Eighth SG13 Regional Workshop on "Standardization and Future Networks: Opportunities for Africa Beyond 2020"

Data Handling Procedures and Requirements-aware Cloud Computing

Dr James Agajo

Associate Professor

(PhD. Telecommunication and Computer Engineering)

Federal University of Technology Minna, Nigeria.

Virtual, 1 June 2021

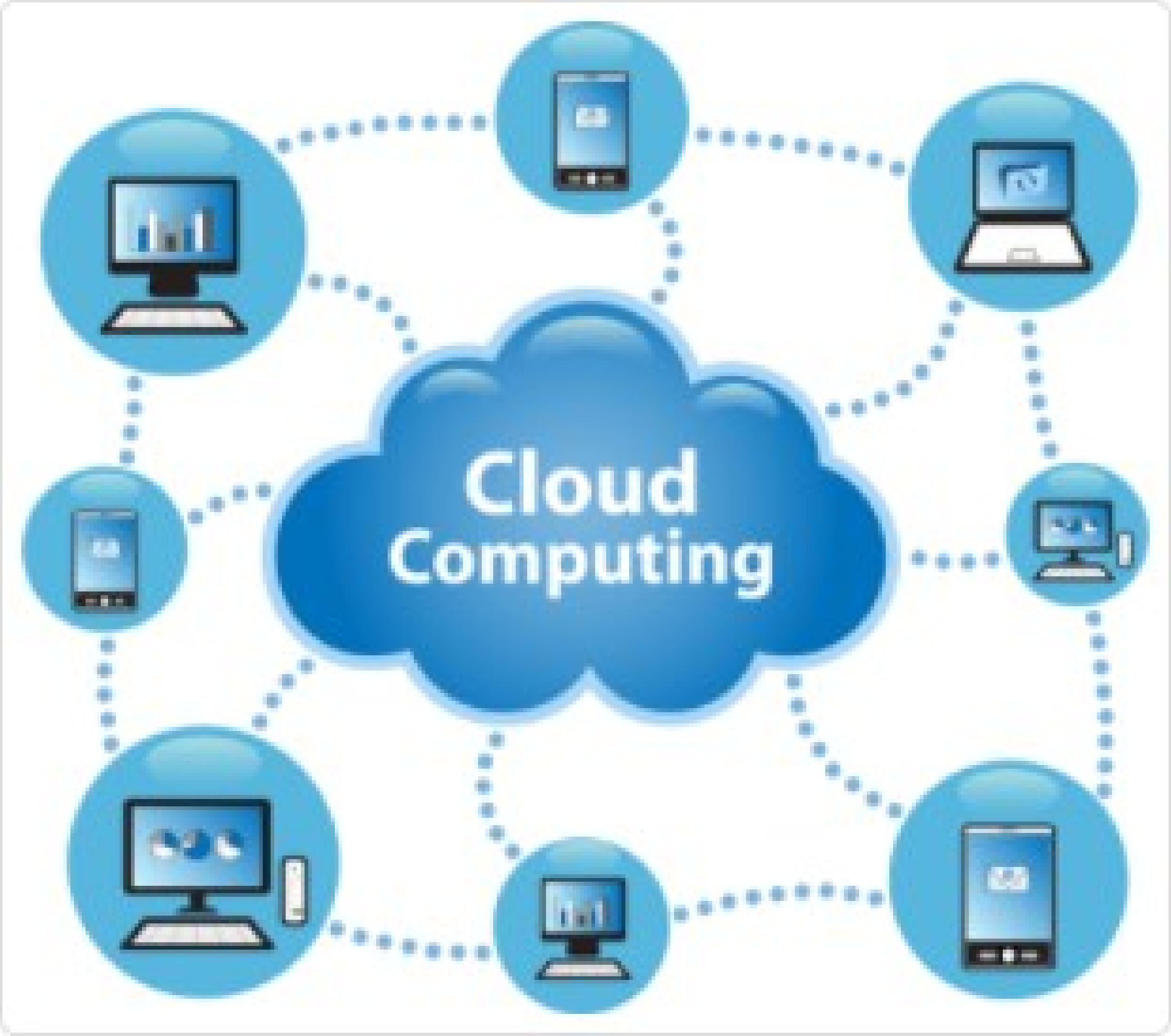
The Big Question

- One major Concern in Cloud Computing is: If the Data sent can actually be secured considering the fact that messages can be intercepted based on what was sent, whom it was sent to, when the message was sent and where the message was sent from and to

Introduction

Cloud Computing

- The “cloud” is just a set of high-powered servers from one of many providers.
- They can often view and query large data sets much more quickly than a standard computer could.
- Cloud Computing” refers to the mechanism that remotely takes this data in and performs any operations specified on that data.



SERVICE MODEL IN CLOUD COMPUTING

WHEN YOU CONSUME CLOUD YOU MUST ENCOUNTER AT LEAST ONE OF THIS THREE 3 SERVICE MODEL

IAAS

- Facility that hold the infrastructure, physical aspect of it
- Hardware
- Data Centre

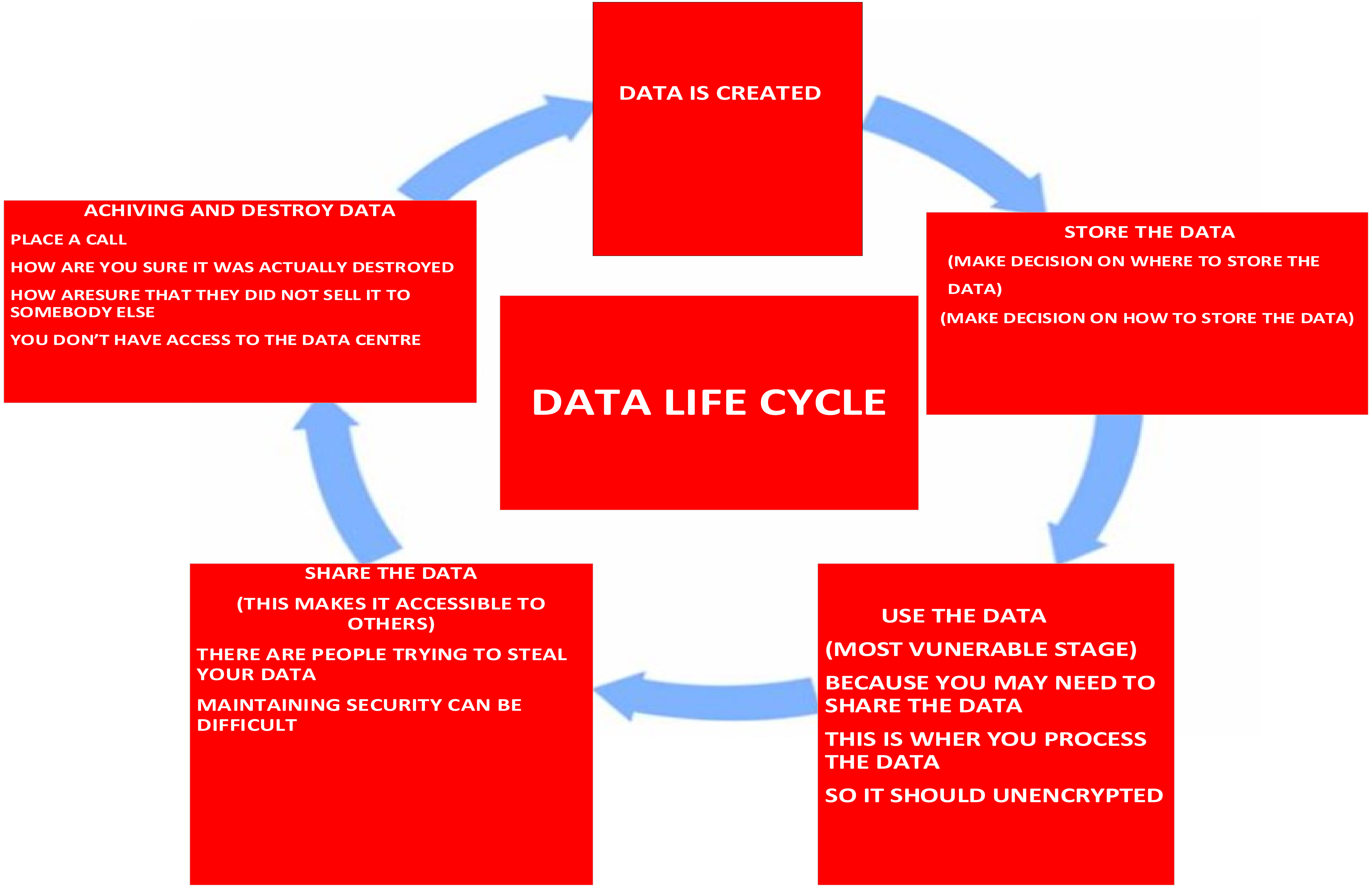
PAAS

- Application development environment
- Integration and middleware

SAAS

- API
- Application
- Data
- Content

Data Life Cycle



DATA IS CREATED

STORE THE DATA

(MAKE DECISION ON WHERE TO STORE THE DATA)

(MAKE DECISION ON HOW TO STORE THE DATA)

USE THE DATA

(MOST VUNERABLE STAGE)

BECAUSE YOU MAY NEED TO SHARE THE DATA

THIS IS WHER YOU PROCESS THE DATA

SO IT SHOULD UNENCRYPTED

SHARE THE DATA

(THIS MAKES IT ACCESSIBLE TO OTHERS)

THERE ARE PEOPLE TRYING TO STEAL YOUR DATA

MAINTAINING SECURITY CAN BE DIFFICULT

ACHIVING AND DESTROY DATA

PLACE A CALL

HOW ARE YOU SURE IT WAS ACTUALLY DESTROYED

HOW ARESURE THAT THEY DID NOT SELL IT TO SOMEBODY ELSE

YOU DON'T HAVE ACCESS TO THE DATA CENTRE

DATA LIFE CYCLE

DATA HANDLING PROCEDURE IN CLOUD COMPUTING

Data Handling:

- **Data handling** is the process of ensuring that **data** is stored, archived or disposed off in a safe and secure manner during and after the conclusion of a research project.

- This includes the development of policies and **procedures** to manage **data** handled electronically as well as through non-electronic means .

Data Handling

- Data Handling:
- Users and companies have certain requirements how their data should be handled. Companies, e.g., often want sensitive customer data to be stored in the jurisdiction of their headquarters.
- These preferences may either be intrinsic to the user or company, or driven by statutory regulations.
- The EU, e.g., demands that personal data of customers is only stored and processed within the EU or countries with comparable privacy laws (safe harbor principle).
- However, when outsourcing data to the cloud, users and companies essentially lose control over their data.

Data Handling should be best Handled:

- Protecting sensitive corporate and customer data should be a priority if you're considering a virtualized environment that enables a vendor to manage or store that data.

- Before you put your data in the hands of a vendor, demand that the vendor demonstrate its data protection and business continuity capabilities.

- And when you decide to move forward, make sure that your negotiated agreement is explicit about the vendor's ongoing obligations to protect your data and holds the vendor liable for failure to satisfy those obligations.

CLOUD DATA HANDLING CHALLENGES

- Users and companies have certain requirements how their data should be handled.
- Companies, e.g., often want sensitive customer data to be stored in the jurisdiction of their headquarters.
- These preferences may either be intrinsic to the user or company, or driven by statutory regulations.
- The EU, e.g., demands that personal data of customers is only stored and processed within the EU or countries with comparable privacy laws (safe harbor principle). However, when outsourcing data to the cloud, users and companies essentially lose control over their data [4]–[6], [9].
- In the following, we identify data handling challenges that have to be addressed technically when outsourcing data to the cloud.
- Addressing these challenges allows to mitigate the anticipated loss of control over data.
- The two main challenges are location of storage and duration of storage.

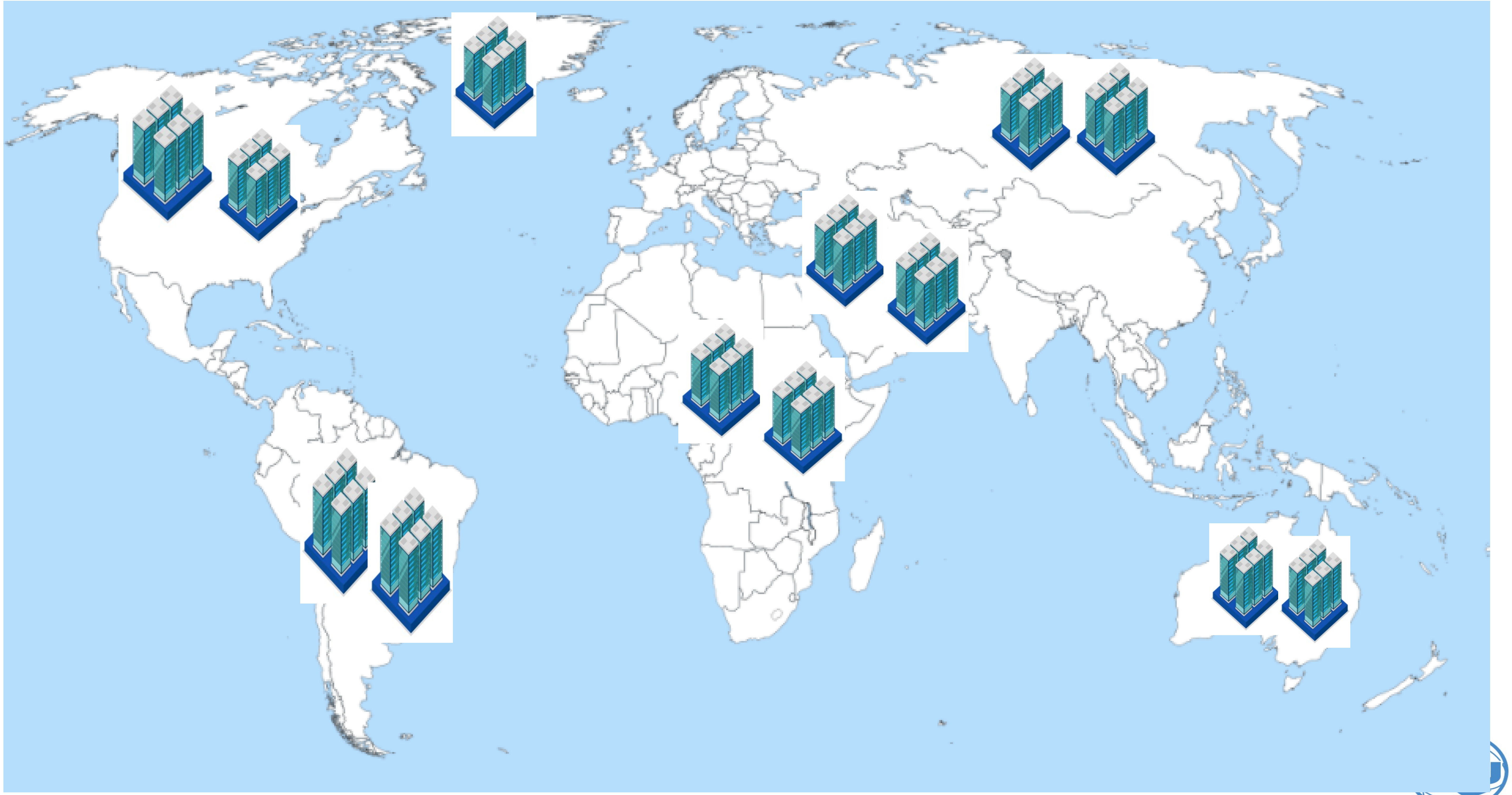
Location of Storage

- Storing data outside certain legislative boundaries (often even without noticing), raises severe concerns [4], [9].
- One prominent reason for this is the enforcement of data protection laws.
- As already mentioned, the EU forbids the transfer of personal data to oversea jurisdictions with weaker privacy laws.
- The only exception is the safe harbor principle, which allows providers in countries with weaker privacy laws to voluntarily follow the EU privacy law and thus become eligible for receiving data.
- However, also other legal requirements besides data protection have an impact on the location of storage. In Germany, e.g., companies are not allowed to store any tax relevant data outside the EU.
- Meeting these requirements with today's cloud services is virtually impossible.
- This essentially results from a lack of necessary information. In order to handle data compliant with these regulations, all involved entities need information where a specific data item is allowed to be stored and a way to communicate these restrictions.

Duration of Storage

- For the duration of storage, we differentiate between maximum as well as minimum storage duration requirements.
- The maximum duration of storage specifies a point in time at which the data has to be deleted.
- This is driven by the perception of users who want their data to be deleted once it is not needed anymore.
- Recently, this approach has also been discussed as the “right to be forgotten” in the EU’s regulation process [10].
- The key challenge here inherently results from the desired redundancy (for reliability and performance) as well as the distributed nature of the cloud.
- Contrary, the minimum duration of storage specifies a point in time before which the data must not be deleted. duration of storage.
- it is crucial that the storage provider knows in advance when the data should be deleted earliest

De-Centralizing Data Centres



Current Status

- However, it is observed that current cloud offers, especially in an intercloud setting fail to meet some basic requirements.

- Users have no way to specify their requirements for data handling in the cloud.
- Also providers in the cloud stack even if they were willing to meet these requirements can thus not treat the data adequately.

Requirements-aware Cloud Computing

Major contenders Stakeholders

- Regulators

Government Agencies
Law Makers
Policy Makers

USERS

- Individuals
- Co-operate Organization

Service Providers

- Internet Service Providers
- Vendors

DATA GOVERNANCE

- **Data Classification**

A high Level Description of essential and valuable information categories(Confidential regulated)

- **Policies on Information Management**
- What Activities are allowed for different types

Location and Jurisdiction

Where should the data be geographically located

What are the Legal and regulatory implication

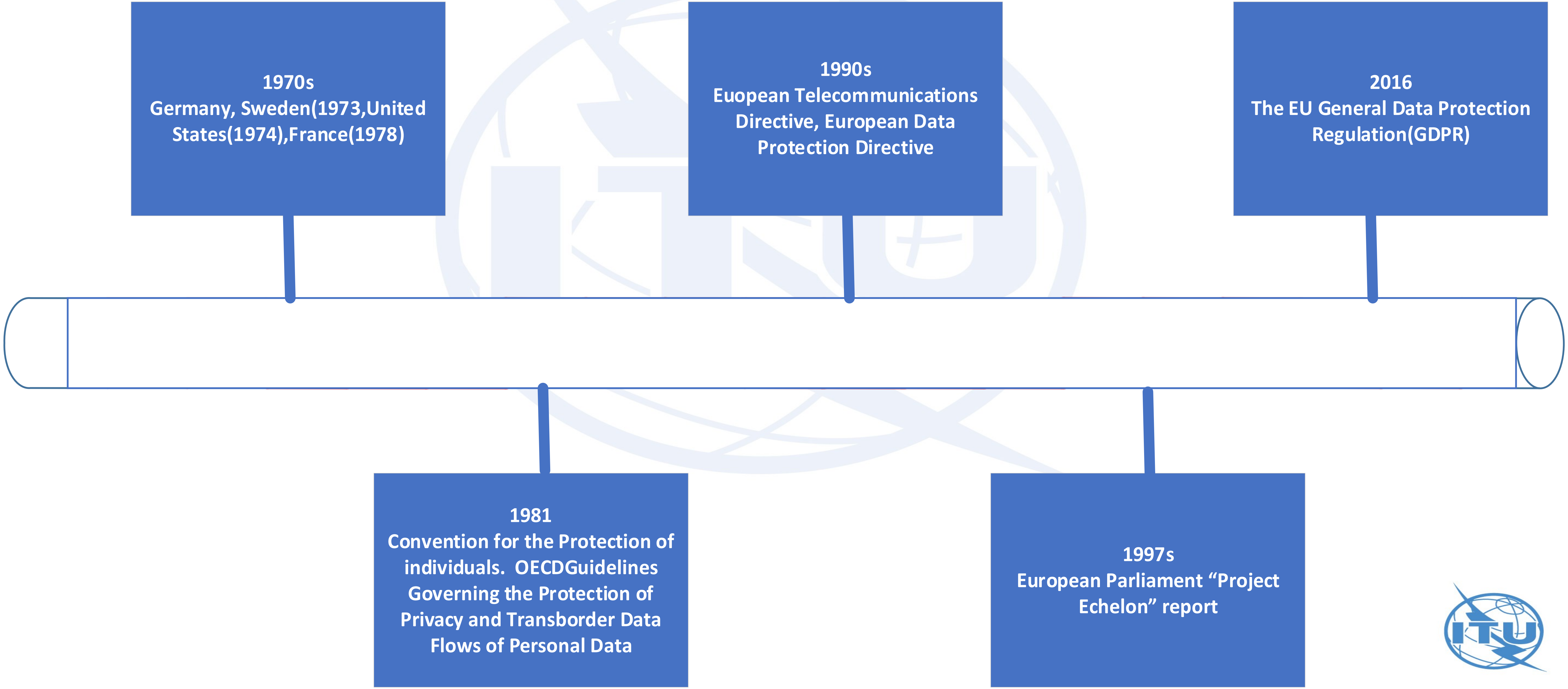
- **Authorization**

Who is allowed to access different types of information

- **Custodianship**

Who is responsible for managing the information behest of the owner

GLOBAL DATA PROTECTION



1970s
Germany, Sweden(1973,United States(1974),France(1978)

1981
Convention for the Protection of individuals. OECDGuidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

1990s
Euopean Telecommunications Directive, European Data Protection Directive

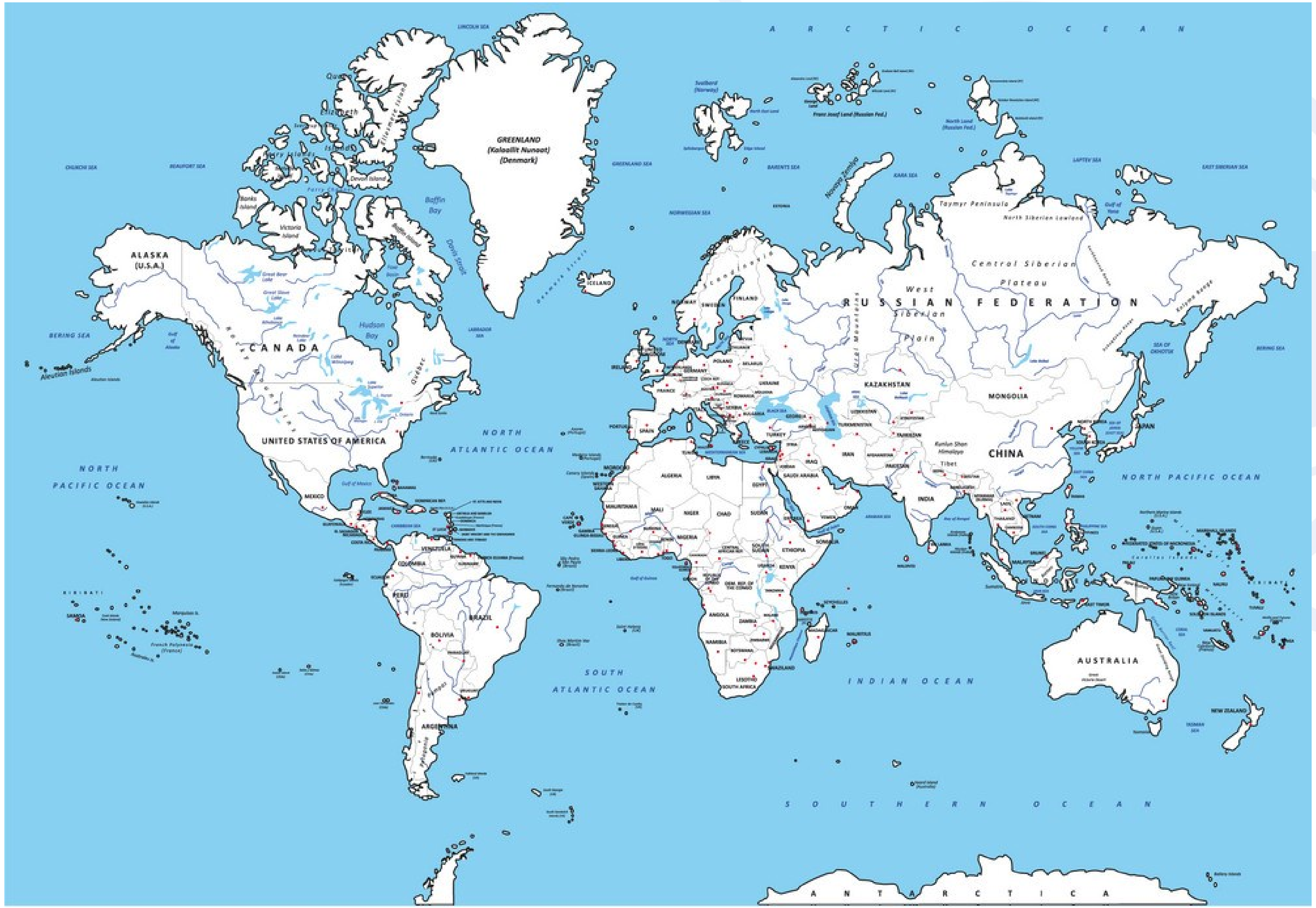
1997s
European Parliament “Project Echelon” report

2016
The EU General Data Protection Regulation(GDPR)

Data Privacy Laws

- Data Privacy Laws
- 120 Countries have data privacy Laws
- 2015-16 was a period of very significant progress for international data Privacy agreement Privacy

International Privacy Data Protection



- Law
- Definitions
- Authority
- Registration
- Date Protection Officer
- Transfer of Data
- Data Security
- Breach Notification
- Enforcement
- Electronic Marketing
- Online Privacy

Organization for economic co-operation and Development(OECD) Privacy Requirement

- Collection of Limited Principles
- Data quality Principle
- Purpose specific Principle
- Use limited principle
- Security Safe Guard Principle
- Openness Principle

EU General Data Protection Regulation

- Increased Territorial Scope
- Penalties
- Consent
- Data Subject Right

Important Note:

Even if you are not in Europe you could be prosecuted for violating GDPR laws you cannot use the data of European citizen from any part of the world

Privacy and Data Policy Compliance

- Legal Environment
  - Application Law
  - Jurisdiction Law
- Scope and purpose of the Processing
- Categories of the Personal Data to be processed

- Allowed hosting geographies
- Categories of users allowed
- Data retention Constraints
- Required Security Measures
- Data breach obligation Status

Contractual Obligations

- Numerous Contractual Obligation may apply for the protection of Personal Information.
- Required Data is only utilized or used in accordance with the way it was collected and to fulfill that function or task
- Information is not permitted to be shared or disseminated to entities or parties without the explicit permission of the data owner
- Right to have the information amended, Modified or deleted in accordance with data protection and privacy laws.
- Data controller retain responsibility of data passed to a data processor

Impediments

Restriction of Cross-Border Transfer

- Multiple laws and regulation do not allow information to be transferred across borders or to location where level of Privacy or Data Protection is deemed to be weaker that their current requirement

- Clarify Laws or Privacy bodies, prior to transfer or Agreement to transfer

International Legislation Conflict

- Cloud Computing introduces multiple legal challenges

- Inability to apply local laws to a global technology Offering.

- Lack of legal practitioners and professionals specializing in technology law

- A lot of body lawyers don’t understand cloud data law

WAY OUT OF THE IMPEDIMENT

Proposing Policy Framework In Data Handling

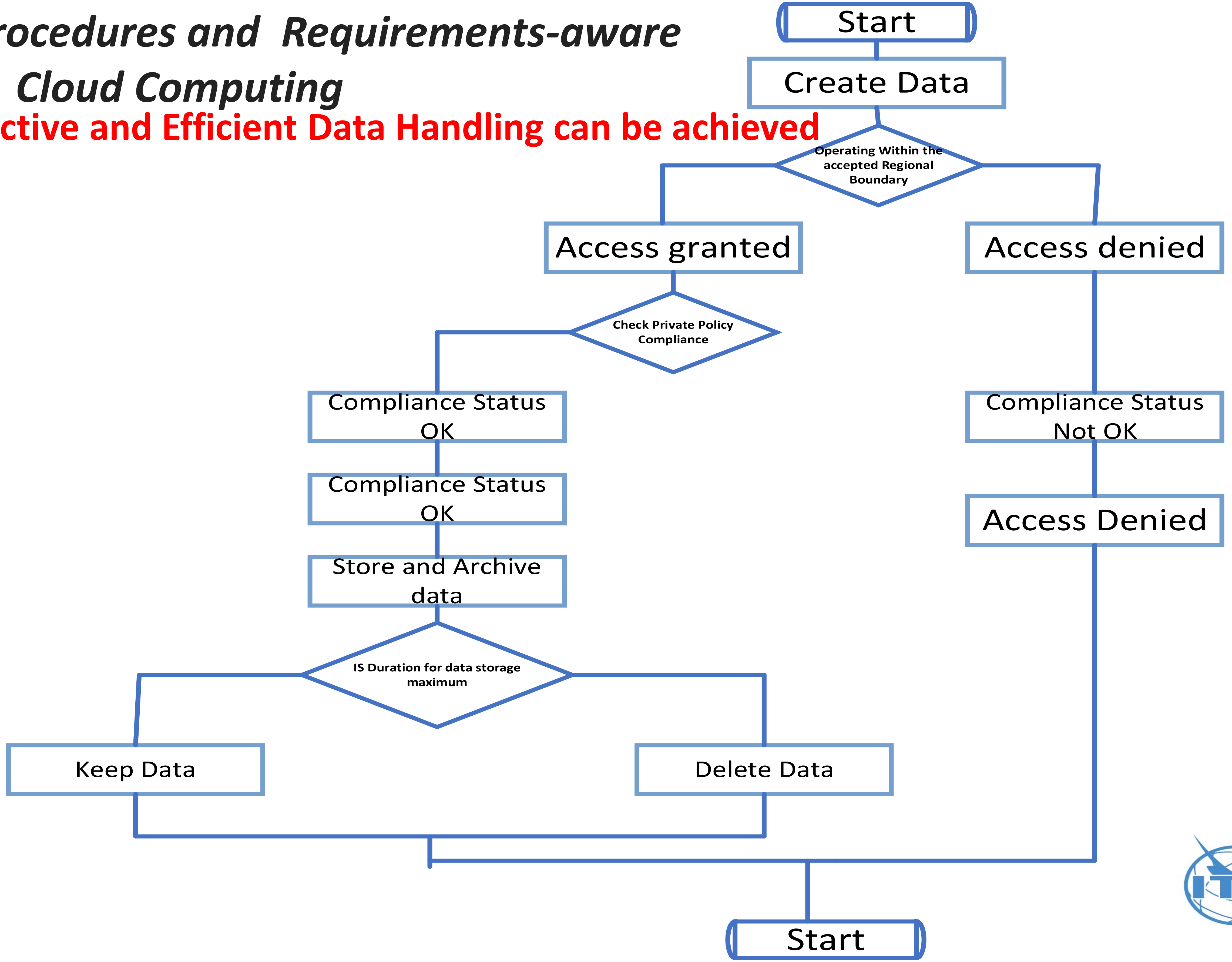
- A **policy framework** on how to harmonise other policies which will also sets out a set of procedures or goals, which might be used in negotiation or decision-making to guide a more detailed set of **policies**.

Legislation,Regulation, and Standards requirement

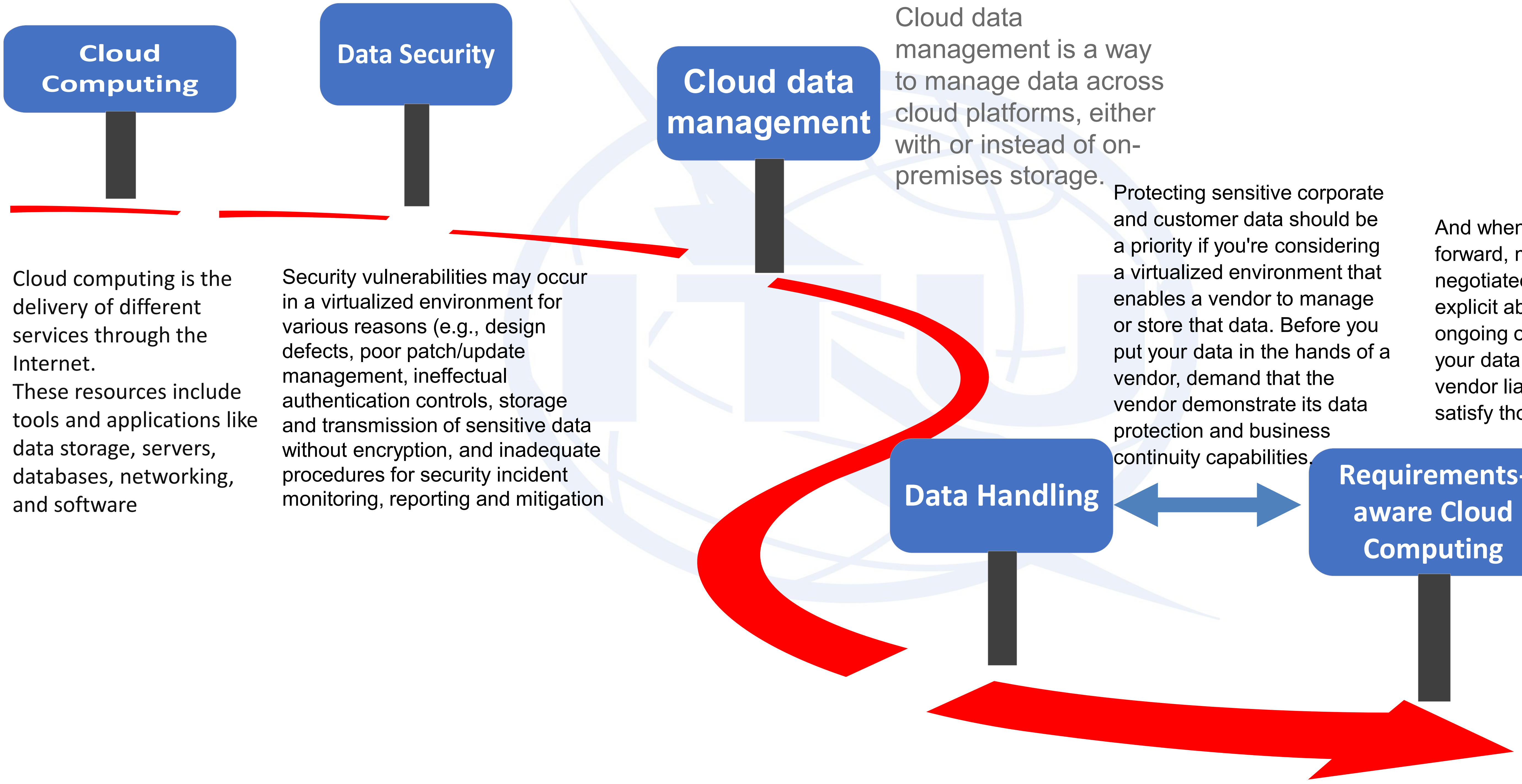
- Data Mapping
- Data classification
- Data retention procedure
- Monitoring and maintenance

Data Handling Procedures and Requirements-aware Cloud Computing

Flowchart on how Effective and Efficient Data Handling can be achieved



Cloud Computing Data Flow Process



Cloud Computing

Cloud computing is the delivery of different services through the Internet.
These resources include tools and applications like data storage, servers, databases, networking, and software

Data Security

Security vulnerabilities may occur in a virtualized environment for various reasons (e.g., design defects, poor patch/update management, ineffectual authentication controls, storage and transmission of sensitive data without encryption, and inadequate procedures for security incident monitoring, reporting and mitigation

Cloud data management

Cloud data management is a way to manage data across cloud platforms, either with or instead of on-premises storage.

Data Handling

Protecting sensitive corporate and customer data should be a priority if you're considering a virtualized environment that enables a vendor to manage or store that data. Before you put your data in the hands of a vendor, demand that the vendor demonstrate its data protection and business continuity capabilities.

Requirements-aware Cloud Computing

And when you decide to move forward, make sure that your negotiated agreement is explicit about the vendor's ongoing obligations to protect your data and holds the vendor liable for failure to satisfy those obligations.

National Institute of Standards and Technology

- Full name
- Email address
- Email address
- National identification number
- Password number
- IP address
- Vehicle registration plate number
- Driver’s license number
- Face, Fingerprint, or handwriting
- Credit card numbers
- Digital identity
- Birth Certificate
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Conclusion

- The paper enumerated the concept of Cloud Computing
- The work also try to answer the big question on Data Handling
- The paper evolved a flow process on how effective and efficient Data handling can be achieved

References

M. Henze, M. Großfengels, M. Koprowski, K. Wehrle, Towards Data Handling Requirements-aware Cloud Computing, IEEE 5th International Conference on Cloud Computing Technology and Science, 2013

[2] M. Henze, R. Matzutt, J. Hiller, E. M¨uhmer,J. H. Ziegeldorf, J. v. Giet, and K. W., Complying with Data Handling equirements in Cloud Storage Systems, IEEE Transactions on Cloud Computing,2020

[3] K. L. Jackson, Online webinar , Handling Cloud Computing Data Protection and Piracy Challenges, retrieve online https://www.youtube.com/watch?v=gSMzzDEyL2Q

[4] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow,"Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability," in Proc. ICIW,2009.

[5] N. Grozev and R. Buyya, "Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey," Software Pract Exper, 2012.

[6] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A Cloud Design for User-controlled Storage and Processing of Sensor Data," in Proc. IEEE CloudCom, 2012.

[7] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in Proc. IEEE CloudCom, 2010.

[8] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, 2012.

[9] H. Takabi, J. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security Privacy, vol. 8, no. 6, 2010.

[10] M. Henze, R. Hummen, R. Matzutt, D. Catrein, and K. Wehrle, "Maintaining User Control While Storing and Processing Sensor Data in the Cloud," IJGHPC, vol. 5, no. 4, 2013, in press.

[11] D. Bernstein and D. Vij, "Intercloud Security Considerations," in Proc. IEEE CloudCom, 2010.

[12] M. Henze, R. Hummen, and K. Wehrle, "The Cloud Needs Cross-Layer Data Handling Annotations," in Proc. IEEE SPW, 2013.

[13] J. Rosen, "The Right to Be Forgotten," Stan. L. Rev. Online, vol. 64, no. 88, 2012.

[14] ITU SG 13 Study group, Question 19, Future Networks: End-to-end management, governance, and security for computing including cloud computing and data handling, material retrieved online https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/q19.aspx, 2021

[15] ITU-T Technology Watch Report, Privacy in Cloud Computing retrieve online, https://www.itu.int/dms_pub/itut/oth/23/01/T23010000160001PDFE.pdf,2012