European
Commission

Establishing a Trusted Cloud Europe

A policy vision document
by the Steering Board
of the European Cloud Partnership

FINAL REPORT

Prepared for the European Commission
DG Communications Networks, Content & Technology

*Digital Agenda
for Europe*

Internal identification

Contract number: 30-CE-0578903/00-87

LEGAL NOTICE

By the Commission of the European Union, Communications Networks, Content & Technology Directorate-General, Software & Services, Cloud Computing Unit

Neither the European Commission nor any person acting on its behalf is responsible for the use which might be made of the information contained in the present publication.

The European Commission is not responsible for the external web sites referred to in the present publication.

The views expressed in this publication are those of the authors and do not necessarily reflect the official European Commission view on the subject.

ISBN 978-92-79-36734-2
doi:10.2759/44445

This report was prepared for the European Commission by

The European Cloud Partnership Steering Board

In accordance with the European Commission’s communication on "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.9.2012, COM(2012) 529 final

Drafted by Hans Graux, Rapporteur/Facilitator to the Steering Board, and adopted by the following Members of the Steering Board:

Organisation	Representative	Organisation	Representative
President of Estonia and Chair of the Steering Board	Toomas Hendrik Ilves	**Accenture**	Pierre Nanterme
Amazon	Werner Vogels	**ATOS**	Thierry Breton
Austria	Reinhard Posch	**The German Federal Office for Information Security (BSI)**	Michael Hange
Dassault	Bernard Charlès	**Ericsson**	Hans Vestberg
EuroCIO and Daimler	Michael Gorriz	**F-Secure Corporation**	Christian Fredrikson
France	Cécile Dubarry	**Memset**	Kate Craig-Wood
The Netherlands	Dion Kotteman	**Norway**	Katarina de Brisis
Poland	Andrzej Ręgowski	**SAP**	Jim Hagemann-Snabe
Software AG	Karl-Heinz Streibich	**Spain**	Aitor Cubo Contreras
Telefonica Digital	Stephen Shurrock		Léo Apotheker

Preface

The European Union, like most of the world, faces economically challenging times. In such times, it becomes all the more important to recognise and seize new and unique opportunities to drive growth, stimulate innovation, and to provide benefits to citizens, businesses and public administrations.

One of these opportunities is cloud computing. Its direct economic value to the European Union is already substantial, but the impact on innovation and social developments is even bigger, as it enables a transformation to a more connected and more efficient on-line society.

The European Cloud Computing Strategy[1] aims to ensure that this potential is captured in Europe. Gaining and maintaining a leadership position in this market requires quick, coordinated and effective action, so that trust in the cloud would increase.

This document represents an important step in the execution of the Cloud Computing Strategy. It is the result of a collaborative process in which participants of public administrations, cloud businesses, and data protection advocates have joined forces through the European Cloud Partnership, and have worked together to establish a roadmap for European leadership in the cloud.

The adoption of this document, however, does not signal a conclusion of our work. A sense of urgency remains: cloud computing is not a technology of the future, it is the technology of today. This document hopes to set the stage for rapid follow-up action. European businesses and administrations need to become cloud leaders in the global market. This is how we can maintain a strong and competitive position in a challenging environment. Ultimately, that is the goal of the European Cloud Partnership and of this document.

Toomas Hendrik Ilves

President of Estonia
Chair of the Steering Board
of the European Cloud Partnership

[1] See the European Commission's communication on "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.9.2012, COM(2012) 529 final; http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

Executive summary

Cloud computing has the potential to bring significant advantages to European citizens, businesses and public administrations, in terms of cost savings, efficiency boosts, user-friendliness, better security, and accelerated innovation. However, access to cloud services in Europe is currently hampered by a number of uncertainties and challenges, which vary from use case to use case. Depending on the type of data, type of service, and need for enforcement, adoption of the cloud may be impeded by legal, technical, operational or economic barriers, as shown through the examples in this document.

The Steering Board of the European Cloud Partnership recognises the need to address these uncertainties and challenges through specific and targeted actions, so that Europe can reap the benefits from the shift to cloud computing. Industry, public administrations and cloud users should work on the basis of common templates for similar use cases, which can be adopted step by step in order to improve the functioning of the digital single market for cloud services, and to avoid needless duplication of effort and market fragmentation.

This paper presents two groups of actions in order to reach this objective:

- Firstly, a flexible common framework of best practices needs to be created, at the legal, technical and operational level. This common framework, consisting of legal and operational guidelines as well as technical standards, can be voluntarily adopted by cloud providers to show that their offering is in compliance with the common framework, and can be used by buyers of cloud services (in the public or private sector) in order to determine more easily whether a cloud service complies with the requirements of their use case.

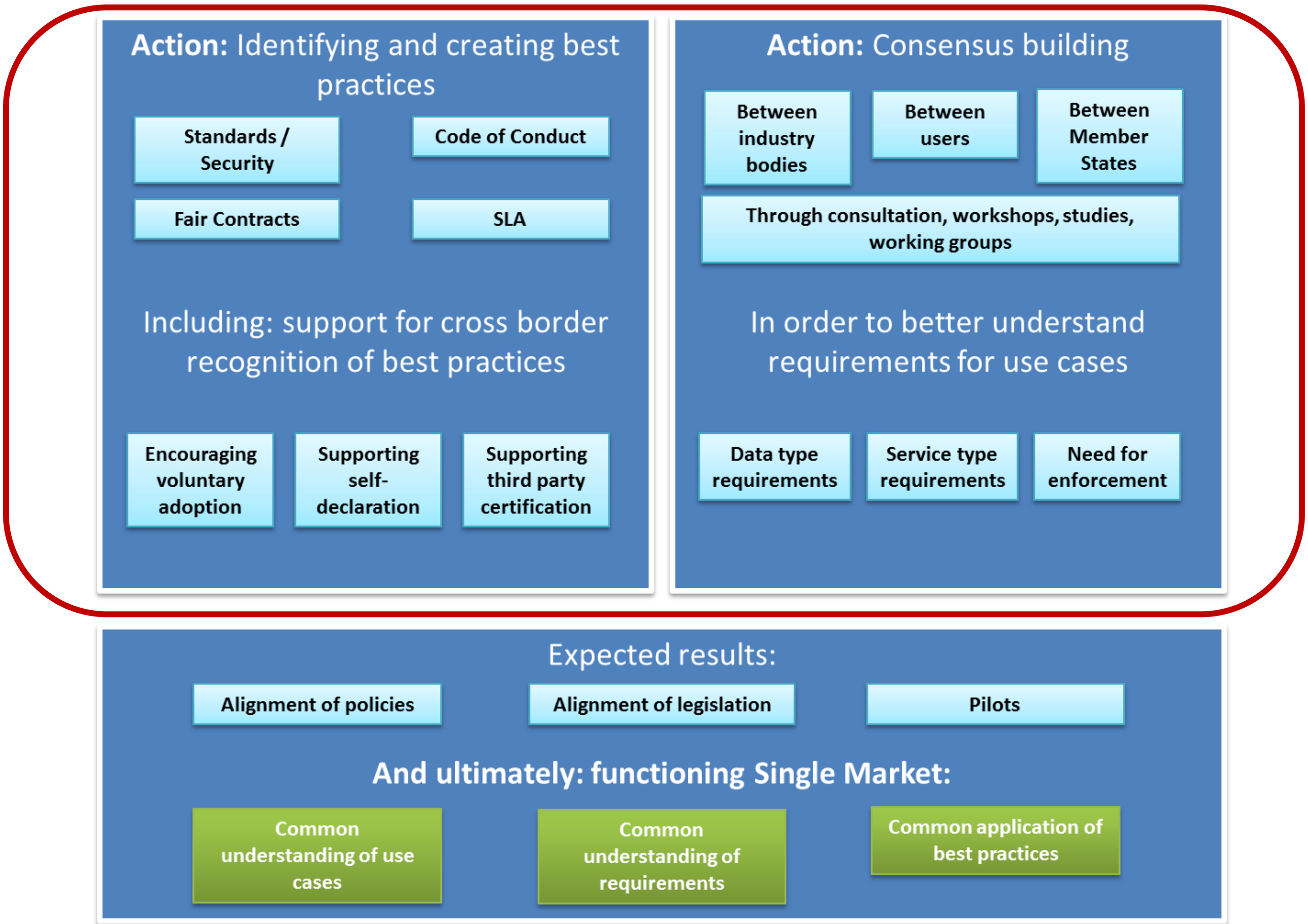
- Secondly, systematic consensus building is required, through public consultations, workshops, coordination groups etc., targeting all stakeholders, including citizens, public administrations, the cloud industry and cloud users. This would result in a common understanding on issues such as risk management, security requirements, privacy needs, enforcement methods, procurement practices, and any need for legislative reform, all of which can differ from use case to use case.

Jointly, these actions will ensure that similar use cases for cloud computing – both in the public and private sector – can be accommodated by a wide range of cloud service providers, offering equivalent and appropriate assurances to their customers. Similarly, this approach will allow cloud providers to provide services offering baseline common and rationally justified expectations, while also facilitating differentiation and innovation.

The challenge is then to achieve a common understanding of these best practices and their role in enabling cloud use cases. The European Cloud Partnership has drafted this paper, containing its own analysis of the current state of play, and its signposts for a strategy that would maximise the benefits offered by cloud computing in Europe. The Steering Board of the ECP expresses its desire to set up a broader consultation around its observations, involving cloud users and cloud providers, in order to seek a broader consensus on the correct actions for the future as set out in this document.

To address this, this paper proposes the concept of the Trusted Cloud Europe: a framework to support the definition of common cloud best practices, linking them to use cases, and applying them in practice.

Trusted Cloud Europe framework



Action: Identifying and creating best practices

Standards / Security

Code of Conduct

Fair Contracts

SLA

Including: support for cross border recognition of best practices

Encouraging voluntary adoption

Supporting self-declaration

Supporting third party certification

Action: Consensus building

Between industry bodies

Between users

Between Member States

Through consultation, workshops, studies, working groups

In order to better understand requirements for use cases

Data type requirements

Service type requirements

Need for enforcement

Expected results:

Alignment of policies

Alignment of legislation

Pilots

And ultimately: functioning Single Market:

Common understanding of use cases

Common understanding of requirements

Common application of best practices

With the support of the Trusted Cloud Europe framework, the European single cloud market can be stimulated, creating new prosperity and a position of digital leadership for citizens, businesses and public administrations.

The potential of the cloud in Europe

Cloud computing is a key enabler for growth, productivity and job creation, capable of generating benefits for citizens, businesses and public administrations. Allowing easy on-demand access to information technology services, cloud computing can significantly reduce capital expenditure, as cloud users only pay for what they actually use. Cloud computing fosters innovative business models and services across all industries, generating new advantages for customers and companies alike. European businesses and public administrations can obtain significant efficiency gains from wide-scale adoption of cloud computing. Small businesses (SMEs) in particular can benefit from the cloud, as they can get access to high-performance IT solutions, which will help them to adapt quickly to new market developments and to innovate and grow their businesses faster.

The expected cumulative economic effects of cloud computing between 2010 and 2015 in the five largest European economies alone is around € 763 Bn.[2] The cloud economy is growing by more than 20%[3] and could generate nearly € 1 trillion in GDP and 4 million jobs by 2020 in Europe[4], with the support of the right policy framework.

Europe is, however, lagging behind other regions in the take-up of cloud computing.[5] Recent revelations about intelligence services surveillance of data have the potential to harm trust in cloud-based solutions. Moreover, due to a lack of regulatory consistency and due to policies which are technologically conservative, cloud computing in Europe remains fragmented, at times making it difficult for European citizens and businesses to reap the full benefits that the cloud undeniably offers.

Without ambitious and decisive actions to counter these trends, the competitiveness of the European economy will be adversely impacted, as the scale and network effects, which are characteristic of cloud computing, will not be widely available to support European growth.

[2] Centre for economics and business research (2010): The cloud dividend report

[3] IDC Worldwide Cloud Black Book, 4Q 2012 update, April 2013

[4] IDC (2012): Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to take up.

[5] Europe trails North America by a factor of 2.4 in the public cloud market. Sources: IDC Worldwide Cloud Black Book, 4Q 2012 update, April 2013; Gartner: Public Cloud Services, worldwide, 2011-2017, 1Q 2013, March 2013.

Therefore, the Steering Board of the European Cloud Partnership has developed this joint statement which proposes a set of coordinated measures by political leaders and industry to enable Europe to rapidly assume a leading role in Cloud Computing. The guiding principle of this statement is the need to support an efficient EU wide single market for cloud services, based on best practices, a common understanding of regulatory requirements and the most effective way of meeting the needs of specific cloud use cases.

Achieving this goal requires actions from a variety of stakeholders, including the elimination of regulatory and market access barriers at both national and EU level, but also the identification and promotion of best practices by industry in respect of applicable laws, technical standardization and operational assurances. In this way, a single market for cloud services will be supported, generating benefits for all European stakeholders:

- On the demand side, European cloud users (citizens, businesses – including SMEs – and public administrations) will be able to choose and use cloud services with confidence, knowing that they adhere to European legal norms and international standards, and that data in such clouds is secure;
- On the supply side, cloud providers will be able provide their cloud services to European customers, without hindrance from national regulatory barriers.

This vision document sets out how this goal can be achieved, by establishing a shared understanding of regulatory and legal norms, and security and trust, common to cloud users and to cloud service providers, and how these can be tied to specific use cases. These solutions should be based on best practices, favouring internationally recognized norms and standards wherever possible to ensure a global perspective that cloud computing inherently requires.

Cloud challenges in Europe and the need for quick action

The European cloud market is currently confronted with a significant number of regulatory and market access barriers that impede both development and commercial exploitation by cloud providers and adoption by cloud users, especially for cross border use cases. Some of these regulatory and market access barriers are linked to legal issues, whereas others are principally tied to trust concerns, technical control, or operational requirements.

In order to understand some of these barriers, the European Cloud Partnership has studied several cross border use cases from both the public and private sector[6], to better understand some of these challenges.

Use case: health care in the cloud

The exchange of health information between hospitals or doctors can be done more cost efficiently and securely through the cloud. However, data protection and privacy concerns impede such projects. User rights (access-edit-delete health data) must be carefully managed across authorized users. End-to-end encryption and anonymisation can provide workarounds, but also severely restrict use cases.

Privileged information can be protected by legal frameworks that stop cloud adoption or limit use cases. Significant benefits could be realised through trusted cloud solutions.

Use case: personal data in cross border clouds

Storing personal data in public clouds is problematic when data is legally considered as sensitive. In such cases, clouds usage is difficult due to varying national legal requirements (e.g. supervision of the infrastructure by health care practitioners for health data). Similarly, national laws can differ on information security requirements, such as the need to have a data protection officer or to audit all data centres, which are legal requirements in some Member States, but not in others.

The lack of full EU harmonisation of data protection rules is a recurring legal barrier.

[6] See the more detailed information in sections 1 and 2 of the working document prepared by the working groups of the ECP. Note that the inputs in this working document represent the positions of individual contributing members of the working groups, and do not indicate any consensus from the ECP as a whole.

Use case: financial services in the cloud

Banks and financial institutions process vast amounts of personal data in the operation of their business. Their activities are subject to national supervisory bodies, which can define rules and requirements for the IT systems that process this data. In some Member States (such as Luxembourg), these guidelines require infrastructure to be established within national borders to facilitate direct inspection by the supervisory bodies.

Even outside of formal laws, norms may exist (issued by supervisors, regulators, sector organisations etc.) which stop or discourage the use of cloud services outside national borders.

Use case: IP-intensive sectors and cloud services

Entrusting information protected by intellectual property (IP) rights can be challenging, due to the legal and business need to control data. In the media business, cloud based media dissemination may conflict with legacy rules that focus on obtaining national/regional licenses or authorisations. Other IP intensive industries (such as e.g. the automotive industry or the chemical/pharmaceutical sectors) prefer private clouds over public clouds in order to keep full control over their infrastructure.

Cloud adoption barriers can vary from sector to sector. Legacy legal frameworks that are not adapted to the global market can cause legal challenges, and operational/business concerns may lead to a strong preference for private clouds.

Use case: science data in the cloud

The scientific community has a clear need for powerful, high capacity and dependable infrastructure that can be used to advance their research without exposing it to data loss, corruption or intrusion. Secure scientific clouds can meet these requirement, and several projects within the EU have been set up to satisfy this demand, including the Helix Nebula project and through GEANT. However, further work is needed to integrate existing science clouds, to promote their adoption, and to enhance their usability.

Secure clouds for science applications offer clear benefits in terms of benefits of scale, integrity and confidentiality. Further EU work is urgently needed to achieve this goal.

Use case: national archives

Archiving laws in Spain require any documents generated and stored by the public sector to be retained, and prohibits moving them from their original archives without a prior Ministerial Order. This can be interpreted as a restriction on moving data to a location outside the country (including cloud services with international data centres) without such an order.

In many cases, there is ambiguity in the law on what is legally possible. In such cases, uncertainty often leads to negative decisions on new technologies, even if there is no overriding justification for this.

While based on a limited set of use cases, the examples above illustrate that barriers vary from use case to use case, and include legal issues, operational concerns, and technological challenges. A recurring concern is the perceived vulnerability of data in the cloud to seizure by authorized public authorities, and more broadly to questions of general jurisdiction and applicable law. Current EU legislation generally favours policies where service providers are subject to the laws of their country of establishment[7]. While this rule is sound in principle, it raises the challenge of making cloud users' data subject to foreign law, and typically also foreign jurisdiction. This may not be palatable or viable for certain cloud users, including in the public sector.

The requirements of each cloud use case differ, and are jointly defined by their **data type** (e.g. health data being particularly sensitive), by **data usage** (e.g. IP protected data requiring licenses for each use) and by the need for **enforcement** (e.g. financial data requiring very strict controls). Cloud services that are able to satisfy all three categories of requirements for a use case can be considered fit for purpose. This requires appropriate risk management practices, in which the risks inherent to each use case are correctly understood, and in which the resulting requirements can be rationally identified.

The challenge is then to achieve a common understanding of these requirements and their role in enabling cloud use cases**. To address this issue, this paper proposes the concept of the Trusted Cloud Europe: a framework for defining best practice and cloud requirements, linking them to use cases, and applying them in practice.**

[7] This is e.g. also enshrined in the European eCommerce Directive's country of origin rule, albeit with exceptions in relation to data protection and consumer protection.

As shown above, the requirements and related barriers differ strongly from use case to use case:

Requirement Sector / use case	Data protection	Intellectual property rights	Confidential information	Outdated legacy laws	Information security concerns	Supervision and inspection	National sovereignty	National security	Jurisdiction / enforceability	Procurement rules
Public sector in general	√		√	√	√	√	√	√	√	√
Taxation and social security	√		√		√	√	√	√	√	
Health care and legal services	√		√		√	√		√	√	
Media and entertainment	√	√	√	√	√	√			√	
Financial services	√		√	√	√	√		√	√	
National archiving	√						√		√	
Manufacturing/consumer		√			√					

- Summary of known requirements across various sectors, '√' indicates a known priority issue -

Based on this limited exercise, the table above would suggest that the most ubiquitous requirements (spanning the most sectors) are data protection compliance, information security, and jurisdiction/enforcement. When applicable requirements cannot be met in cross border public clouds, there is a strong tendency to use only private clouds, or at least only cloud solutions within national borders. As a solution for some use cases, this may be acceptable. For the EU cloud market as a whole however, this is a problem that needs to be resolved.

While more systematic fact finding is desirable to obtain a comprehensive overview of requirements across sectors, these initial inputs show that a set of measures are needed to overcome the current fragmentation in European cloud markets, addressing requirements in relation to data types, data usage and enforcement, through the Trusted Cloud Europe framework.

Supporting the digital single market through Trusted Cloud Europe

The sections above have described some of the challenges currently experienced in the European cloud market by stakeholders, including citizens, businesses and public administrations. The global goal is to achieve a European single market for cloud computing.

This can be achieved by building a set of best practices and common understanding of the requirements that should to be met for each specific use case. This is beneficial to both cloud providers and cloud users: cloud providers can more easily ensure that their cloud services meet the requirements of specific use cases, and cloud users can more easily choose cloud services that are suited for their use case. The Trusted Cloud Europe is a framework for establishing these best practices, linking them to use cases, and applying them in practice.

The TCE framework is a non-legislative and voluntary initiative: it relies on voluntary adherence and participation from cloud providers and cloud users that see a benefit in participating in it, in order to support the development and uptake of the cloud and unlocking the accompanying benefits.

In this section, we will explore how a single market for cloud services can be formed. This requires two groups of action:

- Firstly, a flexible common framework of best practices needs to be created, at the legal, technical and operational level. This common framework, consisting of legal and operational guidelines as well as technical standards, can be voluntarily used by cloud providers to show that their offering is in accordance with the state of the art, and can be used by buyers of cloud services (in the public or private sector) in order to determine more easily whether a cloud service meets the needs of their use case.

- Secondly, systematic consensus building is required, through public consultations, workshops, coordination groups etc., targeting all stakeholders, including citizens, public administrations, the cloud industry and cloud users. This would result in a common understanding on issues such as risk management, security requirements, privacy needs, enforcement methods, procurement practices, and any need for legislative reform, all of which can differ from use case to use case.

The framework formed by these two pillars together – building best practices and building consensus on their use in practice – collectively make up the Trusted Cloud Europe.

Action 1: Building best practices and promoting their cross border mutual recognition

When addressing questions of adherence to legal norms, data control, security certification and accountability, it is important to recognise the impact of existing achievements and ongoing work. These offer some of the quickest solutions, and have often already been implemented and tried and tested through existing cloud services. Others still require some finalisation, or are not well-known or correctly understood by aspiring cloud customers.

The following **actions** can be recommended to address this goal:

1. **Identify best practices, in terms of technical, legal and operational assurances commonly offered by leading cloud service providers and measures generally available to cloud customers, and promote these more systematically.** In many cases depending on the type of cloud computing, existing inputs are suitable, including security certification against existing and often global standards[8], data protection compliance against the EU Standard Contractual Clauses[9], or existing outsourcing techniques based on Hierarchical Storage Management (HSM), Information Lifecycle Management (ILM), automatic replication facilities, and media migration and validation practices. Best practices may also relate to appropriate technological security and access control solutions, including - where proportionate - strong encryption technologies, systematic logging, time stamping, and automated breach detection measures. The key ambition is to establish a coherent toolbox of best practices, thus empowering cloud users to choose the practices which are most appropriate to their use case.

[8] See https://resilience.enisa.europa.eu/cloud-computing-certification and http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

[9] See http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

2. **Establishing new best practices and guidelines** to steer the market towards customer friendly practices. Key ongoing actions include the **standardization of SLAs, the Safe and Fair Cloud Contract initiative, the drafting of a data protection Code of Conduct**[10], which should be endorsed by the Article 29 Working Party in order to ensure its legal authority, and **the development of a Meta-framework of security certification schemes** that can be used to compare and assess cloud computing security certification offerings. [11] Such best practices and similar security/privacy cloud-specific international standards should form a basis for adherence with EU security and privacy legal norms.
3. **Facilitating the cross-border recognition of these best practices**. Adherence to these best practices should be verifiable and auditable without extensive case-by-case checks, since ad-hoc checks are not always financially or operationally viable, especially for citizens or SMEs that lack the know-how and economic resources to conduct such checks. Therefore, the use of **self-declaration, third party audits and one-stop-shop certification/trust marking schemes should be supported where appropriate as a tool to make adherence against the aforementioned best practices, accessible to as broad a market as possible.** Any endorsed certification/trust marking practices should be industry driven and customer centric, voluntary, lean and affordable, technology neutral and based on global standards wherever possible, in order to avoid needlessly increasing costs, especially for SMEs.

It is clear that the economic potential of European cloud services depends on the ability to avoid any semblance of a 'Fortress Europe' model where access to the European cloud market is *de facto* restricted to providers established in the EU. Non-European cloud providers should be able to access the European cloud market on equal terms, and offer services that adhere to the best practices proposed as a part of the Trust Cloud Europe framework, i.e. functional requirements in relation to data type, data usage and enforceability of European laws and fundamental principles.

The Steering Board of the European Cloud Partnership **encourage Member States, cloud users and the cloud industry** to **contribute to the identification and completion of best practices**, and to **support their use wherever appropriate**. All stakeholders should seek to **educate users on the meaning and impact of these best practices, and their suitability for particular use cases.**

[10] See https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct for an overview of the Code of Conduct activities.

[11] See https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy and https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes

The Steering Board furthermore encourages the EU, Member States and cloud industry to seek out opportunities to **support adherence to best practices** (including both self-declarations of compliance and third party certification), and to **promote the use and value of appropriate certification schemes.** A flexible and innovation friendly approach will be crucial during these efforts, as the risk of elevating existing practices to the status of obligations – thus creating future legacy problems and disrupting the potential for new innovations – must be avoided.

The definition of best practices and the facilitation of compliance assessment are two key pillars of the Trusted Cloud Europe framework, allowing the TCE to become a recognizable brand and a mark of quality for cloud vendors, thus creating an additional selling proposition on the global market for cloud services.

Action 2 – Building consensus on the needs of specific use cases and on appropriate solutions.

As shown in the examples above, several challenges still exist that disrupt the cross border offering of cloud services across the internal market. A one-size-fits-all solution to cloud computing does not seem credible or viable, as the needs for specific data or service types may vary quite widely. Personal data may require a higher level of protection than other types of data, and within the broad spectrum of personal data certain categories of information (e.g. health information or financial data) may be more sensitive. Rational risk management practices will therefore be key to ensuring that the needs of individual use cases can be correctly understood and addressed. This is of particular importance for public sector cloud users, who have clear needs that are directly connected to their public interest function.

This can be challenging for cloud providers who may be confronted by different requirements from Member State to Member State, but also for cloud users who may see their cloud ambitions blocked by obstacles that may not be justified. In order to reduce geographic fragmentation, it would be beneficial to build a consensus on how the needs of specific use cases can be satisfied by particular best practices. This can be done through public consultations, workshops, setting up coordination groups etc., targeting all stakeholders. Specifically:

- Consultations and workshops need to target **non-legislative regulators, supervisory bodies, professional bodies and trade associations.** This stakeholder group is just as influential as formal legislators in allowing or disallowing cloud services. These bodies should be encouraged to ensure that their guidelines and policies are at least cloud neutral (i.e. enable cloud services) wherever this is compatible with their goals. Furthermore, national and sector-specific bodies should create coordination groups to align their rules and exchange best practices. In this way, geographic fragmentation could be avoided. They should be encouraged to educate their members on permissible and proper cloud adoption.

- Consultations and workshops similarly need to target **cloud users, including citizens, SMEs and larger businesses**, either directly or via representative bodies such as consumer protection organisation, data protection/privacy protection associations, or NGOs, since their data may be entrusted to the cloud. **Education and awareness raising** will be key to ensure that cloud users are able to ask the right questions – where are my data hosted, how are they secured, what are my rights and how can I exercise them – which can only be meaningfully raised and understood with sufficient understanding of the cloud computing paradigm. In addition, these consultations should examine **how enforcement can be made more accessible**. Given that particularly citizens and SMEs have limited resources for engaging in legal proceedings, enforceability depends on the establishment of a credible and accessible dispute resolution mechanism. This does not imply that the most stringent enforcement is necessary for any cloud service, irrespective of its scope or intended use, but rather that cloud users must have access credible and understandable options for recourse in case of incidents.

- Finally, consultations and workshops need to target **Member States,** in order to **determine which barriers (if any) they encounter in adopting cloud computing,** and in order **to share best practices** where available. **Alignment, reform and harmonization of legal frameworks and policies may be appropriate in some cases where legislation creates unnecessary barriers to the internal market.** Several ongoing actions already support this goal. The **ongoing harmonization of EU Data Protection Rules** is a key example: national legal divergences are a challenge for vendors, which smaller providers sometimes struggle to manage. Inversely, cloud users (including public administrations and business users) hesitate to entrust their data to clouds, for fear of compliance issues and liability. The Steering Board welcomes the harmonization efforts, and stresses the importance of a common interpretation of data protection rules in Europe, as foreseen within the ongoing negotiations on a EU Data Protection Regulation, as an essential condition for a single market for cloud computing.

Collectively, these consultations and workshops should help citizens, businesses and Member States to build a consensus on their challenges, as dictated by their individual interests and backgrounds, and to seek common solutions, building on best practices in the cloud market. An example of the latter are **cloud-active procurement policies** which have been adopted by some Member States. While details vary from country to country, such policies generally require administrations to at least consider cloud technologies (including both public and private clouds) for their IT procurements, and to ensure that their requirements do not needlessly exclude cloud technologies[12]. The objective of such policies is to change the mindset of procurers, to stimulate cloud adoption, and to ensure that the benefits of the cloud can be maximized by re-using successful services whenever possible.

Such policies and practices allow laws, policies, and all related requirements to converge step by step around the needs of specific use cases, thus facilitating access to the internal cloud market for cloud providers which adhere to these requirements.

This gradual approach appears most viable to address concerns that are felt in particular by the public sector. Most Member States are presently exploring their options for the use of cloud technology (e.g. by deploying virtualization techniques and application stores within their own private IT infrastructures), preparing for the moment that public cloud services can be verified to be reliable and secure, and that privacy protection can be guaranteed. Member States will be empowered in making the choice between replacing or amending their own internal infrastructure by rented infrastructure from an external cloud provider.

Examples of expected convergences and alignment opportunities include notably the following:

- **Alignment of procurement rules and practices:** Procurement rules in some Member States can make it difficult to sell cloud solutions to the public sector. This is burdensome to public administrations, which can be barred from technologically and economically advantageous solutions, but also for cloud providers, who are faced with different requirements from country to country. By sharing best practices, Member States can **ensure that their procurement legislation and policies will become cloud enabled**. Furthermore, they could **work towards developing common approaches to public procurement of cloud computing, or towards the mutual recognition of any existing national accreditation schemes,** so that providers do not need to seek different certifications, accreditations or approvals in different Member States. Similarly, Member States can **share effective national budgeting policies to ensure that pay-as-you go models** (moving from capex to opex) can be enabled.

- **Reduction of data location restrictions:** Member State practices and in some instances national laws restrict the possibility of storage and processing of certain data (especially public sector data) outside their territory. If common requirements can be found for similar use cases, **Member States can choose to gradually phase out data location restrictions when they are deemed unnecessary.** This does not imply that data controls should be abandoned; it is often possible and advisable to **replace formal legal requirements** (such as geographic location of the data) **by the corresponding functional requirements** (such as ensuring the accessibility and security of the data). State-of-the art security technologies could be regarded for some use cases as an alternative to data location restrictions. This goal oriented approach

[12] In some cases, Member States have opted for 'cloud first' policies, which sometimes include stronger support for cloud technologies, e.g. by requiring procurers to prioritize cloud computing purchases where possible, or to justify any decision not to use cloud computing when a suitable cloud solution was available.

is technologically neutral, conducive to supporting innovation and new technologies, and enables public policy objectives to be more effectively reached.

- **Establishment of common templates to address jurisdiction and enforcement** concerns. Some of these concerns (notably on surveillance by national security bodies) can only be addressed in the longer term and exceed the remit of the European Cloud Partnership. However, practical solutions may develop as a result of consultations with Member States, the cloud industry and cloud users, which are able to address some of these concerns. For instance, Member States could voluntarily **establish and accede to multilateral cooperation agreements, to clarify under which conditions they (or their authorized public sector bodies) will access data hosted by cloud providers established in their country**. Such opt-in agreements may also include rules with respect to cooperation obligations by cloud providers, or on the enforcement of foreign legal decisions. Such agreements would be aligned with applicable EU and national laws and jurisprudence, notably EU data protection law and especially the envisaged cooperation between national data protection authorities under the new EU Data Protection Regulation.

- **Setting up public sector pilot cloud services at EU level:** the public sector faces specific challenges and needs which are linked to their public policy objectives. This also implies that cloud solutions need to be tailored towards these unique needs. As a natural step in the alignment process, Member States could **pilot public sector cloud applications with EU assistance, with a view to creating common building blocks and ensuring that fragmented national approaches and duplication of efforts are avoided**. Within the ECP, representatives of the Member States were polled on suggestions for pilot cases, with the following policy areas suggested as being particularly conducive to cloud pilots[13]:

  - **Public sector document management and communication.** This would e.g. include national archives, library management, e-mail/e-delivery of documents towards the public sector, or public sector information (PSI) portals. Such use cases focus on the public sector need for confidentiality, trustworthy storage, and redundant capacity that would benefit from a distributed (cloud based) solution.

  - **Scientific research and data analysis,** in the form of a science cloud which could support the European research community through significant virtualized storage and processing power, supporting ‘big data’ analysis, data mining, advanced analytics and science grids in a secure and trustworthy manner.

[13] For more details, see the working document, section 3.

Inputs for such pilots are already available, including via projects such as Helix Nebula and GÉANT (science clouds), Hermes Preservation Services (digital archiving), CloudForEurope (cloud computing for the public sector in general), the technical solutions created by various large scale pilots (such as STORK, PEPPOL, SPOCS and epSOS[14]), the secure communications network S-TESTA, and a legal framework that would underpin the sustainability of some of the required services (electronic identification, signing, time stamping, delivery, etc.) through the proposal for a Regulation on Electronic Identification and Trust Services[15]. The main goal would therefore be to bring the existing building blocks together, to identify and address any remaining gaps, and to bring them to an operational stage.

The primary challenge for these pilots is funding, with many Member States noting that new pilots are unlikely to be viable without EU level funding. Funding may be found under a future grant agreement as part of Pre-Commercial Procurement (PCP) or Public Procurement of Innovation (PPI), e.g. as part of Specific Challenges from Horizon 2020 work programme[16]. The execution of these pilots would also support and expand research and development efforts around cloud computing in Europe, contributing to the development of a strong and innovative European cloud industry offering.

The Steering Board of the European Cloud Partnership **requests the Commission to assist in setting up and executing the aforementioned consultations with cloud users, the cloud industry and public administrations,** in order to build a consensus on the proper application of best practices to meet the needs of specific use cases.

The EU, Member States and industry bodies should be **encouraged to seek cross border alignment of their rules, policies and practices**, in order to ensure that the internal market for cloud services operates effectively.

[14] See http://ec.europa.eu/digital-agenda/en/egovernment for details on these large scale pilots

[15] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF for the proposed Regulation.

[16] The aforementioned CloudForEurope initiative has been funded following a successful response to a Call for Proposals under the FP7 work programme.

Concluding remarks

As this paper has shown, there is a need for action to support the development and adoption of cloud computing in Europe. A single digital market, free of needless barriers or restrictions should be the ultimate objective, in which all cloud users have access to high quality, secure and trustworthy cloud services. This goal can be achieved by relying on the identification and consistent application and promotion of best practices, and by building a consensus between citizens, businesses and administrations on how these should be applied, consistent with legal norms and policies.

Collectively, these actions should ensure that the potential benefits of cloud services can be unlocked to as wide an audience as possible, without unique dependence on potentially lengthy legislative reform. Voluntary certification by third parties or self-declaration against identified best practices could act as a mark of quality for cloud vendors, and thus create an additional selling proposition on the global market. This will also make it easier for aspiring cloud users to choose a high quality partner that adheres to European best practices and expectations.

The European Cloud Partnership calls upon policy makers at the European and national level, and upon cloud providers and cloud users, to support this approach and to implement the proposed actions towards establishing the Trusted Cloud Europe framework, and thus enabling a single digital market for cloud services in Europe.

Furthermore, the Steering Board of the ECP is conscious of the importance of establishing a broad consensus on the appropriate road forward. Therefore, **the Board expresses its desire to set up a broader consultation around its observations, involving cloud users and cloud providers, in order to identify the right actions for the future**.

The building of a single market for cloud computing is an urgent objective. Cloud computing is not a technology of the future, it's the technology of today. The actions aim to ensure that results can be provided that cloud vendors and cloud users can adopt right away, and that will help grow the market and drive new innovations. This requires voluntarism, and the genuine desire from Member States and cloud businesses to drive progress through all of the actions described above.

The European Cloud Partnership thus recognizes that timing is of the essence, and emphasizes that the proposed actions must be initiated as soon as practicable. Provisionally, the following time table can be presented:

Action	Owner	Deadline
Finalisation of a model **Code of Conduct**, and obtaining its endorsement by the Article 29 Working Party	Industry and users	Ongoing. Finalisation by end 2014
Finalisation of **SLA guidelines and the Safe and Fair Cloud Contract initiative guidance** at the EU level (including issues of reversibility/interoperability)	Industry and users	Ongoing. Finalisation by end 2014
Finalisation of **ongoing data protection harmonization efforts in Europe, as foreseen within the ongoing negotiations on a EU Data Protection Regulation**	EU, MS, Industry and cloud users	Ongoing. Finalisation in 2014-2015
Organising consultations with cloud users (citizens, business and public administrations) to ensure acceptance of the Code, SLA guidelines and Cloud Contract initiatives	EU, MS, Industry and cloud users	Finalisation by end 2014
Implementing and supporting certification mechanisms (in the broad sense, i.e. including self-declaration, third party audits and one-stop-shop certification/trust marking schemes) against best practices, including in relation to security, Code of Conduct about Security and against the CoC and SLA / Fair Contract	EU, MS and Industry	Finalisation by mid-2015
Uptake of the CoC, SLA/Fair Contract and security certification by Industry (if finalised successfully)	Industry	Finalisation by mid-2015
Consensus building through public consultations, workshops, setting up coordination groups etc., **targeting professional bodies and trade associations at the EU level** to ensure that their (non-legislative) guidelines and policies are cloud neutral	EU and Industry	Initiation by early 2015
Consensus building through public consultations, workshops, setting up coordination groups etc., **targeting cloud users (citizens, businesses and public administrations)** to ensure that they are transparently informed and to find **effective enforcement mechanisms.**	EU, MS, Industry and users	Initiation by early 2015
Consensus building through public consultations, workshops, setting up coordination groups etc., **targeting Member States** to identify any explicit and implicit legal roadblocks to cloud computing in key cloud use cases.	EU, MS, Industry and users	Initiation by early 2015

Study on data categorisation from the perspective of MS, in order to identify required assurances from a legal and technological perspective (including enforcement)	EU, MS and users	Initiation by early 2015
Selection and initiation of selected cloud pilots	EU, MS and Industry	Initiation by end of 2015

Ultimately, all of Europe needs to form a single market for cloud computing based on best practices and a common understanding of these best practices and their role in enabling cloud computing, in order to become a leader in trustworthy cloud provision and cloud adoption in the global market. This is the only way to maintain a strong and competitive economy in a challenging environment.

European Commission

**Establishing a Trusted Cloud Europe –
A policy vision document by the Steering Board of the European Cloud Partnership**

Luxembourg, Publications Office of the European Union

2014 – A4 – 28 pages

ISBN 978-92-79-36734-2
doi:10.2759/44445

KK-01-14-281-EN-N

For further information

European Commission
Directorate-General for Communications Networks, Content & Technology

Directorate Net Futures
Software & Services, Cloud

B-1049 Brussels

cnect-e2@ec.europa.eu