Trusted Cloud Europe

Response by the Cloud Legal Project
http://cloudlegalproject.org
(Centre for Commercial Law Studies
Queen Mary University of London)

1. Questionnaire

1. "The lack of full EU harmonisation of data protection rules is a recurring legal barrier."
DISAGREE
Lack of full EU harmonisation of data protection rules is indeed a recurring legal barrier to use of cloud computing, but it is not the only legal barrier – these rules also need to strike a better balance between data protection and the use of cloud computing generally. Much uncertainty has been caused by national data protection authorities' and courts' inconsistent interpretations of basic concepts such as 'establishment' and 'personal data'. The greater barrier is the lack of international harmonisation of data protection rules, rather than intra-EU differences, which is more an additional cost than barrier per se. The impact on controllers and processors also differs. Please see Millard (ed), Cloud Computing Law (OUP 2013), Chapters 7 to 10.

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."
AGREE
Credible and accessible dispute resolution mechanisms will be necessary, but not sufficient. The devil is in the detail. Who will run such mechanisms, eg data protection authorities? How will they be funded? Allowing consumer groups and the like to take quasi 'class actions' may also assist. It will also be important to ensure clear harmonisation, eg of minimum thresholds for enabling citizens to enforce data protection law breaches (financial harm vs 'moral' harm).

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
Government policy may require data to be stored only in in-country data centres for national security or other reasons, eg the UK government offshoring guidance (national security) https://www.gov.uk/government/publications/government-ict-offshoring-international-sourcing-guidance. Cloud is still relatively new and societal fear, uncertainty and doubt regarding the unknown, particularly where it involves technology, will need to be addressed through awareness raising, education and the promulgation of trustmarks etc as mentioned below.

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."
DISAGREE
European economic potential depends partly on that ability, because in order for European cloud users to reap the full benefits of cloud services it is important that they are not restricted to European providers but are free to choose the cloud services that are the most efficient and effective for their business models, business and legal needs and their financial positions. However, other factors may also be relevant. Measures designed to protect the security/privacy of EU citizens should not be lowered or sacrificed simply to avoid being perceived as 'Fortress Europe'. Controlling data flows does not equate to Balkanisation (often used as a synonym for Fortress Europe).

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

6. "Privileged information can be protected by legal frameworks that stop cloud adoption or limit use cases."
AGREE
Sector, and content-specific, regulations may be barriers to the adoption or use of cloud. This is, however, a complex area involving multiple legal and regulatory regimes that apply to diverse sectors and use cases in various different ways. While analysis, and possibly reform, of many such restrictions may be appropriate, that would be a long-term project. In the meantime, promoting greater awareness regarding technical measures available to protect particular types of content in cloud environments would be helpful.

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
Technical solutions will often be appropriate, but as mentioned the detailed measures should be proportionate to the risks involved. Best practices regarding data deletion or 'restriction' or blocking should also be identified. The human factor must not be ignored, as it is the cause of many security breaches, and here awareness raising, education and training will be key, eg logs are no use if they are not checked, or breach detection measures if they are not acted upon.

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."
NO OPINION
The difficulty will lie in exactly *how* to make TCE a recognisable brand and mark of quality.

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
However, some ability to conduct ad hoc checks, subject to reasonable restrictions on who can conduct them (regulators, certificators, independent third party experts, etc), frequency, and so on may be important for trust, accountability and transparency.

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
Cloud computing can not only create significant cost savings but is being used to meet specific business needs eg http://searchcio.techtarget.com/news/2240212159/Survey-For-cloud-computing-use-business-needs-trump-cost-savings-as-top-driver and to provide competitive advantages http://www-03.ibm.com/press/us/en/pressrelease/42304.wss.

2. Discussion group

2.1 Building Consensus

"Consultations and workshops need to target non-legislative regulators, supervisory bodies, professional bodies and trade associations… cloud users, including citizens, SMEs and larger businesses… Member States."
AGREE

2.2 Adherence to Best Practices

"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."
AGREE
The identification, or development, and promotion of suitable best practices and appropriate certification schemes will be the biggest challenge, especially as they may change quickly.

2.3 Small and Medium-sized Enterprises (as users and suppliers)

“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."
AGREE

2.4 Data Location Restrictions

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

2.5 Cloud-Active Procurement Policy

"…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. The objective of such policies is 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."
AGREE
Cloud-active procurement policies may be beneficial if clear practical guidance is provided, they are subject to suitable safeguards, and they are flexible enough to adapt to the fast-changing cloud market.

2.6 Procurement Practices

"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."

What do you think? Is this the right approach for IT/cloud procurement? Are these the right actions for procurement? Are there missing actions? What is the most important action on this topic? Who are the most important stakeholders as regards procurement?

AGREE

Best practices should be shared as much as possible among Member States, while considering procurement legislation and policies and working towards common approaches or mutual recognition. These practices and national schemes and accreditations (see Millard (ed), Cloud Computing Law (OUP 2013), chapter 5), and information regarding public sector use of cloud, should also be made public to benefit and encourage private sector cloud users. Anecdotally, payment models have sometimes been a barrier to public sector adoption of cloud, and national and local governments should enable and facilitate use of opex models.

3. Additional comments

Sector, and jurisdiction, specific document and data retention requirements may be an obstacle to adoption of cloud in Europe. Examples include requirements to keep business records in particular formats, and sometimes specific locations, for tax and other purposes. In due course such requirements should be identified and, where appropriate, modified to avoid unnecessary obstacles to use of cloud on a pan-European basis. In the meantime, the creation of additional such obstacles should be avoided.