	Autonomous Vehicles	Vehicle to Everything Connectivity	Advanced Public Transit		
	Smart Infrastructure & Operations	Smart Parking	Smart Journey Planning	Multi-modal Transit Hubs	Intelligent Traffic Management	Ride-Hailing/Ride-Sharing
					Tolling & Congestion Charging	

Figure 2. Smart Cities Priorities and Use Cases[2]

Cities have been investing into smart cities programs for almost ten years, but many failed to scale pilot projects because they encountered governance, technical and regulatory challenges. The result of those investments was often a plethora of fragmented pilot projects that did not scale from a corridor or neighborhood to the entire city. Or segments of the resident population were excluded from the intended benefits. Or technology solutions were not re-usable across cities, thus did not allow for efficient cross-border best practice exchange and did not enable tech suppliers to generate solid revenue growth that can be re-invested in further innovation. In the past two years, many European cities have started to achieve the intended improvements in quality of life, economic prosperity and resilience. The cities that succeeded in orchestrating the ecosystem appropriated budget. They set up programs to make sure that all residents were included in the benefits. They managed to deliver quick wins in specific use cases, and then re-use the modular solutions they had built to extend the capabilities across the whole community. To realize the benefits of the significant investments that will go into smart cities in the coming years, these good practices should spread around the region, and solve open ecosystem governance, technical interoperability and regulatory challenges, such as the balance between data protection and potential benefits of artificial intelligence.

European spending on Smart Cities initiatives related technologies is expected to grow from $33.7 billion in 2020 to **$49.3 billion** in 2023

Source: IDC Worldwide Semi-annual Smart City Spending Guide, December 2019

[2] Source: IDC Smart Cities Use Cases

3 ANALYSIS

In the IT back end, the European public sector cycle of continuous innovation is supported by multi-tier architectures, where systems are decoupled from vertically integrated stacks to layers of computing, data management, modular application micro-services and people-centric user interfaces. So that processes can be orchestrated in an agile manner, and data can be shared flexibly through application programming interfaces (APIs). These so called third platform architectures – as opposed to first platforms dominated by mainframes and second platforms characterized by the two tiers of clients-server – require more elasticity to scale services up and down at low cost, must secure access to capabilities from any device across an expanding network edge, need IT management processes that iterate between development and operations in an agile manner. This is what cloud computing and related application development and deployment approaches, like open source containers, enables governments to do.

3.1 Demand side analysis

European governments have adopted all types of cloud computing deployment models, from public cloud, to on-premise private clouds (see figure 3); thus, they organically built more complex hybrid, multi-cloud environments. All countries have adopted policies and programs to promote cloud adoption:

- The UK was at the forefront with the G-Cloud program, which included a cloud-first policy, a cloud marketplace, security certification standards and a private cloud hosted service joint venture[3].
- Italy also published a cloud policy and more recently launched a service marketplace for certified providers of cloud services.
- France invested in the “Cloud de Confiance” initiative
- Poland’s Joint State IT Infrastructure Program (WIIP) was announced in 2019 and resulted in technical dialogues with service providers, pilot cloud computing projects, the launch of the Cloud Service Provisioning System (ZUCH) and the development of a Cloud Cybersecurity Standards (SCCO).

It must be noted that differences exist across countries, because of different stages of maturity. The UK HM Government was the earliest adopter of a program, leading the way with more than 30% of government organizations adopting public cloud. Whilst the two largest members of the European Union, Germany and France, where strict data sovereignty requirements and a fragmentation of IT demand across levels of government has kept public cloud adoption below 20%. With other countries, like Spain, Italy, the Netherlands and the Nordics that have learned lessons from the UK and, then, cautiously followed a similar model of creating cloud policies, supplier certification guidelines and government wide cloud contract frameworks.

[3] https://crownhostingdc.co.uk/

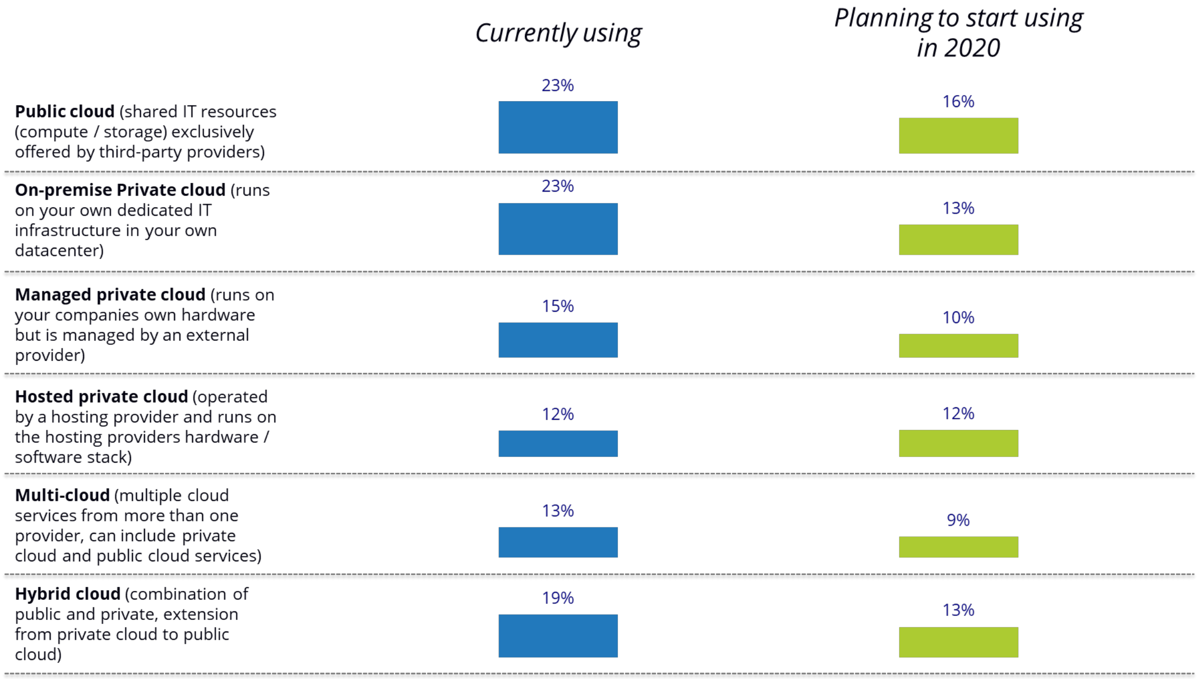


Figure 3. European Governments' Adoption of Cloud Computing by Deployment Model[4]

Notwithstanding the progress, cloud adoption in government remains well below that of other industries, like education institutions, retail and manufacturing companies, where rates of adoption of public cloud surpass 30%. The top barriers to public sector cloud adoption include:

- **Policy and regulatory concerns** –
  - Public sector executives need to comply with EU regulation like GDPR and the NIS directive that protect privacy of personal data and resilience of critical digital services. Those needs are hard to reconcile with the appetite to buy services from global cloud providers, whose headquarters are subject to legislation that supersedes EU regulation. (D-PA Challenge 1)
  - Across Europe there are no public procurement rules that mandate to "buy local" or "buy national", like there are in other countries, like the United States or China; however there is an overall push - including in the DIRECTIVE 2014/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on public procurement and repealing Directive 2004/18/EC - to simplify procurement practices to facilitate participation from SMEs.
- **Architectural constraints** –
  - Government executives want data and workload portability across providers and the ability to integrate cloud with legacy systems.
  - They expect application data architectures, application logic and user interfaces to adapt to their business processes.
  - They demand fine-grained elasticity at low marginal costs, including the ability to spin new workloads in emerging technology areas, such as training machine learning algorithms and managing IoT devices at the edge, such as video-cameras and environmental sensors. Public cloud contracts often include some form of threshold, whereby users have the purchase a minimum number of users within certain ranges.
  - In the case of niche industry specific requirements, global cloud providers that need to standardize services to offer low prices and fast innovation cannot offer fully aligned offerings, in particular at the SaaS level.

[4] Source: IDC European Tech and Industry Pulse Survey - conducted in Q3 2019 and including 291 central and local government IT and non-IT executives, across Europe

- **Organizational barriers** –
  - Many European government entities, particularly at the local government level, are small (see figure 4). They have a limited budget to acquire or train technical and business skills to develop, deploy and manage cloud services.
  - Their budgeting and procurement policies and processes are geared towards a strict distinction between capital expenditure to acquire systems and operating expenditure to run them.
  - IT operating models often rely on a centralized function that manages IT assets and services.

Cloud services require a shift towards operating expenditure and open up the door to "shadow IT" purchases from mission executives and managers that do not have a comprehensive view of how their choices impact overall costs, interoperability and system security.

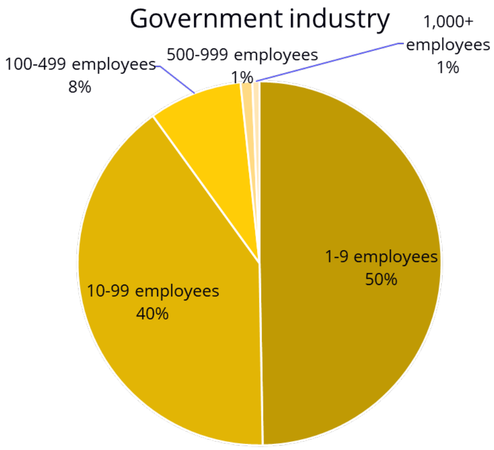


Figure 4. European Government industry Structure (Includes entities classified as "L-Public Administration, Defence and Compulsory Social Security activities" by NACE Rev. 2)[5]

3.1.1 Top cloud use cases

European government cloud adoption is not equal across use cases. Different applications have different needs in terms of regulatory compliance, architecture and organizational attributes. The combination of all factors determines whether governments run some of their systems on their own on-premise cloud data centers versus hosted private cloud and public cloud services.

The use cases **where security and data protection regulatory requirements are less stringent,** elasticity and scalability requirements are more pressing, and organizational change is less complex to implement tend to run on public cloud or hosted private clouds. This is for example the case for (see figure 5) application development and testing, website hosting, storage. And increasingly for ERP and CRM applications, where global software suppliers have migrated their portfolio to the cloud, for use cases like HR, order management and contact center management.

Conversely, use cases, **where security and data protection requirements are more stringent,** elasticity and scalability requirements are not as important, while the need to integrate with many legacy systems and processes prevail, and organization change is complex, because it touches the core of government operations, tend to run on legacy architectures in on-premise data centers. This is the case of industry-specific solutions, like public safety command and control center, tax and other revenue collection applications, welfare benefit management.

[5] Source: IDC analysis based on Eurostat and National Statistical Offices

Emerging technologies, like the Internet of Things, artificial intelligence, and blockchain are at an early stage of adoption in the public sector. This means they require **fast iterations** to develop and test new solutions, before they can be scaled. Also, they can be **computing intensive** in terms of volume and speed of data ingestion (e.g. security camera data feeds), consumption of vast amounts of data (e.g. training of anti-fraud ML algorithms), and recording of transactions (e.g. blockchain enabled land registries). These characteristics make IoT, AI and Blockchain use cases not only suitable for cloud computing, in many cases implementation of these emerging technologies almost requires the use of cloud computing, since "on premise" deployments are impractical. For example in the context of smart cities, where there is the need to scale capabilities like device management, data exchange, predictive analytics and dashboarding across use cases, these capabilities are readily available as cloud services.

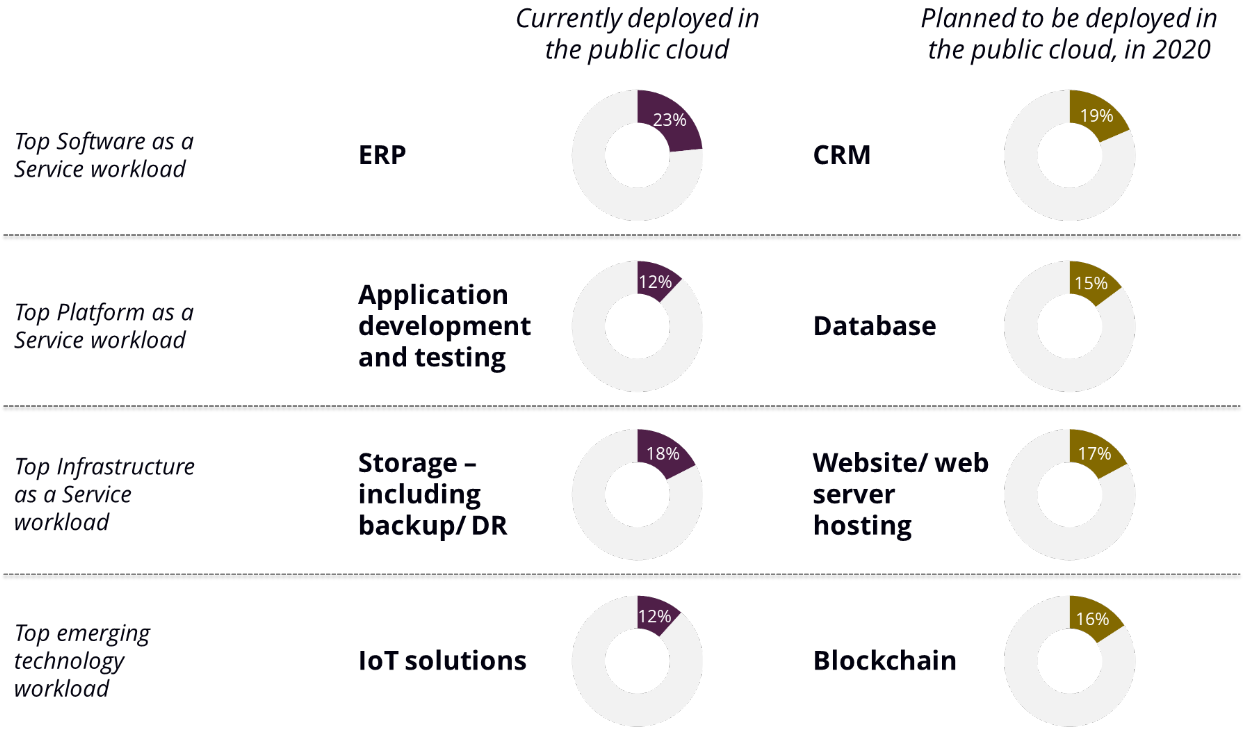


Figure 5. European Governments' Top PUBLIC Cloud Use Cases[6]

3.2 Supplier analysis

The European public sector purchases cloud capabilities and services from a variety of channels, from local resellers to cloud marketplaces. The choice depends on the size of the public sector organizations, whereby smaller agencies and smaller regional and local councils, rely on local resellers, whereas large national government departments often buy from European or global suppliers, as part of broader contracts. The choice of channel also depends on the type of deployment model and workloads, because agencies that want to buy a few instances of storage as a service in the public cloud to build a backup copy of a non-sensitive data set will go directly to a cloud service provider, while a government organizations that needs to use the cloud to integrate legacy back office systems with a new digital front-end in a secure manner will need the expertise of a systems integrator. Government cloud procurement policies also influence purchasing behaviors, for instance the UK government G-cloud framework and marketplace, drove over £5bn of cloud related spending, of which 44% with small and medium enterprises.

[6] Source: IDC European Tech and Industry Pulse Survey - conducted in Q3 2019 and including 291 central and local government IT and non-IT executives, across Europe

3.2.1 Coordinated supplier arrangements and analysis

The European public sector has a long history of IT service coordinated provisioning. Government agencies within individual Union Member States and across European borders have cooperated to design, develop and deliver IT solutions for thirty years. These collaborations took various shapes and forms, in terms of governance and operating models:

1. Regional shared services centers were set up in countries including Denmark, Finland, Italy, Germany, Spain and the UK. The goal was to achieve higher critical mass across neighboring regional and local governments to increase operational efficiency and quality of service. Some of these were set up as a central entity, others operated as decentralized peer networks.
2. Whole of government services were deployed, at the national government level, to have standard services, such as one-stop-shop citizen portals, citizen identity management, electronic signature, e-procurement and e-invoicing. The strategic goal was to reduce duplication of efforts across all levels of government. In some cases, these services were delivered by a central government entity, usually within a large cabinet level department, in other cases, a central policy/strategy agency set the procurement framework, but then tasked third-party suppliers to deliver services that were mandated to interoperate with a common standard node. In this respect, two parallel initiatives undertaken by the UK Government Digital Service, Verify (a federated identity service that failed to meet expectations) and Notify (a notification service used by nearly 500 organizations in more than 1,500 public services, which is estimated to save taxpayers £35 million a year), indicated that the difference between success and failure is due to: setting ambitious but achievable targets, delivering key milestones, rather than expecting one big-bang go live date, defining clear accountability for the solution development, listening to feedback from the government entities using the service.
3. European grids were created to deliver services to academic and research centers. Their primary goal was to offer knowledge sharing and computational capabilities at scale. Most of them operate through a dedicated legal entity that was jointly governed by institutional users.
4. European Union programs supported innovative digital services that could be scaled in member countries or become cross-border services - in domains like tax, customs, immigration, and smart cities platforms - to empower European citizens and businesses to have a seamless experience across the Digital Single Market.

These collaborative programs offer many lessons on the strength, weaknesses, opportunities and threats of collaborative supply of IT services in the public sector that can be leveraged when designing the strategy and governance of a federated cloud service:

- Strengths – The key strengths of public sector IT collaboration are the deep domain expertise, which comes from establishing and nurturing a close relationship with the user community, and the openness to share best practices across that community. These shared services also offered the opportunity to create a critical mass in an industry where demand is very fragmented.
- Weaknesses – The weakest link of collaborative IT service development, deployment and delivery across public sector entities is the complexity of governance. Designing and enforcing the structure and processes that are needed to make decisions on strategy, architecture, budgeting, procurement, management of IT assets, capabilities and services across multiple government departments and jurisdiction is a slow process that can lead to suboptimal results, where political balance of power can prevail over efficient resource allocation.
- Opportunities – Government shared IT services and collaborative programs at the national and international level have a unique opportunity to embrace cloud computing as a delivery model, while embedding their deep domain expertise into the cloud services that they develop, creating true community clouds that standard public cloud services cannot match. In their role as community cloud providers, public sector shared services/federated operations should make decisions on what they operate directly and what they broker. Given the higher level of industry specific requirements at the application layer and much lower at the infrastructure layer, public sector community clouds should become brokers of IaaS providers and concentrate on developing and operating both “public sector suitable” PaaS and “public sector specific” SaaS.

- Threats – The biggest threat to IT collaboration across public sector entities comes from commercial ICT suppliers, particularly the global ones, that have a scale and pace of innovation that public sector entities and programs cannot match, because of the governance complexities.

4 INFRASTRUCTURE COMPONENT ANALYSIS

European public administrations and the EU private sector use many of the same underlying capabilities of cloud computing: computing provisioning, storage, connectivity, and cloud performance monitoring at the infrastructure layer, service and process orchestration, load balancing, data ingestion, aggregation and visualization at the platform layer, and CRM, ERP and analytics at the application layer.

Public sector organizations also have specific business and technical needs, including:

- At the application layer: revenue collection, public safety dispatch and investigation, social service case management.
- At the platform layer: context specific APIs, messaging, open data management, identity and access management, master data management, application of ethical data governance principles to artificial intelligence, and security and data protection governance.
- At the interface with edge infrastructure: management of edge devices, such as police officer wearable cameras.

At the platform level, these requirements apply across multiple government use cases, missions and across borders, pointing to an opportunity to develop those capabilities and scale them into a financially sustainable offering. The European Union is already supporting projects, such as PolicyCloud and NextGEOSS, where cloud-based data platforms can help deliver capabilities for evidence based policy-making. These projects address a range of policy challenges, including climate resilience, environmental monitoring, food security and fighting radicalization, but they could be extended to transportation and critical infrastructure planning, public health, education and other key policy areas.

Other European federated cloud initiatives, such as IDS and GAIA-X, can help accelerate the realization of the benefits of cloud computing in public administrations. It will be important that they make sound governance choices that enable them to dynamically orchestrate a catalogue of service that they will provide directly vs. those that will be brokered from trusted public cloud providers.

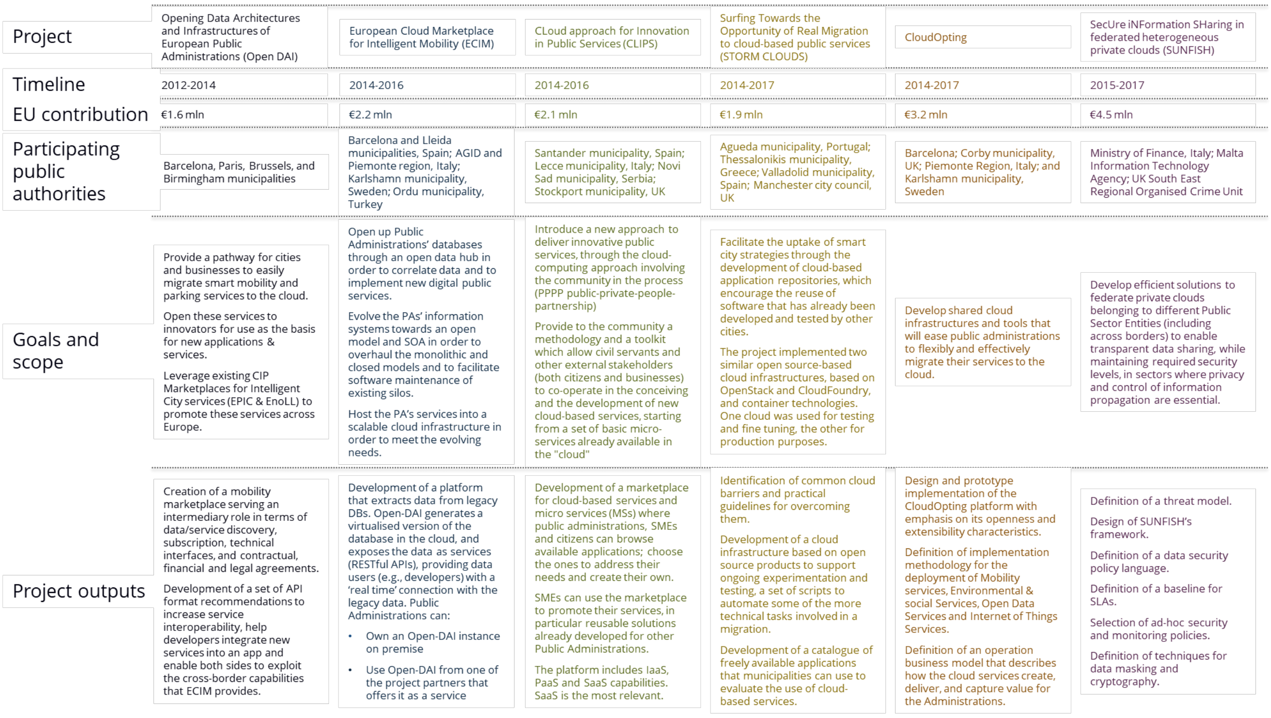
5 R&I PROJECT ANALYSIS

The European Commission has funded and orchestrated several projects to help European public administrations adopt cloud computing. A review of some key projects indicates that (see figure 6):

- There has been a strong focus on filling the technology gaps, particularly in terms of PaaS services that facilitate secure sharing of public data (both open and more sensitive datasets).
- Outcomes of projects included many toolkits, methodologies, ontologies that can be reused across member states.
- Most projects saw the active participation of city/municipal administrations, which resulted in many smart cities use cases being the focus of prototypes and outcomes.
- A strong emphasis was placed on open source components, but commercial solutions were also considered and involved in many of the projects.
- Various exploitation models were explored, from public sector entities participating in the projects that became operators of the services, to disseminating toolkits so that commercial providers could embed them into their own solutions, to creating dedicated legal entities (private or PPPs) to become operators.

On the matter of exploitation models, an analysis of two archetypes can provide some lessons learned:

- At one end, the projects that tasked the participants to become operators of the services, usually failed to scale. These projects were valuable for the participating entities, because they empowered public administrations to experiment with leading edge solutions that otherwise would not have been funded, because budgets would have been appropriated for less risky technology investments. Many also developed solutions that were based on open standards, so technical re-usability was guaranteed. But business re-usability was not. That means no investment was dedicated to build the product management, marketing and sales management and support services that allow a typical commercial IT provider to grow their business. As a consequence, the uptake of these solutions beyond the project participants was minimal. Many of the cloud projects described in figure 5 experienced this situation.
- At the other end, the projects that promoted the uptake of standard, reusable components among commercial IT suppliers that already had the product management, marketing and sales and support services capabilities experienced slightly higher take up. One example of such projects is FIWARE. Although not strictly a cloud project, FIWARE was initiated as an EC Funded project, it blossomed into a framework of open source platform components that experienced good take up. In particular, its core capability, the context-broker that aggregates and processes data by making them relevant for specific use cases through RESTful APIs, is experiencing a good take up in the smart cities space across many European countries, from Spain, to France, to Italy, to Portugal and so forth. One of the key success factors of FIWARE was the creation of a foundation participated by Atos, Engineering, Orange, and Telefónica. The foundation nurtured the community, by empowering developers and users to adopt FIWARE, promoting the platform across the ecosystem, continuously augmenting its capabilities, protecting the trademark and code of conduct, and validating usage through quality assurance, training and advisory services.



Project	Opening Data Architectures and Infrastructures of European Public Administrations (Open DAI)	European Cloud Marketplace for Intelligent Mobility (ECIM)	CLoud approach for Innovation in Public Services (CLIPS)	Surfing Towards the Opportunity of Real Migration to cloud-based public services (STORM CLOUDS)	CloudOpting	SecUre iNFormation SHaring in federated heterogeneous private clouds (SUNFISH)
Timeline	2012-2014	2014-2016	2014-2016	2014-2017	2014-2017	2015-2017
EU contribution	€1.6 mln	€2.2 mln	€2.1 mln	€1.9 mln	€3.2 mln	€4.5 mln
Participating public authorities	Barcelona, Paris, Brussels, and Birmingham municipalities	Barcelona and Lleida municipalities, Spain; AGID and Piemonte region, Italy; Karlshamn municipality, Sweden; Ordu municipality, Turkey	Santander municipality, Spain; Lecce municipality, Italy; Novi Sad municipality, Serbia; Stockport municipality, UK	Agueda municipality, Portugal; Thessalonikis municipality, Greece; Valladolid municipality, Spain; Manchester city council, UK	Barcelona; Corby municipality, UK; Piemonte Region, Italy; and Karlshamn municipality, Sweden	Ministry of Finance, Italy; Malta Information Technology Agency; UK South East Regional Organised Crime Unit
Goals and scope	Provide a pathway for cities and businesses to easily migrate smart mobility and parking services to the cloud. Open these services to innovators for use as the basis for new applications & services. Leverage existing CIP Marketplaces for Intelligent City services (EPIC & EnoLL) to promote these services across Europe.	Open up Public Administrations' databases through an open data hub in order to correlate data and to implement new digital public services. Evolve the PAs' information systems towards an open model and SOA in order to overhaul the monolithic and closed models and to facilitate software maintenance of existing silos. Host the PA's services into a scalable cloud infrastructure in order to meet the evolving needs.	Introduce a new approach to deliver innovative public services, through the cloud-computing approach involving the community in the process (PPPP public-private-people-partnership) Provide to the community a methodology and a toolkit which allow civil servants and other external stakeholders (both citizens and businesses) to co-operate in the conceiving and the development of new cloud-based services, starting from a set of basic micro-services already available in the "cloud"	Facilitate the uptake of smart city strategies through the development of cloud-based application repositories, which encourage the reuse of software that has already been developed and tested by other cities. The project implemented two similar open source-based cloud infrastructures, based on OpenStack and CloudFoundry, and container technologies. One cloud was used for testing and fine tuning, the other for production purposes.	Develop shared cloud infrastructures and tools that will ease public administrations to flexibly and effectively migrate their services to the cloud.	Develop efficient solutions to federate private clouds belonging to different Public Sector Entities (including across borders) to enable transparent data sharing, while maintaining required security levels, in sectors where privacy and control of information propagation are essential.
Project outputs	Creation of a mobility marketplace serving an intermediary role in terms of data/service discovery, subscription, technical interfaces, and contractual, financial and legal agreements. Development of a set of API format recommendations to increase service interoperability, help developers integrate new services into an app and enable both sides to exploit the cross-border capabilities that ECIM provides.	Development of a platform that extracts data from legacy DBs. Open-DAI generates a virtualised version of the database in the cloud, and exposes the data as services (RESTful APIs), providing data users (e.g., developers) with a 'real time' connection with the legacy data. Public Administrations can: • Own an Open-DAI instance on premise • Use Open-DAI from one of the project partners that offers it as a service	Development of a marketplace for cloud-based services and micro services (MSs) where public administrations, SMEs and citizens can browse available applications; choose the ones to address their needs and create their own. SMEs can use the marketplace to promote their services, in particular reusable solutions already developed for other Public Administrations. The platform includes IaaS, PaaS and SaaS capabilities. SaaS is the most relevant.	Identification of common cloud barriers and practical guidelines for overcoming them. Development of a cloud infrastructure based on open source products to support ongoing experimentation and testing, a set of scripts to automate some of the more technical tasks involved in a migration. Development of a catalogue of freely available applications that municipalities can use to evaluate the use of cloud-based services.	Design and prototype implementation of the CloudOpting platform with emphasis on its openness and extensibility characteristics. Definition of implementation methodology for the deployment of Mobility services, Environmental & social Services, Open Data Services and Internet of Things Services. Definition of an operation business model that describes how the cloud services create, deliver, and capture value for the Administrations.	Definition of a threat model. Design of SUNFISH's framework. Definition of a data security policy language. Definition of a baseline for SLAs. Selection of ad-hoc security and monitoring policies. Definition of techniques for data masking and cryptography.

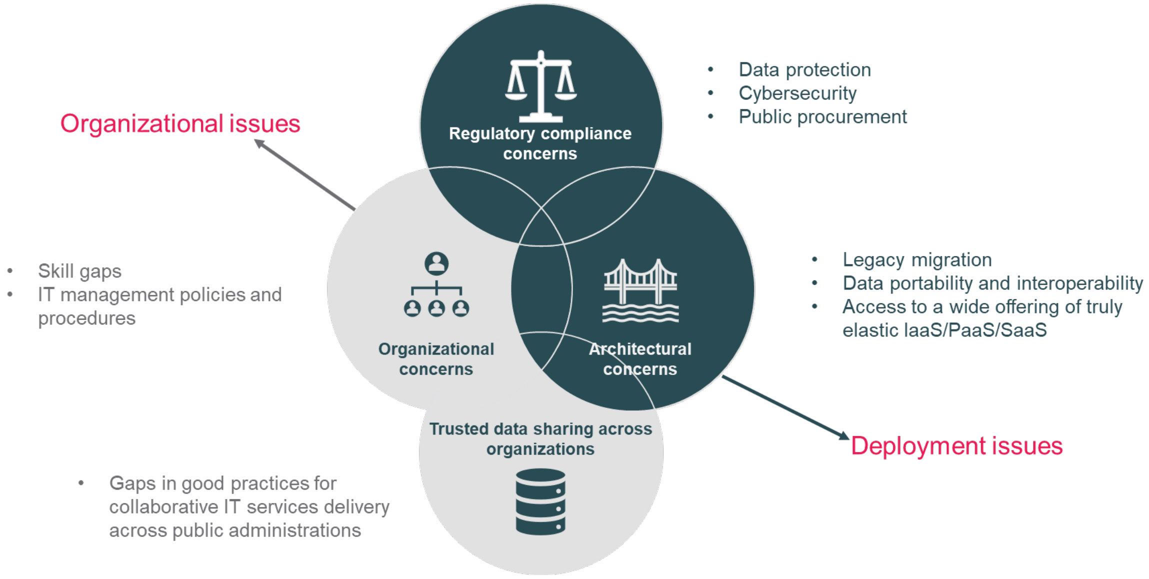
Figure 6. Overview of EC funded public administration cloud projects[7]

[7] Source: Cordis and projects' websites

6 CONCLUSIONS

European public administrations are embracing cloud computing as a key enabler of digital transformation of public services. However, they are late adopters compared to other industries because of (see figure 8):

- **Regulatory compliance concerns**, around data protection, sovereignty, security and public procurement.
- **Architectural constraints**, about migration of legacy, portability, interoperability and cost of truly elastic resources.
- **Organizational barriers**, such as skill gaps and IT management policies and procedures.
- Trusted data sharing across organization, such as a gap in good practices for data and service sharing


Organizational issues
Regulatory compliance concerns
• Data protection
• Cybersecurity
• Public procurement
• Skill gaps
• IT management policies and procedures
Organizational concerns
Architectural concerns
• Legacy migration
• Data portability and interoperability
• Access to a wide offering of truly elastic IaaS/PaaS/SaaS
Trusted data sharing across organizations
Deployment issues
• Gaps in good practices for collaborative IT services delivery across public administrations

The European Commission can coordinate efforts across member states in all three areas to enable European public administrations to realize the benefits of cloud computing.

- Policy and regulatory compliance
  - To grow trustworthiness of cloud among public sector end-users and favor more homogeneous adoption of cloud across the European Union the EC should:
    - Collect and share best practices on data sovereignty and security across public sector entities.
    - Promote standard certification and auditing instruments that make it easier for cloud providers to comply with existing regulation and help public sector cloud buyers gain more transparent understanding of contractual conditions.
    - Continue to negotiate agreements with non-EU countries to prompt harmonization with the EU rules that are considered a global best practice.
  - Innovative procurement – the launch of one or more federated cloud initiative should be set up as a vehicle to facilitate market participation for European SMEs, because the federation would allow them to achieve higher critical mass, while operating within a loosely coupled framework that let them pursue their competitive differentiators. The federation should not become a rigid, consolidated operating unit that cannibalizes SMEs market opportunities in the public and private sector
- Architecture development – to promote European innovations that can accelerate public sector legacy IT modernization, the EC should:
  - Make available research and innovation funding that help academia, public sector users and IT industry jointly develop capabilities that can fill the market gaps.

  - Stimulate the IT industry and academia to develop legacy to cloud migration toolkits that make best practices re-usable across member states.
  - Help academia, public sector users and IT industry prioritize industry specific platform capabilities that can be scaled across member states to achieve a larger critical mass. Focus in particular on data spaces, such as environmental protection, transport and critical infrastructure planning, safety and security, and public health, where collaboration can empower evidence-based decision-making.
- Organizational change – to nurture the competencies that help European public administration efficiently use cloud services, the EC should:
  - Encourage knowledge transfer between IT industry and public sector end users, for instance through internship, secondment programs. Leverage R&I projects through external validation and dissemination of findings.
  - Stimulate the IT industry and academia to develop cloud management toolkits that make best practices re-usable across member states.
  - Innovate procurement policies that allow public administration to pilot, select and scale cloud services in an agile manner.
- Data sharing – the European public sector has a long history of shared services, but it struggled to realize the benefits of those programs, beyond delivering affordable and reliable infrastructure to medium to small administrations that otherwise would not have the scale.

7 CHALLENGES AND RECOMMENDATIONS

D-PA Challenge 1: Difficulty complying with regulations like GDPR, NIS Directive. Public sector executives need to comply with EU regulations that protect privacy of personal data and resilience of critical digital services.

D-PA Recommendation 1: Collect and share best practices on data sovereignty and security across public sector entities.

D-PA Challenge 2: Limits in EU-regulatory-compliant products/services from existing CSPs (EU-based or otherwise). Comprehensive product suites from global CSPs are appealing but, in shared responsibility environment, they do not reduce risks for EU-based clients. Stringent security and data protection regulatory requirements drive public administrations to stay on premise or, at best, move to hosted private cloud deployments. Notable applications with such requirements include public safety command and control center, tax and other revenue collection applications, and welfare benefit management.

D-PA Recommendation 2: Promote standard certification and auditing instruments that make it easier for cloud providers to comply with existing regulation and help public sector cloud buyers gain more transparent understanding of contractual conditions.

Also D-PA Recommendation 10.2.

D-PA Challenge 3: Risk associated with using US-based CSPs and therefore being affected by US legislation. US CSPs are subject to US legislation, such as the CLOUD ACT, which supersedes EU regulation.

D-PA Recommendation 3: Continue to negotiate agreements with non-EU countries to prompt harmonization with the EU rules that are considered a global best practice.

D-PA Challenge 4: Integration of legacy Public Administration applications. It is challenging and expensive to integrate the many legacy systems found in public administration into cloud solutions, since they would need to be rewritten and/or re-architected.

D-PA Recommendation 4: To promote European innovations that can accelerate public sector legacy IT modernization, the EC should stimulate the IT industry and academia to develop legacy-to-cloud migration toolkits that make best practices re-usable across member states.

D-PA Challenge 5: Public Administration expects perfect IT adaptation. Government executives expect IT application data architectures, application logic and user interfaces to adapt to their business processes. This expectation results from a shortage of resources and limited awareness both of practices in other jurisdictions and the flexibility that might be available from current solutions.

D-PA Recommendation 5: Determine legacy requirements across the PA sector. Survey public administrations to characterize the functions of existing legacy systems, and common business practices, analyze to find common requirements, and analyze the gap with available solutions from ISVs (SaaS or not).

D-PA Challenge 6: Limited skills and expertise. Many European government entities, particularly at the local government level, are small. They have a limited budget to acquire or train technical and business skills to develop, deploy and manage cloud services. CSPs are not always able, or have the economic incentives to scale their support services to deal with the specific requirements of European public administrations

D-PA Recommendation 6: Favor coordinated procurement and management of cloud services. Support procurement of cloud services in a coordinated manner through national or regional cloud marketplaces. Favor exchanging best practices of shared IT services in government that can jointly manage cloud services across small entities.

D-PA Challenge 7: Budgeting, procurement and IT operating models are not well-suited to cloud-based solutions. Public administration budgeting and procurement policies and processes are geared towards a strict distinction between capital expenditure to acquire systems and operating expenditure to run them. IT operating models often rely on a centralized function that manages IT assets and services. By contrast, cloud services require a shift towards operating expenditure and potentially give mission executives and managers more flexibility in finding and procuring the cloud-based IT solutions that best meet their needs.

D-PA Recommendation 7.1: Encourage knowledge transfer between IT industry and public sector end users, for instance through internship, secondment programs. Leverage R&I projects through external validation and dissemination of findings.

D-PA Recommendation 7.2: Stimulate the IT industry and academia to develop cloud management toolkits that make best practices re-usable across member states.

D-PA Recommendation 7.3: Innovate procurement policies that allow public administration to pilot, select and scale cloud services in an agile manner. Make procurement policies and cloud services re-usable across member states.

D-PA Challenge 8: Success factors and best practices for providing coordinated IT services are not well understood. Public Administrations have explored a number of coordinated IT approaches, including federation, but the results of these initiatives have been mixed. Examples, successful and unsuccessful, can be found in regional shared service centres and whole-of-government efforts. Key success factors and best practices have not been identified.

D-PA Recommendation 8.1: Evaluate coordinated public administration IT service efforts. Identify and codify success factors and best practices found in successful regional shared service centres and whole-of-government efforts. Practices to examine include supplier certification guidelines, inclusion of services into the service catalogue based on a strategic Make-or-Buy analysis, and government wide cloud contract frameworks. Models such as federation (such as practised by EGI), and open standard foundations (such as FIWARE) should be considered.

D-PA Recommendation 8.2: Support innovative procurement from one or more coordinated cloud initiatives to facilitate market participation for European SMEs. Coordination, perhaps through best practices, identified in Recommendation 8.1, such as federation, would allow SMEs to achieve higher critical mass, while operating within a loosely coupled framework that lets them maintain their competitive differentiation. The initiatives should not become a rigid, consolidated operating unit that cannibalizes SMEs market opportunities.

D-PA Challenge 9: IT governance complexity in Public Administration hampers development and deployment of new solutions, regardless of technology or deployment model. Designing and enforcing the structure and processes that are needed to make decisions on strategy, architecture, budgeting, procurement, management of IT assets, capabilities and services across multiple government departments and jurisdiction is a slow process that can lead to suboptimal results, where political balance of power can prevail over efficient resource allocation.

D-PA Recommendation 9: Pilot coordinated IT development using best practice governance. Support efforts to coordinate development/deployment of IT capabilities using best practice governance identified in D-PA Recommendation 8.1.

D-PA Challenge 10: Public Administration requires comprehensive IaaS/PaaS solutions, which are primarily available from global providers/hyperscalers. The biggest threat to IT collaboration across public sector entities comes from commercial ICT suppliers, particularly the global ones, which have a scale and pace of innovation that public sector entities and programs cannot match because of the governance complexities. But high dependency on global hyperscalers increases the risks of lock-in with their technical solution, lack of control on the provisioning and continuity of services, such as in the case of pandemics or natural disasters.

D-PA Recommendation 10.1: Qualify/certify "public sector usable" IaaS solutions. These certifications should not only look at security and data protection requirements, but also at openness of solutions, agility to accommodate different deployment models, such as creating back up copies on premise without adding too much to the total cost of ownership of the solutions

D-PA Recommendation 10.2: Support efforts to develop/operate "public-sector-suitable" GDPR-compliant PaaS solutions. Support creation of PaaS solutions, in particular distributed data management solutions, to enable public administrations to work together, share data productively, while at the same time controlling access to proprietary and/or competitive data. Solutions should ensure GDPR compliance, as well as providing context specific APIs, messaging, open data management, identity and access management, master data management, application of ethical data governance principles to artificial intelligence, and security and data protection governance. More standard PaaS capabilities such as service and process orchestration, load balancing, data ingestion, aggregation and visualization should also be included.

D-PA Challenge 11: Public Administration requires sustainable sector-specific SaaS solutions, which either need to be developed or, if they exist, are challenged by limited markets. Major SaaS providers need to standardize services to offer low prices and fast innovation, and therefore cannot offer services that align well with Public Administration's "niche" requirements.

D-PA Recommendation 11: Facilitate/partner in the development of "public-sector-specific" SaaS solutions. In each functional area identified as a result of D-PA Recommendation 5, coordinate and support the affected community of public administrations and potential SaaS providers to develop awareness of solutions, track early or pilot implementations, and encourage broader adoption. Where there are significant, but common gaps in functionality, support efforts by ISVs to bridge those gaps and, if necessary, transition to appropriate public SaaS cloud solutions. Promising sector specific applications could include revenue collection, public safety dispatch and investigation, and social service case management. Focus as well on data spaces, such as environmental protection, transport and critical infrastructure planning, safety and security, and public health, where collaboration can empower evidence-based decision-making.

D-PA Challenge 12: Open standard based solutions have not always been successful. EC-supported efforts to support solutions for Public Administration have assumed that creating open standard-based solutions would ensure success. While these could theoretically be adopted by any public administration, not all have been successful because service operators lacked product management, marketing and sales and support capabilities.

D-PA Recommendation 12.1: Evaluate successful open-standard solutions. There are examples of successful deployment of solutions around open standards, such as FIWare. These should be evaluated to identify success factors and best practices.

D-PA Recommendation 12.2: Ensure operators of "public-sector-specific" SaaS solutions have skills required for sustainability. Service operators should be supported (or chosen) so that the service benefits from product management, marketing and sales and support capabilities.

D-PA Challenge 13: Many smart cities programs have failed to scale beyond pilot projects because they encountered governance, technical and regulatory challenges. The result of those investments was often a plethora of fragmented pilot projects that did not scale from a corridor or neighborhood to the entire city. Or segments of the resident population were excluded from the intended benefits. Or technology solutions were not re-usable across cities, thus did not allow for efficient cross-border best practice exchange and did not enable tech suppliers to generate solid revenue growth that can be re-invested in further innovation.

D-PA Recommendation 13: Evaluate successful smart city projects. The cities that succeeded in orchestrating the ecosystem appropriated budget. They set up programs to make sure that all residents were included in the benefits. They managed to deliver quick wins in specific use cases, and then re-use the modular solutions they had built to extend the capabilities across the whole community. To realize the benefits of the significant investments that will go into smart cities in the coming years, these good practices should spread around the region, and solve open ecosystem governance, technical interoperability and regulatory challenges, such as the balance between data protection and potential benefits of artificial intelligence.