Grant Agreement N°: 871920
Topic: ICT-13-2016
Type of action: CSA

Horizon Cloud – The Forum for Strategy Focused Cloud Stakeholders

D3.1: Strategy analysis report and Cloud Computing

Revision: v.1.0

Work package	WP 3
Task	Task 3.1, Task 3.2
Due date	31/12/2020
Submission date	18/01/2021
Deliverable lead	EGI
Version	1.0

DOI: 10.5281/zenodo.5530740

Abstract

The European Commission is actively setting priorities for the upcoming Multiannual Financial Framework of the European Union covering the 2021-2027 period. Among the different identified priorities, “A Europe fit for the digital age” explicitly supports digitalisation. Cloud computing, as a fundamental brick of a digital Europe, will play an even stronger role in European economy and society by embracing core European values, spanning fundamental individual rights to market openness and environmental friendliness. To tackle Europe digitalisation priority, the European Commission defined “A European strategy for data” and “A new Industrial Strategy for Europe”, including a strong focus on data spaces and federated cloud infrastructures.

To support the work on the definition of priorities for the upcoming programmes, this report explores the question of how supply and demand can be improved in terms of quality and conditions of use, and increased to boost European innovation in the following cloud computing areas:

1. Effective cloud federation models to stimulate the creation of a European public cloud service market leveraging existing capacities;
2. Edge computing, its market growth, and the implications of the edge/cloud infrastructure balance switching from today’s 20% data at the network edge and 80% in cloud-based infrastructure to 80% at the network edge and 20% in cloud-based infrastructure;
3. Adoption of green computing principles to the whole lifecycle of cloud computing delivery to support the transition toward a carbon-neutral (if not carbon-negative) digital society by 2050.

In response to this, the paper summarises a supply and demand analysis conducted by the H-CLOUD project aiming at identifying the status, challenges, and opportunities that Europe is facing with regards to the adoption and provision of cloud computing with a specific focus on federated cloud, edge computing, and green computing. The paper explores key challenges and opportunities from the perspective of demand in six key sectors: public administration, healthcare, transport, energy, agriculture and manufacturing[1]. In addition to these, the paper focuses on the needs of small- and medium-sized enterprises (SMEs). These seven perspectives are referred to as “demand scenarios”.

From this analysis, a number of early conclusions were developed to create discussions with, and feedback from, experts and have been incorporated into this Deliverable that updates and consolidates the Green Paper v1.0 released for H-CLOUD Summit in November 2020. The content of this deliverable will be synthesised into version 1.0 of the White Paper, identifying common motivations and use cases, and analysing those use cases in order to structure and prioritise recommended actions intended to accelerate cloud adoption. Version 1.0 of the White Paper will again be distributed to the broader stakeholder community for feedback and consultation, leading to version 2.0 in April 2021 and the final strategic plan by the end of 2021.

Ultimately this will help the EC frame their future funding programmes, and the European stakeholders to coordinate key actions to achieve common strategic goals contributing to European competitiveness and ability to innovate in cloud computing.

Keywords:

Cloud Computing, Strategy, Demand, Supply, Edge, Federation, Green ICT

[1] These sectors are among the key sectors covered in “A European strategy for data”.

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.3	30/03/2020	Initial Draft	Editors: Mark Dietrich (EGI), Federico M. Facca (MARTEL) and Phil Jones (EGI). Contributors: Carla Arend (IDC), Monique Calisti (MARTEL), Gabriella Cattaneo (IDC), Massimiliano Claps (IDC), Gianni Dalla Torre (EGI), Enol Fernández (EGI), Tiziana Ferrari (EGI), Angele Giuliano (AL), Peter Meadley (AL), Steve Robertshaw (AL).
V0.4	20/04/2020	Responding to feedback of Advisory Board and EC; version provided to participants in webinars from April 24 to May 12, 2020	As above
V0.7	19/08/2020	Reflect feedback from webinars and survey on cloud computing throughout document; reflect new EC strategies (such as EU Strategy for Data) throughout document; added section on Research and Innovation portfolio; updated Annexes 2, 4, 5, 8-12; new Annex 17.	As above
V0.8	11/11/2020	Revised Demand-side analysis for Agriculture; new demand-side analysis for Manufacturing; revised supply-side analyses for Green ICT and Cloud Federation; added analysis of R&I portfolio; new Annexes 7, 9, 14 & 15; updated Annex 17.	As above
V0.9	14/11/2020	Reflect feedback from Horizon Cloud Summit	Mark Dietrich (EGI), Federico M. Facca (MARTEL)
V1.00	18/01/2021	Final Internal Review	Mark Dietrich (EGI), Federico M. Facca (MARTEL), Alessandra Massaro (IDC), Angele Giuliano (AL)

Disclaimer

The information, documentation and figures available in this deliverable, is written by the H-CLOUD (Horizon Cloud – The Forum for Strategy Focused Cloud Stakeholders) – project consortium under EC grant agreement 871920 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Project co-funded by the European Commission in the Horizon Cloud Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to H-CLOUD project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

Cloud computing is a megatrend that is a key enabler for data-driven innovation. It is expected to bring enormous benefits for citizens as stated in the recent EC Communication on Shaping Europe's digital future. It is acknowledged that coordinated efforts are necessary at the European level to make sure that innovation can ultimately make a difference to industry, public administration and eventually society at large.

The European Commission is actively setting priorities for the upcoming Multiannual Financial Framework (MFF) of the European Union covering the 2021-2027 period. Among the different priorities, digitalisation is driven by the "A Europe fit for the digital age" priority. EC also published different strategies to support the EU digitalisation, including: "A European strategy for data"[2] (EUSD) and "A New Industrial Strategy for Europe"[3] (NISE). In these strategies, Cloud computing is considered a fundamental brick of a digital Europe that will play an even stronger role in European economy and society by embracing core European values, spanning fundamental individual rights to market openness and to environmental friendliness. Nevertheless, for many organisations, "cloud adoption" is neither simple nor a "one size fits all" process. It is often complex, requiring detailed planning, skilful execution and careful consideration of return on investment. "Data-driven innovation" is even more difficult for many organisations, and the right conditions and supports will be necessary to encourage and enable this essential component of Europe's future. The *High Impact Project on European data spaces and federated cloud infrastructures,* presented in EUSD, aims at supporting such data-driven innovation by simplifying cloud services adoption.

The European Commission tasked the H-CLOUD project to analyse the *status quo* and provide recommendations for future work programmes with the support of the European Cloud Community. As stated in the EUSD, "the digital transformation of the EU economy depends on the availability and uptake of secure, energy-efficient, affordable and high-quality data processing capacities, such as those offered by cloud infrastructures and services, both in data centres and at the edge". Consistent with this premise, H-CLOUD focuses on edge computing, cloud federation, and green computing, their role and relevance in different "use cases" and the barriers to adoption for different key stakeholders.

This version of the Green Paper presents the results of literature research covering market and strategy reports, policies, and available information on Digital Europe, Horizon Europe and Connecting Europe Facility 2 programmes, as well as feedback from a series of webinars with subject matter experts conducted between April 24 and June 23, 2020. These sources of information have been analysed from the demand and supply perspective. In the demand side analysis, we focused on the domains prioritised in the draft orientation for the Digital Europe Programme for federated cloud. In the supply analysis, we focused on the priorities proposed by the EC: federated cloud, edge computing and green computing. The analysis of the single aspects has been consolidated into common challenges and preliminary recommendations aiming at stimulating further the discussion with stakeholders.

In the next phases, we will widely distribute the Green Paper to collect feedback from to the broader stakeholder community for further feedback and consultation. Following the public consultation, a White Paper will be realised to consolidate Green Paper findings and recommendations.

Major findings emerging from the analysis

Major Challenge M1: Complying with GDPR, the NIS Directive and related regulation has a significant impact on cloud adoption and creates a significant burden, particularly for smaller organisations. This challenge was highlighted in the public administration (*D-PA Challenge 1*), transport (*D-T Challenge 2*) and healthcare (*D-H Challenges 3 and 4*) domains,

[2] EC. Communication: A European strategy for data. 2020.

[3] EC. A new Industrial Strategy for Europe. 2020

as well as a general challenge for cloud adoption from the supply side perspective (*S-T Challenge 2*). It is also reflected in concerns about how effective Cloud Codes of Conduct are in helping client organisations ensure their compliance with important regulations (supply landscape, *S-L Challenge 8*). This challenge highlights the importance of “the availability and uptake of secure … data-processing capacities” as noted in the EUSD, as well as highlighting how such secure capacities are still not readily available to European citizens and organisations.

A variety of approaches were identified to address this challenge:

- Collect and share best practices on data sovereignty and security. (For public administration: D-PA Recommendation 1; and healthcare: D-H Recommendation 5.)
- Promote standard certification and auditing instruments that make it easier for cloud providers to comply with existing regulation and help cloud buyers to gain more transparent understanding of contractual conditions. (For public administration: D-PA Recommendation 2.)
- Direct EPDB, EPDS and ENISA to update and expand technical and governance guidelines to enable cloud-based services, including innovative ones, that align with GDPR and the NIS Directive requirements. Also, ensure that there are mechanisms to enforce those policies and offer guidance through codes of conduct. (For transport: D-T Recommendation 2.1.)
- Clarify “shared responsibilities” for regulatory compliance in cloud implementations, as well as how cloud provider compliance with GDPR and “Cloud Codes of Conduct” must be complemented by compliance efforts by cloud users themselves. (For supply: S-L Recommendation 8.)
- Examine availability of accessible market offerings of GDPR-compliant solutions (perhaps as PaaS platforms) that might make "safe" cloud adoption easier. This recommendation is discussed in three demand scenarios (public administration, D-PA Recommendation 10.2; transport, D-T Recommendation 2.2; and healthcare, D-H Recommendation 4) as well as in two supply side analyses (supplier landscape, S-L Recommendation 3; and technology landscape, S-T Recommendation 2).

Major Challenge M2: Limited skills and expertise especially in smaller organisations. Even if there would be no concerns about regulatory compliance, moving to the cloud takes skills and resources that many smaller organisations do not have. They have a limited budget to acquire the technical and business skills needed to develop, deploy and manage cloud services. This challenge is discussed in three demand scenarios (public administration, *D-PA Challenges 4, 5 and 6*; transport, *D-T Challenge 3 and 5*; agriculture, *D-A Challenge 1*; manufacturing, *D-M Challenge 4*; and SMEs, *D-S Challenge 1*), as well as in one supply side analysis (edge technologies, *S-E Challenge 2*). This challenge is also present in the healthcare demand scenario, which also has smaller organisations struggling with cloud adoption. This challenge is recognised in the recently published EUSD, the New Industrial Strategy for Europe[4] (NISE), and the SME Strategy for Sustainable and Digital Europe[5] (SSSDE).

Limited skills are particularly a challenge for smaller organisations that depend on legacy applications, for which cloud migration is not easy and may require capacities beyond those available in the organisation. Incentives for ISV-to-SaaS vendor transitions could have an indirect impact on cloud adoption in several demand scenarios. The SaaS market is large and fragmented so these sorts of incentives could be effective (specific approaches are described in *D-PA Recommendations 5, 10 and 11.2*).

Major Challenge M3: Secure and trusted data access, sharing and processing across different organisations. Organisations from many sectors need secure data access and sharing capabilities to enable their businesses to grow, rather than just complying with

[4] EC. A new Industrial Strategy for Europe. 2020
[5] EC. An SME Strategy for a sustainable and digital Europe. 2020

regulations. Often this business growth (or mission effectiveness for public good organisations such as healthcare providers) requires managing data that is distributed across organisational boundaries. Data governance requires coordinated approaches among the different stakeholders that ensure coordination and verification of the ways data are used and processed. Solutions supporting such scenarios need to be robust and affordable, or their adoption will be limited. This challenge is discussed in five demand scenarios (transport, *D-T Challenge 1*; energy, *D-E Challenge 4*; public administration, *D-PA Challenge 8;* agriculture, *D-A Challenge 4*; manufacturing, *D-M Challenge 3*; and healthcare, *D-H Challenge 1 & 2*) as well as in one supply side analysis (technology landscape, *S-T Challenge 3*).

This challenge is implicit in the EUSD's planned creation of common European data spaces, both cross-sector and in nine specific sectors, intended to foster data-driven innovation across Europe. The need is very clear in each of the sectors identified, but solutions, both technological and organisational, must become more mature in order to address this challenge.

Major Challenge M4: Access to a wider offer. The dominance of US IaaS and PaaS vendors limits the options available to clients looking to move to the cloud: use the powerful, yet often proprietary software environments offered by those dominant vendors, or work to combine and integrate services offered by smaller, EU-based providers. This places smaller providers at a price disadvantage and can create additional implementation burdens on clients of these EU-based providers. This especially affects smaller client organisations. At this stage, for more traditional cloud IaaS and PaaS offerings, it may be difficult to witness the rise of EU-wide competitive offerings, but in specific segments, such as edge computing, distributed data management or SaaS, there may still be opportunities. This challenge is discussed in the public administration (*D-PA Challenge 10)* agriculture *(D-Challenge 3)* and SME *(D-S Challenge 2)* demand scenarios, as well as the supplier landscape analysis (*S-L Challenge 1 and 2*).

Key barriers to the adoption of federated cloud solutions

An important aspect of Major Challenge M4 relates to the difficulty, for many clients, of integrating services across multiple cloud providers and possibly with the clients' own private cloud capabilities. This integration may be motivated when clients want to combine best-in-class services from different providers, to combine service territories across national borders or when groups of organisations (e.g. in healthcare) want to share or pool data or data-processing services. When performed by the client, this integration is called "multi-cloud" or "hybrid cloud".

When this integration is performed by service providers and/or multiple client organisations, this is called "federated cloud". Federated cloud allows various services provided by individual federation partners to be planned, deployed and delivered seamlessly to clients in an integrated manner. Federation requires both technical and operational integration, which typically requires the creation of a federated organisational structure to manage the collaborative effort.

In general, federation is a form of multi-organisational alliance in which some processes and related policies and activities are governed and coordinated in a collaborative way, and sometimes delegated to a central body by the federation members, while other processes, policies and activities remain the responsibility of the members of the federated alliance (the federation members). Ideally there should be some asset or resource, common to many of the partners, which can be shared across the federation to better serve clients.

As an alternative to federation, service providers might commit to making their services interoperable, through adherence to standards or other boundary conditions, rather than performing the integration themselves. Such services can then be advertised or even directly accessed through a "cloud marketplace" that identifies the specific conditions, standards or other characteristics of each service. While such a marketplace approach may not require creation of a separate organisation (for example to manage standard-setting and certification processes), both approaches face similar challenges and require similar collaborative, coordinated activities, so we consider them together in this analysis.

Federated clouds and federated data are receiving extra attention in the current environment. As this analysis has concluded, important ecosystems in public administration, healthcare and transport/mobility need to enable the secure access, sharing and analysis of sensitive data already being stored and managed by ecosystem players – often on private cloud infrastructure. On the supply side, in October 2019 the governments of Germany and France announced the Gaia-X federated cloud initiative, with a strong focus on creating a federated data capability. The EUSD specifically calls for the creation of a European Cloud Federation (EUCF).

Challenges to creating effective federated clouds arise in both technical and organisational areas. Specific challenges are identified, and recommendations made, related to the planned creation of a EUCF.

S-F Challenge 1: Coordinated/federated approaches must be structured around the objectives of their stakeholders, balancing community focused initiatives with pan-European solutions. The needs of different stakeholder communities must be balanced against the need for common or aligned solutions. The effectiveness of any federation will depend strongly on the clarity of its value proposition and how it is constituted to realise that value proposition.

Recommendations prescribe a number of steps required for success:

- Develop detailed business cases for identified scenarios in each of the nine sectoral data spaces described in the EUSD that quantify the societal gains and costs to achieve the desired benefits and ascertain feasibility and related ICT innovation needs.
- For each business case, select the most appropriate federation business model that fulfills the requirements while providing the best value with the optimal effort.
- Create an open infrastructure and testing capability that could flexibly support demonstrations, proofs of concept and pilots of how federated cloud and federated data solutions could be assembled, operated, managed and governed, including collection of data that would validate the business cases developed earlier.
- Support the creation of multiple EUCF-affiliated initiatives and their cross-domain collaboration, which will specify domain-specific use cases, objectives and beneficiaries, federation partners and stakeholders, governance and decision-making mechanisms, scope of possible federated activities, and applicable business models.
- Develop a lightweight model for the EUCF as a coordinating body of sector- or use-case-focused European federated cloud initiatives, supporting coordination of their research and innovation activities, cross-sector collaboration on interoperability, facilitating best practice operations, and providing relevant shared services such as certification activities.
- Implement a EUCF with a phased approach that flexibly aligns activities across multiple domains, and that allows achievement of “quick wins”. Pilot projects and demonstrators will clarify requirements and identify applications and use cases where an early version of the EUCF can achieve success, which in turn will build credibility and support.
- Set up the EUCF following known organisational recommendations.
- Evolve existing best practices and standards (e.g. ITIL, FitSM, etc.) for federated service management to ensure federated cloud initiatives have reference requirements, processes, procedures and policies that ensure the compatibility of service delivery and planning across different initiatives. Develop “starter kits” to assist with implementation of each federated business model, with sample templates for required governance and service management processes (definitions, roles, process maps, etc.).

S-F Challenge 2: Defining, Evolving, Selecting, Agreeing on and Managing the Architecture, Technical Standards and Tools for Federated Clouds and Distributed Data Access and Exchange. Creating a distributed yet federated, technically effective data-processing system is an active subject of research – many technical approaches are being studied, and many technical approaches are in use in the community, but they are not converging into “standards” because the underlying technologies are rapidly evolving and because the scope of integration is expanding from the data centre out to the more heterogeneous edge computing environment. Where distributed capabilities need to work together, there must nevertheless be an agreement on the framework of the system (the architecture) and the standards to be adopted within that framework, even in the face of this rapid change. Establishing a platform architecture enables technical discussions to be modularised and compartmentalised and facilitates agreement on standards that enable specific services to interoperate.

Related recommendations include:

- Develop and evolve a Federated Cloud Reference Architecture (FCRA), to the extent possible incorporating the NIST CFRA, EGI and Gaia-X's technical architectures, and evolve it to ensure conformance of emerging federated cloud initiatives. This should specifically characterise how practical compliance frameworks and portals would align with the EUSD's contemplated "Cloud Rulebook" and "Service Marketplace" concepts.
- Create and maintain a federated cloud interoperability framework as an evolving suite of technology, standards and tools that are consistent with the FCRA allowing interoperability within a given federation and across multiple federations, compliance with European values and clear identification of a suite of interoperable components. This suite of components would help EU customers navigate the many options for cloud-based solutions and would help formalise how they are described and the possibilities for integration.
- Coordinate research and innovation activities in Horizon Europe by aligning cross-domain, cross-use case research and innovation activities of common interest for different federation stakeholders to increase synergies, innovation potential and avoid duplication across the industry, research and public administration sectors.

S-F Challenge 3: Federated data has great potential to support secure, private sharing of data held by many different organisations. Best practice roadmaps are urgently needed to ensure that federated data sharing initiatives are established and operated efficiently while preserving and ensuring the highest level of trust that affected sensitive data will be kept private and secure.

Recommendations include:

- Create guidelines for implementing different data sharing approaches using federated data platforms.
- Support efforts to increase semantic interoperability for data within and across sectors are critical and must also include harmonisation of data usage models to enable automated, yet secure and appropriate, data sharing.
- Develop regulatory sandboxes that would allow experimentation and scaled-up testing of privacy-preserving technologies.
- Continue support for research, innovation and deployment of existing privacy-preserving technologies in practical application domains. These technologies are at various technological readiness levels (TRL) and would benefit from continued investment and support for early stage adoption and deployment.
- Support creation of technical standards for preserving privacy. Such standards would provide risk assessment tools, test suites for validation of performance, as well as evaluation of data for sensitive content.
- Continue support for research, innovation and deployment of distributed data analytics tools, as well as data placement tools, that minimise security privacy risks and maximise speed, computational and network efficiency as well as energy efficiency.

Key barriers to the adoption of edge computing

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. It refers to the "edge" of the network, where a network connects with specific devices, such as smartphones, wearable devices, and Internet-of-Things (IoT) devices. Clearly, "geo-localised" processing, ensuring, for example, compliance with GDPR, is a central element to enable data spaces as envisioned in EUSD.

Key challenges for edge computing are listed below.

S-E Challenge 1: Concern about stranded edge investments. Investing in the wrong emerging technology is a risk. The supply side should facilitate edge adoption and deployment by mitigating the risk of lock-in.

H-CLOUD analysis highlights that this challenge should be supported by: strategies helping edge technology maturation and skills development *(S-E Recommendation 2)*, creation of an ecosystem of interoperable and/or federated public edge infrastructure offering (*S-E Recommendation 3*), investing on automation and openness edge solutions (*S-E Recommendation 4*), and promoting development of common edge standards across the different industries (*S-E Recommendation 5*).

S-E Challenge 2: Edge is complex and expensive for SMEs. Help smaller organisations to improve their readiness and maturity, and reduce the complexity of edge computing adoption, while making it affordable.

This challenge should be supported by strategies helping edge technology maturation and skills development *(S-E Recommendation 2)* and investing on automation and openness of edge solutions (*S-E Recommendation 4*).

S-E Challenge 3: Uncertain return on edge investments. Facilitate the widespread use of edge technology, so it reaches critical mass as a public edge capability.

This could create an opportunity for Tier 2 providers, notably those associated with mobile networks, to take a more prominent role in edge infrastructure build out, leveraging their existing footprint of distributed facilities. Research and Innovation initiatives should investigate solutions, for example leveraging federation and multi-edge approaches, to allow the creation of widespread edge infrastructure across different providers (*S-E Recommendation 3)*.

S-E Challenge 4: Ensure scalability and affordability of edge computing solutions and deployments to cope with the demands of the foreseen usage scenarios, also by small players.

Research should continue to explore automation of cloud continuum from infrastructure layer up to the final application, taking into account different scenario-specific demands and contributing to open source initiatives *(S-E Recommendation 4).*

S-E Challenge 5: Concerns about edge interoperability. Edge computing research and innovation solutions are coming from the telecommunications sector as well as multiple Industry 4.0 initiatives, but their approaches are diverging. This will create interoperability issues and increase the complexity of adoption and management.

The analysis highlights the relevance of promoting development of common edge standards across the different industries and sustaining them by including them as requirements in public tenders (*S-E Recommendation 5*).

S-E Challenge 6: Limited investment on trusted data access solutions for the edge. As of today, most of the solutions available for trusted access to data rely on specific hardware facilities - software based solutions are still lacking. This severely limits the flexibility and potential adoption of public edge infrastructure offering where guarantees about trusted access to data are required.

Research should explore open reference solutions for trusted computing at the edge supporting multi-tenants in isolation and compatible with the different EU privacy and security regulations (*S-E Recommendation 6*).

This challenge was in the spotlight of one of the H-CLOUD webinars, and clearly highlights how some core enablers are still missing or not mature enough to support the implementation of EUSD vision. Trusted data access is essential for data spaces where confidential or sensible data are exchanged and processed. Without maturity of such capacities, data spaces may not reach a sustainable uptake.

Key barriers to the adoption of green cloud

Green cloud refers to the adoption of green principles to the whole lifecycle of cloud computing delivery.

Key challenges for green cloud are listed below.

S-G Challenge 1: The data centre energy efficiency standards landscape is weak. Develop energy efficiency standards for Europe, in Europe. Start from the KPIs that already exist but choose them wisely as some are no longer fit for purpose. [Research and Deployment]

S-G Challenge 2: ICT devices need to be used for longer periods to better amortize their environmental impacts when they were constructed. They also need to embrace processors which are able to turn down their performance (and energy consumption) when appropriate. Electronic device recycling needs to be taken up far more extensively and manufacturers should make it easier to wipe old devices. Ensure the right to repair. [Research and Deployment]

S-G Challenge 3: The manner in which the natural world is being exploited to satisfy the demand for digital devices and services is alarming. We need to find more efficient ways of storing and processing data, or to invent completely new ways of storing and processing data.

S-G Challenge 4: The distribution of processing through federation and/or migration to the edge counters environmentally-beneficial trends toward processing centralised in the cloud (particularly in hyperscale data centres). The environmental impacts of billions of edge/IoT devices and the wireless/cellular networks required to connect to them are not well understood, making it difficult to develop environmentally-sensible policies around edge computing. [Policy, Research]

S-G Challenge 5: The way in which policy making, in the digital context, impacts the Green Deal needs to be considered right at the start of any policy development process. [Policy]

S-G Challenge 6: The impact of specific ICT activities on the environment is poorly understood. ICT manufacturers should audit and report upon the environmental impact of the manufacture and operation of their goods and services. Data centre and network operators should report their energy consumption and environmental footprint in a way that enables citizens and ICT users alike to understand the environmental impacts of their ICT choices, and governments and policy-makers to encourage environmentally aware decisions. Possible changes in the environmental footprint of the ICT sector should be projected based on this more detailed data, enabling timely mitigation of potentially harmful increases, whether coming from video streaming, edge computing, gaming, AI or any other ICT-related initiative. [Research, Policy]

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

D	Deliverable
DOA	Description of Action
CC	Cloud Computing
ECC	European Cloud Computing
EC	European Commission
SRIDA	Strategic Research, Innovation and Deployment Agenda
WP	Work Package

1 INTRODUCTION

H-CLOUD is a Coordination and Support Action (CSA) project supporting the creation of a Strategic Research and Innovation Agenda for the future European Commission funding programmes. The specific topics covered in this paper include: edge computing, green ICT, and the potential adoption of cloud federations[6] in Europe[7]. The European Commission (EC) tasked H-CLOUD to look not only at cloud-related research and innovation aspects, but also at the existing challenges of cloud service adoption, implementation, and effective use that can hinder competitiveness and prevent the successful addressing of societal challenges. To cover this wide agenda, this document uses a structure to expose the diverse set of issues that arise across multiple views, on both demand and supply sides.

This deliverable provides an initial discussion document designed to identify the problems of adoption and implementation in connection with these specific cloud topics. A more detailed analysis of a strategy for research and innovation is planned later in the H-CLOUD work plan.

From a methodological point of view, this paper contains a framework created to break down the variety of adoption and implementation challenges and map them to potential recommendations. An important part of the feedback H-CLOUD is seeking at this stage concerns the validity of this model.

This version has been revised to reflect the EC's recent communications "A European strategy for data" (EUSD) and "A new Industrial Strategy for Europe" (NISE) as well as expert feedback received in five webinars conducted between April 24 and June 23, 2020.

On the demand side, the plan is to build upon the initial demand side scenarios to develop a clear view of the variety of cloud service adoption challenges that the markets and sectors currently face. At the same time, the project and the European Commission want to promote discussions with supply side specialists, who can further assess, develop and expand upon the supply side issues. The discussion will strengthen the Green Paper presented in this deliverable into a White Paper.

1.1. The policy context

In past years the European Commission (EC) largely invested in Digital Single Market establishment, including a number of actions specific for Cloud computing. With the upcoming Multiannual Financial Framework (MFF) of the European Union covering the 2021-2027 period, the European Commission (EC) is setting new priorities and directions that complement and expand strategies defined in the previous MFFs. EC announced that the focus will be on six priorities[8]:

- **A European Green Deal**, with a goal motivated by the realisation that "becoming the world's first climate-neutral continent by 2050 is the greatest challenge and opportunity of our times".
- **An economy that works for people**, under the ideal that "The EU's unique social market economy allows economies to grow and to reduce poverty and inequality. With Europe on a stable footing, the economy can fully respond to the needs of the EU's citizens."

[6] In general, federation is a form of multi-organisational alliance in which some processes and related policies and activities are governed and coordinated in a collaborative way, and sometimes delegated to a central body by the federation members, while other processes, policies and activities remain the responsibility of the members of the federated alliance (the federation members). Ideally there should be some asset or resource, common to many of the partners, which can be shared across the federation to better serve clients.

[7] Please see Annex 1 for definitions of technical terms associated with cloud and edge computing.

[8] EC. 6 Commission priorities for 2019-24. 2019

- **A Europe fit for the digital age,** by empowering people with a new generation of technologies and sustaining the Digital Single Market Strategy to create better and larger opportunities for European companies
- **Protecting our European way of life**, promoting a "vision for a Union of equality, tolerance and social fairness".
- **A stronger Europe in the world**, to reinforce European role as responsible global leader working to ensure the highest standards of climate, environmental and labour protection.
- **A new push for European democracy** to ensure a stronger role of European citizens in the decision-making process and in the setting of European priorities.

Cloud computing may play a key role not only by addressing the digital challenge in Europe, but also by supporting the other priorities by embracing specific core European values:

- Fundamental individual rights (e.g. security and data privacy),
- Market openness (e.g. interoperability and free flow of data) and
- Environmental friendliness and supporting the transition to a sustainable planet.

EC to tackle the above priorities proposed two key strategies: "A European strategy for data" (EUSD) and "A new Industrial Strategy for Europe" (NISE). These strategies broadly build on the High Impact Project on European data spaces and federated cloud infrastructures, a core European project to unleash the potential of the data economy and digital single market in Europe.

The High Impact project foresees the creation of data spaces: cloud-enabled ecosystems to exchange and process data in different sectors in compliance with EU regulations. Such data spaces will build on a set of federated cloud-edge services available across Europe providing a harmonised set of "enablers" to build data spaces ensuring interoperability, facilitating data movement and implementing EU data privacy and data security regulations.

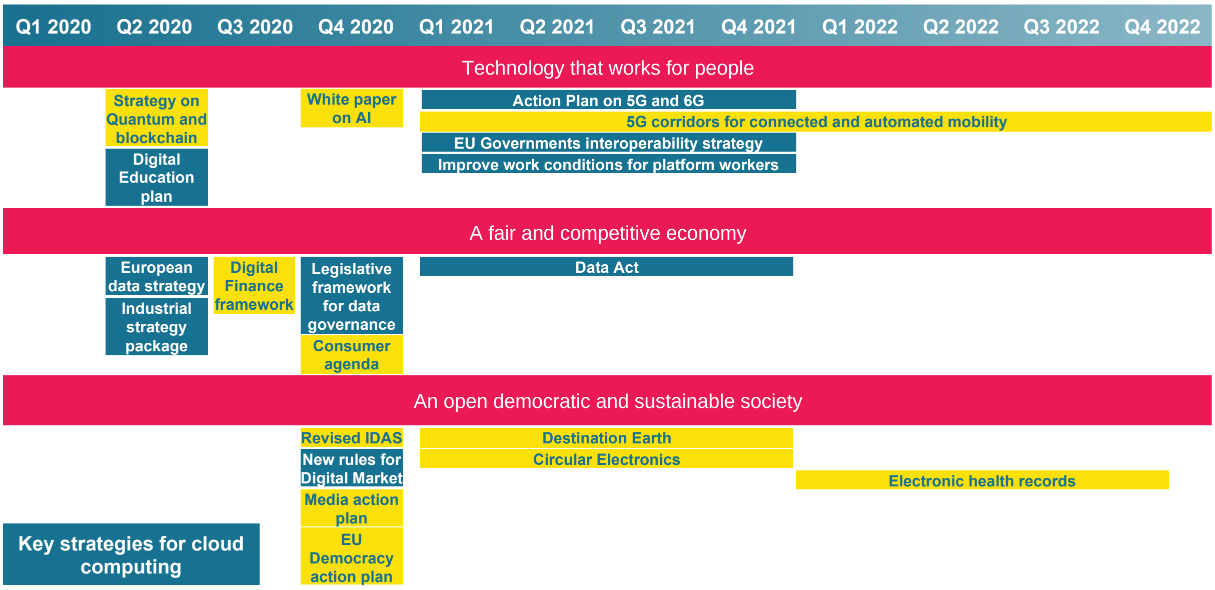
Q1 2020
Q2 2020
Q3 2020
Q4 2020
Q1 2021
Q2 2021
Q3 2021
Q4 2021
Q1 2022
Q2 2022
Q3 2022
Q4 2022
Technology that works for people
Strategy on Quantum and blockchain
Digital Education plan
White paper on AI
Action Plan on 5G and 6G
5G corridors for connected and automated mobility
EU Governments interoperability strategy
Improve work conditions for platform workers
A fair and competitive economy
European data strategy
Industrial strategy package
Digital Finance framework
Legislative framework for data governance
Consumer agenda
Data Act
An open democratic and sustainable society
Revised IDAS
New rules for Digital Market
Media action plan
EU Democracy action plan
Destination Earth
Circular Electronics
Electronic health records
Key strategies for cloud computing

Figure 1. EC strategies timeline

Key instruments of the new MFF 2021-2027 supporting the digital transformation in Europe and the implementation of "A European strategy for data" are:

- Horizon Europe[9], the new research and innovation programme.
- Digital Europe[10], a new deployment programme building the strategic digital capacities of the EU.
- Connecting Europe Facility 2[11], focusing on the creation of transnational digital infrastructures.

Each of these programmes plays a key role in Europe’s digitalisation. The Digital Europe programme is specifically intended to support the deployment of mature research and innovation outcomes. Previously, this deployment phase was seen as a “Valley of Death” where research and innovation initiatives often failed to find traction and exploitation. The Digital Europe programme is intended to bridge this valley so that research and innovation results achieve market penetration and have impact. As noted by EC representative Pierre Chastanet in the Horizon Cloud Summit, “the EC aims to invest in innovative technologies that are not yet on the market and that will drive the future competitiveness of Europe.”

The COVID-19 pandemic increased the demand for digital services that are key to increase resiliency of public administration, business and citizens. In line with this trend, digital services have a primary role in the financial instruments introduced by the commission to recover Europe from the COVID-19 impact and to transition Europe toward a more resilient, green and digitally enabled society, namely the Recovery Fund and the Next Generation EU programme.

H-CLOUD, through the analysis presented here and in future work based on the Green Paper outcomes, will support the definition of the above European programmes taking into account the need to bridge the “Valley of Death” between research outcomes and market take up. (Please see Appendix 2 for more extensive discussion of the policy context.)

1.2. The methodology

The work leading to this Green Paper has been organised to create and deliver meaningful insights and recommendations for public and private investments with a view to a more extended strategic research, innovation and deployment agenda that will follow the Green Paper.

[9] https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en

[10] https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027

[11] https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-2021-2027-have-your-say-cef2-digital

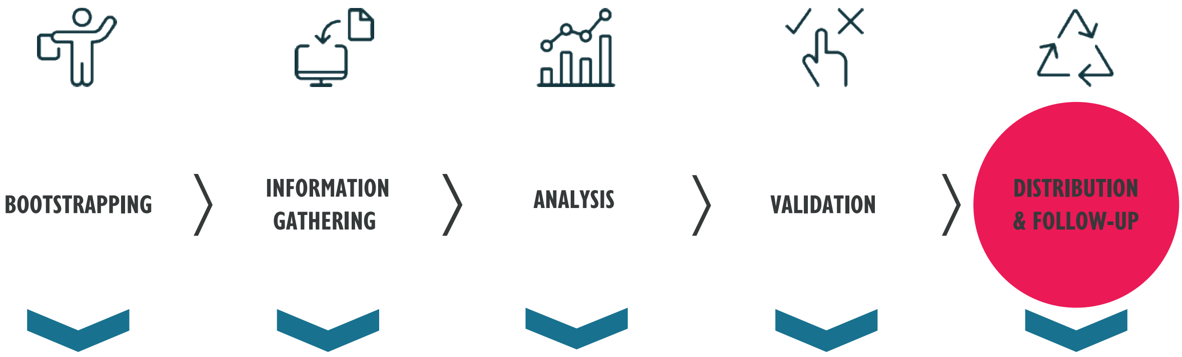

Figure 2. Green Paper methodology

This required an initial definition of an agile and effective methodology to allow the extraction of valuable information from the many sources available online and offline, while maintaining close coordination with the European Commission and dealing with a quite challenging timeline. The work was organised as follows.

- **Bootstrapping.** H-CLOUD project met the EC representatives in January 2020 to discuss EC priorities in relation to the development of cloud computing future work programmes. During the meeting, the EC representatives highlighted three priorities:
  - Effective cloud federation models to stimulate the creation of a European public cloud service market leveraging existing capacities;
  - Edge computing, its market growth, and the implications of the edge/cloud infrastructure balance switching from today's 20% data at the network edge and 80% in cloud-based infrastructure to 80% at the network edge and 20% in cloud-based infrastructure;
  - Adoption of green computing principles to the whole lifecycle of cloud computing delivery to support the transition toward a carbon-neutral (if not carbon-negative) digital society by 2050.
- **Information Gathering** has gone through two main channels: online and offline in order to create a solid knowledge base. Key resources used in this version include:
  - Market research and strategy reports related to cloud computing;
  - Policy documents related to cloud computing and more in general the Digital Single Market;
  - Available source of information related to Horizon Europe, Digital Europe and Connecting Europe Facility 2 programmes;
  - Feedback from the H-CLOUD Advisory Board;
  - Landscape of Cloud research projects and best practices in cloud computing adoption.
- **Analysis.** Information collected from various sources contributed to the analysis phase. The analysis, taking into consideration the upcoming importance of Digital Europe, started from focusing on domains listed as priorities in the related draft documents. The analysis focused on the two complementary aspects: Demand (focusing on five domains prioritized in Digital Europe for federated cloud) and Supply (where the three priorities indicated by EC have been explored). For the different demand domains and supply side areas we analysed challenges, identified common ones and consolidated them. Where possible we proposed recommendations as hypotheses, with the aim of stimulating discussion from the stakeholders. Challenges and Recommendations have

been labelled as ***Policy*** to highlight the ones related to the regulatory agenda, ***Research*** to identify the ones related to Horizon Europe, and ***Deployment*** to identify the ones related to Digital Europe and Connecting Europe Facility 2.

- **Validation.** The European Commission and a set of experts have been invited to provide feedback that was consolidated in this previous version of the Green Paper. Beyond that, the Horizon Cloud Summit in November 2020 provided a stage for different stakeholders to provide their view on the Green Paper and related outcomes. Based on the outcomes of the Summit discussions, the Green Paper has been finally revised in this deliverable.
- **Synthesis**. The findings presented in this deliverable will be further synthesised into version 1.0 of a White Paper. In particular themes, motivations, use cases and priorities common to the seven demand sectors will be identified, and related technical and organisational requirements for each use case will be used to structure and prioritise the recommendations developed for this deliverable.
- **Distribution & Follow-up.** The synthesised findings presented in version 1.0 of the White Paper will be distributed and promoted across the various H-CLOUD channels in early 2020. This will be the basis for further consultation and co-creation processes, run in conjunction with the H-CLOUD Advisory Board, expert groups and other stakeholders, that will lead to version 2.0 of the White Paper and to the shaping of the first version of the strategic research, innovation and deployment agenda by April 2021.

2. DEMAND SIDE AND SUPPLY SIDE ANALYSIS

To tackle the potentially wide and complex scope of this document, the project decided to adopt a view of demand side and supply side. This is consistent with the landscape analysis H-CLOUD discussed with the EC (see Figure 3).

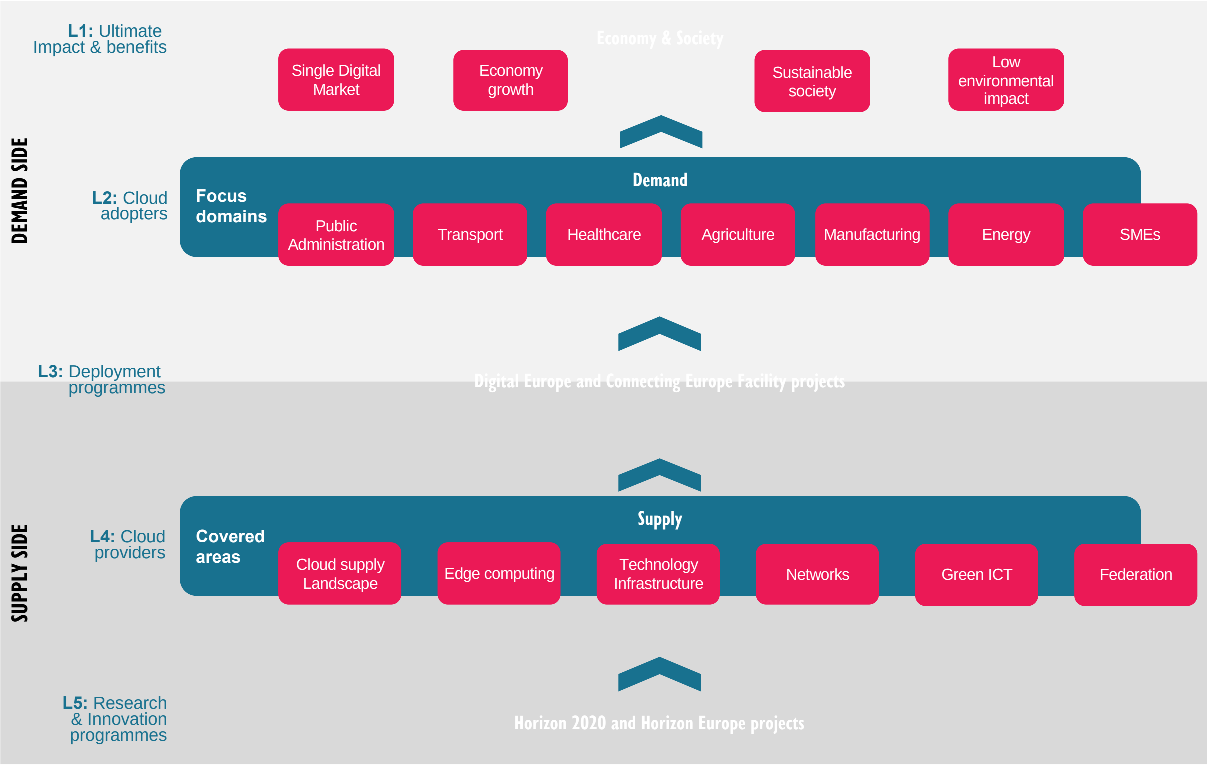

Figure 3. Framework for demand side and supply analyses

Layer 1 shows the ultimate beneficiaries and outcomes. This layer relies on Layer 2, the adoption and exploitation of digital and cloud services and technologies across industry and the public sector. This is referred to as “the demand side”.

Layer 3 supports the wider adoption of cloud-based solutions through deployment programmes, helping to bridge the gap between research and the market. Layer 4 represents the landscape of cloud computing and other infrastructure providers. Beneath this lies Layer 5, the Research and Innovation programmes and projects, that supports the exploration of new technologies answering to demand side challenges. These two last layers are referred to as “the supply side”.

This paper expanded this model to analyse the challenges in both the demand side and the supply side.

2.1. The demand side scenarios and analysis

For the demand side analysis, the paper aims to expose the diversity of challenges that would expose the supply side and the cloud, edge, green and other issues. To make this examination tractable H-CLOUD selected a set of demand side scenarios, specifically six of the sectors covered in the “A European strategy for data”: public administration, healthcare, transport, energy, agriculture and manufacturing. To provide a horizontal perspective, the needs of SMEs were also examined. While these demand scenarios are not exhaustive it was expected that they would collectively expose a variety of demand side issues of potentially broader significance. This analysis is meant to be further developed through community input.

This approach exposes specific needs from each demand scenario, to identify issues in the broader supply side, and to go deeper into the research and innovation programmes. In doing so H-CLOUD concentrated on identifying issues within the scope of the focus areas set by the EC, namely, cloud, edge, green computing and federation.

Our analysis of the demand scenarios revealed two important aspects of the demand side challenges. First, there are different types of challenges. These types can be defined according to the degree of complexity of the deployment and to the organisational complexity where solutions are deployed. H-CLOUD developed a demand framework to classify and analyse the different demand challenges relative to these two dimensions. Although developed to characterise the challenges in cloud adoption this framework can be used to analyse any IT implementation project.

Second, within any organisation, the process of deployment is composed of two steps: adoption and implementation.

- Adoption addresses the questions: “Is this right for our organisation, and what stops or enables us to consider taking it on?”
- Implementation addresses the question, “Having decided to adopt this solution, how do we make it work in our organisation, and make sure we and our stakeholders/clients can use it to our mutual benefit?”

Within the demand framework, H-CLOUD identified distinct challenges across the various demand scenarios and classified them so they can be clearly analysed. From there, potential solutions to these challenges have been developed. The classification of different adoption/implementation situations is elaborated in the sections below.

2.1.1. Varying degrees of cloud deployment sophistication

Cloud deployment scenarios vary depending on their complexity, and they can be classified as follows.

A. Relatively simple deployment and migration scenarios typically involve individual applications moving to cloud services, or applications integrating multi-cloud and hybrid-cloud solutions. In this case, they face well known problems that have been solved in multiple cases. They may be a challenge for one organisation, but they have been solved in many other organisations.

B. Applications with data protection requirements or requiring access to distributed data held by multiple organisations or providers. This is common in domains like climate change research, earth science, evidence-based policy making, research and development in pharmaceuticals and life-sciences sectors and insurance companies, as well as smart city and autonomous driving solutions. In such cases, the potential for unauthorised access, hacking or even simple movement of data where it should not be, becomes important. In these scenarios, security is paramount, and more effort is required in the design of applications and their cloud-based implementation. As more parties are involved, combining heterogeneous data sources, the complexity of this challenge increases.

C. Deployments requiring a more sophisticated combination of edge, cloud, AI solutions combined with big data present the highest potential for differentiation and competitive exploitation, bringing wider benefits for an industry or the wider population. In this case, a sophisticated application may be only a relatively small part of that organisation’s challenge, however it can have a disproportionate potential for leverage and future success. The more sophisticated deployment challenges require more sophisticated skills and knowledge.

Of course, there is overlap across these broad deployment sophistication types. Recognising these broad deployment sophistication categories helps to break down the problem into component parts.

2.1.2. Varying degrees of organisational complexity

Analysis also revealed distinct examples at various levels of organisation breadth, size and complexity. Each level introduces a new complexity factor to the deployment problem. For instance, deployment in a single large organisation is less complex than deployment across a whole sector of many organisations.

H-CLOUD distinguished four main levels of organisational complexity at which deployment may occur:

1. **Level 1**. Smaller, simpler organisation. At this level, typically the deployment of a technology by a single smaller and simpler organisation is a relatively self-contained problem, even if challenges may arise regarding data security.
2. **Level 2.** Complex organisation in a sector or industry (e.g. an automotive company, utility or public administration organisation), potentially including the supply chain of the considered organisation. At this level, the complexity of cloud service adoption increases if the organisation's reach extends across a supply chain, across countries and/or across different applications (e.g. public administration organisations with multiple services). In these types of organisations, even relatively simple migrations of applications to cloud services can be challenging.
3. **Level 3.** Whole sectors covering multiple organisations, for example, implementing a function or service across the utility sector or energy sector, and the deployment of public administration applications across countries. At this level deployments reach across multiple players, typically in the same sector, for example, extending a public administration service across multiple countries, or an industry seeking to gain benefits from cross industry integration. As the degree of sophistication of these deployments increases so does the complexity. Even deploying simple applications across multiple different players in a single sector can be a difficult task.
4. **Level 4**. Multiple industries or sectors. For instance, in the smart cities context, the challenge consists in having to coordinate players from multiple sectors. Typically, this may involve the coordination and integration of multiple players, from different sectors, deploying multiple applications across multiple locations. These applications need integrating to become, for example, a whole smart city view.

2.1.3. The demand framework used for analysis

The four levels of organisational complexity and three levels of deployment complexity are the dimensions that H-CLOUD identified to classify challenges in cloud adoption and implementation. The resulting combinations are illustrated in Table 1.

Table 1. Example challenges mapped to the demand framework

Organisational complexity	**Deployment sophistication**		
	A: Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination. Involving multiple organisations and sectors	Multiple sectors and players, deploying simpler applications and prototypes as spot solutions. (e.g. trials of individual smart city applications)	Integration of personal data across a smart city from multiple sources. Security challenge of multiple applications	The integrated application of solutions involving the coordination of multiple sectors and players. e.g. aspirational Smart Cities.
Level 3: Multiple organisations collaborating across the same sector	Sectors seeking coordination and cooperation and pooling insights across mainstream applications. Sectors looking for insights and sharing consistent (non-personal) data across the sector (e.g. energy, utilities sharing asset data).	Sectors with vast data sets looking for shared insights across sectors (e.g. environment, health, media). Public sector cross border or cross entity collaboration. Sharing data held across separate entities (e.g. personal data, police bodies, etc.)	Sectors applying a sophisticated coordinated response to challenges. e.g. transport addressing environmental impact across parts of the sector, or large-scale Edge and AI deployments.
Level 2: Single larger, more complex organisations, including their customer networks and supply chains	Larger & more complex organisations seeking efficiencies and staying up to date. e.g. creating multi-clouds & hybrid cloud solutions as they migrate parts of suite of applications to cloud for efficiency. Challenges of data security and integration across applications.	Larger organisations managing data protection and security across multiple on premise and cloud-based deployments. e.g. commercial organisations protecting customer data, public administration omni-channel services.	Organisations seeking a sustainable competitive edge. e.g. organisations adding sophisticated & specialist applications such as edge with AI to manage processes or gather insights for long term modelling. Includes use of insights from external data sources, added alongside their core applications.
Level 1: single, simpler smaller organisations	Smaller organisations seeking efficiencies: e.g. SMEs migrating core administration, sales & servicing	Smaller organisations protecting sensitive data and ensuring security.	Smaller organisations creating or using innovative technology for competitiveness or as offering. e.g.

	systems to the cloud platforms (e.g. finance, CRM, etc.) for efficiency gains.	Smaller organisations sharing and using other sources of personal data.	Innovative SMEs creating sophisticated AI solutions, or using large data sets for insights product development offering.

The analysis of the demand scenarios, using this demand framework, highlighted three important aspects:

1. The different challenges from the demand side map to the matrix.
2. Some challenges are specific to the demand side sector, others to the complexity of deployment, and others to organisational complexity.
3. Several challenges are common across different scenarios.

Analysis also illustrated how risk and market opportunity increase with the organisational complexity and deployment sophistication, as summarised in Table 2.

Table 2. Risk and market opportunity mapped to the demand framework

Organisational complexity	**Deployment sophistication**		
	A: Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination	Few examples. New area. Much to learn. Still a challenge. Necessary step to 4B. Increasing integration complexity even for more basic applications.	Enormous opportunity for synergy and insights. Comes with commensurate increase in risk.	Even fewer examples. Definite challenge, but potentially the greatest opportunity.
Level 3: Multiple organisations, same sector	Many sector examples exist. Problems & barriers at simpler levels are specific to sectors (e.g. public administration).	Increasing opportunity for synergy across a sector, with accompanying risk. Data security and protection issues are increased when heterogeneous organisations have to cooperate.	Large opportunity across individual industries. Challenges with data sharing and technology compatibility and interoperability. Important step towards 4B.
Level 2: Single larger organisation & supply chain	Known & common problem. Plenty of services and experience in this area.	Necessary application of data protection and security. Known problems and well proven solutions.	Multiple examples around and emerging. High opportunities in players and industries. Uneven uptake across industries. Specialist skills brought

	High opportunity for increased efficiency, but with multiple services comes increased complexity to be managed.	Requires increasing care as complexity increases. Security & data protection, could be considered more of a risk than an opportunity for many organisations.	in and then developed internally.
Level 1: Single small/med size organisation	Well known problem Commodity consulting and services	Necessary provision. Well known problem. Commodity consulting and services. Requires care with data security and protection	Potential opportunity for smaller niche players with specialist opportunities. Skills and training needed. Specific barriers for smaller organisations.

Annex 3 describes in more detail how the H-CLOUD project analysed demand side challenges.

3. DEMAND SIDE CHALLENGES

3.1. Cross-sectoral demand side challenges

A number of cross-sectoral challenges emerged from the analysis of the selected demand scenarios, illustrated below.

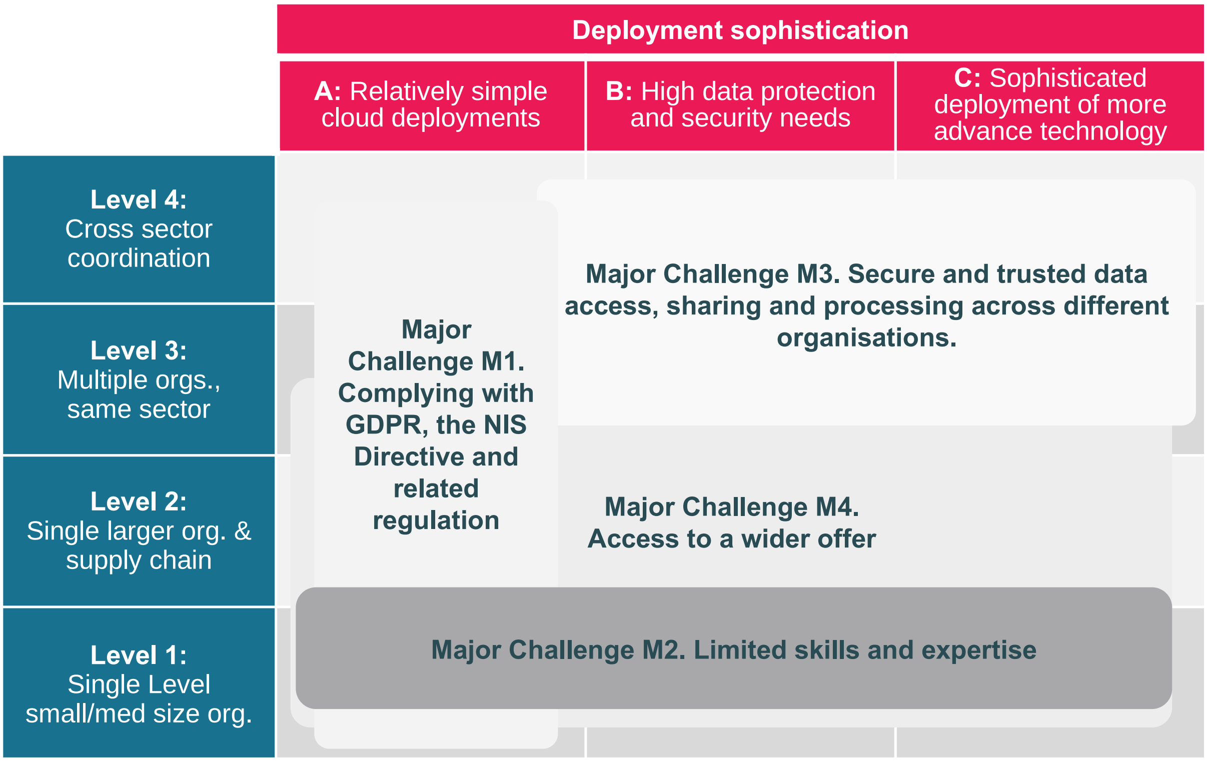
Deployment sophistication
A: Relatively simple cloud deployments
B: High data protection and security needs
C: Sophisticated deployment of more advance technology
Level 4: Cross sector coordination
Level 3: Multiple orgs., same sector
Level 2: Single larger org. & supply chain
Level 1: Single Level small/med size org.
Major Challenge M1. Complying with GDPR, the NIS Directive and related regulation
Major Challenge M3. Secure and trusted data access, sharing and processing across different organisations.
Major Challenge M4. Access to a wider offer
Major Challenge M2. Limited skills and expertise

Figure 4. Common Demand Side Challenges

3.1.1. Major Challenge M1: Complying with GDPR, the NIS Directive and related regulation has a significant impact on cloud adoption and creates a significant burden, particularly for smaller organisations.

This challenge was highlighted in the public administration (*D-PA Challenge 1*), transport (*D-T Challenge 2*) and healthcare (*D-H* Challenges 3 and 4) domains, as well as a general challenge for cloud adoption from the supply side perspective (S-T Challenge 2). It is also reflected in concerns about how effective Cloud Codes of Conduct are in helping client organisations ensure their compliance with important regulations (supply landscape, S-L Challenge 8). It also aligns with the challenge described in the EUSD: “[the EU] will have to improve its governance structures for handling data...”[12].

During the H-CLOUD Summit different experts reinforced the message highlighting that complexity of compliance and data protection legislations are a key factory in limiting adoption and not only in the case of smaller organisations.

A variety of approaches were identified to address this challenge:

- Collect and share best practices on data sovereignty and security. (For public administration: D-PA Recommendation 1; and healthcare: D-H Recommendation 5.) This recommendation aligns with the recommendation below related to Major

[12] EUSD, p.2

Challenge M3: advancing understanding and agreement around data governance frameworks.

- Direct EPDB, EPDS and ENISA to update and expand technical and governance guidelines to enable cloud-based services, including innovative ones, that align with GDPR, the NIS Directive and other requirements. Also, ensure that there are mechanisms to enforce those policies and offer guidance through codes of conduct. (For transport: D-T Recommendation 2.1). This recommendation parallels the EC's intent (stated in its EUSD) to create a 'cloud rulebook': a "compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection and data portability". These technical and governance guidelines would work in concert with mechanisms such as threat registers to identify vulnerabilities of many kinds, including for example, vulnerabilities related to US or Chinese ownership or location of cloud assets. The Gaia-X[13] initiative has taken a similar approach with its "Policy Rules and Architecture of Standards"[14].
- Promote standard certification and auditing instruments that make it easier for cloud providers to comply with existing regulation and help cloud buyers to gain more transparent understanding of contractual conditions. (For public administration: D-PA Recommendation 2.) This builds on the last recommendation: to update and expand technical and governance guidelines. Building on its "Policy Rules and Architecture of Standards", Gaia-X contemplates an extensive third-party auditing and certification capability to validate cloud providers' assertions about their compliance with agreed rules and regulations.
- Clarify "shared responsibilities" for regulatory compliance in cloud implementations, as well as how cloud provider compliance with GDPR and "Cloud Codes of Conduct" (and a "cloud rulebook" in the future) must be complemented by compliance efforts by cloud users themselves. (For supply: S-L Recommendation 8.)
- Explore availability, and support creation, of accessible market offerings of GDPR-compliant solutions (perhaps as PaaS platforms or via marketplaces) that might make "safe" cloud adoption easier. This recommendation is discussed in three demand scenarios (public administration, D-PA Recommendation 10.2; transport, D-T Recommendation 2.2; and healthcare, D-H Recommendation 4) as well as in two supply side analyses (supplier landscape, S-L Recommendation 3; and technology landscape, S-T Recommendation 2).

3.1.2. Major Challenge M2: Limited skills and expertise especially in smaller organisations

Even if there were no concerns about regulatory compliance, moving to the cloud takes skills and resources that many smaller organisations do not have. They have a limited budget to acquire the technical and business skills needed to develop, deploy and manage cloud services. This challenge is discussed in five demand scenarios (public administration, *D-PA Challenges 4, 5 and 6*; transport, *D-T Challenge 3 and 5*; Agriculture, *D-A Challenge 1*, Manufacturing, *D-M Challenge 4*, and SMEs, *D-S Challenge 1*), as well as in one supply side analysis (edge technologies, *S-E Challenge 2*). This challenge is also present in the healthcare demand scenario, which also has smaller organisations struggling with cloud adoption.

Both the EUSD and NISE highlight the need for more workers skilled in digitalisation, big data and data analytics and describe how various existing programs will address these skills gaps. Special attention should be paid to helping organisations develop the more fundamental skills

[13] In October 2019 the governments of Germany and France announced the Gaia-X federated cloud initiative, with a strong focus on creating a federated cloud and data capability.

[14] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.html

required to support cloud adoption. Measures are also needed to ensure that smaller organisations (SMEs as well as smaller public administrations and health providers), which might not be big enough to hire dedicated workers with needed digital skills, still have access to affordable cloud expertise.

Limited skills are particularly a challenge for smaller organisations that depend on legacy applications, for which cloud migration is not easy and may require capabilities beyond those available in the organisation. Incentives for ISV-to-SaaS vendor transitions could have an indirect impact on cloud adoption in several demand scenarios. The SaaS market is large and fragmented so these sorts of incentives could be effective (specific approaches are described in *D-PA Recommendations 5, 10 and 11.2*).

3.1.3. Major Challenge M3: Secure and trusted data access, sharing and processing across different organisations

Organisations from many sectors need secure data access and sharing capabilities to enable their businesses to grow, rather than just complying with regulations. Often this business growth (or mission effectiveness for public good organisations such as healthcare providers) requires managing data that is distributed across organisational boundaries. As noted in the Horizon Cloud Summit, data sharing solutions must ensure that data owners can maintain sovereignty over their data, must have the resiliency and flexibility needed to accommodate a wide range of evolving requirements from data owners and stakeholders, and must be both practical and sustainable. Data governance requires coordinated approaches among the different stakeholders that ensure coordination and verification of the ways data are used and processed. Solutions supporting such scenarios need to be robust and affordable, or their adoption will be limited.

This challenge is identified in five separate demand scenarios:

- Transport, D-T Challenge 1;
- Energy, D-E Challenge 4;
- Public administration, D-PA Challenge 8;
- Agriculture, D-A Challenge 1 & 4;
- Manufacturing, D-M Challenge 2 & 3; and
- Healthcare, D-H Challenge 1 & 2;

as well as in one supply side analysis (technology landscape, *S-T Challenge 3*).

This challenge was selected, by a large margin, as the most important challenge on the supply side by a group of experts convened by H-CLOUD at its webinar on Supply Side Challenges in the cloud market on April 24, 2020. This group commented on the rise of “federated machine learning” as a valuable example of “secure analysis of distributed data”, how such capabilities must incorporate edge computing by definition, and how future processing paradigms might operate exclusively in the edge and completely avoid processing in the core.

The EUSD explicitly notes the need for solutions to this distributed data challenge: “The analytical tools come to the data, not the other way around. This makes it easier to keep the data secure and to ensure control over who accesses what data for what purposes”[15].

In response, the EUSD proposes creation of “data spaces”, both cross sector and in nine thematic sectors, including the five identified in our analysis. “The spaces will include: (i) the deployment of data-sharing tools and platforms; (ii) the creation of data governance frameworks; (iii) improving the availability, quality and interoperability of data – both in domain-

[15] EUSD, p.13

specific settings and across sectors."[16] These actions will require:

  - Developing the tools and software needed to enable secure access, sharing and analysis of distributed data. The EU has supported a number of research efforts in this area[17], but, as noted in H-CLOUD's expert webinar on Supply Side Challenges, tools of this kind have not reached technological readiness levels suitable for wide deployment. The EUSD itself highlights the need for continuing research (supported by the Horizon Europe programme) in "technologies that are crucial for the next stages of the data economy, such as privacy preserving technologies and technologies underpinning industrial and personal data spaces."[18]
  - Advancing understanding and agreement around data governance, in advance of creating any data governance frameworks. This will require analysis of existing frameworks (e.g. the International Data Space Association (IDSA) supports an organisation-centric framework, while The GovLab Project has proposed "data collaboratives" for governance of public good data sets such as humanitarian data[19]), as well as creating community-based venues and fora where consensus on data governance can be reached. The EUSD devotes an entire pillar of its strategy to building "[a] cross-sectoral governance framework for data access and use," and explicit community-based processes to support this construction will be essential.
  - Supporting the effort required to achieve data interoperability, while also recognizing the limits of what can be achieved. For example, the City Data Exchange Project[20] concluded that, even with the best intentions and in a very specific context, data interoperability remains very difficult to achieve. Similarly, the Research Data Alliance has been working since 2013 to achieve interoperability for research data, convening 15 global plenaries over this period, involving over 10,000 members and almost 100 working groups. There have been significant achievements, but more work is needed – even though the RDA benefits from the willingness of its members to work together to solve the problem in the pursuit of knowledge and excellence. Addressing this challenge in the economic sphere will face additional hurdles.

- As noted in the Horizon Cloud Summit, the Gaia-X initiative has taken upon itself the responsibility of realising the EU's vision of data spaces.

3.1.4. Major Challenge M4: Access to a wider offer

The dominance of US IaaS and PaaS vendors limits the options available to clients looking to move to the cloud: use the powerful, yet often proprietary software environments offered by those dominant vendors, or work with more open software suites offered by smaller, EU-based providers. This places smaller providers at a price disadvantage and can create additional implementation burdens on clients of these EU-based providers. This especially affects smaller organisations.

An expert panel of the Horizon Cloud Summit confirmed that while most of the technology building blocks are mature, there is still a need to encourage both small players and the public sector to adopt cloud, in spite of the legacy requirements that exist. The EU cloud industry and EC and Members states need to create momentum, so that there will be an avalanche of cloud adoption. Another observer noted that "a common, trusted and transparent framework is the only way to create a wide cloud market in EU" and that "GAIA-X is on the right track to provide

[16] EUSD, p.20
[17] These will be detailed in H-CLOUD's deliverable D1.3, to be available later in 2020. Examples include RestAssured, HEAT, PRIViLEDGE.
[18] EUSD, p.22
[19] http://datacollaboratives.org/static/files/data-collaboratives-intro.pdf
[20] Municipality of Copenhagen and Capital Region of Denmark. City Data Exchange - Lessons learned from a public /private data collaboration. 2018.

such framework."

At this stage, for more traditional cloud IaaS and PaaS offerings, it may be difficult to strengthen EU-wide competitive offerings, but in specific segments, such as edge computing, distributed data management or SaaS, there may still be opportunities. This challenge is discussed in the public administration (*D-PA Challenge 10), agriculture (D-A Challenge 3)* and SME *(D-S Challenge 2)* demand scenarios, as well as the supplier landscape analysis (*S-L Challenge 1 and 2*).

Experts participating in H-CLOUD's webinar on Supply Side Challenges confirmed that it may be difficult for EU providers to gain significant market share in the IaaS and PaaS markets, but opportunities might exist offering tools to manage cloud native services in a multi-cloud environment, bringing services that can compete with hyperscalers, and avoiding duplication and competition. One participant noted simply that EU-based CSPs are less visible than other providers from a marketing standpoint.

Both the EUSD and Gaia-X propose the "interconnection" or "federation" of cloud providers in order to improve their market prospects, as well as proposing the creation of marketplaces to aggregate both supply and demand across the EU in order to strengthen EU providers. Some aspects of this "federation" effort align with various recommendations above (e.g. clarifying the rules and regulations around cloud services, strengthening auditing and certification capabilities). Observers at the Horizon Cloud Summit noted that cloud service federations, such as GAIA-X, are an opportunity to create a market where freedom of choice is central and EU values are respected.

3.2. Demand side challenges for public administration organisations

The public administration briefing paper (Annex 4) describes a diverse set of challenges.

- Small public administrations face a lack of skills and capacity to migrate to cloud services and need training and support.
- Large public administration bodies implemented multi-cloud and hybrid-cloud solutions to create efficiencies and improve services. This resulted in more complex environments that need extra management effort and technology.
- Across sectors, as fostered by EU policy guidelines, public administrations implemented cross agency and cross border cooperation and coordination.
- At the highest organisational and deployment level, they are implementing smart city technology and coordinating the deployment of multiple sectors in smart city trials, with varying degrees of success.

In addition, as noted in the Horizon Cloud Summit, EU Member States need to match the EC's own support for cloud adoption, but adapting their own IT strategies, evolving from traditional hardware procurement to more flexible policies on cloud technology.

Despite these challenges all countries have adopted policies and programs to promote cloud adoption in the public administration sector:

- The UK was at the forefront with its G-Cloud program, which included a cloud-first policy, a cloud marketplace, security certification standards and a private cloud hosted service joint venture[21].
- Italy 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.

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

- Poland’s Joint State IT Infrastructure Program (WIIP) 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).

Even with these efforts, cloud service adoption in government and public administration remains low – well below that of other sectors. Reported barriers to cloud adoption include:

1. Policy and regulatory implementation challenges: For instance, lack of legal expertise, technical competence, or capital resources to comply with the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive[22].
2. Technical architecture constraints: migrating and integrating with legacy systems, forcing applications and data to adapt to existing processes.
3. Organisational and skill barriers: Many small local government organisations have limited budgets to acquire skills or train staff. Procurement forces a strict OpEx/CapEx split, when cloud services are often charged as OpEx. This creates misalignment between IT function, user and the finance rules.

Where security and data protection are quite stringent, there is the need to integrate many legacy systems and so organisational change can be difficult and in-house solutions are seen as the safest solution. Examples include command and control, tax, revenue and welfare benefit. In contrast, more standard ERP and financial systems can be migrated to cloud-based solutions.

Opportunities for more sophisticated solutions exist using the Internet of things, AI and computing intensive applications (e.g. data feeds from cameras). Some organisations have implemented such approaches directly, whilst others acted as coordinators of others’ expertise (e.g. in smart city implementations). Despite all this cloud deployment issues still exist for both simpler solutions that bring efficiencies and cost savings, and for more sophisticated cloud-based solutions.

The EUSD proposes a sophisticated solution for public administration challenges, with 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.

The public sector has a history of federating together to provide collaborative solutions. These have varied from regional shared service centres, to whole government services and European grids, to EU programmes funded to pilot innovative digital solutions in the Digital single market. There is the potential for federation across specific public administration internal resources and external resource providers.

[22] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Table 3. Demand side challenges for public administration

<table>
<tr><th rowspan="2">Organisational complexity</th><th colspan="3">Deployment sophistication</th></tr>
<tr><th><b>A:</b> Relatively simple cloud deployments</th><th><b>B:</b> High data protection and security needs</th><th><b>C:</b> Sophisticated deployment of more advanced technology</th></tr>
<tr><td><b>Level 4:</b> Cross sector coordination</td><td>The simplest level of smart city deployment.
Many at pilot stage. To be more secure and sophisticated needs a clear path for solutions. (D-PA Challenge 13)</td><td>A few initiatives exist that have explored the data protection and security issues. (D-PA Challenge 13)</td><td>Cities act to coordinate activity across smart city initiatives. Few successes exist. Many at prototype stage (D-PA Challenge 13)</td></tr>
<tr><td><b>Level 3:</b> Multiple organisations, same sector</td><td colspan="2" rowspan="3">Public administration organisations can struggle with regulatory compliance in the cloud (D-PA Ch 1 & 2), data sovereignty issues (D-PA Ch 3), cloud migration of legacy apps (D-PA Ch 4 & 5), IT skills and resources (D-PA Ch 6), procurement and IT governance practices (D-PA Ch 7). Lack of SaaS alternatives appropriate for PA (D-PA Ch 11).</td><td rowspan="2">Organisational challenges with coordinated IT initiatives (D-PA Ch 8), advanced IT development (D-PA Ch 9). Difficulty choosing between widely adopted, yet still deficient, hyperscale solutions, high cost home-grown alternatives (D-PA Ch 10), and partial open standard solutions (D-PA Ch 12).</td></tr>
<tr><td><b>Level 2:</b> Single larger organisation & supply chain</td></tr>
<tr><td><b>Level 1:</b> Single small/med size organisation</td><td>Hard for smaller public administration organisations to exploit leading Edge technology.</td></tr>
</table>

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. [Research, Policy]

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 a 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 centre, 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 (See also *D-PA Recommendation 10.2* below). [Deployment, Policy]

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. [Policy]

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-architectured.

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. [Research, Deployment]

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, analyse to find common requirements, and analyse the gap with available solutions from ISVs (SaaS or not). [Deployment]

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: Favour coordinated procurement and management of cloud services. Support procurement of cloud services in a coordinated manner through national or regional cloud marketplaces. Favour exchanging best practices of shared IT services in government that can jointly manage cloud services across small entities. [Policy, Deployment]

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. [Deployment]

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. [Research, Deployment]

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. [Deployment, Policy]

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. [Deployment, Policy]

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. [Deployment]

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. [Deployment]

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. However, 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 backup copies on premise without adding too much to the total cost of ownership of the solutions [Deployment, Policy]

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. [Deployment]

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. [Deployment]

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. [Research]

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. [Deployment]

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 neighbourhood 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. [Research, Deployment]

3.3. Transport sector challenges

The transport sector briefing paper (Annex 5) highlights the potential of multi-party collaboration, the challenges of rapidly changing technology across the sector, and sustainability challenges.

Change in the sector is causing the blurring of industry boundaries and the redefinition of business models. This is being caused by three trends:

1. The technological innovation of vehicles and fuels.
2. The transition from vehicle-centric passenger mobility, where each transport mode was considered in isolation, to multi-modal, person-centric, mobility.
3. Collaborative logistics changing the transportation of goods and the environmental sustainability of freight.

Digital advances should improve operational efficiency, with the collection of data for advanced analytics and AI creating actionable insights, such as intelligent traffic management, better asset utilisation and better customer experiences. However, all must respect privacy and safety whilst people move.

The specific barriers to adoption for the transport sector are:

- Technical architecture constraints: complex ecosystems still have to integrate with existing legacy applications and proprietary systems. This makes system migration and data interworking far more difficult.
- Policy and regulatory concerns: particularly GDPR and ensuring compliance with the NIS Directive.
- Organisational barriers: Many small transport companies, with limited budgets and cloud skills. Reluctance to use ecosystem platforms. Fear of sharing data and giving away competitive positions. Cities want to use data from transport providers, but transport providers want to retain their data to promote their own services.

Many of the organisational barriers listed are addressed in the EUSD, which proposes to create a common European mobility data space as well as comprehensive programs in its upcoming ‘Smart and Sustainable Transport Strategy’ (Q4 2020). These actions will support existing efforts, such as those by the Digital Transport and Logistics Forum, which is working on a concept of ‘federated platforms’ to define what needs to be done at the EU level to facilitate data-sharing/re-use by connecting different public and private platforms.

There is also growing adoption of IoT, AI, edge, dedicated short range communication (DSRC) or other reliable high-speed networks to connect vehicles. Many industry specific solution providers are re-architecting their solutions as software-as-a-service (SaaS), hosting their applications in turn on major IaaS providers.

On the supply side, European technology players have the opportunity to build industry-specific solutions for both passenger and freight transportation. There are many SMEs in fields like logistics, micro-mobility and vehicle sharing, autonomous and electric vehicles design and manufacturing. These smaller players need secure and interoperable cloud-based services that use open standards, offer transparent contractual conditions, and modular pricing. They also need the digital skills to be able to use cloud-based services to accelerate implementation of digital products and services.

This extends to the providers of actual transport services who also need secure interoperable cloud-based services to accelerate the development and deployment of their digital products and services.

Table 4. Demand side challenges for the transport sector

Organisational complexity	**Deployment sophistication**		
	A: Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advance technology
Level 4: Cross sector coordination	Blurring of traditional industry and business. Collaboration across organisations and sectors. New market entrants.	The sector is a key player in a coordinated approach to smart cities. Early days though.	
Level 2: Single larger organisation & supply chain	Integration of legacy transportation applications (D-T Ch 3).	Secure access, sharing and analysis of distributed data (D-T Ch 1)	Interoperable data (D-T Ch 4)
Level 1: Single small/med size organisation	Difficulty complying with regulations like GDPR, NIS Directive (D-T Ch 2) Limited skills and expertise (D-T Ch 5) Suitability of cloud services and contracts (D-T Ch 8)	Transportation SMEs need secure cloud services that can be integrated (D-T Ch 6) High-tech SMEs need digital skills (D-T Ch 7)	Support Transport SME ecosystem with more suitable cloud services that allow innovative development yet protect competitive positions.

D-T Challenge 1: Secure access, sharing and analysis of distributed data. Transport stakeholders need to securely manage the data held by their organisations while enabling authorized access to and sharing of that data outside the organisation.

D-T Recommendation 1: Support creation of distributed data management solutions, compliant with the GDPR, to enable transport sector organisations to work together, share data productively, while at the same time controlling access to proprietary and/or competitive data. [Deployment]

D-T Challenge 2: Difficulty complying with regulations like GDPR, NIS Directive. Transport executives need to comply with EU regulations that protect privacy of personal data and resilience of critical digital services.

D-T Recommendation 2.1: The European Commission must ensure that EPDB, EPDS and ENISA work closely with cloud operators to update and expand technical and governance guidelines to enable cloud-based services, including innovative ones, like Mobility as a Service and Ride Hailing, that align with GDPR and the NIS Directive requirements. Also, ensure that there are mechanisms to enforce those policies and offer guidance through codes of conduct. [Policy, Deployment]

D-T Recommendation 2.2: Build GDPR-compliance into solutions so that transport clients, and transportation end-users, are not burdened with solving these problems. [Deployment]

D-T Challenge 3: Integration of legacy transportation applications. It is challenging and expensive to integrate the many legacy systems found in the transportation sector into cloud solutions, since they would need to be rewritten and/or re-architected.

D-T Recommendation 3.1: Encourage academic institutions and industry associations to collect and disseminate best practices toolkits for cloud readiness assessment and migration toolkits that are specific to transportation processes and systems, such as booking, payment, navigation, fleet management. [Research]

D-T Challenge 4: Interoperable data. Effective data sharing requires harmonizing data definitions and metadata so that the data can be discovered, accessed and shared as appropriate for meaningful analysis. Metadata plays a very important role for semantic interoperability, otherwise data collected by one stakeholder of the transportation ecosystem for a specific business purpose (e.g. miles travelled collected for fleet maintenance) cannot be leveraged by other parts of the ecosystem (e.g. utilities to offer timely and affordable electric vehicle charging services).

D-T Recommendation 4: Expand data interoperability. The European Commission, in the context of the EUSD, must build on the work started by International Data Space and more recently GAIA-X[23] to address technical, semantic and organisational interoperability. The European Commission can be the unbiased third-party that helps ecosystem stakeholders learn how they can benefit from data sharing, starting with real-life use cases, building on existing data standards such as GFTS[24], GBFS[25], MDS[26] and facilitating the creation of a "Common European mobility data space". Efforts must include creation and adoption of governance structures and processes that drive multiple stakeholders to actually exchange the data, because they understand what they gain from the exchange. A key factor to encourage data interoperability, in this and other sectors, would be also the wide adoption of FAIR Principle[27] [Policy, Research, Deployment]

D-T Challenge 5: Limited skills and expertise. Many transportation sector players are small. They have a limited budget to acquire or train technical and business skills to develop, deploy and manage cloud services.

D-T Challenge 6: Transportation SMEs need secure cloud services that can be integrated through open data standards and APIs, offer transparent contractual conditions, and modular pricing.

D-T Challenge 7: High-tech SMEs need digital skills to be able to use cloud services to accelerate digital products and services for the transportation industry.

D-T Challenge 8: The suitability of cloud services and contracts. SMEs who do not have the purchase expertise end up with discriminatory contracts.

3.4. Energy sector challenges

The energy sector, part of the Digital Europe programme plans, is important as part of the Critical National Infrastructure (CNI) of advanced nations. The analysis of the energy sector

[23] Federal Ministry for Economic Affairs and Energy. Project GAIA-X.
[24] https://developers.google.com/transit/gtfs/reference/
[25] https://github.com/NABSA/gbfs
[26] https://github.com/openmobilityfoundation/mobility-data-specification
[27] https://www.go-fair.org/fair-principles/

demand side challenges spans the whole sector value chain: 1) sources of fuel, 2) electrical power generation, 3) electrical power distribution and 4) power consumption. More details are available in the energy sector briefing paper (Annex 6).

Three main situations present opportunities in the energy sector:

1. Edge-based sensors used to monitor generation, transmission and distribution to improve reliability, flexibility and reduce maintenance costs, coupled with AI to anticipate issues. Requires robust security solutions for across the network, including Edge-based infrastructure.
2. New forms of power generation supervisory control and data acquisition (SCADA) systems are being developed and installed. These operate at local, regional and national levels to better manage the highly distributed power utility assets in a highly secure manner.
3. Edge-based sensors used to monitor extraction and cropping activities to police compliance. The issue here is how to deploy devices to ensure their continued function and effectiveness, alongside privacy issues.

In addition, there are a number of regulatory initiatives[28] driving growth of data in this sector and efforts to share and integrate that data:

- Several EC directives establish accessibility and portability of meter and energy consumption data on a transparent, non-discriminatory, privacy-compliant basis.
- Electricity network operators have newly mandated data-sharing obligations.

The EUSD has proposed the creation of a common European energy data space to support these initiatives, notably in the context of improving the interoperability among smart buildings and products, in order to improve energy efficiency, optimise local consumption and broaden integration of renewable energy sources.

Table 5. Demand side challenges for the energy sector

Organisational complexity	Deployment sophistication		
	A: Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination	Balance "demand side management" with Green ICT. (D-E Ch 8)	Security of energy systems: Requires in depth cloud service security (D-E Ch 1, 2 & 3) Data sharing across the sector to create insights (D-E Ch 4)	Edge opportunities (Requires reliable fast networks) e.g. IoT in generation & transmission & distribution, or monitoring (D-E Ch 5, 6 & 7) Dynamic energy regulation limits adoption of new ICT technology (D-E Ch 9)
Level 3: Multiple organisations, same sector			
Level 2: Single larger organisation & supply chain			
Level 1: Single			

[28] Article 24 Directive (EU) 2019/944.

small/med size organisation			

These opportunities present four groups of challenges and potential for more investigation and research:

Security of energy systems[29]:

D-E Challenge 1: Highly secure cloud-based environments are needed to support very sensitive energy management systems. [Deployment]

D-E Challenge 2: Security must be identified as a priority aspect of applied research in this area, and should be a fundamental component of all energy systems research (from project work-plan to programme design) rather than addressed as a separate issue. [Research]

D-E Challenge 3: Security aspects of federated cloud services might be inherently more secure than centralised cloud services. [Research]

Data sharing across the sector to create insights:

D-E Challenge 4: **Data sharing across the sector.** Data and information need to be able to move freely between cloud services to enable practical information and knowledge sharing to take place. [Research]

Edge opportunities:

D-E Challenge 5: **Edge-based IoT automation** can enable efficiency increases in the generation, transmission and distribution components of the supply chain. [Research]

D-E Challenge 6: **Air- and Space-Based Edge infrastructure.** Edge infrastructure needs to include space-based and loiter-capable lighter than air and air-breathing assets such as dirigibles or drones. [Research]

D-E Challenge 7: **Good network connectivity to support the edge.** Edge infrastructure requires good network connectivity, which is not always available. For instance, 5G deployment cannot be restricted to urban areas in the same way that 4G has been. [Deployment]

Effects of regulation and challenging environmental targets:

D-E Challenge 8: **Balance energy demand side management with green ICT targets.** Balance increased (demand-side) energy efficiency targets and (supply-side) green computing targets. Regulatory measures on either side impact the other. [Policy]

[29] EUSD, p 36, highlights that “work is ongoing to address energy-specific [cybersecurity] challenges, notably: real-time requirements, cascading effects and the mix of legacy technologies with smart/state-of-the-art technology”

D-E Challenge 9: **Dynamic energy regulation limits adoption of new ICT technology.** The very dynamic regulatory environment limits the energy sector’s ability to make plans and innovate. A long-term strategic plan is required to bridge the current gap between policy and consumer-led demands. [Policy]

3.5. Challenges in agriculture sector

This demand scenario looks at requirements and challenges for cloud adoption and data-enabled business in several related sectors, including agriculture and food supply in particular.

3.5.5. Landscape of agricultural sector and agriculture 4.0

The agriculture sector is a multi-disciplinary sector that includes farmers, producers and representative associations, suppliers (seed, fertilizer, feed, supplements, etc.), specialized contractors (e.g. harvesting labour and machines), downstream supply chains, machinery, vehicles and systems (e.g. irrigation), weather forecasting, land use monitoring, and other environmental monitoring systems (nutrient management, water pollution), as well as biology, nutrition and climate scientists.

Processing and analysing agricultural production data, especially in combination with other data on the supply chain and other types of data, such as earth observation or meteorological data, allows for precise and tailored application of production approaches at farm level, and enables farmers to optimize their operations and improve the performance of their own farm business. These activities represent the “digital transformation” of agriculture and have sometimes been termed “precision agriculture” or “Agriculture 4.0”, paralleling the broader “Industry 4.0” concept.

The EUSD has proposed a cross-border pan-European data space focussed on agriculture, intended to enable the digital transformation of the sector. Challenges specifically associated with realizing this common agricultural data space are identified along with more general challenges facing the digital transformation of agriculture.

3.5.5.1. Primary producers

The agricultural sector centres around farms and farmers themselves, the vast majority of which are either subsistence farms or have extremely small economic output. The total number of farms in the EU was 10.5 million in 2016[30], but only 304,000 (2.9%) of these farms had annual output of more than €250,000. (The minimum asset size typically defined for a small- or medium-sized enterprise (SME) is €2 million.) Just 3.3% of all EU farms (347,000) accounted for 52.7% of utilized agricultural area and 55.6% of Europe’s total agricultural output.

Compared with the other sectors considered in this deliverable, “cloud adoption” by the vast majority of farmers and other agricultural producers should probably be interpreted as “digitally enabled”, just as individual citizens might be “digitally enabled” through broadband access to the Internet, availability of modern computers at home or mobile devices, and skills in using those technologies to improve their own lives and well-being. This perspective becomes more significant given that 55.7% of farmers are over 55 years old, and 68.7% have no formal training in farming, only practical experience. When farmers are thinking about digital tools, few are thinking about public cloud, private cloud, multi-cloud, etc. but rather looking for the right application(s) for their personal computers or mobile phones that can help them manage their farms efficiently and take advantage of new services that improve their profitability. Even the largest 3% of farms mostly fall into the “SME” category and face the same constraints on

[30] https://ec.europa.eu/eurostat/documents/3217494/9455154/KS-FK-18-001-EN-N.pdf/a9ddd7db-c40c-48c9-8ed5-a8a90f4faa3f

resources and skills faced by SMEs (see chapter 3.8 and Annex 10).

3.5.5.2. Farm Management Systems (FMSs)

Farm management systems (FMS) are the primary digital enabler for farmers. The FMS category generated $1.5 billion in global revenues in 2017, dominated by many US and Canadian software vendors, as well as offerings from companies in France, UK, Germany, and Italy, and revenues are projected to grow to $1.8 billion by 2023[31]. Some FMS offerings are packaged in software-as-a-service (SaaS) formats with both desktop and mobile interfaces, as well as monthly pricing plans.

FMS products evolved out of several categories:

- Packages that started life as farm-focussed accounting and "enterprise resource planning" (ERP) software, expanding with interfaces to suppliers and customers, as well as data services that integrate data collected from farm machinery, earth observation services as well as IoT devices such as wetness indicators installed at key points on the farm. While a few FMS vendors of this type are significant in size, most are SMEs, with limited resources to support broad development activities related to data sharing, security, privacy, and integration.
- FMS packages integrated with data collected from farm equipment. Farm equipment collects real-time data not only on the operation of the equipment, but also on the actual operations being performed by the equipment and where those operations are being conducted. Manufacturers originally added these tools to create competitive advantage as well as some "stickiness" around purchasing decisions, but they have increasingly recognized that closed platforms cannot achieve market dominance and that customers expect interoperability among these platforms[32].
- FMS packages linked to downstream suppliers, such as Bayer CropScience's Climate FieldView and Corteva's Encirca[33]. Here the focus is to use agronomy (the science of soil management and crop production) to generate insights on planting, irrigation, fertilization, etc. in pursuit of optimal crop yield and quality.

Each of these FMSs promises improvements in productivity and performance through expanded technology and data integration. At the same time, these FMSs are marked by limited integration or interoperability of either services or data[34], making it difficult for farmers even to make confident choices about which FMS(s) to use, much less using them seamlessly to manage their farm activities effectively.

3.5.6. Potential impact of agriculture 4.0

The digital transformation of agriculture could trigger an 8.8% increase in agricultural output in Europe[35], representing roughly €38 billion in potentially increased output.

[31] https://cropom.com/articles/the-farm-management-software-market

[32] https://www.cema-agri.org/images/publications/position-papers/2020-09-08-CEMA-Common_European_Agricultural_Data_Space.pdf

[33] Corteva was formed from the merger of DowAgroSciences, DuPont Crop Protection and Pioneer.

[34] Tummers, J., Kassahun, A., and Tekinerdogan, B. (2019). "Obstacles and features of Farm Management Information Systems: A systematic literature review". In: Computers and Electronics in Agriculture 157, pp. 189–204. issn: 0168-1699. https://doi.org/10.1016/j.compag.2018.12.044. http://www.sciencedirect.com/science/article/pii/S0168169918307944. Munz, Jana, Gindele, Nicola, and Doluschitz, Reiner (2020). "Exploring the characteristics and utilization of Farm Management Information Systems (FMIS) in Germany". In: Computers and Electronics in Agriculture 170, p. 105246. issn: 0168-1699. https://doi.org/10.1016/j.compag.2020.105246. http://www.sciencedirect.com/science/article/pii/S0168169919316126.

[35] https://www.mckinsey.com/industries/agriculture/our-insights/agricultures-connected-future-how-technology-can-yield-new-growth

Farmers' willingness to pay is constrained by their expectations of the benefits of digital transformation. Some research[36] suggests there are limited expectations of such benefits which would provide limited incentives to invest in digital transformation, even for the 300,000 largest farms in Europe. The projections of increased output above translate into more than €400 per hectare of aggregate increased output, but this assumes every farm benefits from all possible improvement scenarios. Implementing the first scenario with positive payback could be more challenging.

In contrast with these macroeconomic estimates, many agricultural enterprises are seeing benefits from their investments in "Agriculture 4.0". For example, GAIA[37] in Australia provides a satellite-based analysis of crop health, delivered to customers via the web, for AU$40/hectare-year, and GAIA presents a case study showing over AU$2,000/ha in resulting financial benefits, or a 50X payback. Idroplan[38], an Italian agritech startup, monitors irrigation and crop protection for wineries for roughly €30/ha-year and has seen benefits ranging from €100-600 per hectare per year (3-20x payback). Clearly there are scenarios where precision agriculture offers a return on investment to farmers.

3.5.7. Challenges to agriculture 4.0 and a European agricultural data space

Generating the benefits described above requires a number of challenges to be addressed:

- Uncertain payback from investments,
- Lack of appropriate, affordable connectivity on the farm,
- Lack of a trusted, much less secure and comprehensive, data sharing/data exchange regime,
- Complexity of integrating both technology (e.g. remote sensors on the farm) and data (e.g. satellite imagery, data collected by farm machinery),
- Difficulty for farmers analyzing and interpreting the integrated data themselves, and lack of trust in insights and recommendations that might be offered by vendors.

As noted above, it is unclear if the benefits of precision agriculture will outweigh their costs. Selected case studies highlight successful scenarios, but it is difficult for farmers to know *a priori* whether specific investments will pay off.

Connectivity on farms has been a long-standing challenge to transformation in agriculture. The EU agriculture community has recognized this challenge and has consistently advocated for improved connectivity in rural areas[39].

Farmers' "sovereignty" over their own data was described as a principle of the 2018 "EU Code of conduct on agricultural data sharing by contractual agreement"[40]. This self-regulatory code of conduct goes some way to address farmers' concerns that data were being collected on their farms (e.g. by farm equipment) without respecting this principle. Work is still needed to implement technical solutions that will facilitate trust in agricultural data sharing solutions, and separate regulatory oversight (rather than self-regulation) may be needed to build trust by the farming community in these solutions[41].

The community has recognized the need for greater interoperability across systems, platforms

[36] https://www.precisionag.com/digital-farming/data-management/what-is-the-value-of-sharing-farm-data/
[37] https://gaia.ag/
[38] https://www.idroplan.org/
[39] Copa-Cogeca perspective on long term vision for rural areas_EN
[40] https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf
[41] Sanderson, J., L. Wiseman, S. Poncini (2018), "What's Behind the Ag-Data Logo? An Examination of Voluntary Agricultural Data Codes of Practice", International Journal of Rural Law and Policy (https://doi.org/10.5130/ijrlp.1.2018.6043). See aso Tatge, J. (2016), "The land grab for farm data", TechCrunch, (https://techcrunch.com/2016/07/06/the-land-grab-for-farm-data/).

and ecosystems. Over the last few years, several platforms focussing on data sharing have been created to improve interoperability, and several large EU-funded projects have focussed on the digital transformation of European agriculture. The ATLAS project[42] specifically targets the "interoperability of agricultural machines, sensors and data services and enable[s] farmers to have full control over their data and decide which data is shared with whom and where".

The EUSD's proposal to create a common European agricultural data space contemplates building on the progress of these initiatives and projects. However, it is unclear how such a common data space would relate to existing initiatives or to existing FMS ecosystems. Participants in an Expert Workshop on a Common European Agricultural Data Space[43], convened on September 8, 2020, raised a number of organisational concerns about the new initiative:

- The new data space might be competitive or threatening to their existing business, rather than complementary.
- How will the business investments, intellectual property and other assets that have been built up over time be protected?
- How will the new data space add value to existing FMS and data sharing offerings?
- How would a new federated approach operate, and specifically how would existing business arrangements (contracts) between participants, or even broader commercial platforms, be accommodated in any transition to a new federated model?

Other issues raised in the Workshop:

- **Semantic Interoperability.** If data is to be "joined up" in a data space, the meaning of each piece of data must be well defined. This "semantic interoperability" is critical to a well-functioning data space in any domain. Participants in the Expert Workshop acknowledged the importance of semantic interoperability, as well as the challenges involved in achieving it. Some participants recommended that there should be respect for existing efforts around interoperability, rather than any imposition of new schemes. (Annex 7 details progress in this area.)
- **Technical Interoperability: Need for a common architecture.** Workshop participants identified the need for an agreed architecture of the data space, allowing participants to map their activities and technical functions onto a larger framework and work together more effectively. This problem requires alignment and harmonization of at least seven high level architectures that have already been proposed over the last two years (detailed in Annex 7).

3.5.8. Data required for a common European agricultural data space

A number of data sources have been identified as important for the functioning and utility of a common European agricultural data space. In contrast to farm-related data and data collected on farms, where data sovereignty and control over data sharing are important concerns (discussed above), the challenge with these common data sources is one of accessibility – ensuring that these data comply with FAIR principles (findable, accessible, interoperable, reusable).

Data sources referenced in connection with a common European agricultural data space fall into four categories (see Annex 7 for a detailed listing):

- Geospatial Data

[42] https://www.atlas-h2020.eu/

[43] Summarizing position papers submitted to https://ec.europa.eu/digital-single-market/en/news/expert-workshop-common-european-agricultural-data-space-0

- Meteorological Data
- Agriculture Reference Data
- Agricultural Administrative Data.

The EUSD proposes, in connection with the Open Data Directive, to support Member States in making their geospatial, earth observation and environment, and meteorological data accessible and available as part of common European data spaces. The range of these data sources highlights the scale of effort that will be required to make them findable, accessible and interoperable.

For example, for Copernicus-based earth sensing data, the European Commission funded the deployment of four separate cloud-based platforms that provide access to distinct sets of Copernicus data and related processing tools (DIAS). These platforms are not federated, so it is difficult to bring these data sets together for analysis and interpretation, which may be needed to support consistent services provided to farmers. The EUSD refers to “interconnection” of both DIAS (referred to as a single entity) and the European Open Science Cloud with the proposed cloud federation, in order to encompass Copernicus data within a broader common data space, but more work will be needed to achieve seamless access and integration, both from a data and a data processing perspective.

The “interoperability” challenge of Copernicus data is linked with an “accessibility” challenge: Earth data, including the open data from the Copernicus programme, are often too big to download and store locally, therefore, co-locating data access services and the related data processing facilities is urgently needed. By contrast, Google Earth Engine[44] is an example of a commercial PaaS cloud service, providing an integrated data, storage, computing, and software environment. The EUSD’s reference to “enhancing the Copernicus ecosystem through the application of European digital technological solutions”[45] may signal action to address this challenge.

As a different example of interoperability challenges, national/regional farm land registries have been incorporated into the EU’s Integrated Administration and Control System (IACS) created to support the Common Agricultural Policy (CAP), but these registries are difficult to access consistently and can exhibit inconsistencies across registries, with individual farms variously identified, making it difficult to integrate land parcel (cadastral) data into FMSs or a common European agricultural data space.

3.5.9. Demand side challenges in the agriculture sector

Table 6. Demand side challenges in the agriculture sector.

	Deployment sophistication		
Organisational complexity	**A:** Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination	“Farm to Fork” value propositions and stakeholder involvement (D-A Challenge 1)	Trusted mechanisms for	Accessibility and Interoperability of

[44] https://earthengine.google.com/
[45] EUSD, p. 17.

Level 3: Multiple organisations, same sector	Clear value proposition for data sharing and data spaces (D-A Challenge 1)	data sovereignty and confidentiality (D-A Challenge 4)	data across the data space (D-A Challenge 5) High performance access to large data sets through the co-location and coordinated provisioning of computing, applications and data spaces (D-A Challenge 6)
Level 2: Single larger organisation & supply chain	Enough flexibility for service providers to differentiate themselves and profit (D-A Challenge 3) Affordable connectivity and IoT devices (D-A Challenge 2)		
Level 1: Single small/med size organisation	Millions of farms are “micro-scale” businesses (<5 employees), with limited/no IT resources or skills (D-A Challenge 1) Affordable connectivity and IoT devices (D-A Challenge 2)		

D-A Challenge 1: Value proposition for farmers in for precision agriculture and data sharing. Regardless of farm size, for the most part farmers remain sceptical of the return on investment in precision agriculture, and in data sharing in particular. For larger farms, and the broader value chain (“farm to fork”), work is still needed to develop compelling business models for complex new solutions. For the smallest farms, of which there are millions across Europe, embracing precision agriculture is difficult given limited resources for this kind of activity.

D-A Challenge 2: **Affordable connectivity and IoT devices.** Precision agriculture and data sharing depend on the availability and affordability of connectivity to each farm, as well as the affordability of the IoT devices that create the data that might be shared.

D-A Challenge 3: **Value proposition for service providers/FMS vendors in the context of a common European agricultural data space.** The EC is perceived by some ecosystem participants as creating a new platform that, if not “competitive”, at least disrupts their current business plans.

D-A Challenge 4: Sovereignty and confidentiality for farm-based data. Limits on the current Code of Conduct, as a self-regulatory approach and one linked to the need for clear and balanced contractual arrangements. Lack of effective and trusted technologies that can be relied upon to protect confidential data while enabling the kind of data sharing that might be beneficial to data owners. Need for trusted oversight mechanisms that will help farmers protect sovereignty over their own data.

D-A Challenge 5: **Accessibility and interoperability of data across the data space.** The “public” data proposed to be incorporated into the Common European Agricultural Data Space will require significant investment before it is easily accessible by average users, or before it will be interoperable with other data sources in the data space or with existing systems already operating in the market.

D-A Challenge 6: **High performance, *in situ,* analysis of distributed big data.** Today this requires local downloads which are undesirable for many reasons. No market solutions exist today, proven at the scales needed for the volume of data required.

3.6. Challenges in healthcare and human health research

This demand scenario looks across many healthcare sectors (see Annex 8). It spans:

- Fundamental research (such as genomics),
- Clinical trials and advanced clinical practice
- Hospital, primary and community care (care delivered outside hospitals through the health system and through at-home social services)
- Public health to prevent and react to health crises that affect the population as a whole.

The healthcare and health research sectors are merging into a continuum of care-provision, as each component offers benefits to the other components. This requires integration of the underlying ICT ecosystems to improve effectiveness (better outcomes) and efficiency.

Many of the challenges identified below are noted in the EUSD, which proposes to create a common European health data space, with both harmonizing legislation and investment in support of interoperable electronic health records, genomic data, medical imaging, laboratory reports, and prescriptions.

Table 7. Demand side challenges for healthcare and health research

	Deployment sophistication		
Organisational complexity	**A:** Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination	Non-health organisations already collect health information from apps. Potential to integrate with health information.	National regulations limit the ability to create data lakes across multiple countries. (D-H Ch 6)	
Level 3: Multiple organisations, same sector	Even anonymised human health research data must be treated as PHI, since it can be re-associated with other data to recreate PHI (D-H Ch 3)	Healthcare ICT functions need to be coordinated across multiple healthcare organisations (D-H Ch 1)	
Level 2: Single larger organisation & supply chain	Barriers to basic cloud service adoption: Many do not have the scale to deploy applications to cloud services. (D-H Ch 4)	Increased need for access and/or transfer of that data across organisational boundaries (D-H Ch 2)	
Level 1: Single small/med size organisation		Large volumes of data drives need for distributed data management. (D-H Ch 5)	

D-H Challenge 1: Healthcare ICT functions need to be coordinated across multiple healthcare organisations. This may require both sharing of sensitive data, and coordination of activities related to that data, as well as collaborative IT functions, such as coordinated enterprise resource planning (ERP) applications.

D-H Recommendation 1: Federation of healthcare ICT functions. [Deployment] Healthcare ICT could benefit from a federated solution, since it has several attributes required for successful "federation", namely:

- the need to combine disparate activities, as well as regional separate activities, into the cohesive improvement of human health,
- the presence of multiple healthcare providers that prefer to operate as peers
- the fact that many healthcare providers are publicly funded and resist the idea that external services to be integrated into their own services should be "purchased" rather than provided as a public good.

3.6.1. Personal health information and increasing use of edge technologies

Personal health information ("PHI") is highly sensitive. This has led to the creation of local siloed IT infrastructure protected by robust security. Unfortunately, the silos mean an historic lack of interoperability of healthcare solutions. National health systems have tried to address these issues whilst managing the risks of such initiatives.

The application of Edge computing, wearable devices, Internet of things (as well as robotics and artificial intelligence) is growing. They occur in remote monitoring and telemedicine, enabling mobile point of care, and "anywhere" healthcare. They are creating new challenges for securely collecting, storing, transmitting and processing PHI.

In practice, several national and regional healthcare systems are creating "data lakes" to support the various "big data" analyses of the healthcare data available across their jurisdictions. Even under the current regime, these data lakes are problematic. Often these data lakes are not distributed; rather data is being brought to a single facility to enable this analysis. Neither are they anonymized. Variations in national regulation of PHI across the EU currently limit the feasibility of creating data lakes with data from multiple countries.

D-H Challenge 2: Different healthcare sectors are integrating, which changes how PHI is handled. Healthcare innovations are driving increased need for access and/or transfer of that data across organisational boundaries. These changes are happening alongside the existing regulations for the storage, transfer and use of PHI. [Policy, Deployment]

D-H Recommendation 2: Create a common distributed data management solution, compliant with the GDPR, and particularly built with "Privacy by Design", in order to enable increased capabilities in the healthcare sector. [Deployment] The actions in connection with the proposed European health data space could support implementation of this recommendation.

D-H Challenge 5: Healthcare data volumes, and current initiatives to aggregate and process significant healthcare datasets, highlight challenges in efficiently accessing, sharing and analysing multi-national, distributed healthcare data while maintaining the protection, security and privacy of that data and avoiding unnecessary data movement and duplication.

D-H Recommendation 5: ECRIN and custom regional/national data lake solutions should be examined to see if they contain the seeds of wider solutions to the problem of distributed personal health data management. [Research]. This could be an important early step in the implementation of the European health data space.

D-H Challenge 6: Variations in national regulation of PHI across the EU currently limit the feasibility of creating data lakes with data from multiple countries.

D-H Recommendation 6: The medical exploitation of aggregated sensitive data in the cloud is recognised as a problem at the EU parliament level. Efforts must be made to overcome the associated problems. [Policy]. Legislative and regulatory harmonization is specifically mentioned in connection with establishing a European health data space.

3.6.2. Aggregation of personal healthcare information

Human health research has sought to balance the value of aggregating large cohorts of patient/sample data against the challenges of protecting the personal health information incorporated in that data. However de-identification and anonymization of genomic data have been shown to offer weak protection against re-identification.

D-H Challenge 3: Even anonymized human health research data must be treated as PHI, since it can be re-associated with other data to recreate PHI.

D-H Recommendation 3: All human health research enterprises must integrate GDPR compliance into their data management tools and policies, even when dealing with data regarded as exempt since it was anonymized. [Deployment] Data technologies supporting the European health data space should provide explicit support for the required privacy controls.

3.6.3. Adoption of cloud services by healthcare providers

The sector has “siloed” traditional healthcare ICT investments plus the need for data protection, security and privacy. Cloud service adoption raises real concerns around security, compliance, and IT governance, and can create a significant obstacle to cloud service adoption. Significant numbers of healthcare providers do not have the scale to take on these adoption challenges.

D-H Challenge 4: Intrinsic concerns by healthcare organisations about implementing compliant data protection, security and privacy could represent a significant obstacle to cloud adoption by this sector. Since the healthcare sector is also fragmented, significant numbers of healthcare providers do not have the scale to take on the challenge of data protection, security and privacy in the cloud, nor do citizens want publicly funded healthcare providers putting resources into duplicated solutions to this problem. They will hinder initiatives to combine the efforts of disparate healthcare providers into the cohesive improvement of human health.

D-H Recommendation 4: Technology solutions are required that simplify the adoption of cloud-based solutions, yet address the sector’s underlying needs. For example, provide GDPR-compliant PaaS components robust enough to meet the needs of the healthcare sector. Indemnify their users against privacy breach fines as long as certified best practices are applied. [Deployment]. The European health data space could act as a “testbed” to evaluate and validate candidate solutions, identifying robust solutions that can be adopted by other actors in the healthcare sector.

3.7. Demand challenges in manufacturing

The manufacturing sector plays a particularly important role in the European digital economy. First of all, because of its size. With 2 million enterprises, 28.5 million employees and €1,820 billions of value added generated in 2017[46], manufacturing is the largest contributor to non-financial business economy value added, accounting for more than one quarter of the total (29.3%) in the EU27. Moreover, manufacturing is the cornerstone of European industrial competitiveness in the worldwide market, in terms of excellence, export capability and technology innovation.

Driven by the convergence between operational technologies (OT) and information technologies (IT), European manufacturers are at the forefront of digital transformation, increasing their investment in multiple advanced technologies, playing a critical role in the emergence of the European digital economy. These innovative technologies include automation, robotics, IoT, data analytics, 3D printing and artificial intelligence. Manufacturing is also leading in the generation and exploitation of industrial data (from data-hungry factories to smart and connected products) which is considered by the European Data strategy a key competitive advantage for Europe. In fact, one of the main objectives of the Data Strategy is to create common European industrial data spaces to promote data sharing and improve competitiveness: in the case of manufacturing, the Data strategy estimates that the potential value of the use of non-personal data in the sector could reach € 1,5 trillion by 2027.

3.7.1. Cloud computing is key for manufacturing

Cloud computing is the underpinning infrastructure strategy that enables manufacturing to adopt and effectively implement the new wave of technology innovation. (Annex 9 explores the

[46] Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Manufacturing_statistics_-_NACE_Rev._2#Structural_profile

opportunities and challenges of cloud adoption by the manufacturing sector.) Cloud and IoT platforms are enabling technologies of automated smart factories, producing smart products through smart materials and an augmented workforce, working with AR/VR (augmented reality/virtual reality) tools and applications, wearables and working with co-bots (collaborative robots, designed for human-machine interaction)[47].

A 2019 survey[48] of 900 EU28 manufacturers determined that 77% of discrete manufacturing enterprises and 65% of process manufacturing enterprises were cloud users. A smaller 2020 survey[49] of manufacturers in 15 European countries showed that the share of manufacturers managing IT services across multiple cloud locations and providers was already 69%, a high level of uptake showing the speed of diffusion of the trend towards more sophisticated and complex cloud management.

IDC expects that by 2022, 70% of manufacturers will use cloud-based innovation platforms and marketplaces for cross-industry and customer co-development that creates 50% of new products and service ideas. In addition, product life-cycle management (PLM)-based cloud deployments will continue to rapidly evolve to become digital innovation platforms that support the service-centric approach of marketplaces[50].

Information technologies (IT) and operational technologies OT) are converging in manufacturing (as well as other sectors), and this convergence is both an enabler of smart manufacturing and a driver of organisational complexity. The integration of enterprise and shop applications enables data-centric computing and smart manufacturing platforms. The main benefits of convergence include the improvement of operational performance (throughput/service reliability at same or lower costs), more efficient resource sharing, better and more comprehensive security, improved product and service quality, and of course greater agility and flexibility[51]. This convergence has been an ongoing process for several years but is now reaching the upper levels of the organisation, through integrated IT/OT governance models, where investment decisions regarding control systems and execution systems are made through a shared services organisation, a centre of excellence, or a corporate function. In addition, decision making about investment and priorities for operations is undertaken as a single unit. Within three years, 50% of European enterprises should have an integrated IT/OT governance model. In addition, IDC expects that 40% of manufacturers by 2022 will employ a cloud platform that crosses traditional IT boundaries and integrates operational technology.

In this context, IDC identified multiple emerging digital transformation use cases where cloud computing plays a critical enabling role, such as intelligent shop-floor operations coordinated across multiple factories, omni-channel order orchestration and fulfilment to improve the customer experience (requiring real-time data sharing), quality and compliance monitoring and advanced digital simulation[52].

Cloud computing is also critical for data sharing in manufacturing value chains between manufacturers, their suppliers and their customers. According to the ATI survey, discrete manufacturing is the first sector in Europe for adoption of B2B industrial platforms for data sharing, with 20% uptake in 2019. However, data sharing in the manufacturing industry is still limited by relevant challenges of insufficient standardization, interoperability and lack of trust and motivation. This is why the EC is pushing for the launch of European shared data spaces in several key industries but particularly in manufacturing. Relevant B2B data sharing initiatives prioritize manufacturing, such as those promoted by the Industrial Internet Consortium (IIC

[47] IDC's Worldwide Artificial Intelligence Spending Guide Taxonomy, 2020: Release V2, 2020

[48] Advanced Technologies for Industry (ATI) project survey 2019, n=900, conducted by IDC on behalf of DG GROW and EASME.

[49] IDC European MultiCloud survey, Q2 2020, n=165 - Countries covered: AT, FR, DE, IT, NL, SE-DK-NO, PT, ES, UK, CZ, PL, RU, CH

[50] IDC FutureScape: Worldwide Manufacturing Product and Service Innovation 2020 Predictions

[51] Big Data Challenges for Smart Manufacturing, BDVA WhitePaper 2020, https://www.bdva.eu/sites/default/files/BDVA_SMI_Whitepaper_2020.pdf

[52] Source: IDC Worldwide Digital Transformation Spending Guide, July 2020

Layered Databus)[53], the IOTA Foundation (IOTA Data Marketplace)[54] and the International Data Spaces (IDS) Association[55]. According to the BDVA Smart Manufacturing Industry (SMI) Whitepaper, the IDS Reference Architecture Model is gaining momentum as an emerging de facto standard with the potential to rival or set the bar for other international data sharing space solutions, such as those by the Edgecross consortium[56] and the Industrial Valuechain Initiative[57] (both in Japan), and the MadeInChina2025 strategy[58] for the Chinese manufacturing industry. Its origins in Industry 4.0 make it particularly suitable for SMI applications. In the cloud environment, the Gaia X[59] collaborative initiative launched by the German and French governments and industries to develop a federated data infrastructure in Europe is raising strong interest by manufacturers as a way to solve cloud interoperability issues and at the same time guarantee digital sovereignty in Europe.

3.7.2. Cloud, edge computing, AI in manufacturing

Edge computing is a way to process data away from centralised storage, keeping information on the local parts of the network – edge devices. The move to edge computing in manufacturing is gaining steam, driven by the diffusion of IoT networks and AI applications leveraging data in real-time, where edge processing is more efficient, for applications such as intelligent shop floor monitoring and predictive maintenance of smart products. However, edge computing is not displacing the cloud but becoming another component of the flexible computing infrastructure required by the extreme dynamism of the manufacturing context, which spans from edge to cloud and back. The choice to balance centralized cloud platforms and edge platforms varies depending on the type of industry and the use cases.

In this distributed environment AI is needed for resolving key challenges, like (1) how to take into account what, where and when data is collected and analysed; (2) how to design services to respond to changes in application behaviour or data variability; and (3) how to react to changes and trigger rules associated with the content of the data and models[60]. This mix of technologies is paving the way for transformational use cases emerging in manufacturing, such as real-time production control, from visibility up to "zero touch" factories, advanced quality tracking and reporting based on autonomous visual inspection, outcome-based business models, based on data streams gathered for service execution and predictive maintenance. Nevertheless, this requires considerable investment for digital technologies on the shop floor. Enterprises must have increased computing power and sensor use, as AI solutions place extensive demand on IT infrastructure. AI solutions are based on adaptive algorithms which need constant optimization to enhance quality and process efficiency of shop-floor operations, requiring data flows in real time to be managed by the IT infrastructure. Manufacturers need different approaches in which the production lines are monitored and machines are integrated with real time sensors, thereby gathering real-time data and checking for any defects.

3.7.3. Cloud computing for sustainability in manufacturing

A key goal for future industrial production is guaranteeing the triple sustainability objective (i.e. environmental, economic and social). European manufacturers are developing circular economy strategies in order to minimize waste, reduce their carbon footprint and optimize their energy consumption moving towards renewable energy sources. All these processes are heavily data-centric and cloud infrastructures are often required to manage these challenges.

[53] https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf
[54] https://www.iota.org/
[55] https://www.internationaldataspaces.org/
[56] https://www.edgecross.org/en/
[57] https://iv-i.org/wp/en/about-us/whatsivi/
[58] http://english.gov.cn/2016special/madeinchina2025/
[59] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[60] Big Data Challenges for Smart Manufacturing, ibidem

For example, both for sustainability goals and to respond to market demands, manufacturers are investing in intelligent PLM (product life-cycle management) and SLM (Service life-cycle management) which are based on cloud platforms. AI-enhanced PLM and SLM can improve human decision-making during product development and service delivery, resulting in optimal customer, or consumer, experiences[61].

However, this transition creates new challenges. According to the BDVA Whitepaper on smart manufacturing, in order to ride the *servitisation* wave, an overall interoperability between product, data and services is needed as well as the development of new standards that extend their respective lifecycles. Then, of course, new privacy-preserving and data confidentiality/sovereignty processing architectures are needed, alongside lifecycle product models which are able to integrate the different stakeholders of complex long living products (such as ships, aircrafts, machinery, but also cars and smart appliances) in interoperable product lifecycle data models and for the industrial assets in standard asset administration shells. Digital twins (dynamic digital representations of physical systems, continuously updated with data about the performance of the twinned physical system) are an important example of such product lifecycle models.

As a technology, cloud computing is potentially environmentally friendly because it minimises energy consumption through virtualisation, multicore architectures, and the efficient scheduling of resources. Concerning energy efficiency, many manufacturers are deploying energy data management systems (EDMS), a tool used to collect, compress, and analyse data from various sources and output. Traditionally, an EDMS is set up locally and embedded into existing infrastructures, however, sometimes, the EDMS is moved to the cloud to allow faster and cost-effective analysis of energy data.

3.7.4. Cloud and manufacturing: key challenges

D-M Challenge 1: Cloud Management Challenges. Cloud computing is evolving fast towards an integrated approach to the development of value-added services, reflecting organisations' increasing need to seamlessly leverage edge and cloud resources from multiple cloud providers[62]. This requires new approaches, processes, and tools that link different platforms via a common methodological foundation that addresses all infrastructural layers. Over two-thirds of enterprises have created cloud centres of excellence to serve as focal points for defining business KPIs and operational processes, which are in turn used for decisions about where to deploy applications. End-user experience, cloud cost tracking, transaction health, compliance, and security policies all need to be consistent across multiple clouds and applications.

D-M Challenge 2: Cloud Data Privacy and Security. Requirements regarding security, privacy, and traceability in cloud environments are increasing with the number of organisations involved in data-driven services, as well as with the growing complexity of distributed networks. Organisations along the value chain require more than just to connect; they must also meet all data security, protection, and governance policy requirements. When data is transferred across company boundaries, new data security and privacy challenges arise around protecting stakeholders' interests. New technologies – such as those used for distributed ledgers, homomorphic encryption, multiparty computation, and federation – can enhance security-framework traceability and privacy during cross-company data exchange and acquisition. The trade-off is that storing data (hashes and signatures) in a blockchain or distributed ledger and performing operations using homomorphic encrypted data leads to the additional consumption

[61] IDC FutureScape: Worldwide Manufacturing Product and Service Innovation 2020 Predictions
[62] Cost-Efficient Request Scheduling and Resource Provisioning in Multiclouds for Internet of Things, Xin Chen, Yongchau Zhang, and Ying Chen, IEEE Internet of Things Journal, 2020

of computing and storage resources. These challenges must be met by suppliers and users at the industry-value-chain level, not simply at the individual-enterprise level.

D-M Challenge 3: Standardisation, Interoperability, and Data Portability. European organisations 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. And they demand fine-grained elasticity at low or marginal cost, including the ability to create 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. European suppliers must rise to these challenges and develop their offerings to respond to these needs. Investments are needed in the development of standards and interoperability in the multicloud environment. New collaborative initiatives are arising which could help to solve the challenges of interoperability and standardization in B2B data sharing and industrial data platforms, such as the IDS (International data spaces) proposed architecture and Gaia X to develop a European federated data infrastructure.

D-M Challenge 4: Skills and Organisational Challenges. Many European entities, particularly small and medium-sized enterprises, have insufficient budgets to gain (through acquisition and/or training) the technical and supplier management skills necessary 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 centralised function that manages IT assets and services. Cloud services require a shift towards operating expenditure, which opens the door to shadow IT purchases from line-of-business executives and managers who do not have a comprehensive view of how their choices impact overall costs, interoperability, or system security.

3.8. Demand challenges in SMEs

SMEs make up 99% of the European economy and account for 66% of all employment in the EU (see Annex 10 for additional detail as well as references for data). This analysis considers the challenge of “simpler organisations” as opposed to those classified as SMEs. The classification SME can cover a range of organisations some of which can be quite complex in their structure, business models and quite sophisticated in their use of digital technologies.

Adoption of cloud services amongst SMEs varies across the EU member states, partly reflecting comparative national strengths. SME cloud service adoption lags significantly behind adoption in large companies and has increased at a much slower rate.

Moreover, as noted in H-CLOUD’s webinar with SME experts on April 28, 2020, there are both “low-tech” and “high-tech” SMEs, and there is a large digital divide between them, so it is almost impossible to collectively refer to these organisations as one cohesive unit. Their different levels of technology maturity need a completely different approach to ensure that their diverse requirements are addressed.

There are several trends to remark upon:

1. Adoption propensity by each enterprise reflects the adoption rate of that enterprise’s vertical industry.
2. SMEs located in high cost nations have had more pressure to reduce costs.
3. Cloud service uptake has coincided with digital breakthroughs that encourage aggressive competition.
4. US and EU IaaS and PaaS cloud providers offer scalable virtual IT infrastructures.

5. There are still many small companies using old legacy systems that are not yet in the cloud.
6. Economic difficulties due to COVID19 and similar crises have pushed SMEs towards digitisation more than ever before.

3.8.1. The diverse needs of SMEs and how they are served

In general, SMEs have two types of needs:

- General needs such as email, data storage etc.,
- Special need such as high computing power

Adoption often starts when the suppliers of standard software (ERP, CRM, Office productivity) migrate to become SaaS cloud providers and take their customers with them. The large providers (Amazon, Google, Microsoft) are the obvious targets for cloud service adoption. When choosing providers, SMEs focus on simplicity and brand awareness, security and peace of mind, cheap prices (initially at least) and flexibility, the ability to scale up and down as required.

However, there are gaps in the larger cloud service providers' offerings that European providers could exploit.

1. **Value for money including for larger uses.** The larger cloud providers can be very expensive. When a smaller company needs high throughput and high performance, the price can become prohibitive.

2. **Sensitive data location fully in Europe:** With GDPR, the SMEs need to ensure their personal and sensitive data is fully in Europe. However, there is evidence that some business sectors are still not giving this much thought.

3. **IP protection security issues:** For companies creating sensitive intangible intellectual property, (e.g. drug discovery in the pharmaceutical sector) the large cloud service providers do not offer comfort. Such companies prefer to keep their services in house.

4. **Value added services that integrate with EU/country level services:** Many countries have implemented local eGovernment services. Should regional cloud service providers choose to integrate with this and provide a seamless workplace it would save productive time that is otherwise spent moving between cloud services.

5. **Interoperability problems between off-the-shelf solutions.** Many small companies use local SaaS systems that however fail to talk to each other and create additional headaches for the companies. This was highlighted by experts in the H-CLOUD SME webinar. Large cloud providers might not look into fixing such problems as they are deemed too small to be interesting.

6. **Wider accessibility of data.** Data-based business models are becoming more popular due to their lower barrier to entry and as such the availability of trusted data is imperative. Data spaces where data can be shared securely are important, as is the increase of dataflows between businesses and governments. Usage-rights of such data must be re-evaluated in order to minimise any possible disadvantages for SMEs.

Several of these points align with the Cloud services marketplace proposed within the European strategy for data, in which the ability for service providers to participate will be conditional based on "the use of transparent and fair contract conditions". These conditions are not always present within the current market, specifically to micro-enterprises and SMEs.

3.8.2. Employment issues

A large barrier faced by many SMEs wanting to migrate to, or exploit a cloud service, is the lack of skills and difficulty recruiting potential employees with the right skills. Whilst this is a wider problem, SMEs are particularly affected by it. This is not simply about technical skills, but also business skills. For instance, being able to answer questions such as, 'Why should we buy cloud services as a part of our strategy?' and 'What advantages would adopting cloud-based solutions give to our business?"

This was further highlighted by expert participants in the SME webinar held on 28th April where participants stressed the point that especially for the micro and small companies, it is nigh on impossible to have the specialised staff requirement to work on cloud computing issues, and it is usually the actual entrepreneur/owner itself that has to understand the systems. Therefore, they need greater support also by business support organisations.

Potentially, greater collaboration between vocational and educational establishments could help. However, the draw is always to the larger players who offer a high-quality training and experience on the CVs of future employees. Various EC supported initiatives have tried to address these SME specific issues.

This issue is highlighted within the SME Strategy for a Sustainable and Digital Europe in which, through the support of the Digital Europe Programme, a "Digital Crash Course" will be developed, enabling SME employees to become proficient in the latest technologies.

Further to this, a programme for "digital volunteers" is also mentioned, allowing "young skilled people and experienced seniors to share their digital competence with traditional businesses". In addition to the digital volunteers programme, an "SME to SME approach" is mentioned within the New Industrial Strategy for Europe, in which the increase in tech-savvy SMEs can be leveraged in order to assist industrial firms adapt and develop new forms of work for the digital age.

This approach has already created new opportunities, but improved forms of protection must be implemented, and support must be provided to help with this new economy.

3.8.3. Specific demand challenges for smaller companies and SMEs

Table 8. Demand side challenges for SMEs

Organisational complexity	Deployment sophistication		
	A: Relatively simple cloud deployments	**B:** High data protection and security needs	**C:** Sophisticated deployment of more advanced technology
Level 4: Cross sector coordination	A role for niche smaller players with enabling technology: How to support and enable wider cross industry initiatives.		
Level 3: Multiple organisations, same sector	How to be an innovative player: Cost of access to large data volumes. Restrictive contracts. Volume of data vs where to process it. (D-S Ch 3)		How to be an innovative player in the market? Protection of IP in the Cloud: IP risks and challenges. Potential opportunities for smaller niche players in specialist areas. (D-S Ch 3)
Level 2: Single larger organisation & supply chain			
Level 1: Single small/med size organisation	Availability of skills and resources (D-S Ch 1) Suitability of cloud services and contracts that enable savings and innovation (D-S Ch 2)		

D-S Challenge 1. Lack of skills and resources to help SMEs adopt and exploit cloud technologies. Challenges include migration of legacy applications to the cloud especially when these have been created several years ago and it is not worth it to migrate to cloud environments as the investment would be too prohibitive for small and medium companies.

D-S Recommendation 1.1. Help SMEs build skills and competence in the labour force. Foster collaboration projects between SMEs and vocational educational colleges or universities to address this issue. Create a pool of cloud experts that could work freelance at a subsidised or low cost to give services to SMEs. These could be students in their last years of Universities or entry level employees that are looking to build their curriculum. Similar solutions have been deployed in Nordic countries with good success. In addition, an “SME to SME approach” is mentioned within the New Industrial Strategy for Europe, in which the increase in tech-savvy SMEs can be leveraged in order to assist other companies and develop new forms of work for the digital age. [Deployment]

D-S Recommendation 1.2. Create deployment calls that focus on SME issues and not on supply or research. These can be focused on verticals within the SMEs daily issues for example. Accounting in the cloud or inventory management in the cloud or HR or similar. These calls should look at micro and small traditional companies and not just at medium innovative or high-end ones.

D-S Recommendation 1.3. Financial assistance for SMEs transitioning from legacy systems to web / cloud-based solutions. Create a fund to assist with these efforts, perhaps in the form of vouchers, but instead of buying innovations or consulting, they can buy cloud services. Care however needs to be taken that these vouchers will be used with local providers that can give support to the small companies in their local language and understanding their local requirements [Deployment, Policy]

D-S Recommendation 1.4: Creation of secure data spaces where trusted data can be shared between business and governments. Usage-rights will need to be reviewed to ensure fair use and eliminate any possible disadvantages for SMEs.

D-S Challenge 2. The suitability of cloud services and contracts. The adverse cost of cloud services for large uses. SMEs who lack the purchase expertise, end up with discriminatory contracts. The lack of access to local eGov from hyperscale customers.

D-S Recommendation 2.1: Setup contractual frameworks which are not discriminatory for SMEs. Use the "Think Small First" principle in order to make it a mandatory check for contracts and ensure that SMEs would not be impacted negatively. Within the EUSD, the Commission refers to its proposed Cloud Rulebook which it aims to compile by Q2 2022. This rulebook will offer a "compendium of existing cloud codes of conduct and certification" with support from the relevant authorities of the Member States. [Deployment]

D-S Recommendation 2.2: Support for SME access to eGov services. Help SMEs access the structural funds that would allow them to Integrate eGov services in a simple way using country based public cloud. Incentivise member states to use local bottom up funds and to make available their public cloud to give an option to the big cloud providers. [Deployment, Policy]

D-S Recommendation 2.3: Provide interoperability between software and cloud providers. Ensure that small companies that might use a variety of off-the-shelf cloud-based solutions will be able to transfer data seamlessly between them. Promote such solutions on a European marketplace aimed for SMEs [Deployment]

D-S Recommendation 2.4: Creation of a Cloud services marketplace. Require that the ability for providers to list their services on such a marketplace be conditional to the use of transparent and fair contract conditions. This would offer service providers a visible presence on a platform which SMEs could then use to acquire cloud solutions in full confidence. This Cloud Services marketplace is directly reflected within the EUSD, which the Commission intends to facilitate by Q4 2022.

D-S Challenge 3: How to guarantee IP protection in the cloud, allowing lower cost technology to be used with confidence. This concern is also identified within the New Industrial Strategy for Europe whereby the Intellectual Property Action plan is to "assess the need to upgrade the legal framework, ensuring a smart use of IP, better fight IP theft."

D-S Recommendation 3.1: Innovative IP/Copyright pilot projects. Support projects that investigate IP / copyright issues of materials placed in the cloud. [Deployment, Policy]

D-S Recommendation 3.2: Build SME confidence in cloud deployments. Encourage high-tech SMEs to create bridges from private to public clouds using strong protection measures (encryption or other). Promote such deployments and services to the low-tech SMEs. [Deployment]

4. SUPPLY SIDE CHALLENGES

This section looks at the supply side, its structure, components, and challenges and how this affects the range of demand side challenges identified above. This section addresses:

- The European supply side cloud ecosystem (cloud services, cloud suppliers, the edge market and emerging standards).
- The edge computing landscape, and barriers to adoption and implementation.
- The cloud infrastructure and technology landscape.
- The implications of green ICT.
- The potential for federation and other mechanisms of cooperation.

The supply side ecosystem and its role in various client IT architectures is illustrated in Figure 5 below.

The adoption and implementation questions for the supply side mirror the questions on the demand side. The implementation question becomes, “How do we best offer these services to the end users, to help them adopt and implement their solutions.” And “How do we create a value proposition around this offering”. From the adoption perspective, each player is making decisions about the technology and infrastructure underpinnings that support the specific offering and value proposition. Underpinning both questions is the economic sustainability foundational one, “Can we create sustainable income streams from these investments?”.

The demand side looks to the supply side when they make their decisions. The demand side players consider their long-term technology architecture framework, how to retain flexibility and avoid being locked into a dead-end technology. They want solutions and value. They want simple, reliable, commodity offerings in some areas, and sophisticated solutions in others, that will give them advantage and a potential competitive edge.

Each supply side player will ask these questions in different ways, depending on:

- Its own position in the market (structure of its market segment, the potential for associations and affiliations, its strength and bargaining power).
- The range of approaches it can adopt (e.g. open-source/proprietary, the rate of change of the technology options, emerging trends, the choices it and its competitors make, the architectural direction it has chosen to take, the standards it has adopted).
- The longer-term social, environmental and economic implications of its choices.

Supporting the supply side players, EC research and innovation programmes are developing ideas and solutions that could be adopted, brought to market and implemented in client organisations, either on the supply side, or on the demand side.

Against this background, demand side players are choosing what technologies they adopt and are building solutions with those technologies in hopes of solving their organisational challenges. This section explains both the structure and nature of these supply side players, the implications for the supply side players and for the demand side.

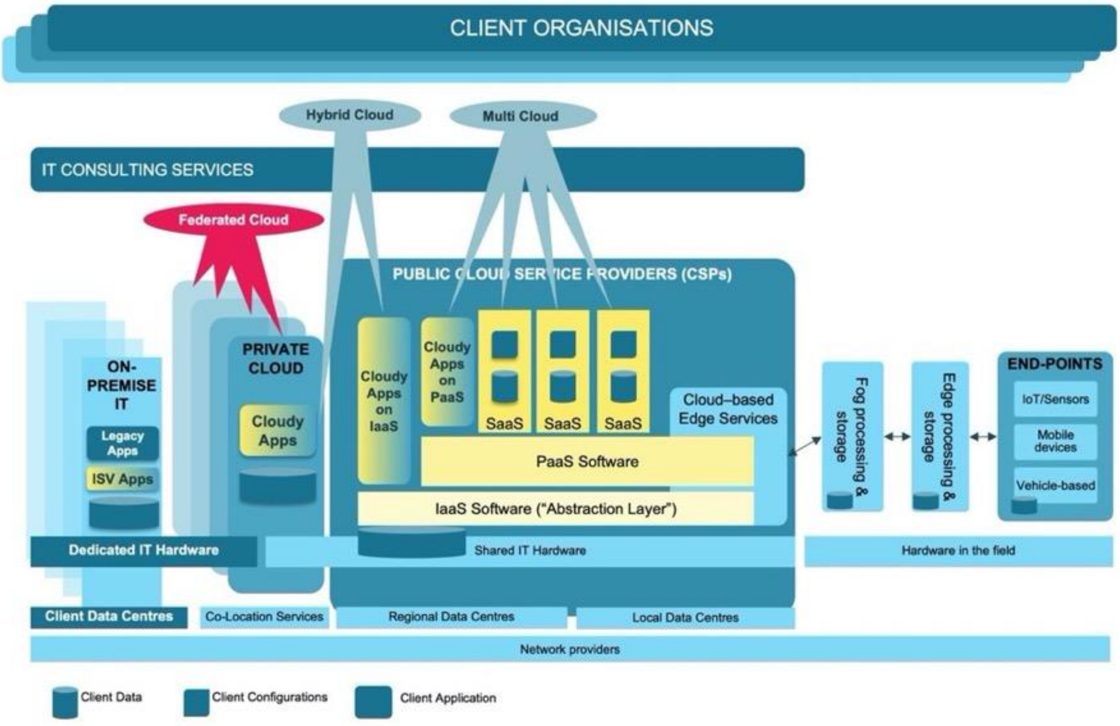

Figure 5. Supply side ecosystem and its role in various client IT architectures

4.1. The European cloud services supply side ecosystem

This section summarises the briefing paper on the European cloud services landscape (please see Annex 11 for detailed discussion). It explores the size and concentration or fragmentation of the public cloud and services markets, how they develop and where challenges and opportunities lie. Figure 6 maps the key challenges found against the Supply Side Ecosystem illustrated in Figure 5.

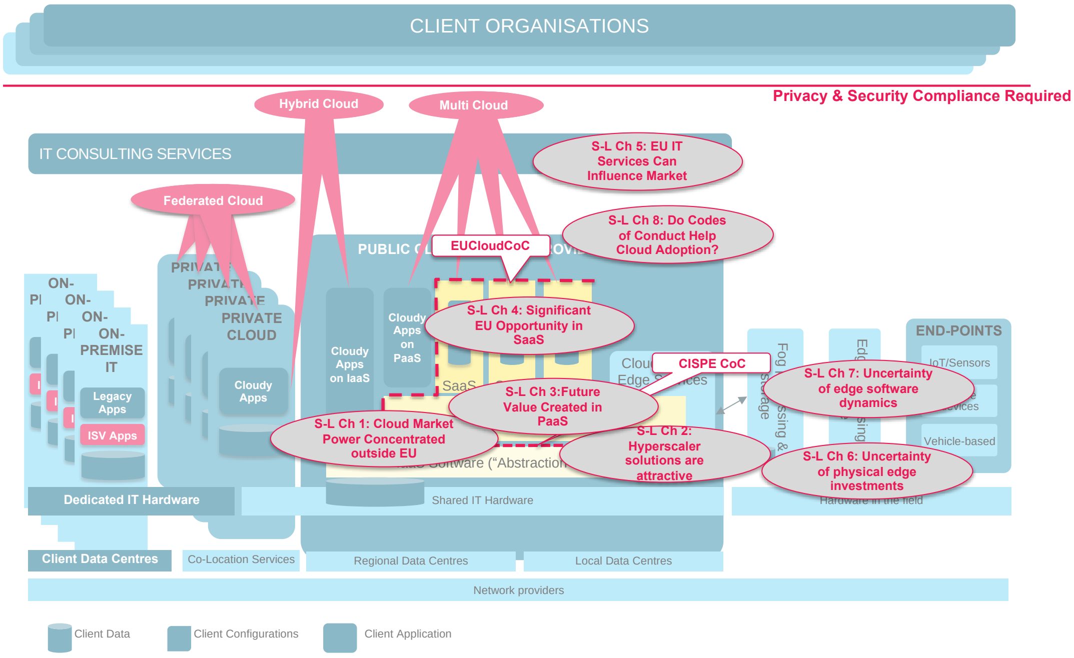

Figure 6. Cloud supply landscape challenges mapped to supply side ecosystem

4.1.1. The overall cloud services market

The size of the public cloud services market in Europe was roughly $48bn for 2019, having grown by 27% since the first half of 2018. The European market is dominated by US-based vendors, with only two vendors in the top 10 headquartered in Europe. The US-based vendors have been consistently increasing their market share. As the table below shows, the levels of market concentration and competitive strength differ considerably by type of market.

Table 9. Public cloud services market in Europe[63]

Service Model	Size & share *(H1 2019)*	Growth *(H2 2018)*	Concentration	EU players	Players tracked
IaaS	$4.1b (19%)	27%	Highly concentrated: AWS 48%, MS 7%, IBM 4%	4 in top 10: Orange, Vodafone, T-Systems, Atos with only 11% of market	29
PaaS	$3b, (14%)	37%	Moderately concentrated: Top 4 (MS, AWS, Salesforce, Google) have 46% of market. Next 7 have 22%.	2 in top 10: SAP & Siemens	115
SaaS	$14.4b, (67%)	25%	More fragmented: Top 3 (MS, Salesforce, SAP) have 21%. Next 7 have 17%.	2 in top 10: SAP & Visma	367

Comments received in H-CLOUD's webinar of experts on supply side challenges indicated that European cloud providers may face difficulties in the market simply because they do have as strong a marketing presence as many of the larger US providers.

S-L Challenge 1. The top public IaaS and PaaS providers are non-EU and dominate the market. How can EU providers compete with US IaaS/PaaS providers with the same reliability, scale and become preferred providers?

The software suites and platforms available to clients who use the dominant cloud service providers offer significant ease-of-use and effectiveness, but they also make those clients dependent on those architectures and lock them in to their services.

S-L Challenge 2. Proprietary solutions from large cloud providers are very appealing to clients – their effectiveness and usability are more important to clients than the risk of "lock-in" and architectural dependency.

S-L Recommendation 2.1. Support development of cloud-based solutions that can be provided/used by EU cloud providers and that offer as good or better ease of use and effectiveness compared to proprietary solutions. [Deployment]

S-L Recommendation 2.2. Evaluate how well "cloud switching" policies allow clients to migrate from proprietary platforms to other providers. [Deployment]

[63] IDC. Worldwide Semiannual Public Cloud Services Tracker. November 2019

4.1.2. The role of PaaS and a value creation layer going forward

The PaaS layer is where potentially most value will be created because it is an enabler of the cloud application software layer. The more robust and sophisticated it is, the less users of more sophisticated applications or platforms need to worry about the infrastructure details. The simpler that layer is to use, the easier it is to create and exploit cloud applications.

The PaaS layer is an important enabler of both cloud computing applications and edge computing deployment and applications. PaaS is also a good place to ensure a uniform data protection/security/privacy capability.

End users will want to create applications in the cloud and therefore need the platforms that support their developments. IaaS providers are pushing up into the PaaS layer with their container and microservices functionality. Software suppliers (those who provide SaaS) create PaaS platforms to enable customers to create extensions to the SaaS services.

Both IaaS and SaaS providers are moving into the PaaS. IaaS players to extend their reach and serve a wider community. SaaS players need PaaS because it enables their software applications.

S-L Challenge 3. Most value will be created in the PaaS layer in the future. This requires a strategy to increase the competitiveness of EU providers in the PaaS Layer and increase their effectiveness as enablers of EU based applications.

S-L Recommendation 3. A “GDPR compliant” cloud abstraction layer for cloud deployments (that sits above the physical infrastructure) might be useful for both large and small organisations looking to deploy cloud technology. Other tools to increase competitiveness could include creation of a centrally managed service and tool catalogue, potentially by the EC or at least endorsed by the EC, substantial marketing support for products appearing in that catalogue, and strong governance and audits to make sure that the catalogue is up to date and that security standards are met. [Research, Deployment]

4.1.3. The dynamic and diverse public SaaS market

While the leading vendors are US-based, with only 2 European vendors in Top 10 (SAP and Visma), market power is distributed, and, because of the massive variety of use cases, European vendors are better able to compete. IDC[64] tracks 367 providers in this space, but that is not the totality of the market. The SaaS market is very dynamic because many software vendors are transforming to become SaaS providers, and are looking for a partner in the IaaS and PaaS space to run on.

S-L Challenge 4. The SaaS market is the one with the largest size in terms of EU participation, as independent software vendors (ISVs) are moving to the SaaS market.

S-L Recommendation 4.1. Investigate barriers that are limiting EU software industry to move toward SaaS business model. [Policy]

S-L Recommendation 4.2. Strengthen competitiveness of EU SaaS providers. [Deployment]

S-L Recommendation 4.3. Supporting EU ISVs in a faster transition from old business models to SaaS provisioning is a priority. [Deployment]

4.1.4. A wide range of other services that support cloud and edge solutions

The provision of public cloud services creates opportunities for IT service providers. The cloud technology market comprises multiple layers:

[64] IDC. Worldwide Semiannual Public Cloud Services Tracker. November 2019

1. IT hardware vendors providing server, storage and networking equipment (traditional IT hardware vendors like Dell, HPE, Cisco, Huawei).

2. The infrastructure software vendors providing middleware and infrastructure software:
   a. virtualization vendors, and
   b. the system and service management vendors.

3. Cloud hosting service providers, who sell, manage or resell cloud services.

4. The solution providers, such as consulting and integration organisations, who help architect the cloud solutions, migrate applications to cloud services and also operate cloud environments.

Most public cloud service vendors maintain ecosystems of partners to deliver their services to the end customer. There is high fragmentation in the cloud IT services market, similar to the fragmentation of traditional IT services. Given the complexity of integrating and securing the edge and cloud value chain, it is likely that the solutions and technology competitive landscape will remain relatively heterogeneous.

S-L Challenge 5. Although fragmented, the EU-based cloud-related IT services ecosystem can potentially act as a strong influencer on cloud adoption across the EU.

S-L Recommendation 5. Work with the EU-based cloud-related IT services ecosystem to reduce barriers to cloud adoption and identify tools that could maintain or increase the market share of EU-based cloud providers. Efforts could include support for accessing results and deliverables from EC-funded R&I projects, case studies and promotion of successful EU-based implementations. [Deployment, Policy]

4.1.5. Larger cloud players moving into edge solutions and services

The European edge infrastructure market is much smaller (under $3.5 billion), than the wider cloud services market ($47.7 billion). This edge market has two related components:

- Specific edge infrastructure: Anything outside the datacenter, from endpoint to core (European spending approx. $1bn)

- Edge-related core computing infrastructure: All edge/IoT computing processes that occur inside an organisation's IT data centre. (European spending $2-2.5bn)

The major public IaaS and PaaS vendors (mostly US) are adding to their portfolios with offerings for edge computing. This suggests ambitions to build an Edge computing platform. In the short to medium term (2018-2023), spending on edge infrastructure is forecast to grow faster (21% CAGR) than spending on edge computing platform infrastructure (14% CAGR)[65]. This suggests that the larger cloud platform vendors are in a position to exert significant influence over the edge market in this period.

Bargaining power for edge solutions may remain more balanced as edge computing becomes pervasive and a wide number of market participants work with the end customers. However, the increase in edge infrastructure investment by the larger cloud service providers suggests they will still exert significant influence over the edge market.

S-L Challenge 6: Uncertainty over who will invest in physical edge infrastructure.

S-L Challenge 7: Uncertainty over who will dominate the software stack that runs on edge infrastructure.

For additional analysis and recommendations regarding edge solutions, see Section 4.2.

[65] IDC. EMEA Edge and Core Internet-of-Things Infrastructure Forecast, 2019-2023. 2019.

4.1.6. Cloud codes of conduct (CoC) and cloud standards play a role

In Europe, there are a number of codes of conduct for cloud services emerging. CISPE and EUCloudCOC provide guidance on how to implement GDPR when using cloud services. SWIPO focuses on data portability and cloud switching, i.e. on facilitating cloud users in the change of service provider. These codes of conduct may be appearing because the supply side understands the data protection, security and architectural challenges of cloud implementations and are actively working with policy makers to address them. Also, potentially EU cloud service providers see this as a way to protect them from US dominance. Both codes of conduct have applied to become ISO standards. However, the extent to which codes of conduct make the cloud adoption process easier for client organisations is unclear and was acknowledged in the Horizon Cloud Summit.

The Gaia-X initiative indicates that the certification processes of the EU Cloud Code of Conduct would be a good model to manage certification against the wide range of standards being developed by Gaia-X.

S-L Challenge 8. ‘Codes of conduct’ and standards may not be helping EU clients adopt cloud solutions and at the same time maintain compliance with EC regulations such as GDPR.

S-L Recommendation 8. Evaluate the impact of ‘codes of conduct’ and standards on EU cloud adoption and identify mechanisms for improving adoption while maintaining GDPR compliance. [Policy]

4.2. Edge computing, supply side drivers and barriers to adoption

This section summarises the supply side purely from the perspective of edge computing. It explores the drivers of edge computing and how the adoption of IoT is driving the need for computing at the edge, and the potential investment growth.

It describes the generic applications of edge computing, their growing importance amongst organisations and how that varies across sectors, and the potential in a variety of market sectors. However, there are barriers and risks associated with the adoption of edge computing, so these are also explored. (See Annex 12 for more information.)

Figure 7 maps the key challenges found against the Supply Side Ecosystem illustrated in Figure 5.

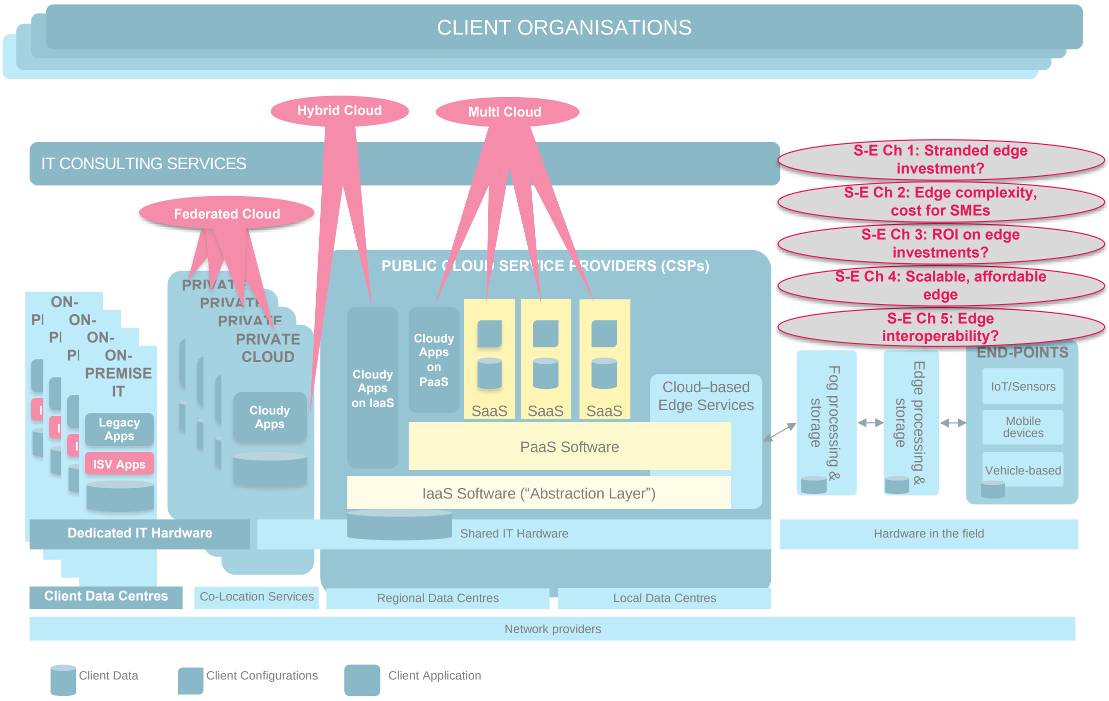

Figure 7. Edge computing challenges mapped to supply side ecosystem

A definition of edge computing, and its variations, is available in Annex 1 "Technical Definitions".

4.2.1. What are the drivers of edge computing adoption?

Data Acquisition & Pre-processing, Security and/or Monitoring, Data Analytics, and Location Services are the top applications targeted with edge computing today[66]. IoT expenditure is increasing investment in edge infrastructure as more 'things' become IoT-enabled. Currently, around 10% of enterprise-generated data is created and processed outside a traditional on-premise or cloud-based data centre. By 2023, IDC[67] predicts this figure will reach 73%. IDC forecasts an investment of $12 billion in 2023 on IoT edge infrastructures in Europe.

This availability of edge data leads to an associated investment in data-intelligence applications. According to the Industrial Internet Consortium[68], the three main drivers for the adoption of edge computing infrastructure are:

1. Managing the increasing amount of data generated from large numbers of new devices. It is expected that there will be more than 30 billion IoT devices connected by the end of 2020[69].
2. Supporting low latency, real time analysis. Much data from the edge requires real time analysis. A 100ms delay could be the difference between an autonomous vehicle avoiding a collision, or not.
3. Increasing data security and privacy. Moving data from its source to cloud services inevitably increases the surface of attack. Edge-based processes can mitigate this risk but can also introduce different risks.

[66] Futurum Research. EDGE COMPUTING: From the Edge to the Core to the Edge. 2018
[67] IDC. European FutureScape, 2018
[68] Industrial Internet Consortium. Introduction to Edge Computing in IIoT, 2018.
[69] Statista. Internet of Things - number of connected devices worldwide 2015-2025, 2016.

4.2.2. What is stimulating the importance and potential growth in edge computing?

Edge computing has potential benefits across a wide range of market sectors, including as well scientific applications. With no surprise, the main adopters are telecommunications and media organisations, given the importance of edge resources for their solutions. Telcos are not only adopters, but central to any edge to cloud ecosystem as providers of the "transport" layer between the edge and the core. Despite the potential relevance of edge computing to their business, most markets are still behind telecommunications organisations in their adoption.

Discussion at the Horizon Cloud Summit highlighted two elements acknowledged by the European Commission:

- The trend toward edge is an opportunity, but EC, looking at the state of the market, realizes that there is not just one flavour of edge, and different flavours of edge may be linked to different business models. From one perspective this is positive because it triggers competition, but from another perspective, it may limit interoperability between different "edges". As for the cloud services, there should be interoperability allowing users to move data and workloads seamlessly across different edge operators.
- EU has all that is required to be successful in the development of solutions for the cloud-edge continuum. EU has a strong industry in micro edge devices and a vibrant service industry. The EC's role is to support the development of a collaborative environment for all actors in the market. So, again, EU will stay open to any actor in the cloud market, but the market has to be competitive and the rules have to apply to everybody.

Edge computing is enabling change and in turn, increasing the value of other systems and activities. Edge computing is being driven by operational parts of organisations, rather than IT departments (who may eventually end up owning and maintaining it).

One observer at the Horizon Cloud Summit pointed out that the projected rapid growth of both edge computing and data being generated in the edge create an opportunity for EU service providers to create a unique competitive advantage against global hyperscale cloud providers.

4.2.3. Edge computing adoption issues

Whilst the research shows a great potential for adoption of edge computing in different application areas and sectors, market research also identifies issues that may limit such adoption. Early edge deployments show that organisations are concerned about:

1. Their ability to manage assets, control costs, and ensure physical and data security.
2. Lack of skills: one in five organisations lacks the internal skills needed to support edge computing adoption.
3. The distributed and often remote nature of edge IT makes human intervention in edge components expensive and potentially unaffordable.
4. Telecommunication industry and industrial IoT players are promoting a variety of technologies and standards for edge computing. This may lead to interoperability issues and create additional barriers.

Moving computation to edge infrastructure may also increase costs for hardware acquisition and maintenance, possibly slowing adoption.

As the supply side develops edge service and technology offerings, there is uncertainty in the demand side about which solutions are likely to succeed and when public offers will be available at scale. Potential users want to avoid lock-in but cannot anticipate how technological directions or market-ready solutions will evolve. Overall, uncertainty about the edge market and technology is slowing investment.

Given these barriers to adoption, IDC predicts that the overall expenditure on edge computing is not likely to increase in the next 24 months.

S-E Challenge 1: Concern about stranded edge investments. Investing in the wrong emerging technology is a risk. The supply side should facilitate edge adoption and deployment by mitigating the risk of lock-in.

Recommendations: See challenges E2, E3, E4 and E5 below.

As noted in Section 3.8 above, SMEs are even less ready to adopt edge computing. An IDC survey reveals that many are not ready due to investment costs, lack of skills and lack of public offers.

S-E Challenge 2: Edge is complex and expensive for SMEs. Smaller organisations need help to improve their readiness and maturity, and reduce the complexity of edge computing adoption, while making it affordable.

S-E Recommendation 2. Develop a European strategy focusing on SME adoption that supports the deployment and the maturation of edge computing technologies while in parallel fosters the development of needed skills in the European market, to ensure that adoption by SMEs will not suffer the same issues as cloud computing. [Deployment and Policy]

European programmes supporting the implementation of EUSD and NISE will clearly need to ensure that proper focus is included on maturing edge computing technologies and supporting related upskilling, especially for SMEs. This is essential to support wide deployment and adoption of EU data spaces and federated cloud infrastructures spanning the cloud-edge continuum.

4.2.4. Edge computing supply side challenges

The supply side analysis indicates that large investments are being made in the hardware and software platform segments to support edge computing. However, most of the available solutions, especially by large public IaaS providers (e.g. AWS Snowball), are not interoperable and aim at moving data from the edge to specific cloud services or platforms.

Unlike the US, there is also no public “edge infrastructure as a service" (EIaaS) offering. Specifically, there appears to be no publicly accessible EIaaS offering in Europe (although some are appearing in the US). Such an offering would be important for small players that do not have the capacity to afford investment on creating edge infrastructures for their business, and that would benefit from moving the edge cost model from CAPEX to OPEX.

The situation seems motivated by a) large players trying to reap the most out of their current investments in core cloud infrastructure offerings; b) complexity and cost of maintaining large edge infrastructures with current technologies.

Observers at the Horizon Cloud Summit offered an alternative scenario, where effective peer-to-peer edge technologies might allow smaller players to take advantage of edge opportunities without having to wait for investments from larger players.

H-CLOUD webinars evidenced that a European Cloud infrastructure federation (or marketplace in its earliest steps), as envisioned in the EUSD, should aim at incorporating edge resources and to make them easier to access.

S-E Challenge 3: Uncertain return on edge investments. Enabling conditions must come about to facilitate the widespread use of edge technology, so it reaches critical mass as a public edge capability.

S-E Recommendation 3. Embrace the opportunity to establish an interoperable and/or federated European public edge infrastructure market by defining policies that will preserve European core values (such as data privacy), while not creating market barriers. [Research and Deployment]

While the federation or marketplace of traditional cloud infrastructures may not have a sufficient market appeal due to the market dominance of large players, the increasing demand for edge resources (or services) may open interesting new opportunities. This, in particular as discussed also in the H-CLOUD webinars, could create an opportunity for Tier 2 providers, notably those associated with mobile networks, to take a more prominent role in edge infrastructure build out, leveraging their existing footprint of distributed facilities and human resources. The webinars evidenced that so far operators are not yet fully embracing the edge approach and opening their edge resources to the ecosystem of their stakeholders interested in edge capacities. Research and Innovation initiatives should look into solutions, for example leveraging federation and multi-edge approaches, to allow the creation of widespread edge infrastructure across different providers.

There are questions over the scalability of largely distributed cloud-edge infrastructure. Especially where it combines different private and public infrastructures. It may not be possible to scale such applications using the same solutions and technologies used today. Beyond that, solutions need to be affordable to ensure that also small players have the financial capacity of adopting them. In particular, H-CLOUD webinars evidenced how edge computing is central to enable processing where data is store as demonstrated by early pilots using federated machine learning at the edge. Webinars also evidenced how large part of the complexity is in enabling seamless migration of applications and/or data from cloud to edge and their orchestration in the cloud continuum. It is also clear that in several scenario, everything may happen at the edge without “cloud” involvement, thus simplifying the complexity of application architectures.

S-E Challenge 4: Ensure scalability and affordability of edge computing solutions and deployments to cope with the demands of the foreseen usage scenarios, also by small players.

S-E Recommendation 4. Promote the deployment at scale of edge computing solutions. Available platforms are still limited in the ability to manage a large number of edge endpoints, and installing/maintaining those endpoints will be costly. Research should continue to explore automation of cloud continuum from infrastructure layer up to the final application, taking into account different scenario specific demands. [Research and Deployment]

EUSD and NISE successful implementation will largely depend on successful wide deployment of edge infrastructures and services. In fact, edge processing capacities may play a key role in several data space verticals, such as agriculture, health, manufacturing and mobility. The implementation of the high impact project needs to ensure that edge capacities will be affordable, or their adoption will not take up.

S-E Challenge 5: Concerns about edge interoperability. Edge computing research and innovation solutions are coming from the telecommunications sector as well as multiple Industry 4.0 initiatives, but their approaches are diverging. This will create interoperability issues and increase the complexity of adoption and management.

S-E Recommendation 5. Establish a forum promoting a tighter collaboration between different industries to facilitate the convergence of the different solutions related to edge computing, with the aim to define a single and unified standard for edge computing infrastructure in Europe. Public authorities should play a role in supporting such a standard by including it in relevant public procurements [Policy, Research and Deployment]

Research and Innovation solutions should research methods and technology implementations to ensure that edge computing solutions scale as foreseen by the market usage scenarios. Deployment initiatives should not only cover core cloud infrastructures, but also public and private edge infrastructures able to support specific domains such as smart cities and health care scenarios.

The implementation of the ambitious High Impact Project on European data spaces and federated cloud infrastructures (cf. EUSD) demands interoperable solutions. The more complex achieving interoperability will be, the more complex will be the technical governance of European federated cloud infrastructure building on edge computing facilities. The definition and adoption of a single reference standard for Edge, and hence its inclusion as requirement in the implementation of the project via tenders or other mechanisms will be instrumental to this aim.

H-CLOUD webinars evidenced that the collaboration between edge stakeholders (spanning from telco operators, to small cloud players and technology providers) is essential to achieve the creation of European edge ecosystem.

S-E Challenge 6: Limited investment on trusted data access solutions for the edge. As of today, most of the solutions available for trusted access to data rely on specific hardware facilities - software based solutions are still lacking. This limits a lot the flexibility and potential adoption of public edge infrastructure offering where guarantees about trusted access to data are required.

S-E Recommendation 6. Support the research and deployment of trusted data processing environments. Europe cloud industry should deliver an open reference solution for trusted computing at the edge supporting multi tenants in isolation and compatible with the different EU privacy and security regulations [Research and Deployment]

This challenge was remarked upon in one of the H-CLOUD webinars, and clearly highlights some core enablers yet missing or not mature enough to support the implementation of EUSD vision. Trusted data access is essential for data spaces where confidential or sensible data are exchanged and processed. Without maturity of such capacities, data spaces may not reach a sustainable uptake.

4.3. Supply side: infrastructure and technology landscape analysis

This section looks at the range of technologies and infrastructure that underpin cloud services, to create a wider technical context on cloud technology and the technical challenges of deployment. It includes an analysis of some of the EC projects that have supported this area, as well as some technical implications of the choices organisations make about their cloud and edge technology. (Please see Annex 13 for more detail, as well as sources for data referenced in section 4.3.)

Figure 8 maps the key challenges found against the Supply Side Ecosystem illustrated in Figure 5.

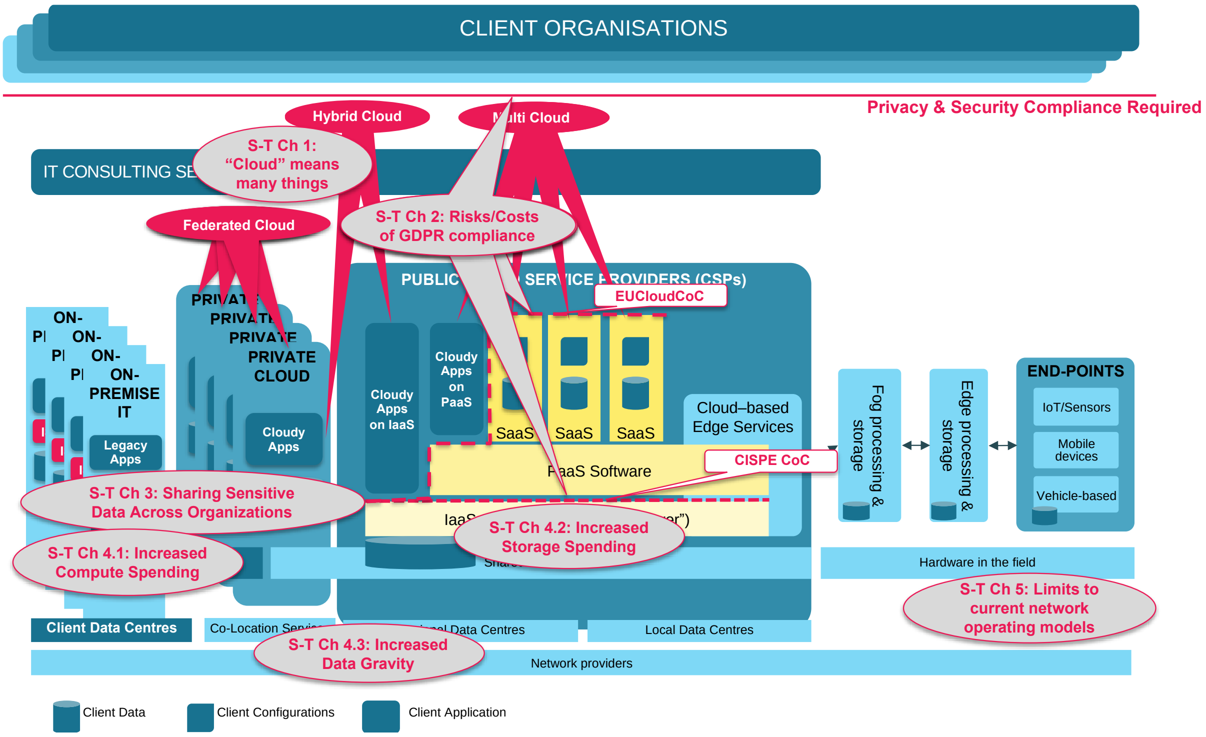

Figure 8. Infrastructure and technology landscape challenges mapped to supply side ecosystem

At the outset it is important to understand that the term "cloud" is used in a wide range of contexts, and with a wide range of intended meanings. Annex 12 explores these in detail.

S-T Challenge 1. The term "cloud" has a wide range of explicit and implicit meanings.

Consideration of the actual cloud adoption process highlights the risks faced by organisations when implementing solutions in the cloud. Cloud adoption is neither simple nor a "one size fits all" process. It is often complex, requiring detailed planning, skilful execution and careful consideration of return on investment. Large and small organisations undertake a complicated migration process, but gaps in skills and expertise in smaller organisations can limit their ability to move forward. Large and small organisations take on risks associated with potentially exposing personal information: large organisations look to mitigate those risks by choosing proven tools and products, while small organisations may decide to avoid those risks by not moving forward.

Comments received in H-CLOUD's webinar of experts on supply side challenges indicated that cloud adoption may also be hindered by the perceived cost of moving data to and from the cloud, which also creates penalties for switching cloud providers. Other experts noted the need for tools to manage multi-cloud implementations and the value of a shared marketplace in which different stakeholders can collaborate rather than compete.

S-T Challenge 2. Large organisations are concerned about the risk and costs associated with complying with EU privacy and security regulations, including GDPR.

S-T Recommendation 2. A "GDPR compliant" cloud abstraction layer for cloud deployments (that sits above the physical infrastructure) might be useful for large organisations looking to deploy cloud technology or re-architecting their solutions in response to tighter regulation. [Deployment, Policy]

Groups of organisations are also challenged in using the cloud to solve important data sharing tasks that would improve efficiency and effectiveness. There are no secure tools for data access and sharing that can support these objectives, although several EC-supported R&I projects have explored potential solutions to this problem.

These conclusions were reflected by experts participating in H-CLOUD's webinar on supply side challenges:

- Policies limit data processing to data holders, including at the edge, limiting data transfer to safe results.
- Federated [machine] learning is a good example.
- Applications need to be ported to the edge (as well as to the cloud) to enable sharing of data between edge and cloud.

S-T Challenge 3: Various groups of organisations need to share sensitive data with the group, but do not have the tools or frameworks to do so while complying with EU privacy and security regulations, including GDPR.

S-T Recommendation 3: Support development of "GDPR compliant" tools and/or frameworks that enable secure access and sharing to distributed data. These tools might function through peer-to-peer software components that are certified to be GDPR compliant, or through participation in coordinated structures such as federation. [Research, Deployment, Policy]

Several decades-old paradigms for the IT sector are changing, as underlying technology evolves. Key paradigm shifts are:

Compute: The end of both Moore's Law (1965) and Dennard Scaling (1974) means that compute price/performance will no longer improve significantly each year. At the same time compute requirements are growing exponentially with global digital transformation (including growth in training and distributed deployment of AI models, where compute requirements for training alone are growing 10x per year).

S-T Challenge 4.1: Significant growth in compute spending. The trend is no towards longer economic lifetimes for compute investment and reduced pressure to refresh so rapidly. This may also limit the future appeal of cloud-based solutions on a "total cost of ownership" basis.

Storage: Data volumes are projected to growing 27% per year on average[70], with growth in some sectors such as research exceeding 50% per year. By contrast storage costs are projected to fall by only 15% per year[71]. Increased focus on archival data storage further increases absolute data storage volumes (by an estimated 10-20%).

S-T Challenge 4.2: Significant growth in storage spending. Storage costs are becoming a more significant component of ICT budgets, even as compute spending increases more rapidly than seen in decades.

Networking: The rate of networking bandwidth growth is significant but still lags behind the growth of compute and storage demands. Dataset sizes are projected to increase faster than network capacities. Transferring meaningful amounts of data will take more time in the future (even with network upgrades).

S-T Challenge 4.3: Increased data gravity. It will be increasingly important to process data where it is stored.

S-T Recommendation 4.1: Bring compute to the data. Increasingly the data required for analysis will be distributed, should not require transfer to a "central" location for processing, and instead the processing should be applied to the data where it is stored. For "big science" projects, it may not even be feasible to collect data for processing in one place, since the size of that data may require extreme investments in storage and processing or create unacceptable delays associated with data transfer. Moreover, the environmental cost of

[70] IDC 2018

[71] CERN. Storage IT Technology and Markets, Status and Evolution. 2018.

reproducing, transferring and then storing this “big data” is becoming more and more significant. [Research]

S-T Recommendation 4.2: Analyse data where it is generated. Today, data generated at the edge is a special case, but will increasingly become the dominant case. Data processing (including AI training and inference) at the edge should be beneficial compared to the investments in intermediate networking and centralized storage and processing required to support centralized collection/concentration/processing of that data. [Research]

In contrast to these longer-term paradigm shifts, recent experience with the worldwide response to SARS-CoV-2 has demonstrated how traditional network engineering practices make important assumptions about network usage patterns and quality of service. These assumptions no longer apply in the sort of remote work, online oriented world seen today. This highlights how deeply those assumptions could affect and indeed limit the aspirations of the Digital Single Market.

S-T Challenge 5: To ensure that society benefits from future developments in cloud computing and other related new technologies, Europe needs to develop networking techniques that are able to accommodate rapid shifts in large-scale user behaviour and location. It is unclear if 5G technology can deliver this adaptability across the entire region.

S-T Recommendation 5: Support creation of networking and service delivery capabilities that can adapt both to new patterns of demand, but also new patterns of infrastructure investment and location. [Deployment]

Annex 13 identifies a number of research and Innovation projects that have the potential to help in these areas.

4.4. Green computing: the environmental implications of the ICT lifecycle

H-CLOUD was asked specifically by the EC to look at green computing. The scope was wider than simply how edge technology, moving data and the choice of computing resources would affect energy consumption. The policy of EC strategies is to reduce environmental impact. So, the analysis addressed energy efficiency and environmental impact from a structural view of cloud services.

The Green Computing briefing paper (Annex 14) takes a structural view of cloud services. It considers cloud services from the perspective of them running on a remote server in a data centre (DC), consumed by an end-user working on a local client device which accesses the cloud service over the Internet. It considers the environmental impact and energy consumption in several dimensions, ranging from the main perspective of the data centre through to end-user behaviours and media considerations. Energy efficiency and environmental standards are explored and a definition of Green Cloud, grounded on the Green Deal, is developed. Relevant research and innovation activities are considered in relation to each aspect and the impact of potential challenges on the demand side are developed. Figure 9 maps the key challenges found against the Supply Side Ecosystem illustrated in Figure 5.

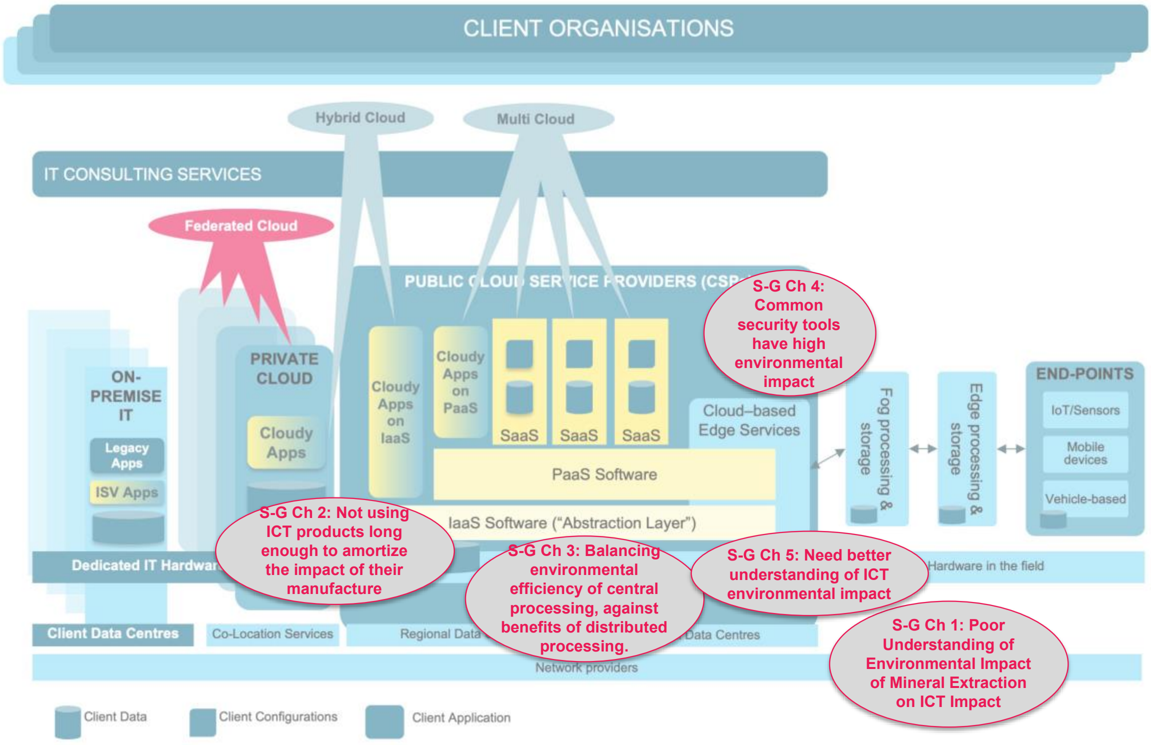
CLIENT ORGANISATIONS
Hybrid Cloud
Multi Cloud
IT CONSULTING SERVICES
Federated Cloud
PUBLIC CLOUD SERVICE PROVIDERS (CSP
S-G Ch 4: Common security tools have high environmental impact
ON-PREMISE IT
Legacy Apps
ISV Apps
PRIVATE CLOUD
Cloudy Apps
Cloudy Apps on IaaS
Cloudy Apps on PaaS
SaaS
SaaS
SaaS
Cloud–based Edge Services
Fog processing & storage
Edge processing & storage
END-POINTS
IoT/Sensors
Mobile devices
Vehicle-based
PaaS Software
IaaS Software ("Abstraction Layer")
S-G Ch 2: Not using ICT products long enough to amortize the impact of their manufacture
S-G Ch 3: Balancing environmental efficiency of central processing, against benefits of distributed processing.
S-G Ch 5: Need better understanding of ICT environmental impact
Dedicated IT Hardwar
Hardware in the field
Client Data Centres
Co-Location Services
Regional Data
Data Centres
Network providers
S-G Ch 1: Poor Understanding of Environmental Impact of Mineral Extraction on ICT Impact
Client Data
Client Configurations
Client Application

Figure 9. Green computing challenges mapped to supply side ecosystem

4.4.1. Data centre energy efficiency

Ten or so years ago it was relatively uncontroversial to claim that data centres had a negative impact on the environment[72]. It was then predicted that growth in energy consumption would reach 100 TWh in 2020. In fact, it is now estimated that global data centre energy consumption is 200 TWh[73].

More recently, however, despite the clear underestimation back in 2009, the impact of data centres on the future environment has become hotly contested, with some researchers continuing to maintain the negative impact analysis[74], and other researchers creating a more positive dialogue[75].

The main area of contention seems to be in the area of the potential for energy efficient systems of all kinds to be developed, with the negative impact adherents predicting that the likelihood of energy efficient systems being developed in the short to medium term as being low, while the positive impact adherents predicting exactly the opposite situation.

Only time will tell which group is right; however, both agree that work in this area is important and should continue, and that policy around Green ICT should be strengthened. However, one of the main problems underlying this contention between the two groups may be found in the manner that the predictive data are gathered and assembled. An interesting industry initiative

[72] Berl, A et al (2009) Energy-Efficient Cloud Computing, in The Computer Journal, Vol 53, Iss 7, PP 1045-1051. Print ISSN 0010-4620. Available online at https://doi.org/10.1093/comjnl/bxp080

[73] Jones N (2018) How to stop data centres from gobbling up the world's electricity. Nature. https://www.nature.com/articles/d41586-018-06610-y#ref-CR2

[74] Andrae A (2020) New perspectives on internet electricity use in 2030, Eng. Appl. Sci. Lett. 2020, 3(2), 19-31 https://pisrt.org/psr-press/journals/easl-vol-3-issue-2-2020/new-perspectives-on-internet-electricity-use-in-2030

[75] Masanet E, Shehabi A, Lei N, Smith S, Koomey J (2020). Recalibrating global data center energy-use estimates. Science, 2020; 367 (6481): 984 DOI: 10.1126/science.aba3758)

has been launched by Cisco: its Global Cloud Index (GCI). This is an ongoing effort to forecast the growth of global data centres, servers, data volume, virtualisation tools and cloud-based IP traffic[76]. As a global (single) source of reliable data, it represents the raw activity that could be used in forecasting energy efficiency and total demand more accurately and with less contention. Notably, the report predicts that the number of hyperscale data centres will grow from 338 in number at the end of 2016 to 628 by 2021, representing 53% of all installed data centre servers by 2021.

Fewer larger data centres are certainly more efficient than a larger number of smaller data centres but they can nevertheless drain the energy out of national infrastructures when they are “parachuted in” to poorly prepared regions (e.g. Ireland and Denmark, both of which had all the progress they were making towards achieving their energy efficiency targets reversed when a hyperscaler was welcomed in[77]).

Hyperscalers take different approaches and employ different tools in the pursuit of zero carbon DCs. They keep successful techniques close to hand and do not share, except to claim why they are better than their competitors. They also rely heavily on offsetting in this pursuit.

Regardless, there are well known techniques for optimizing energy use in the data centre itself, including designing the physical aspects of a data centre to accommodate hot and cold areas, switching servers to the lower power states when they are not in use. Virtualisation in the data centre can be beneficial, as is the ability to “cool down” “hot” servers by switching them to low power states when they are not in use and by increasing the utilization of the already active servers[78]. Algorithms for data compression and data deduplication can also be extremely efficient in specific domains. An energy supplier can also help by deploying variable energy management systems in the supply line.

There are no global energy efficiency standards with which to evaluate DCs – efforts to develop such standards are challenged by the diversity of data centres that exist (from server rooms to hyperscale facilities), but there are many relevant and potentially relevant KPIs[79] to measure their energy efficiency, with some being more relevant and of greater utility than others. The most widely used is power utilization efficiency (PUE), which is easy to understand, but difficult to measure correctly[80]. While most existing KPIs are mathematically related to PUE, others introduce new aspects, such as the share of green energy sources, e.g. the Technology Carbon Efficiency (TCE), or the level of utilisation of the IT resources, e.g. the Compute Power Efficiency (CPE). Notwithstanding this, there are some interesting activities making moves in the right direction, notably those being made in the EU.

The European Best Practice Guidelines and Code of Conduct for Data Centres aim to improve energy efficiency in data centres[81]. Both are closely related voluntary initiatives, working together to identify and focus on key issues aiming to develop agreed solutions.

The ICTFOOTPRINT project was funded under H2020 to build on this initiative in order to raise awareness on metrics, methodologies & best practices in measuring the energy and

[76] Cisco (2020) Cisco Global Cloud Index: Forecast and Methodology, 2018–2023. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[77] Kamiya G, Kvarnström O. (2019) Data centres and energy – from global headlines to local headaches? International Energy Agency https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches

[78] Tesfatsion, SK (2018) Energy-efficient Cloud Computing: Autonomic Resource Provisioning for Datacenters. ISBN 978-91-7601-862-0. Umea University

[79] EN 50600-4: Information technology: Data centre facilities and infrastructures

[80] ISO/IEC 30134-2:2016. The standard runs 25 pages, attesting to the precision that should be used to properly measure PUE.

[81] Acton, M.; Bertoldi, P.; Booth, J.; Flucker, S.; Newcombe, L.; Rouyer, A. 2017 Best Practices Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency. Version 8.1.0. Available online: https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct

environmental efficiency of the ICT sector[82], with D2.5 being of particular interest[83].

The EC has also funded the CLOUD EFFICIENCY study to assess the current and future energy consumption and state-of-the-art of cloud computing services in Europe[84]. The objectives are to propose recommendations for energy-efficient cloud computing, particularly in relation to future research and development, green public procurement and market policies. The study is an ongoing initiative producing very interesting outputs[85], notably identifying that:

- a KPI embracing all efficiency related factors within the cloud computing continuum does not yet exist and recommending that it be developed.
- the energy demands in the network EDGE and in the wireless segment of mobile telecoms are unknown and may be difficult to measure in a distributed environment, recommending basic research to address this shortfall.

4.4.2. Energy efficiency of networks, edge, federated cloud and data spaces

Recent work has added further to the understanding of what is happening in the wireless segment of mobile telecoms, predicting over 10% per annum growth of energy consumption, up from 13.7% of the total network energy consumption in 2013 to 50.6% in 2025[86]. Clearly, the call from Hinterholzer, Hintemann, and Beucker[85] for basic research to address the shortfall should be answered in order to address this increased energy demand in the mobile sector.

The internet consumes a lot of energy, and the energy consumption is growing as more users join[87]. However, this energy consumption pales into insignificance when compared with (e.g.) transport[88]. The two main areas requiring attention in the context of overall power consumption are the access networks (in particular the home terminal equipment) and the core network routers.

There are a number of studies, data, best practises and policies available on cloud data centre energy consumption and environmental impact, but the energy efficiency across the cloud-edge continuum is still a largely unexplored area. This is in part related to the fact that edge computing is a recent development, but also to the more complex nature of cloud-edge continuum. Measuring a closed system like a datacentre, with all its complexity, is still simpler than dealing with energy measurement (or estimation) across an open and distributed system spanning different providers and different technologies.

Energy efficiency across the cloud-edge continuum should be examined on three levels:

- The cloud data centre level. Moving services from the cloud data centre toward the edge will reduce the processing on cloud data centres, and hence the energy consumed within the cloud data centre;
- Moving services from the cloud data centre toward the edge will reduce traffic between the core and the edge and hence reduce energy consumption by the network, although the traffic between edge and devices would remain the same. The extent of any traffic reduction would be scenario specific.

[82] https://ictfootprint.eu/en/about/project
[83] https://ictfootprint.eu/en/d25-third-market-watch-best-practice-report-sdos-update-voice-users-0
[84] https://www.cloudefficiency.eu/
[85] Hinterholzer S, Hintemann R, Beucker S (2019) Recommendations for Future R&TD Policy, part of the study "Energy-efficient Cloud Computing Technologies and Policies for an Ecofriendly
Cloud Market" (SMART 2018/0028)
[86] Lorincz, J.; Capone, A.; Wu, J. Greener (2019) Energy-Efficient and Sustainable Networks: State-Of-The-Art and New Trends. Sensors, 19, 4864. https://doi.org/10.3390/s19224864
[87] Andrae, Anders. (2017). Total Consumer Power Consumption Forecast. Nordic Digital Business Summit, Helsinki
[88] Raghavan, Barath and Ma, Justin. "The Energy and Emergy of the Internet." Hotnets '11. Nov. 14-15 2011. (Dec. 5, 2012) http://www.cs.berkeley.edu/~jtma/papers/emergy-hotnets2011.pdf

- When computing at the edge is possible with small, specialized devices, designed to be activated only when required, there are clear energy efficiency benefits compared to running the same task in a cloud data centre on general-purpose computational capacities. As the scale of the edge computing infrastructure approaches that of a small data centre (for example a server room), edge computing is less efficient than cloud computing. Such inefficiency would need to be compensated by the energy saved by avoiding data transfers to the cloud data centre.

The energy efficiency of federated clouds is also largely unexplored. The drive to create ever larger data centres is based on the understanding that the centralisation of processing power and storage capacity is one way of reducing energy consumption and business costs. However, the notion of federating cloud data centres counters this trend, allowing for the existence of smaller data centres that exist independently and collaborate according to various technical and business rules. The end result is a marketplace of providers[89], the totality of which enables hyper-scale performance with a level of flexibility that is unmatched. However, unless all the federated data centres adopt best practices in energy efficiency, this flexibility comes at the possible cost of reduced energy efficiency compared with that of a single hyper-scale site of similar capacity and performance. Recent research has shown, however, that this cost can be reduced through deploying sophisticated load balancing and scheduling techniques that take energy efficiency into account[90].

EU data spaces[91] may add to the energy efficiency problems for Green ICT. Comprehensive technical detail about how the EU Data Spaces will work in practice is needed. Policymakers should consider the digital service policies they are developing holistically and in particular they should give due consideration to Green Deal impacts.

4.4.3. Green end-user devices, media and gaming

Video streaming currently (2020) accounts for 58% of broadband Internet traffic[92], and 65% of mobile data traffic[93]. Traffic across both network types grew significantly over 2020 as a result of the lockdowns and work-from-home effects of the global pandemic. Game streaming represents a much smaller category of traffic, accounting for just over 4% of broadband traffic and 3% of mobile traffic, although these figures represent significant increases over prior years, again because of the global pandemic. Growth in both categories has raised concern over related environmental impacts and prompted consideration of alternatives to streaming that might be more environmentally friendly, including downloading of videos[94], modifications of game architectures[95], and trading off special purpose gaming devices vs. more general

[89] Cioara T et al., Exploiting data centres energy flexibility in smart cities: Business scenarios, Information Sciences (2018), https://doi.org/10.1016/j.ins.2018.07.010

[90] Giacobbe, M., Scarpa, M., Pietro, R. and Puliafito, A. (2017) An Energy-aware Brokering Algorithm to Improve Sustainability in Community Cloud. https://DOI.org/10.5220/0006300201660173, In Proceedings of the 6th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), pages 166-173 ISBN: 978-989-758-241-7

[91] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces

[92] Sandvine, The Global Internet Phenomenon Report, May 2020, https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf

[93] Sandvine, The Mobile Phenomenon Report, February 2020, https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/Mobile%20Phenomena%20Report%201H%202020%2020200219.pdf

[94] Vidal, John (2017) 'Tsunami of data' could consume one fifth of global electricity by 2025. Climate Home News. https://www.climatechangenews.com/2017/12/11/tsunami-data-consume-one-fifth-global-electricity-2025/

[95] Marsden, Matthew; Hazas, Mike; Broadbent, Matthew (2020) From One Edge to the Other: Exploring Gaming's Rising Presence on the Network. ICT4S2020: Proceedings of the 7th International Conference on ICT for Sustainability June 2020 Pages 247–254 https://doi.org/10.1145/3401335.3401366

purpose devices[96].

In general, electronic device recycling needs to be taken up far more extensively and manufacturers should make it easier to wipe old devices. The right to repair should be strongly championed[97].

4.4.4. Broader issues of Green ICT

Information is literally gobbling up the physical world, atoms are being converted into bits[98]. We can add an information catastrophe to our catalogue of existential crises[99]. Research into more efficient data storage devices and compute processors seems the only obvious solution.

Between them, the biological plastics of chitin and chitosan may be able to replace many of the constructional and/or structural parts of ICT devices. Their bigger brother, Biolith, may be able to replace concrete used in the data centre construction[100]. Experimentation with the kinds of structures that can be made out of these materials is required.

4.4.5. Green ICT challenges

In line with the above considerations, H-CLOUD identified the following main challenges:

S-G Challenge 1: The data centre energy efficiency standards landscape is weak. Develop energy efficiency standards for Europe, in Europe. Start from the KPIs that already exist but choose them wisely as some are no longer fit for purpose. [Research and Deployment]

S-G Challenge 2: ICT devices need to be used for longer periods to better amortize their environmental impacts when they were constructed. They also need to embrace processors which can turn down their performance (and energy consumption) when appropriate. Electronic device recycling needs to be taken up far more extensively and manufacturers should make it easier to wipe old devices. Ensure the right to repair. [Research and Deployment]

S-G Challenge 3: The manner in which the natural world is being exploited to satisfy the demand for digital devices and services is alarming. We need to find more efficient ways of storing and processing data, or to invent completely new ways of storing and processing data.

S-G Challenge 4: The distribution of processing through federation and/or migration to the edge counters the environmentally-beneficial trends toward processing centralized in the cloud (particularly in hyperscale data centres). The environmental impacts of billions of edge/IoT devices and the wireless/cellular networks required to connect to them are not well understood, making it difficult to develop environmentally-sensible policies around edge computing. [Policy, Research]

[96] Mills, Evan, et al. (2017) An Energy-focused Profile of the Video Gaming Marketplace. Lawrence Berkeley National Laboratory

[97] https://www.bbc.co.uk/news/business-49884827

[98] Vopson MM. (2019) The mass-energy-information equivalence principle, Featured in AIP Advances issue 9. https://doi.org/10.1063/1.5123794

[99] Vopson MM. (2020) The information catastrophe, in AIP Advances 10, 085014; doi: 10.1063/5.0019941

[100] Tang, WJ; Fernandez, JG; Sohn, JJ; Amemiya, CT (2015). "Chitin is endogenously produced in vertebrates". Curr Biol. 25 (7): 897–900. doi:10.1016/j.cub.2015.01.058. PMC 4382437. PMID 25772447

S-G Challenge 5: The way in which policy making, in the digital context, impacts the Green Deal needs to be considered right at the start of any policy development process. [Policy]

S-G Challenge 6: The impact of specific ICT activities on the environment is poorly understood. ICT manufacturers should audit and report upon the environmental impact of the manufacture and operation of their goods and services. Data centre and network operators should report their energy consumption and environmental footprint in a way that enables citizens and ICT users alike to understand the environmental impacts of their ICT choices, and governments and policy-makers to encourage environmentally aware decisions. Possible changes in the environmental footprint of the ICT sector should be projected based on this more detailed data, enabling timely mitigation of potentially harmful increases, whether coming from video streaming, edge computing, gaming, AI or any other ICT-related initiative. [Research, Policy]

4.5. The potential of cloud federation

Federation is a form of multi-organisational alliance in which some processes and related policies and activities are governed and coordinated in a collaborative way, and sometimes delegated to a central body by the federation members, while other processes, policies and activities remain the responsibility of the members of the federated alliance (the federation members). Ideally there should be some asset or resource, common to many of the partners, which can be shared across the federation to better serve clients.

Federation is often discussed in the context of multi-cloud integration (federated cloud) and data sharing (federated data)[101]. Our analysis refers to both federated cloud and federated data more generally as federated IT service structures, or “federations” for short.

Federations are currently receiving extra attention as mechanisms to increase service capacity and capabilities in a multi-supply environment to augment each individual federation member’s ability to serve a wider user base. As this deliverable concludes, inherently distributed systems can benefit from federation. Important examples exist in public administration, healthcare and transport/mobility and research, as they need to enable the secure access, sharing and analysis of sensitive data already being stored and managed by multiple players in a community – often residing in private cloud infrastructure. On the supply side, in October 2019 the governments of Germany and France announced the Gaia-X federated cloud initiative, with a strong focus on creating a federated cloud and data capability. The EU discusses both cloud federation and data spaces (related to federated data) in its communication “A European Strategy for Data”[102] (EUSD). There is also ongoing research on “federated cloud technology”, much of it EC-funded and adopted by digital infrastructures to address challenging data processing requirements of research communities.

Annex 15 explores aspects of cloud federation and coordinated organisational structures more generally. Figure 10 maps the key challenges found against the Supply Side Ecosystem illustrated in Figure 5.

[101] Data sharing, for reasons of privacy, security, and both energy and technical efficiency, is increasingly likely to involve controlled access to distributed data sets held by different data stewards (federated data), rather than gathering data into a single database or data lake (data pooling).

[102] EC. Communication: A European strategy for data. 2020.

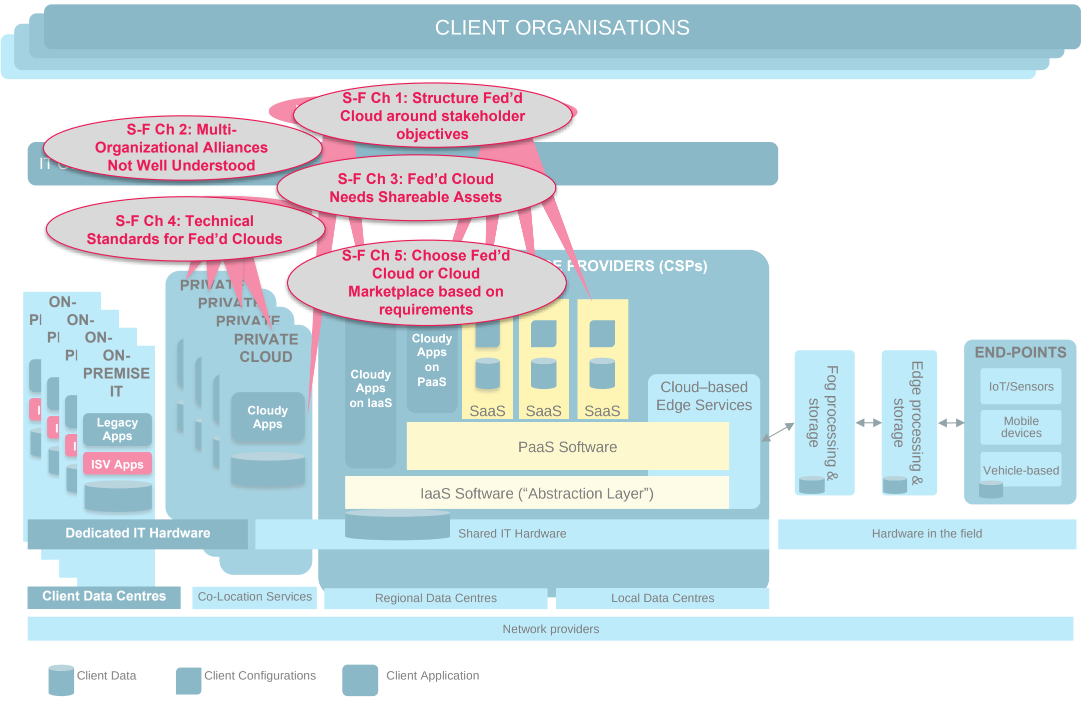

Figure 10. Federated Cloud Challenges Mapped to Supply Side Ecosystem

4.5.1. Introduction to federations

As discussed in section 4.3, many cloud customers need to integrate services from multiple public cloud providers and with their own private cloud capabilities depending on their use case. This integration may be triggered when customers want to combine best-in-class services from different providers, to combine service territories across national borders, or when groups of organisations (e.g. in healthcare) want to share or combine data or data-processing resources funded by multiple independent national funding agencies.

When this service integration is performed by a single customer, it is called "multi-cloud". Customers sometimes hire outside consultants to perform the desired integration.

When this integration is performed collectively by multiple partners, this is called "community cloud", "industrial cloud/B2B platform" and "federated cloud", depending on the circumstances. All of these require cooperation and coordination of the participating service providers. Federations encompass the governance, processes, policies and technical solutions used by multiple service providers to cooperate and coordinate their services, focussed particularly on coordinating service planning, delivery and management. The providers themselves are referred to as federation members.

If services from multiple cloud providers do not need to be integrated, customers' needs might be addressed by cloud marketplaces: central platforms providing discovery and access services (discussed in section 4.5.5 below). Coordination among providers is achieved through adherence to a single business model (set by the marketplace's operator) and its rules of participation.

4.5.1.1. Essential characteristics of federations

Federations (federated IT service structures) exhibit several essential characteristics[103]:

- A federation is an alliance of multiple organisations.
- Participating organisations are "members" of the federation and collaborate for common goals.
- Each federation has a "federating entity" at its core – which can be either virtual or a real organisation separate from any member.
- Depending on the type and purposes of each federation, members can agree to conform with technical standards and operating procedures that enable interoperation, collaboration and sharing.
- Participation can involve a degree of sharing resources (including services, data, metadata or other assets).

"Collaboration for common goals" is an essential characteristic of federations. For different federations, those agreed goals can range from self-interest (e.g. "improving the profitability of federation members") to the public good (e.g. 'advancing scientific knowledge", "improving health care"). A federation's commitment to public good objectives can create benefits for both providers and customers. For service providers (members), a higher purpose can make it easier to agree to conform to more stringent technical standards and operational processes. For customers, a federation's commitment to a higher purpose can increase trust in the federation and its services and motivate greater take-up of those services.

4.5.1.2. Federation business models

There are many possible business models for federations, depending on the type of processes, policies and activities that are federated. These business models address three primary dimensions of organisation:

- the degree to which services are integrated for the customer,
- the degree to which service planning, delivery and management are coordinated among members, and
- the degree to which providers conform to technical, organisational and legal standards.

Different levels of service integration, service coordination and standards compliance enable different benefits for both federation members (the federated service providers) and federation customers.

How a federation delivers services to customers fundamentally defines its value proposition for those customers. In the most sophisticated case, all federation's services are fully interoperable and integrated and make it easy for a customer to discover, select, access and use the services it needs. Several integration options are possible[104] (see Annex 15 for complete descriptions):

- Full Integrator
- One Stop Shop
- Reseller

[103] These essential characteristics are reflected in section 2.1 of the NIST Cloud Federation Reference Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf

[104] The service integration dimension reflects analyses found in "FedSM D3.1: Business models for Federated e-Infrastructures" (https://zenodo.org/record/3982794#.XzVSrxNKj_Q) and "EOSC Pilot D5.1: Initial EOSC Service Architecture" (https://eoscpilot.eu/sites/default/files/eoscpilot-d5.1.pdf)

- Structured Marketplace
- Open Marketplace.

A given federation may offer services at different levels of integration at the same time. For example, some federated services will be tightly integrated, while others will only be available as "resold" services with lower levels of integration and service coordination. The extent of this integration will be a function of the standards to which various providers conform, and the extent to which service management is coordinated.

Well-integrated services depend on well-coordinated service management. Two frameworks offer best practices for service management that can be employed in any IT service organisation and that are especially valuable when services from multiple suppliers need to be delivered, effectively, to a given customer: FitSM[105] and Service Integration and Management[106] (SIAM).

FitSM identifies fourteen distinct service management processes that should be coordinated among multiple service providers in a multi-supply environment. The "Full Integrator" business model requires most or all of these service management processes to be coordinated, in turn requiring service providers to agree on related standards and procedures. The "One Stop Shop" business model requires a lower level of process coordination.

Service coordination creates benefits for federation members. For example, managing support requests that could involve multiple suppliers benefits not only from coordinated *Incident and Service Request Management* (one of the service management processes in FitSM), but also consistent *Customer Relationship Management* and consistent *Supplier Relationship Management*.

Well-integrated services depend on compliance with appropriate organisational, technical and legal/regulatory standards.

- Service management standards and procedures enable the coordination of service management, which in turn enables the most complete integration of services.
- Complying with technical standards or agreeing to use common software tools or components (e.g. OpenStack[107] or Kubernetes) may be required for interoperability and integration.
- Transparent and trustworthy disclosure of legal and regulatory compliance is critical.
- Compliance in each of these three domains is handled differently:
- Each service provider's compliance with service management standards and procedures is assessed and monitored by the federating entity.
- Compliance with technical standards can be evaluated by external services or by the federating entity as agreed within the federation.
- Assertions of legal and regulatory compliance would be the responsibility of the providers themselves.

Interactions among these different types of compliance can affect the other dimensions. For example, when services are tightly integrated, with fully coordinated service management, differences in legal or regulatory status among the different services can still reduce compliance of the integrated service.

4.5.1.3. The benefits of federation

Table 10 illustrates how specific aspects of federation generate benefits for both providers and

[105] https://www.fitsm.eu/
[106] https://www.scopism.com/free-downloads/
[107] https://www.openstack.org/

customers of a federated cloud.

Table 10. Benefits from different federation business models

Federation business model	Benefits for service providers	Benefits for customers
Open Marketplace	● Increased visibility ● Access to a larger pool of customers, greater take-up of services	● Increased variety in service offerings ● Easier/ cheaper identification, comparison and selection of different service offers in the federation
Structured Marketplace	● Reduced need to invest in peak capacity ● Local investments encouraged by higher ROI ● Ability to serve a broader market, while limiting operating costs ● Ability to offer expanded services ● Operating costs can be reduced	● Easier access to more/better resources ● Better/wider services available to customers in underserved territories or market segments ● Get support in the local language ● Greater confidence in identification, comparison and selection of interoperable service offers from the federation ● Reduce "vendor lock-in" ● Confidence knowing that standard, balanced contracts are being used ● Easier to implement robust access controls (e.g. with single credential) ● Easier/cheaper assembly of services ● Confidence they are complying with all EU and relevant national laws and regulations ● Know that the data and information that they have placed in the federation will be handled in accordance with EU values ● Increased trust in federation partners
Reseller	● Services can be resold by federation to customers outside normal service territory	● Access to expanded range of interoperable services that otherwise would not be available (e.g. in the country/region, in the customer's preferred language)
One Stop Shop	● Reduced need to hire specialized personnel ● Reduced need to invest in specialized service management processes ● Reduced costs	● Better integration of the cloud services portfolio used ● Ability to implement complex use cases ● Easier/cheaper integration of desired services ● Ability to support a wider range of specific use cases coming from a broader user base ● Improved service and support ● Common support channels
Full Integrator	● Provider's service delivery capabilities are enhanced by integrating with specialized services, resources and expertise from other providers	● Consistent and efficient management of multiple service providers

Some of these benefits can be generated through bilateral agreements between providers, but federated organisations create efficiencies by simplifying the process for multiple providers and by performing common tasks on behalf of partners.

4.5.1.4. Examples of federation

Federated cloud has been successfully adopted by research infrastructures to implement data-centric exabyte-scale computing facilities, pooling national investments to implement a distributed European extreme scale infrastructure that offers inherent secure access to computing resources, storage, data and applications.

The EGI Federation[108] is a successful example of an international cross-border federation (delivering more than 1.1 million CPU cores and 1 Exabyte of storage across EU and non-EU countries) based on a decentralized operational model according to which management of service delivery and access policies are governed at national or regional level, with a central coordinating body responsible for defining and enforcing federation-wide policies and providing central services that enable the federation to function.

Annex 15 lists 25 examples of federations worldwide, categorizing them according to their domain of activity (e.g. healthcare) as well as the federation business model that appears to be in use.

- Research federations represent the majority of the examples (14 out of 25). This is probably because the federated model is well suited to the situation where nationally funded research organisations in different countries want to support international research but also want to spend money within their own borders. The higher purpose of research federations (support for the advancement of knowledge) also makes it easier to organize a research federation.
- The *Open Marketplace* business model also represents the majority of examples (13 out of 25, 9 of them operating in the research domain), probably because this model is the simplest to organize. Annex 15 also lists 4 *Structured Marketplace* and 3 *Reseller* business models, although 2 commercial *Resellers* actually shut down operations.
- EGI and the Worldwide LHC Computing Grid (WLCG) are listed as *Full Integrator* research federations, reflecting their strongly integrated service catalogues, as well as strongly coordinated management processes.
- Twelve of the 25 examples federate compute infrastructure (IaaS) using the open source OpenStack virtualization software. This reflects OpenStack's broad appeal across the IT world, regardless of domain.

4.5.2. Recommendations for creating a European Cloud Federation

As discussed above, realizing the benefits of federation requires federation members to cooperate and coordinate their activities, and this can be most easily motivated when the federation is supported by a common business model among the participating members.

S-F Challenge 1: Coordinated/federated approaches must be structured around the objectives of their stakeholders, balancing community focussed initiatives with pan-European solutions. The European landscape for cloud- and data-driven innovation is complex and fragmented, with many potential use cases, customers, providers, innovators, and stakeholders. The EUSD itself addresses a range of requirements and opportunities across nine sectors of the economy. The needs of different stakeholder communities must be balanced against the need for common or aligned solutions. The effectiveness of a EUCF will depend strongly on the clarity of its value proposition and how it is constituted to realize that value proposition.

Annex 15 explores organisational research that suggests best practices for creating effective multi-organisational alliances such as federations. These best practices are reflected in the

[108] https://www.egi.eu/

following recommendations.

S-F Recommendation 1.1: Develop detailed business cases for identified use cases in each of the nine sectoral data spaces described in the EUSD that quantify the societal gains and costs to achieve the desired benefits and ascertain feasibility and related ICT innovation needs. Identify existing initiatives and high-impact use cases (e.g. existing health data hubs), elaborate specific data sharing use cases building on existing good practices. Identify data and cloud resources that might be good candidates for sharing and re-use through federated structures. Quantify specific gains and costs for businesses, research organisations and Public Administration to use federated cloud and data services as a platform for cross-sector data sharing involving private data, public data and governmental data. Ideally this would follow a process similar to that described by the High-Level Expert Group on Business-to-Government Data Sharing[109] (page 48) which starts by identifying the problem to be solved, the conditions for data re-use, possible compensation structures, and then considers the optimum model for data access. Conduct a requirement and gap analysis to identify services needed from a EUCF, as well as the stakeholders that would need to be involved in their delivery and supervision. This analysis may identify clusters of requirements where solutions at the correct technological readiness level are available and could be deployed, for example to ensure secure and interoperable access to data and cloud services. This analysis will also identify gaps in existing solutions that should be prioritized for additional research and/or development. [Deployment, Research]

S-F Recommendation 1.2: For each business case, select the most appropriate federation business model that fulfils the requirements while providing the best value with the optimal effort. Consider whether the proposed action is a response to a market failure, which can be corrected with a temporary action, or whether continued support is needed to correct a systemic problem.

S-F Recommendation 1.3: Create an open infrastructure and testing capability that could flexibly support demonstrations, proofs of concept and pilots of how federated cloud and federated data solutions could be assembled, operated, managed and governed, including collection of data that would validate the business cases developed in S-F Recommendation 1.1. Before establishing a formal EUCF, invest to encourage participation in federated cloud and data sharing pilots and create a dedicated virtual support and training centre. This would bring together a number of customer organisations (e.g. public administrations, industries and research organisations with a specific data sharing use case) to define requirements, which would then be addressed by providers integrating existing tools (i.e. no research and minimal software development), and solutions would be supervised using best-practice federated governance models. As skills are a major asset for a successful repurposing and re-architecting of applications by potential cloud customers, a support centre will be necessary to provide the technical expertise needed for an effective use of the pilot infrastructure. Particular attention should be paid to provider costs and assessments of value received, in order to identify sustainable business cases for continuing operation. Based on the analysis presented in this document, promising use cases can be found in each of the public administration, transport/mobility and health care sectors, for which sectoral data spaces are all proposed in the EUSD. [Deployment]

S-F Recommendation 1.4: Support the creation of multiple EUCF-affiliated initiatives and their cross-domain collaboration, which will specify domain-specific use cases, objectives and beneficiaries, federation partners and stakeholders, governance and decision-making mechanisms, scope of possible federated activities, and applicable business models. [Deployment]

S-F Recommendation 1.5: Develop a lightweight model for the EUCF as an umbrella coordinating body of sector- or use-case-focussed European federated cloud initiatives, supporting coordination of their research and innovation activities, cross-sector collaboration

[109] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

on interoperability, facilitating best practice operations, and providing relevant shared services such as certification activities. [Deployment]

S-F Recommendation 1.6: Implement a EUCF with a phased approach that flexibly aligns activities across multiple domains, and that allows achievement of "quick wins". Recommendations 1.1 through 1.4 highlight the many topics that must be addressed before a EUCF can be organized and functional. Pilot projects and demonstrators will clarify requirements and identify applications and use cases where an early version of the EUCF can achieve success, which in turn will build credibility and support. [Deployment]

S-F Recommendation 1.7: Set up the EUCF following known organisational recommendations. Based on research into multi-organisational alliances, a EUCF should adopt the following approaches [Deployment]:

- Form a central organisation focussed on the coordination efforts required to make a EUCF work,
- Establish and follow well-documented procedures (for example, governance protocols) to improve its effectiveness,
- Establish communications mechanisms that support a broad set of interfaces among the EUCF, its primary and affiliated members, typically through working groups and committees,
- Establish monitoring and evaluation mechanisms to track EUCF performance against its objectives,
- Identify funding mechanisms and a business plan to ensure sustainability of the EUCF's activities and particularly its central coordinating body.

S-F Recommendation 1.8: Evolve existing best practices and standards (e.g. ITIL, FitSM, etc.) for federated service management to ensure federated cloud initiatives have reference requirements, processes, procedures and policies that ensure the compatibility of service delivery and planning across different initiatives. Develop "starter kits" to assist with implementation of each federated business model, with sample templates for required governance and service management processes (definitions, roles, process maps, etc.). [Deployment]

4.5.3. Federated cloud architecture and services

A cloud federation requires the management of a common set of policies and procedures, shared, scalable and secure cloud-based solutions for data and infrastructure access across the federation, and a layer of federation services to manage resource allocation and other central processes. The federating entity governs the reference standards, policies and requirements to achieve the interoperability of the primary pooled resources, as well as interoperability with any adjunct services.

S-F Challenge 3: Defining, evolving, selecting, agreeing on and managing technical standards and tools for federated clouds and distributed data access and exchange. Creating a distributed yet federated, technically effective data-processing system is an active subject of research – many technical approaches are being studied, but they are not converging into "standards" because the underlying technologies are rapidly evolving and because the scope of integration is expanding from the data centre out to the more heterogeneous edge computing environment. Where distributed capabilities need to work together, there must nevertheless be an agreement on the standards to be adopted, despite this rapid change. Thus, cloud federation requires participating service providers to agree on standards that enable their services to interoperate, at least for a defined period and/or in the context of serving a particular market (e.g. research or public administration).

This challenge highlights how technical choices can only be made in the context of the “business” role and “purpose” of the federated cloud. For example, EGI and EOSC prioritize service management (i.e. the “use case” or “business case”) over technical standardization and accommodate different technical approaches, as needed, in favour of the objectives of their users and clients according to their use case requirements.

Different services, different technologies, and possibly multiple standards will probably be needed to meet the requirements associated with use cases that are priorities for any federated cloud initiative, particularly one as broad as the EUCF. While different tools and processes might be used in different use cases, a consistent architecture should be created to organize those tools and processes.

For example, EOSC is charged with supporting a wide range of scientific requirements, set by a diverse range of scientific communities. EOSC has defined a three-part architecture for its “federating core” – the fundamental asset of the EOSC, composed of the technical, human, policy and resource elements required to facilitate, monitor and regulate as appropriate day-to-day transactions across the federation[110]. (The cloud architectures for EOSC, Gaia-X and NIST are examined in detail in Annex 15.) As with EOSC, the NIST CFRA describes a framework for defining and structuring the activities of a cloud federation, without specifying the technologies, standards or tools that will be used to execute each activity. The NIST CFRA was explicitly created to align and streamline the efforts of many different federated cloud initiatives, as well as offering guidance to federated initiatives in non-technical domains. Relevant standards are called out in Section 8 of the CFRA report, but their inclusion does not constitute endorsement.

Annex 15 highlights how different technical architectures can overlook key components of a complete federated cloud capability. Gaia-X in particular focuses on compliance and documentation of non-functional characteristics, as well as the mechanisms for secure data transfer, but provides limited guidance for operational activities (for example, who do customers call when there is a problem using Gaia-X?). Although the NIST CFRA mentions many important “human-to-human” functions, such as customer support, the CFRA focuses on the technical, machine-to-machine aspects of cloud federation.

S-F Recommendation 3.1: Develop and evolve a Federated Cloud Reference Architecture (FCRA). To the extent possible incorporate the NIST CFRA, EGI and Gaia-X’s technical architectures, and evolve it to ensure conformance of emerging federated cloud initiatives. This should specifically characterize how practical compliance frameworks and portals would align with the EUSD’s contemplated “Cloud Rulebook” and “Service Marketplace” concepts. [Deployment]

S-F Recommendation 3.2: Create and maintain a federated cloud interoperability framework as an evolving suite of technology, standards and tools that are consistent with the FCRA allowing interoperation within a given federation and across multiple federations, compliance with European values and identification of interoperable components. This suite of components would help EU customers navigate the many options for cloud-based solutions and would help formalize how they are described and the possibilities for integration. This recommendation is similar to “product labelling” recommendations in other industries, making it clear what is included in a given component, how it works, how it works with other components, and any limitations on performance.

S-F Recommendation 3.3: Coordinate research and innovation activities for funding in Horizon Europe by aligning cross-domain cross-use case research and innovation activities of common interest for different federation stakeholders to increase synergies, innovation potential and avoid duplication across the industry, research and public administration sectors. This recommendation is meant to increase innovation

[110] EOSC Federating Core Community Position Paper v1.01

capacity of the EU programmes by ensuring that EU funded research and innovation has a large potential of adoption by multiple stakeholders across different sectors.

Annex 15 identifies a range of technical and operational services that should be framed by the federation architecture, including both services for customers and services required to ensure effective federation operations.

4.5.4. Federated edge solutions

Federated edge solutions provide a pathway to creating efficient "public edge solutions" that could help accelerate edge adoption and implementation in Europe. Federated edge would require automated discovery, selection, and provisioning of services and/or resources. Contracting and payment could still be managed in a more predictable fashion, limiting dynamic provisioning to those resources offered by eligible edge service providers, or alternatively in a manner similar to the growing trend toward microservices, where small financial charges are made for many small service executions (i.e. individual instances of downloading and processing data from a particular remote device).

The benefits of federated edge computing are clear for both providers and customers:

- For providers: Edge service providers, even those well positioned in the market (e.g. major mobile operators), can improve the value of their services when they are combined with others, and they can potentially reach new customers.
- For customers:
- Deployment of cloud-edge solutions can be scaled across Europe.
- Edge-based services can be accessed without requiring customers to own their own intermediate edge equipment.
- Data can be processed close to the source with edge-based services, rather than requiring all data to be "pushed" to the cloud.
- Edge-based services can be adopted without being locked into the use of one cloud solution (multi-homing).

4.5.5. Federated data solutions

The EUSD and other initiatives highlight the growing importance of federated data clouds. As documented elsewhere in this deliverable, important ecosystems in public administration, healthcare and transport need to enable secure access, sharing and analysis of sensitive data already being stored and managed by ecosystem players – often on private cloud infrastructure. There is some potential for federated data clouds to create "data as a service" capabilities that can be accessed more broadly, yet still on a controlled basis, to enable the projected societal benefits of both "big" and "open" data.

Both the EUSD and Gaia-X separate their treatment of data spaces from an underlying federated cloud capability. However, data is stored, physically, in that same federated cloud capability. As data volumes increase, and as the data in a "data space" becomes more distributed across multiple data owners and data storage systems, the physical reality of "where is the data" becomes significant. Research communities in the earth sciences and life sciences have already responded to this challenge by developing the ability to "bring compute to the data," with initiatives like Copernicus DIAS and the Global Alliance for Genomes and Health (GA4GH). Similar problems are growing in public health, life science, astronomy, as well as in industry – requiring similar or better solutions.

This Green Paper has already identified this as Major Challenge M3: "Secure and trusted data access, sharing and processing across different organisations". The following recommendation responds to this Major Challenge:

S-F Challenge 3: Federated data has great potential to support secure, private sharing of data held by many different organisations. Best practice roadmaps are urgently needed to ensure federated data sharing initiatives are established and operated efficiently while preserving and ensuring the highest level of trust that affected sensitive data will be kept private and secure.

S-F Recommendation 3.1: Guidelines for implementing different data sharing approaches using federated data platforms. The best practice roadmap for federated data sharing should include specific guidelines for using federated platforms to enable the different forms of operational approaches to be easily adopted by data sharing communities.

S-F Recommendation 3.2: Efforts to increase semantic interoperability for data within and across sectors are critical and must also include harmonization of data usage models to enable automated, yet secure and appropriate, data sharing. Existing data usage models should be systematically analysed in hopes of finding common philosophies and features that can form the basis for a common, cross-sector usage model that could facilitate greater levels of properly governed data sharing.

S-F Recommendation 3.3: Develop regulatory sandboxes. These sandboxes would allow experimentation and scaled-up testing of privacy-preserving technologies, while ideally exempting the enterprises that need data from the responsibility to prove that they have all the necessary security measures in accordance with the legal precepts.

S-F Recommendation 3.4: Continued support for research, innovation and deployment of privacy-preserving technologies. Both the BDVA[111] and e-SIDES[112] reports enumerate a number of recent or ongoing projects to develop, refine and deploy these technologies in practical application domains. While these technologies are at various technological readiness levels (TRL), and not mature enough for “production” deployment, they are nevertheless promising and would benefit from continued investment and support for early stage adoption and deployment.

S-F Recommendation 3.5: Support and contribution to the formation of technical standards for preserving privacy. Such standards would provide risk assessment tools, test suites for validation of performance, as well as evaluation of data for sensitive content.

S-F Recommendation 3.6: Continued support for research, innovation and deployment of distributed data analytics tools, as well as data placement tools, that minimize security privacy risks and maximize speed, computational and network efficiency as well as energy efficiency.

[111] Timan, T. & Z. Á. Mann (eds) (2019) “Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies”, October 2019. BDVA. https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf

[112] Cappiello, Cinzia & Gal, Avigdor & Jarke, Matthias & Rehof, Jakob. (2020). Data Ecosystems: Sovereign Data Exchange among Organizations. Report from Dagstuhl Seminar 19391. https://drops.dagstuhl.de/opus/volltexte/2020/11845/. e-SIDES (Ethical and Societal Implications of Data Sciences), Deliverable 3.2, Assessment of existing technologies (2018), https://e-sides.eu/resources/deliverable-d32-assessment-of-existing-technologies

5. RESEARCH, INNOVATION AND DEPLOYMENT LANDSCAPE ANALYSIS

The European Cloud Computing (ECC) Portfolio explores the European cloud landscape with the objectives of mapping it in all its dimensions, identifying the positive outcomes of the work undertaken by the European cloud community and spotting potential gaps, and creating a viable knowledge resource for the community. It will be the basis for the development of an easily searchable online catalogue of relevant cloud-related initiatives.

5.1. Description of ECC Portfolio

The European Cloud Computing (ECC) Portfolio encompasses a total of 210 initiatives (111 profiled in the first release and 99 added in this second release) relating to cloud computing, with a specific focus on federated cloud, edge computing, and green computing. In the R&I context, 96 H2020-funded projects were identified; 114 initiatives have resulted from desk research in the deployment area, of which 38 relate to the public sector, 65 come from the private sector (industry collaborative clouds), and 11 are from public-private partnerships.

In this updated European cloud landscape, the desk research has identified:

- 68 federated cloud initiatives – 16 from R&I and 52 from deployment
- 52 edge initiatives – 33 from R&I and 19 from deployment
- 11 green IT initiatives – 5 from R&I and 6 from deployment
- 95 initiatives addressing cloud, but with no specific reference to the three H-CLOUD key areas above mentioned – 51 from R&I and 44 from deployment.

This analysis of the European cloud landscape, including 210 R&I projects and deployment initiatives, shows that:

- The European cloud market is maturing across all European industries and adoption has grown across all models (public, private, and, in particular, hybrid).
- Federated cloud is the focus of several deployment initiatives, not only in the public sector, where there are no competitive barriers that hinder collaboration, but also in the private sector, where the growth of ecosystem-based business models are driving multiple companies to cooperate, even across industries, to innovate products and services, and enhance operational efficiency.
- Several research and innovation projects are focused on Platform as a Service and edge computing solutions.
- Green computing outcomes are the by-product of innovations that make cloud and edge architectures efficient, but not the sole focus of projects and initiatives.

The innovative solutions that are the subject of R&I projects and the governance models that are being scaled in deployment initiatives must be brought together to make federated cloud mainstream. They should focus on maximising:

- The efficiency of the European computing infrastructure – including the energy efficiency that aligns with the ambitions of the EU green deal
- Fostering data-driven innovation by focusing on specific use cases where technology can make an impact on priority European industries, like public sector, manufacturing, utilities, transportation and agriculture
- Ensuring trusted use of data in compliance with data privacy and security regulations and ethical guidelines.

Successful federated cloud services with large-scale adoption are still a long way from reality.

Several challenges need to be overcome, and considerable work must be done before they become mainstream. At the current stage of maturity, public sector organisations have a better chance of developing and adopting federated cloud services within a region or country because of a long tradition of building shared services. As for the private sector, the emergence of ecosystem centric business models, such as B2B marketplaces, and innovation communities are creating active demand for cloud federation but require strong alignment of incentives to be scaled.

The edge computing ecosystem is still emerging in Europe and will depend a lot on the timeframe of the roll-out of 5G technologies. The edge ecosystem has many different layers, and a better understanding of the interrelation between cloud and edge is required. In addition, the layer at which federation makes sense in the edge ecosystem needs to be understood.

With European organisations now including requirements for the sustainability of IT equipment into their supplier requirements, green IT and energy efficiency have become design criteria for next-generation IT infrastructure. When building out edge infrastructure, thinking about the lifecycle of the equipment and defining standards and guidelines for lifecycle management are important.

5.2. Preliminary analysis of ECC Portfolio: Success Stories and Good Practices Guide

The Success Stories and Good Practices Guide identifies and describes initiatives providing added value to what is currently considered state of the art within the European cloud landscape and presents challenges and recommendations for future actions in the cloud computing field.

Success stories and good practices have been identified primarily through a series of executive interviews, complemented by desk research.

The qualitative research encompasses European initiatives that have taken place or are being developed on a local, national, European, or global level and have been collected from different sources. Taking as reference the sources used in the European Cloud Computing Portfolio (i.e., H2020 cloud-related funded projects, IDC's industry cloud tracker, and IDC Government Insights research), the research expanded beyond these sources and included the GAIA-X use-case directory, the International Data Spaces (IDS) use-case directory, and the Cloud28+ directory, as well as major EU telecommunications companies and governments' websites.

The interviews aimed at assessing whether the cloud-related initiatives could be considered success stories and good practices based on five identified criteria: business impact, technology innovation, organisational structure, data governance, and environmental & sustainability performance.

For the first release of the Success Stories and Good Practices Guide, the H-CLOUD team identified 65 potential success stories relating to cloud computing, federated cloud, edge computing, and green computing. Out of 65 initiatives, 29 were considered to include good practices, following interviews performed from June to September 2020. Within the public sector, 10 relevant cases were identified; 11 were identified in the private sector, 6 in research and innovation (R&I), and 2 in public-private partnerships (PPPs).

The main findings of the analysis concerning key H-CLOUD topics are described below.

Cloud federation

Cloud federation has the potential to realise the economies of scale of a large cloud provider, while ensuring that both end users and small and medium-sized suppliers of technology services are not locked into one monolithic infrastructure and platform. However, many questions remain regarding the feasibility of cloud federation:

- What are the incentives to do it?
- Who guarantees that all participants in the federation live up to the same security standards?
- What is the commercial model?
- How do you ensure that all participants can deliver the same minimum service level?
- What is the right governance structure?
- How do you create customer trust in the federation?
- How do you advertise and market the federation?
- How do you technically set up the federation?

The initiatives featuring good practices that were analysed as part of this research offer learnings to overcome those challenges from multiple points of view.

Business Impact: The key success factor for federation is adoption/participation. As indicated by public-sector initiatives featuring good practices, such as Statens IT and G-Cloud, an increase in the number of users of shared, community, or federated services generates a positive network effect. Higher participation drives economies of scale in terms of procurement and management. Good-practice knowledge sharing across participants favours continuous improvement in terms of technology and governance innovation. The French government's SPOTES programme defines and monitors a set of KPIs that tracks participation from multiple perspectives: user experience/satisfaction, number of transactions, number of registered users, number of tickets, and number of services offered.

However, it must be noted that it is difficult to achieve widespread adoption and collaboration. That is because:

- The federation may replace someone’s authority or job, so it will encounter organisational resistance.
- The federation may include multiple industries, with multilateral collaboration having no clear business case but requiring commitment to and experimentation with innovative use cases, an example being IDS.
- The federation may include competing companies that are concerned about disclosing trade secrets.
- The business case for the individual participating cloud providers might not be clear; business demand from customers might not be present; and the funds available for marketing the federation may be limited.

Technology Innovation: The good practices analysed are advancing the federated cloud technology innovation frontier along three main paths:

- Cloud provisioning and deployment across multi-cloud environments; for instance:
  - Logius is developing a Kubernetes container-based orchestration layer that aims to enable service rollout to AWS, Azure, and government private-cloud data centres. This orchestration layer, built on open source (OpenStack and OpenShift), aims to include all the capabilities necessary to manage a cloud federation, from service catalogue to performance dashboard and backup.
  - COLA’s MiCADO solution extends virtual machine management beyond the level offered by Terraform and container management beyond the level offered by Docker Swarm and Kubernetes.
  - CloudSME is taking container orchestrator technology to market that allows organisations to use multiple cloud platforms and move their workloads and data independently of the underlying infrastructure.

    - City Network is one of 20 OpenStack-based cloud providers in Europe, and it is building an open-standards-based cloud infrastructure that could be federated with other OpenStack-based cloud providers – if customer demand for it exists.
    - ThreeFold Grid offers a blockchain-based solution whereby any organisation can supply compute resources to the federated cloud grid based on an installed common operating system with security attributes included, and the whole federated infrastructure is managed automatically by blockchain.
- Securing access to federated resources; for instance:
    - Sunfish assumes blockchain and DLT can be used in the future to ensure the verifiability of communication among federation partners, to manage compliance with contractual terms (smart contracts), and to register the status of resources across the federation.
- Reducing the cost of operating across multicloud environments; for instance:
    - Statens IT is building a shared tenant-based system with sub-tenants for users that can be swapped so that the user organisation can avoid purchasing a lot of new licenses.

Governance/Organisational Change: Realising the benefits of collaborative initiatives, such as community clouds and federated clouds, revolves around the ability to bring people together through the service lifecycle, from design and financing to implementation, operation, and consumption. This requires:

- Creating organisational and cultural change mechanisms that foster collaboration; for instance:
    - The first Helix Nebula project identified cultural and organisational differences between cloud service providers and organisations from the research community – including prejudice against commercial providers and the cloud in the research community and differing assumptions about procurement practices. HN Science Cloud's PCP approach enabled these differences to be aired in a structured, goal-oriented context and solutions to be found that worked for both sides. HN Science Cloud assembled objective information to counter distrust. It conducted detailed TCO studies to resolve disagreements and misperceptions about the comparative costs of cloud-based and -owned infrastructure, as well as establishing automatic testing suites to objectively validate functional performance and compliance with specifications.
    - The French government's SPOTES invests in knowledge sharing through virtual events, seminars, educational material, and blogs that are made available on the marketplace to maintain momentum even during the COVID-19 crisis.
    - The Danish Statens IT initiative joined Euritas to learn from peer government IT modernisation programmes around Europe. The initiative invested in personnel certification and security clearance, to offer high-quality information assurance, and in training, to enhance technical personnel-customer relationship capabilities, to better align their offerings with the needs of individual government departments.
    - Establishing structures and processes that make the collaborative supply of cloud services efficient, effective, and compliant with regulations; for instance:
    - Cloud28+ created a federation at the service catalogue level, whereby participating cloud vendors advertise their services through the Cloud28+ digital platform and marketplace.

- G-Cloud realised an efficient and effective marketplace for certified cloud providers that want to supply services to the UK public sector.
- The Austrian Federal Government separated technology innovation (EGIZ) from technology implementation (BRZ) to focus all government innovation decisions on interoperability standards, feasibility, and prototyping and then to define a minimum set of guidelines. At the operational level, the key goal is to keep EGIZ's service catalogue commercially competitive in the long run for the Austrian Federal Government. EGIZ and BRZ collaborate closely, but they are managed and funded separately so as to maintain independent decision making. They also employ different sets of expertise.
- The Irish central government established a three-tiered IT governance model that includes: a) a civil service management board, which includes secretary generals of every department, with the government digital strategy discussed twice a year; b) a subgroup co-chaired by two of the most influential secretary generals (from the Finance Department and Welfare Department), where collective decision making happens about the government's digital strategy; and c) an ICT advisory board, including the heads of IT of every department, where more technical and tactical guidelines and action plans are discussed.
- The work of GAIA-X is divided into different workstreams for specific topics: a) user ecosystems and requirements, b) technical implementation, and c) a cross-function unit known as the Joint Requirements Expert Tribe. This unit consists of two groups that are convened on a flexible basis and that deal with topics when interdependency between the workstreams is strong. The project structure is agile in that it can be adapted over time, in line with framework conditions, and guarantees collaboration across separate topics.

Data Governance: The analysed good practices are advancing federated cloud data governance capabilities along two main paths:

- Information assurance guidelines and certifications for suppliers of cloud services: Public sector and public private partnership good practice examples offer the most important learnings here. In fact, G-Cloud, WIIP, GAIA-X, and IDS have put in place a certification process that is used consistently to verify supplier’s compliance with information assurance policies, before they are authorised to provide the service, and to audit them when they are operating in the environment.
- Data interoperability architectural standards and principles: Multilateral multi-industry programmes like GAIA-X and IDS strategically focus on interoperable data exchange. For instance, the IDS connector is a container architecture that can be implemented in different ways, depending on the scenario – on micro-controllers, sensors, mobile devices, and servers and in the cloud.

Environmental Sustainability: The economies of scale of cloud data centres have a positive impact on environmental sustainability. Cloud data centres can afford to invest in features like power-saving stand-by modes, energy monitoring software, and efficient cooling systems and can increase server utilisation rates through virtualisation and automation. The public-sector regional IT shared service centre interviewed as part of this study provides evidence of how even a medium-sized private cloud data centre can reduce its energy bill by more than 50%. However, two factors must be considered for the realisation of environmental sustainability benefits:

- The energy efficiency of the existing IT infrastructure to be replaced with cloud: The more modern, virtualised, and efficient the legacy infrastructure is, the lower is the potential positive impact of cloud.

- The expected growth of IT infrastructure demand: cloud's elastic pricing and provisioning models often induce a growth in usage, hence offsetting the energy efficiency per unit with overall growth in consumption.

Edge computing

Edge-related good practices can be divided into two main categories: what edge allows today, as a combination of already available resources, technologies, and approaches, often in collaboration with cloud; and how different aspects of edge technology are being developed and innovated.

Business impact: The business impact is present across all the private initiatives analysed and in the City of Valencia initiative, which underlines how end-user organisations are looking at edge innovation to gain business benefits. Nevertheless, each initiative measures success and business impact in a different way. The City of Valencia's Smart City initiative focuses on a data-sharing platform that enables the delivery of a broad list of services. In the private sector, the number of edge endpoints deployed, the number of locations in which such solutions are deployed, and the number of clients adopting such solutions are, generally speaking, good KPIs for indicating the success of an initiative and its ROI. Additional KPIs include:

- Measuring how clients use the edge platform, the number of accesses to edge information, and the number of to edge applications is a popular way of understanding success (e.g. Vivacity Lab, Axis, and Wordsensing)
- Measuring the outcomes of the use case supported is another key point. These initiatives clearly underline that edge is not a universal fit; the solution, the technology, and the partner ecosystem are strictly dependent on use-case needs, which is why the business success of the edge initiative in question relates strictly to the success of the use case supported. Vivacity Labs measures this through traffic efficiency on roads equipped with edge intelligent cameras, and BrianzAcque via the volume of water dispatched and the service level delivered to citizens. A leading car manufacturer based in the EU correlates success in a factory in CEE with the service availability obtained by continuously monitoring uninterrupted power supplies. Wordsensing looks at how much customers/partners are saving by deploying the company's solutions, as well as the increases in the safety of workers, citizens, and the environment that edge-based geotechnical data management enables.

Technology innovation is another big impact resulting from the initiatives analysed. The approach of distributing computing capabilities is not a new trend, but edge can be seen as an emerging technology, with hardware and software platform innovations opening up new possibilities. Moreover, when edge computing is combined with other emerging technologies/innovation accelerators, it offers great potential. The LightKone research initiative, for example, focuses on a new architecture for computing and storing data at the edge, guaranteeing continuous alignment without the need for the core. The private initiatives researched specifically feature solutions that combine the Internet of Things, artificial intelligence, and analytics. Both Axis and Vivacity Lab, for example, enable artificial intelligence at the IoT edge (in smart cameras), with the former focusing on the deployment of more efficient hardware and the latter focusing on algorithm deployment. The solutions of BrianzAcque and the leading car manufacturer are based on the collection of IoT sensor data. Likewise, Worldsensing gathers IoT data, with its solution adding a layer of data analytics at the edge.

Green IT

Green IT is increasingly an important topic in the cloud industry, with several cloud service providers announcing ambitious goals with regards to CO2 neutrality. However, compute needs will only increase globally, and offsetting the carbon emissions for computing will require clear goals and a focussed strategy.

Compute efficiency can be increased by moving to a highly virtualised, or even better containerised, infrastructure that is centralised in a data centre. The regional government shared services centre that was analysed managed to reduce its electricity bills by 50% by moving to a highly virtualised architecture. Containers are even more efficient than virtual machines.

The question is, Will the move to edge deployments make the entire infrastructure more or less efficient and sustainable? So far, we have not found evidence from the analysed projects to answer this question. We have not found projects or initiatives that were primarily looking at green IT. Green IT has emerged as a by-product of deploying modern compute paradigms, such as virtual machines, containers, and microservices.

Challenges and recommendations

When looking for good practices in the areas of cloud, federation, edge, and green IT, the research found that many challenges are being addressed with creative solutions, but there is still a long way to go to come up with a general set of good practices that can be applied broadly.

The main challenges that have emerged through the interviews centre around ability to identify business incentives, create a viable governance model, and make a business impact in the European market. If one objective is to improve the market penetration of European solutions in the areas of cloud, federation, edge, and green IT, then stronger incentives for users to adopt them and for companies to develop and market these solutions are needed. When there is no customer demand, it is likely that such solutions will not mature or be adopted.

Cloud federation

Federation projects are more successful in the public sector than in the private sector because the strategic incentive is strong to have full control over and sovereignty of IT infrastructure in the public sector, whereas the business incentives to create a federation are absent in the private sector.

The key challenges identified in the H-CLOUD Green Paper are confirmed by the good-practice research effort:

1. Coordinated/Federated approaches must be structured around the objectives of their stakeholders, balancing community focused initiatives with pan-European solutions.
2. Universal challenges including defining, evolving, selecting, agreeing on, and managing the architecture, technical standards, and tools for federated clouds and for distributed data access and exchange.
3. Federated data has great potential to support the secure private sharing of data held by many different organisations.

We have learned of ways to overcome these challenges. For example, Cloud28+ created a community of service providers with a shared business interest. These providers publish their services using a joint service catalogue on the Cloud28+ platform; City Network has adopted OpenStack as its underlying technology to enable federation at the technology architecture level; and Aquacloud, Polymore, and GAIA-X are working to provide a standard data model to create value for participants in their ecosystems.

Edge Computing

The H-CLOUD Green Paper highlighted various edge-related challenges, mostly resulting from ad-hoc innovation from different initiatives in this space, often without coordination or even collaboration on basic principles and standards. Concerns include ROI on standard edge investments, the scalability and affordability of solutions, especially for SMEs, and interoperability.

Many of the initiatives featured in this report are actually active in researching and developing new solutions that leverage edge computing as a key part of their setup. For these initiatives, the business case is often quite clear, as edge is seen as the enabler of use cases that could not be developed in other ways, thus diminishing doubt regarding ROI for edge solutions. The edge cases analysed did not reach the level of complexity of cloud computing, whereby scalability has become the ability to orchestrate and automate workloads across thousands of devices. In the edge cases researched, due to the use cases involved, scale was not an issue.

Among the challenges the organisations interviewed have are standardisation, interoperability, and vendor lock-in, especially related to IoT and software development for edge platforms.

The main challenges related to edge computing emerging from the interviews are technological and legal:

- Technological aspects: Edge innovation is still in its infancy. Developments in chip manufacturing (silicon), hardware infrastructure, and software platforms are creating new possibilities, but coping with technology advances is challenging. Companies like BrianzAcque rely on partners to manage innovation. Those that, instead, want to drive innovation, such as Vivacity Labs, try to attract talent in universities, which is not an easy task. When innovative solutions are being developed, technical standards can sometimes be an obstacle. Vivacity Labs, Axis, and Worldsensing all view standards as a barrier, especially with regard to IoT connectivity, for which many standards are available. No plans exist for a common industry standard.
- Legal aspects mainly relate to GDPR compliance. Companies found it difficult to adapt to the new legislation. But other regions are now adopting similar policies, which places companies already equipped to comply with GDPR standards at an advantage.

The analysis of good practices has revealed some actions that would be beneficial for the edge environment, the first of which is to invest in building the skills needed to sustain the next wave of innovation. Deep technical skills around firmware and software development, hardware infrastructure optimisation, and AI algorithm elaboration are key. Skills to integrate multiple technologies into complex solutions will also be important. As the telecom sector evolves towards the new standard, which supports edge-to-cloud integration by its nature, it is crucial to bring to market a mature 5G strategy, across multiple countries, connected to the development of the European edge ecosystem. Easing and rationalising regulations and governance concerning cloud in Europe is also recommended. Edge and cloud are part of the same data-flow continuum. Having strict regulations that are not aligned with worldwide standards could slow the adoption of edge-to-cloud solutions and hinder market development.

Green IT

Green IT is the least developed area of the three, with the fewest identified initiatives featuring good practices. In order to drive awareness and accountability in this area, it is important to create a set of KPIs on which projects, initiatives, and private companies need to report. Further research in this area is needed before we can identify relevant challenges and provide good examples of how to successfully overcome those challenges.

Some Observations on Effective Research and Innovation Projects

Numerous research & innovation projects have been funded by the EU with the intention of reducing obstacles in the adoption of cloud computing, edge computing, and other emerging technologies. The projects explored in detail in this report should be regarded as typical. In addition to the structural characteristics described earlier, they share a number of other practices, which should be regarded as positive:

- The active participation of organisations, including public administrations and SMEs, and well-defined use cases, with solutions successfully developed and prototyped by the projects.

- The development of reusable toolkits, methodologies, and ontologies and a strong emphasis on creating open-source components, without excluding commercial solutions.
- The exploration of various exploitation models – from public sector entities participating in projects that become operators of the services to disseminating toolkits so that commercial providers can embed them into their own solutions and creating dedicated legal entities (private or PPPs) to become operators.

Unfortunately, these practices are necessary but insufficient for successful exploitation. Two common scenarios illustrate the challenges:

- Projects tasked participants to become operators of the services, but these usually failed to expand and gain scale. These projects were valuable for the participating entities because they empowered project participants to experiment with leading-edge solutions. Many developed solutions were based on open standards, so technical reusability was guaranteed but business reusability was not. No mechanisms existed to resource important product management, marketing, and sales management and support functions, which are critical for the commercial success of an IT product. As a result, few organisations outside of the projects adopted these solutions.
- Projects deliberately promoted the uptake of reusable standard components among existing IT suppliers that already had the product management, marketing, and sales and support services capabilities needed, and somewhat better adoption was achieved. One example of such a project 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 and achieved good uptake. In particular, its core capability – as a context broker that aggregates and processes data by making it relevant for specific use cases through RESTful APIs – is experiencing good uptake in the Smart Cities space across many European countries, including Spain, France, Italy, and Portugal. One of the key success factors of FIWARE was the creation of a foundation that included the participation of 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.

6. OVERALL CONCLUSIONS AND NEXT STEPS

This deliverable (Green Paper v1.01) summarises a supply and demand analysis conducted by the H-CLOUD project aiming at identifying the status, challenges, and opportunities that Europe is facing with regards to the adoption and provision of cloud computing with a specific focus on federated cloud, edge computing, and green computing. The paper identifies key challenges and opportunities through the perspective of demand in six key sectors: public administration, transport, energy, agriculture, healthcare and manufacturing. In addition to these, the paper focuses on the needs of small- and medium-sized enterprises (SMEs). These six perspectives are referred to as "demand scenarios".

From this analysis, a number of early conclusions were developed to create discussions with, and feedback from, experts, and have been incorporated in this deliverable that include as well the feedback and consultation and publicly discussed in the upcoming H-CLOUD Summit (25-26 November 2020). Following this broad consultation, outcomes will consolidate into a White Paper.

Ultimately, this will help the EC frame their future funding programmes, and the European stakeholders to coordinate key actions to achieve common strategic goals contributing to European competitiveness and ability to innovate in cloud computing.

APPENDIX A: LIST OF BRIEFING PAPERS (AVAILABLE SEPARATELY)

1. Technical Definitions [unchanged from v0.4]
2. Policy Context [unchanged from v0.7]
3. Demand Analysis Approach [unchanged from v0.4]
4. Public Administration Demand Scenario [unchanged from v0.7]
5. Transport Demand Scenario [unchanged from v0.7]
6. Energy Demand Scenario [unchanged from v0.4]
7. Agriculture, Food, Weather and Climate Demand Scenario
8. Healthcare Demand Scenario [unchanged from v0.7]
9. Manufacturing Demand Scenario
10. SME Demand Scenario [renumbered but unchanged from v0.7]
11. Cloud Services Supply Landscape [renumbered but unchanged from v0.7]
12. Edge Computing Development and Supply [renumbered but unchanged from v0.7]
13. Cloud-based Infrastructure and Technology [renumbered but unchanged from v0.7]
14. Green ICT
15. The Potential of Cloud Federation
16. Case Study: GAIA-X Initiative [renumbered but unchanged from v0.4]
17. Research, Innovation and Deployment Projects including European Cloud Computing Portfolio