4.1 Strike a balance

Trends in Telecommunication Reform 2013 reviews existing privacy and data protection frameworks in the European Union (EU), as well as from a diverse group of countries representing the developed and developing world. Many countries that have adopted or are considering the adoption of data protection regulation have followed the European model, so the review treats Europe in the greatest depth. The European model also usefully illustrates the problems presented to business and the economy by the lack of clear and consistent laws implemented seamlessly across international borders. [30]

At a regional level, the European Union Data Protection Directive (more simply referred to as the European Directive) was enacted in 1995. Under the European Directive, data protection obligations are generally imposed upon data controllers, while data processors are subject only to specified security requirements. But differing definitions used in different European countries, along with the blurred categorization of a cloud service provider as a controller or processor, lead to ambiguity. [30]

The client is often responsible for the full burden of data protection obligations and compliance, despite having little control over the actions of the provider or movement of the data. Cloud clients are required to exercise due diligence with respect to choosing a provider who offers sufficient guarantees of reliability, competence and security safeguards to be compliant with relevant laws. [30]

4.2 The transborder flow of data

Under the European Directive, personal data must not be transferred to countries outside the European Economic Area that are judged to have inadequate personal data protection measures. Amazon, for example, has created a European Cloud to provide customers with confidence that data will not cross borders in breach of the Directive. The United States Safe Harbor Scheme is also accepted as adequate for the purposes of transferring certain personal data, subject to some notable exceptions and to specific due diligence. [30]

Cloud computing, however, is typically conducted without a stable location and providers are unlikely to be based only in specified countries. The customer may not be able to ascertain the real-time location of data that are being processed or stored. Regulators face the same problem, which renders restrictions on transborder data flows difficult to enforce. [30]

If transfers need to be made to countries outside those that have "adequate" laws, standard contractual clauses may be required. These clauses contain non-negotiable provisions that set out transfer and security measures deemed adequate under the European Directive. [30]

International businesses can adopt binding corporate rules for the regular transfer of data throughout their corporate networks. [30]

Accountability is key to ensuring compliance and thus audit rights are becoming increasingly important to clients. However, the granting of these rights presents a practical problem for providers who use shared infrastructure for their clients. Granting access may itself compromise the confidentiality and security of data belonging to other clients. [30]

4.3 What laws apply in the cloud?

There is no universally binding privacy legislation covering all countries of the world. Of the 89 countries that have adopted privacy or data protection laws, many regulate international data flows as a mechanism for protecting individual privacy and enforcing national policies. [30]

The European Union's e-Privacy Directive targets public communication network providers and states that personal data should only be accessed by authorized personnel for legally authorized purposes, and that stored or transmitted personal data should be protected against accidental or unlawful destruction, accidental loss or alteration, and against unauthorized or unlawful storage, processing, access or disclosure. Personal data are defined broadly as "any information relating to an identified or identifiable natural person". [30]

On 25 January 2012, the European Commission published its proposed changes to the EU Data Protection Directive in an attempt to harmonize the current "fragmented and outdated" data protection legislative framework. Proposed changes include the following [30]:

- National regulatory authorities will have the power to take action against organizations in other Member States in certain circumstances and may issue fines of up to EUR 1 million or 2 per cent of a company's annual turnover in some cases.
- The definition of personal data will be expanded to cover any information relating to a data subject, and the regulations will require an individual's explicit consent to allow data capture.
- The regulations will apply beyond the EU, to include non-EU entities that process personal data relating to EU citizens.
- Organizations will be required to report data breaches without undue delay and, if feasible, within 24 hours of the breach.
- Data controllers will be required to carry out data protection impact assessments appoint data protection officers and inform third parties of any breaches.
- Individuals will be given a new "right to be forgotten" under certain circumstances and will no longer be required to pay to access their data.
- International data transfers will be subject to a more detailed regulatory framework requiring safeguards to be put in place and authorities to undertake prior checks, while the derogations available to data controllers will be more restrictive.
- The controversial nature of the proposed reforms has, however, provoked lobbying and debate. This could mean long delays before implementation. [30]

4.5 Experiences of countries

Cloud computing adoption to developing countries, the suggested framework Based on Experiences from:

- **Meanwhile, in the United Kingdom**, for example, the courts have narrowed the meaning of personal data, stating that the data must be biographical in a

significant sense, and must focus on the individual, rather than on some other person or transaction or event. [30]

- **In France**, the amended Data Processing, Data Files and Individual Liberties Act is regulated by the proactive National Commission on Computers and Liberties. The Commission has published guidance on the legal processing of personal data, imposing notification and cooperation requirements on data controllers, as well as requirements to keep personal data secure and, in certain circumstances, to obtain the Commission's approval prior to processing. [30]
- **In Germany**, personal data are to be obtained directly from the data subject unless required by law for a genuine business purpose or if disproportionate effort would be required and there are no indications that the data subject's interests would be affected. Further, the Federal Data Protection Act puts particular emphasis on designing data protection systems to process as little personal data as possible, for example by making the data subject anonymous or by using pseudonyms. [30]
- **In the United States**, legislation changed dramatically following the attacks of 11 September 2001 with the introduction of the US Patriot Act. The Act permits the sharing of personal data of anybody suspected of involvement with terrorism or money laundering activities. This has resulted in the possibility of broad access to — and sharing of — personal information. [30]
- The right to privacy has been recognized by the US Supreme Court based on the US Constitution, despite there being no such explicit constitutional right. Many states have privacy protections within their own constitutions. Only California has extended the protection of data from government interference into an obligation on the private sector. [30]
- Later, the establishment of the National Security Agency which was given a wide range of discretions to access individual and corporate information.
- **In Canada**, the Canadian Charter of Rights and Freedoms contains a right "to be securing from unreasonable search or seizure", which the courts have extended to protect an individual's "reasonable expectation of privacy". Recent case law from the Court of Appeal in Ontario has also introduced a common law tort of invasion of privacy ("intrusion upon seclusion"). Canadian laws do not restrict international transfers of personal data, but any transfer remains the responsibility of the disclosing party. [30]

- **Brazil** has yet to implement specific data protection legislation although its Constitution does set out fundamental rights to both privacy and secrecy of correspondence. The Civil Code also provides that an individual may request relief from any threat to personality rights, and that the private life of an individual is inviolable. There are also broad protections within the Consumer Protection Code. These include consumer rights of access and correction to any recorded personal data. [30]
- **South Africa** has no specific data protection legislation, but a right to privacy is set out within its Constitution. There are also relevant personal information provisions contained within the Consumer Protection Act 2008 and the Electronic Communications and Transactions Act 2002. Compliance with the latter is voluntary and any adherence must be recorded in an agreement with the data subject. A new Protection of Personal Information Bill has been tabled in the South African Parliament. [30]
- **Saudi Arabia** has no specific data protection legislation, although a right to privacy is established in a number of its laws. In particular, Saudi Arabia's Basic Law of Governance sets out the overriding principle that all correspondence and communications between parties should be kept strictly confidential and should not be disclosed. [30]
- If no legislation is applicable, the courts will apply sharia (Islamic law). The sharia principles establish a tort claim for damages for the wrongful disclosure of a person's personal information where that disclosure results in loss or harm to the individual. [30]
- **The United Arab Emirates** does not have any specific data protection legislation, although a right to privacy is set out within its Constitution and in various laws. The Constitution states that an individual enjoys "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law." In addition, the Penal Code establishes certain rights of privacy and the protection of personal data. [30]
- **India** There is no specific constitutional right to privacy in India, although the Supreme Court has established that privacy should be included within the right to life and personal liberty. The collection and processing of personal data is regulated under the Information Technology Act 2000, which states that

companies must maintain reasonable security practices while processing personal data, and that if obtained under a contract, such data must not be disclosed in breach of that contract without the data subject's consent. [30]

- **Japan** As a member of Asia-Pacific Economic Cooperation (APEC), Japan subscribes to APEC's approach to privacy. The Act on Protection of Personal Information regulates the collection and use of personal data in Japan. Any form of data handling is covered, but the Act applies only to situations involving the personal information of 5000 or more individuals. The Act imposes common obligations of consent, security and providing information, alongside additional requirements to supervise employees and third parties who handle the personal data. [30]
- **Sudan** the right of access to information, a draft was circulated in 2007 but did not complete the legislative cycle of approval, it has been activated again in 2014 and still under review [31].

In Sudan there is law to criminalize assault on the integrity of the data and the safety of systems and networks information in Informatics Crimes Act of 2007 [21].

Clause (9.8) address the assault on the safety of information systems through criminalize sabotage system, or disability deliberate, and the legitimate use of IT systems, including communications systems [21].

Clause (6), criminalize the reality objection of intentional messages, without the authorization of the public prosecutor or the competent authority, or the owner of the information piece by eavesdropping, or capture/ intercept messages through technical means, in place of arrival, or in origin or within the information system. The aim of this material is to protecting the right of transferring data in all forms of electronic data transmission [21].

In Sudanese Act of 2007, Clause (23 \ 1) criminalize the Offences information against, every act of induction or subscription for the purpose of committing any of the offenses stipulated in that law [21].

➢ Global Symposium:

Regulators are the participants in the Global Symposium for Telecommunications Regulators (GSR) in 2012; they identified and approved of regulatory guidelines related to best practices to promote innovation, investment and competition in the field of infrastructure and cloud computing services and the protection of consumer interests.

Dynamic and the effective regulation would facilitate advantage of cloud computing and allows it to achieve success to serve as a catalyst for economic growth [55].

Guidelines [55]: It's highlighted the need for further international cooperation on cyberspace issues, including freedom, security and respect, as the need for technological neutrality in producing effective regulation.

1. ***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.
2. ***Broadband infrastructure:*** Regulators need to work to reduce barriers to broadband deployment, actively facilitate build-out of national fiber-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 un-served and underserved areas, including emergency and accessibility-enhanced services.
3. ***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.
4. ***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, or conducting incentive auctions. In addition, policies that generally encourage the harmonization of international spectrum and communications device approvals must be encouraged.
5. ***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, while carefully assessing the impact of their decisions on all market players.

6. ***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.
7. ***Enforcement:*** Regulators need to establish a means of identifying breaches to ensure they are able to respond effectively.
8. ***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.
9. ***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.
10. ***Net neutrality:*** A certain level of traffic management is necessary to minimize network congestion. Regulators and policy makers should seek to implement measures to oversee the use of traffic management techniques to ensure that those do not unfairly discriminate between market players.

    Regulators also need to review existing competition laws to determine whether the regulatory tools, such anti-discriminatory law or regulations that are already in place adequately address the competition issues that tend to impact net neutrality.
11. ***Quality of service and experience (QoSE):*** A number of regulators enforce minimum QoSE 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 and service providers will have to ensure transparent and clear terms and conditions of contracts signed by costumers. Regulators also need to ensure the publication of comparable information on the availability and QoSE and, when necessary, introduce minimum requirements for QoSE in order to avoid degradation of the quality provided to customers.
12. ***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.
13. ***Privacy & data protection:*** International agencies as well as national policy makers and regulators must work together to develop efficient, effective,

proportionate and readily 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.

14. ***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.
15. ***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.
16. ***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.
17. ***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.
18. ***Capacity building:*** As cloud computing is expected to be one of the main drivers of future growth of digital economies, regulators and policy makers can actively contribute to the development of a new generation of educated and technology-savvy workforce by ensuring the timely and effective introduction and spread of new and improved products and processes in the economy, reinforcing the ability of individuals and businesses to continuously create wealth, and putting a premium on all forms of learning, with close attention to both indigenous knowledge and the transfer of knowledge.
19. ***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.
20. ***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.

These guidelines are based on contributions from Algeria and AREGNET / Lebanon, Burkina Faso, Colombia, Egypt, France, Mauritius, Poland, Sri Lanka, Sudan, Swaziland, Switzerland, Thailand, United States and Zimbabwe [57].

4.6 Recommendations for best practice

Is the current patchwork of regulation fit for purpose in the cloud? The short answer is no. National regulation with respect to privacy and data protection was established 20 to 30 years ago and did not foresee the advent of a global digital ecosystem. Existing regulations are now outdated. [30]

To address the challenges raised by the cloud ecosystem, *Trends in Telecommunication Reform 2013* recommends steps that can be taken by policy-makers and regulators, some of which are highlighted here. [30]

- **Facilitate cloud literacy:** Regulators should assist consumers to make informed choices about what personal information they put in the cloud by enhancing their understanding of the commercial value and potential use of their data. Citizens need to know to whom to complain if their information is misused. [30]
- **Develop expertise:** Policy-makers and regulators should keep up to date with technical and social developments in the cloud, and with the views of all stakeholders, so as to be in a position to establish and enforce relevant laws. [30]
- **Adopt laws that are fit for purpose:** International and national policy-makers should work together to develop efficient, effective, proportionate and enforceable laws to protect the individual's reasonable expectation of privacy. Responsibility should also be devolved to stakeholders to develop self-regulation. [30]

- **Review existing laws:** Policy-makers internationally should review existing laws to facilitate the national and international use of cloud services. The development of common standards and interoperability requirements will facilitate transborder information flows with appropriate security and privacy protections. [30]

McCauley's Cloud Service Best Practices McCauley's Paper suggest that the legal practitioner should look for the following practices in a legal cloud provider ("**the Wish List**") [32]

- **Transparency:** Cloud computing platforms should explain their information handling practices and disclose the performance and reliability of their services on their public web sites.
- **Use limitation:** A cloud provider should claim no ownership rights in customer data and should use customer data only as its customer's instructor to fulfill contractual or legal obligations.
- **Disclosure:** A cloud provider should disclose customer data only if required by law and should provide affected customers prior notice of any compelled disclosure.
- **Security management system:** A cloud provider should maintain a robust security management system that is based on an internationally accepted security framework (such as ISO 27001) to protect customer data.
- **Customer security features:** A cloud provider should provide customers with configurable security features to implement in their usage of the cloud computing services.
- **Data location:** A cloud provider should tell customers the countries in which customer data is hosted.
- **Breach notification:** A cloud provider should notify customers of known security breaches that affect the confidentiality or security of the customer data.
- **Audit:** A cloud provider should use third-party auditors to ensure compliance with its security management system.
- **Data portability:** A cloud provider should make available to customers their data in an industry-standard, downloadable format.

- **Accountability:** A cloud provider should work with customers to designate appropriate roles for privacy and security accountability.[32]