OpenForum Europe's response to the Trusted Cloud Europe Survey

OpenForum Europe welcomes the opportunity given by the European Commission to comment on the 'Trusted Cloud Europe' document recently put out by the European Cloud Partnership. We have already publicly expressed our overall support for this initiative which we believe to be a step in the right direction towards achieving a safe and trusted environment for public and private organisations to use, buy and sell cloud computing services. We regret however that the online questionnaire has been drafted in such a way that risks over-simplifying some complex issues. Hence when we felt that no clear-cut answer could be given we have chosen to give our own opinion, with comments.

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

OFE OPINION

A large part of the economic benefits of cloud computing comes from economies of scale gained from the ability for Cloud Service Providers (CSP) to offer public cloud offerings across multiple territories. While diverging national data protection rules might not be as much of a problem for the provision of private clouds (usually under a single legal regime), they can represent a significant legal barrier for public cloud offerings. This fragmentation can also lead to small, national-based CSP being deterred from offering their services in other countries. However, we urge the Commission and Member States to closely involve all stakeholders and including in particular CSP and cloud users in the ongoing data protection harmonisation efforts in Europe. There are concerns the proposed Regulation could cause uncertainties for different categories of CSPs.

2. "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."

OFE OPINION

Whilst both parts of the statement is undeniably true we remain guarded about the establishment of a (new) mechanism, and would question both the thinking on the form of that mechanism and whether existing approaches can be aligned to the requirements. Typically mechanisms can themselves impose market costs which disadvantage SMEs.

3. "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."

AGREE

The document suggests to "replace formal legal requirements (such as geographic location of the data) by the corresponding functional requirements". This is a sound recommendation but as this passage rightly points out there is a need to look beyond just formal legal requirements, at other

factors which are inhibiting the take-up of cloud.

4. "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."

AGREE

Cloud services are by definition a global market where providers compete on an inherently equal basis, providing services built on global, open standards and an open approach to the underlying infrastructure – i.e. the business model underpinning the internet itself.
A model favouring a limited number of state-funded 'national champions' insulated from competition might be appropriate for sectors characterised by high barriers to entry and an oligopolistic structure, such as telecommunications or aerospace.
This is not the case of the cloud computing market. The only way that cloud users will reap the full benefits of low-cost, flexible cloud services is in a single, global marketplace where providers compete on equal and fair terms. This is equally true for European based suppliers accessing non-European markets and services, as for those providers established outside the EU. The focus should be on supporting the individual needs of European based users and supporting the innovative potential for users and suppliers across Europe. The concept of mandatory Schengen type data areas is naïve and unrealistic and whilst may be well intentioned will be highly damaging to European service providers.

5. "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 Trusted Cloud Europe framework, i.e. functional requirements in relation to data type, data usage and enforceability of European laws and fundamental principles."

AGREE

See answer to question 4. There is no business need to differentiate on geographic establishment, but instead focus on functional competitiveness based on best practice.

6. "Privileged information can be protected by legal frameworks that stop cloud adoption or limit use cases."

NO OPINION

It is unclear on the scope of definition of 'privileged' in this context.

7. Providers and consumers of cloud services need "technological security and access control solutions, including - where proportionate - strong encryption technologies, systematic logging, time stamping, and automated breach detection measures".

AGREE

Just like any other aspect of IT solution such measures may well be necessary to respond to specific consumer needs and create the necessary confidence to use cloud services. Here again it is important that these needs are expressed in user based functional requirements appropriate to use, rather than prescriptive requirements. Best practices, appropriate for new use within Cloud can continue to be encouraged and identified for specific use scenarios in order to facilitate understanding.

8. If Trusted Cloud Europe were to "become a recognizable brand and a mark of quality for cloud vendors", this would create "an additional selling proposition on the global market for cloud services."

DISAGREE

In general, we believe that public authorities should refrain from creating "recognisable brands" to drive adoption of any technology – be it cloud or any other. This is a complex task requiring not only a thorough technical and business expertise, but also frequent updating. As such, this role is generally best filled by market players working within structured organisations, in the same way as fora and consortia operate for Standards. We would also question whether any regional brand would prove effective in a global scenario.

9. "Ad-hoc checks [for legal norms, data control, security certification and accountability] are not always financially or operationally viable, especially for citizens or SMEs that lack the know-how and economic resources to conduct such checks."

AGREE

This comment rightly highlights the need to facilitate access to the recognition of certification / trust marking schemes, for instance through self-declaration. As in our response to question 2 there needs to be substantial recognition that for SMEs such schemes can become a blocker to competition imposing unnecessary costs and overheads. Key must therefore be assessment of user appropriateness, applicability, and access.

10. As cloud computing could create significant cost savings, Chief Information Officers of every Member State's administration should aim "to change the mind-set 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" through adopting cloud-active procurement policies.

AGREE

The single greatest influence a Public Administration can have on the growth and dynamics of an emerging market is through its public procurement processes. This is true for the European Institutions as much as national and local administrations. Regrettably past practice has instead led

to lock-in to closed services, minimising future potential for innovation and sharing. Public administrations have a key role in driving adoption through their internal use of cloud services. One possible way to reinforce this principle would be to put in place a mechanism whereby technical specifications of public contracts needlessly excluding (open) cloud solutions could be reported by market players.