BSA The Software Alliance

Trusted Cloud Europe

Response of BSA| The Software Alliance

Overall comments

- BSA welcomes the Commission's efforts to promote the uptake of cloud computing. Our members share the goal of achieving a "single digital market, free of needless barriers or restrictions . . . in which all cloud users have access to high quality, secure and trustworthy cloud services.

- Cloud computing has an enormous potential to bring significant advantages to European citizens, businesses and public administration, in terms of cost savings, efficiency boosts, user-friendliness, better security and accelerated innovation. We, therefore, welcome the Commission's effort to raise awareness around this potential, promote the adoption and uptake of cloud services by both the public and the private sector and address the potential challenges that may hamper this.

- BSA strongly endorses the Commission and the Trusted Cloud Europe vision document's rejection of data protectionism and the idea of a "Fortress Europe". We also share the aim of reducing data location restrictions / data localization mandates. Indeed, such policies would only run contrary to the borderless nature of the cloud and will harm, rather than promote, cloud uptake.

- The cloud computing market in Europe today is vibrant and highly diverse. A range of providers compete on service levels, privacy and security protections, and even data storage locations. Competition in the market will continue to drive innovation in response to market needs. EU cloud policy should seek to encourage this diversity in innovation, rather than constrain it.

- Because cloud computing is not a monolithic industry, any best practices adopted should not be a "one size fits all" proposition. The cloud industry encompasses many different types of services, providers, and ways of deployment (including commonly referred concepts such as Infrastructure as a Service, Software as a Service, and Platform as a Service, private, public, and hybrid clouds). Best practices, when formulated, should respect and promote this multiplicity of technologies, business models, and provider types.

- We share the view that any framework including best practices for cloud providers and users should be voluntary and rely on industry led, global standards and practices wherever possible. This approach ensures that Europe's cloud providers can compete fully in the cloud market, which is inherently global.

- The concerns identified by the Trusted Cloud Europe report, including in relation to the lack of a harmonized data protection regime, are real. However, we do not believe that a stand-alone cloud regulatory framework is necessary to address these concerns. The cloud, like other technologies, is subject to a range of existing and upcoming legislation in the EU, including Directive 95/46 and a raft of rules on consumer rights. Regulating the cloud separately is unnecessary and would lead to additional costs, complexities, and conflicting obligations.

- We encourage the Commission to continue educating consumers and businesses about the tremendous potential benefits of the cloud, and the many different service options the cloud offers. Customer education is the single most important element of a program to drive cloud confidence, and will speed the uptake of cloud services in Europe.

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

Divergent Member State implementations of existing data protection rules in conjunction with unclear applicability of laws do present barriers to the adoption of cloud services in Europe, by increasing compliance costs for cloud providers and by complicating the operational delivery of cloud services. While differing legal requirements present challenges for many industries, cloud computing is particularly adversely affected by this "patchwork" because of the uniquely cross-border nature of cloud services.

We therefore welcome efforts by the European Commission to achieve greater harmonization in this field via the proposed General Data Protection Regulation. We are concerned by the Regulation's highly granular and highly prescriptive approach, however. We recognize that the Regulation is intended to enhance harmonization, for the benefit of cross-border industry. But prescriptive rules are not appropriate for the cloud computing industry, or any other rapidly-evolving technology area. Such rules threaten to constrain innovation, including innovation in more privacy-protecting technologies. Prescriptive rules will also rapidly become obsolete as technology evolves.

The better approach is to set rules that are principle-based so that they are future proof and can effectively stand the test of time while also requiring organizations to be accountable for compliance with those rules; and establishing a "one stop shop" so that controllers are clear what rules apply while users may still be able to go to their local Data Protection Authority with complaints. Enabling providers of pan-European services to deal with a single regulator instead of 28 is among the most important steps the EU can take to facilitate the deployment of pan-EU cloud services, and will reduce compliance burdens without undermining legal protections for customers and data subjects. Principles, including the one-stop shop, are technology and business model neutral, and as such should be prioritized over more prescriptive approaches.

While enforcement of existing legislation and principles are necessary and important, these should allow companies to continue developing innovative technological solutions. Such framework, accompanied by underlying tools such as codes of conduct, can provide the flexibility required in a fast-moving connected world and enable the accountability and enforceability needed to cultivate trust. It would also encourage industry to listen and respond to user concerns, both by providing innovative solutions that protect data and by adopting and adhering to appropriate common codes of conduct.

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."**

BSA agrees that consumers and small enterprises must have access to efficient and cost-effective mechanisms to enforce contractual rights in the cloud. Indeed, those rights, enshrined in the European consumer protection acquis, apply equally to cloud services and have been enforced against providers that do not adhere to the law standards. In order to avoid unnecessary complexity and redundancy, we encourage the Commission to first study existing laws and redress mechanisms, and consider whether there is in fact a need for additional measures. Existing mechanisms that address these concerns, and which should be further taken into account by the Commission in the context of cloud computing, include:

- **The European Small Claims Procedure**. This procedure, set out in Regulation 2007/861, is available to both consumers and SMEs, for claims of up to €2,000 – including in relation to certain contract disputes which could arise in a claim relating to cloud computing services.

- **TRUSTe**. Many cloud providers adhere to the TRUSTe framework, which includes a dispute resolution mechanism. Adherence to the TRUSTe framework is not compulsory for cloud providers, but intense market competition has led many cloud providers to offer this framework to customers, including consumers and SMEs. Cloud providers that refuse to cooperate with the TRUSTe dispute resolution framework risk losing the valuable TRUSTe certification.

- **Consumer protection laws and regulatory frameworks**. Consumers are protected in the European Union by a wide range of regulatory frameworks, including both European directives (e.g., the recently-adopted Consumer Rights Directive) and additional Member State-level protections. Protections under national laws may also extend to small businesses. These laws include a wide variety of generally effective dispute resolution procedures, including via various ombudsman, consumer rights regulators, trading standards bodies, and national small claims procedures.

Additional education campaigns would help improve the effectiveness of the above mechanisms, by ensuring that consumers and SMEs have easy access to information to help them avail themselves of these procedures.

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."**

BSA agrees that barriers to cloud services can take many forms, ranging from explicit legal prohibitions to industry norms that discourage cloud uptake. In assessing these norms, it is imperative to distinguish between those that are driven by legitimate customer needs and concerns and those that are simply disguised restrictions on trade.

Some norms, for example, reflect the particular sensitivity of certain types of data – such as the financial or health information. Cloud providers are working hard to develop robust protections, via organizational, technological, and geographic innovations, to respond to the needs of cloud customers in these sectors.

However, in other cases, requirements limiting cloud services are unwarranted, and represent no more than "digital protectionism" – e.g., restrictions on the flow of commercial data across borders; national technology-certification and standards policies that distort international competition; and preferences for local IT products in government procurement. These and other forms of IT-focused protectionism threaten to inhibit digital trade, stifle innovation and slow economic growth to the detriment of European enterprises and customers.

In its Digital Trade Report[1], BSA has put forward some more detailed observations and possible solutions to this phenomena, that include ways to promote technology innovation globally, and ways to "level the playing field", without creating new barriers to digital trade.

[1] http://digitaltrade.bsa.org/

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."**

BSA strongly agrees that a "Fortress Europe" model would not bring substantive benefits to Europe.

A "Fortress Europe" model, which prevents European companies and consumers from accessing the wealth of options in the cloud market offered from beyond Europe, may appear to "protect" Europe from external competition. But in reality, by restricting cloud services that would otherwise be available to European companies and consumers, a "Fortress Europe" model would damage European competitiveness and economic growth.

Like the internet, cloud services are global in nature. Being able to move data among large data centers in multiple geographic areas allows cloud computing providers to pool IT resources and consolidate overheads and purchasing power; this, in turn, results in significant cost and efficiency benefits for consumers as well as environmental benefits that flow from using fewer data centers. Because new rules that enable secure, simplified data transfers are essential to European competitiveness, we welcome reform that seeks to bring robust protections to international data transfers while allowing for flexibility and avoiding digital protectionism in Europe.

Equally, we encourage the speedy conclusion of the current discussions and the renewal of strong commitment to the Safe Harbor Decision in order to re-establish legal certainty around this core pillar of data transfer underpinning one of the most important trade relations in the world, that between the EU and the US.

Cloud services are increasingly part of the operational make-up of modern companies, forming a new factor of production for many products and services. Restricting or limiting choices available to European companies would place those companies at a disadvantage when competing on world markets, by reducing their ability to procure the best possible cloud services for their situation and needs and potentially increasing the costs of products and services. It is unclear what substantive benefits, if any, a "Fortress Europe" model would deliver to compensate for these downsides.

In contemplating "Fortress Europe," policymakers should also bear in mind the EU's role as a global normative leader. A "Fortress Europe" model may well be copied by other markets seeking excuses to enact protectionist laws – fragmenting the marketplace and reducing the opportunities for European businesses to compete in foreign jurisdictions.

We welcome the suggestion to address jurisdiction and enforcement concerns. BSA strongly encourages international dialogue on these issues so that concerns do not end up undermining the potential of cloud computing, neither innovation nor economic growth in general.

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."**

BSA agrees that non-European headquartered cloud providers should be able to access the European cloud market on equal, technology neutral terms. Adherence to best practices by both European and non-European providers will help increase consumer and business confidence in cloud services, speeding their adoption.

Wherever possible, best practices should be formulated in accordance with global standards that are industry led, such as ISO 27001, rather than solely through European forums, in order to achieve an international and interoperable market for cloud products and services.

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

BSA agrees with this assessment. Certain regulatory frameworks, such as rules relating to attorney-client privileged information or sensitive patient health data, may slow or even prevent cloud adoption.

However, the market is responding effectively to these restrictions. New advances, including organizational and technical security measures, new cloud privacy standards, encryption technologies, and data center security measures, are providing increasingly robust levels of security and confidentiality. Market offers, including complex hybrid private-public clouds, allow customers to select privacy levels and security requirements in a layered fashion, suitable to their requirements. So although these regulatory and policy frameworks *do* present barriers to cloud adoption, many of these challenges are being addressed by vibrant marketplace competition.

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.**

We agree that consumers of cloud computing and other digital services (including both private-sector and government users) need assurance that cloud providers both understand and appropriately manage the security risks associated with storing data and running applications on cloud systems.

To achieve the necessary level of security, cloud providers have adopted a range of practices and procedures commensurate with the sensitivity of the data involved, including:

- Compliance with well-recognized, transparent and verifiable security criteria.
- Robust identity, authentication and access control mechanisms.
- Comprehensive and ongoing testing of security measures before and after deployment.

Consistent with our recommendation above that prescriptive regulations should be avoided in this field, BSA believes that *specific* technical and organizational measures should not be mandated for the cloud computing industry. Such requirements would, if enacted, undermine the EU's current technology neutral approach to cybersecurity. In the long term, prescriptive requirements would also undermine the overall security of the cloud ecosystem, by rendering the cloud industry's security mechanisms more monolithic, more predictable, and less responsive to rapidly changing cyberthreats.

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".**

We would be cautious regarding a transformation of the Trusted Cloud Europe initiative into the development and deployment of a "Trusted Cloud Europe" mark. A trustmark could have advantages in terms of enabling consumers to better evaluate and compare cloud offerings. But it is not necessarily the case that such a mark will be beneficial in the fast–developing cloud computing market.

Customers and consumers generally want the latest products and services available on the market, offering newer and stronger security and privacy protections than prior solutions. Market demand in turn drives rapid innovation in cloud-based privacy and security. Any trust mark or certification program will need to be flexible enough to accommodate this constant innovation, so that it does not impede the delivery of state-of-the-art solutions.

The risk of such trustmark criteria becoming obsolete would be high and the administrative burden likely unmanageable, in particular where consumer cloud services are concerned. Any certification that contains requirements that are overly prescriptive and/or lock providers and customers into bypassed technology will not remain a marker of quality for long.

If the EU does decide to move forward with a "Trusted Cloud Europe" brand, BSA recommends that:

- The process to formulate this certification be open to input from stakeholders throughout the cloud ecosystem, and the certification criteria and processes be subject to ongoing review.
- Administration costs resulting from any new certification scheme be kept to a minimum, to ensure that cloud providers large and small can afford to participate in the scheme.
- The Trusted Cloud Europe mark should be awarded on the basis of criteria applied consistently throughout Europe, without deviations in different Member State markets. A consistent approach is important to ensure that variations do not arise within the digital single market, and that cloud providers are not required to comply with multiple, divergent obligations.
- Compliance should be wholly voluntary, based on self-assessment and the regime should not become a de facto or de jure barrier to access certain markets (e.g. the government / public procurement markets).
- The scheme should be based on global standards and consistent with existing international standards and certifications, in order to avoid duplicating burdens or creating inconsistent or unduly onerous requirements for cloud providers. Many cloud providers already adhere to standards such as ISO/IEC 27001 or CSA Security, Trust & Assurance Registry (CSA STAR). Other certifications, such as ISO/IEC 27017, and ISO/IEC 27018, are under development.

  Any Trusted Cloud Europe mark should avoid proliferating new standards and certifications unless a gap is spotted; too many certifications will generate rather than mitigate customer confusion.
- Organizations defining the schemes should not be able to make arbitrary alterations to what is or is not in the scheme.

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"

Ad hoc checks are not a viable option to ensure cloud service provider accountability. Similarly, mandated, one-size-fits-all certification schemes also have their limitations; as described above, such schemes can quickly become obsolete, and lose value as barometers of the robustness of a provider's mechanisms.

Importantly, however, marketplace competition is already driving cloud providers to offer tools that enable customers to assess compliance levels. Some cloud providers, for example, offer services that are regularly audited by independent and verifiable third parties. Security standards, such as ISO 27001, are already certified by external auditors on a regular basis for some providers. Terms of service can provide rights for customers to access audit reports. Within the last several years, major providers have also begun to offer additional layers of control and compliance, for example via adherence to European model clauses in the context of data processing agreements that provide robust rights for customers using cloud services.

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.**

BSA fully supports the Report's conclusion that CIOs in all Member States should work to stimulate the adoption of cloud services wherever possible. By enabling governments to pay for only as much infrastructure as needed, and by providing instantaneous access to updates and service innovations, the use of cloud services can significantly reduce administration costs for governments. (One IDC study found that almost all cloud users see cost reductions, tending to peak between 10% to 20% of operational IT costs.[2])

These benefits will be enhanced, and accessed much more rapidly, through the adoption of cloud-active procurement policies. In turn, innovative new government services, that are more responsive and less costly, may also stimulate further economic growth.

We hence support the proposal that "Member States can share effective national budgeting policies to ensure that pay-as-you go models (moving from capex to opex) can be enabled". Such initiatives, matched with appropriate EU guidance and funding, would provide support to achieve the overall objective of a single European market for cloud.

BSA strongly supports these initiatives and would be happy to continue dialogue with any government and the Commission, on how such policies can be designed for maximum impact.

[2] *See*: http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-gcattaneo-presentation.pdf.