



GSR12 BEST PRACTICE GUIDELINES ON REGULATORY APPROACHES TO FOSTER ACCESS TO DIGITAL OPPORTUNITIES THROUGH CLOUD SERVICES*

The growth of cloud computing has the potential to offer tremendous cost savings, efficiency and innovation for government, businesses and individuals around the globe. For entrepreneurs and businesses, big and small, cloud computing delivers unique economic leverage that means investment can translate into impressive returns and costs savings. With the advent of cloud computing, digital resources are now becoming accessible over multiple networks anywhere, anytime. Yet, reaping the full potential of cloud computing will require cooperation and collaboration between governments, industry and consumers to build confidence in cloud based services. Importantly, the growth of cloud computing will depend on ubiquitous and affordable broadband networks to which service providers have access on a non-discriminatory basis.

We, the regulators participating in the 2012 Global Symposium for Regulators, recognize that effective and dynamic regulation can facilitate key inputs for cloud computing to thrive and spur economic growth. Therefore, we have identified and endorsed these regulatory best practice guidelines to promote innovation, investment and competition in cloud infrastructure and services, and protect consumer interests.

Awareness raising and promotion of uptake by the public sector: Cloud services and the opportunities and savings they make available to governments around the world should be actively pursued and promoted. Bringing awareness of these opportunities will generate economic opportunities and provide great value to citizens, consumers and businesses.

Broadband infrastructure: Regulators need to work to reduce barriers to broadband deployment, actively facilitate build-out of national fibre-optic networks and international connectivity links, including submarine cables, and promote infrastructure sharing and coordination of civil works, including across sectors, as well as policies to speed rights of way access, and installing data-centre infrastructure. This will provide incentives for content delivery networks and data-center companies to install locally. It is also necessary to ensure the deployment of services in unserved and underserved areas, including emergency and accessibility-enhanced services.

IP interconnection: Regulators should seek to ensure that all users derive maximum benefit in terms of choice, price and quality of service and to minimize any distortion or restriction of competition.

Spectrum: For the future of cloud computing services, several actions could be taken to release additional, critically-needed spectrum for wireless broadband, including repurposing spectrum, opening white spaces to unlicensed use, and conducting incentive auctions. In addition, policies that generally encourage the harmonization of international spectrum and communications device approvals must be encouraged.

*

The Guidelines are based on contributions from AREGNET/Lebanon, Burkina Faso, Colombia, Egypt, Poland, Switzerland, Thailand, United States, and Zimbabwe.

Market definition in a converged cloud: Taking into account network and service convergence, promoting migration to NGN and encouraging competition, regulators may consider adopting a light-touch approach to new ICT sector players, such as content and application providers.

Market power: Regulators need to ensure that communication providers do not engage in conduct that constrains the provision of cloud services for reasons that are not transparent, objective, non-discriminatory and proportionate.

Enforcement: Regulators need to establish a means of identifying breaches to ensure they are able to respond effectively. This may be achieved through (1) self-regulatory mechanisms, content service providers notifying the appropriate regulator of breaches of security, (2) ideally changes to certain aspects of data protection legislation which is impossible to monitor and hence unenforceable in practice; and (3) effective mechanisms for complaint handling and resolution of disputes, including alternative dispute resolution mechanisms.

Cloud transparency: Regulators may consider encouraging cloud service providers (CSPs) or introducing specific obligations with regard to notifying users of the chain of providers that underpin the provision of cloud services. Regulators also need to ensure that ISPs provide customers with greater transparency about the traffic management practices being followed by companies on their networks.

Consultative process: Regulators need to consult with CSPs and other market players about the appropriate regulatory treatment and classification of certain cloud services, with a view to issuing guidance providing legal certainty for market entrants and cloud users, for example through conducting multi-stakeholder fora to develop best practices for protecting consumers.

Net neutrality: A certain level of traffic management will always be necessary to minimise network congestion. Regulators should seek to regulate the use of traffic management techniques to apply specific measures in a manner that does not unfairly discriminate between market players.

Regulators may also need to review existing competition laws to determine whether the regulatory tools, such as anti-discriminatory law or regulations that are already in place adequately address the competition issues that tend to impact net neutrality.

Quality of service (QoS): A number of regulators enforce minimum QoS requirements to ensure that customers and edge providers have reliable and uninterrupted services, including access to personal information in the cloud. In order to deliver these services, network providers will have to ensure (1) transparent and clear terms and conditions of contracts signed by customers; (2) the publication of comparable information on the availability and QoS; and (3) disclose minimum requirements for QoS to customers.

Consumer empowerment: Policymakers need to ensure that consumers are empowered to control their personal data and protect their privacy through facilitating Cloud Literacy. Cloud users need to be sure that information stored or processed in the cloud will not be used or disclosed in harmful or unanticipated ways.

Privacy & data protection: International agencies as well as national policy makers and regulators must work together to develop efficient, effective, proportionate and enforceable laws to protect consumers' reasonable expectation of privacy. Responsibility should also be devolved to stakeholders developing self-regulation, for example establishing privacy policies that are transparent and appropriate for the services they provide. Governments should also continue to work together to ensure no single entity adopts privacy regulations that are so burdensome that they restrict the free flow of information or prevent CSPs from maximizing the cost saving inherent in those services.

Cloud standards: The development and widespread adoption of appropriate national, regional and international technical and organizational standards are required to address a range of concerns

among cloud providers and users, including the integration of legacy systems with cloud interfaces; data and application portability and security.

Data portability: Proprietary cloud computing application programming interfaces (APIs) can limit customers' ability to switch to a different provider (lock-in effect). Standardizing APIs would facilitate data portability and would allow greater reliability by allowing the same functions to be performed by multiple cloud computing providers.

Interoperability: Interoperability is key for consumers of cloud computing services as it facilitates information flows with appropriate security and privacy protections. Therefore, governments need to support the development of standards and measures that will speed the arrival to markets of communications devices and ensure seamless wireless connectivity and services. Eliminating unnecessary restrictions on the trans-border flow of data is of particular importance.

Demand stimulation: Governments must lead the way in the adoption of cloud-based computing. In addition, efforts need to be deployed to overcome barriers to broadband adoption, pursuing multiple initiatives targeted at both consumers and small businesses.

Research and development (R&D): Promoting R&D activities in the field of cloud computing is an essential tool for designing future-proof digital economies. Close regional and international cooperation with relevant international bodies as well as universities should be encouraged.

Regulatory cooperation: Cloud services impact on a range of regulatory areas, both within jurisdictions and across multiple jurisdictions. Regulators should cooperate and coordinate regulatory decision-making that is targeted at CSPs.

Internationally, governments need to collaborate to increase regulatory predictability related to the cloud and develop common core policy principles that will assist the development and adoption of cloud computing services while avoiding the creation of regulatory barriers to market entry.

Regional cloud: Regional clouds represent a unique opportunity for a group of countries to cooperate in order to promote cloud computing services and take advantage of its benefits while reducing security, confidentiality and other vital concerns through the establishment of regional regulatory frameworks and other protective measures for businesses and consumers.

To that end, a sub-regional approach could be encouraged whereby regulators' associations promote efforts to harmonize regulatory instruments among their member countries.