# Data Privacy Analysis in Cloud Services

## Seminar Kick-off

Nov 2, 2023

RuW 2.202
09:00 – 13:00

**Prof. Dr. Kai Rannenberg**
**Dr. Ahad Niknia**

seminar@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

# Agenda

- Organizational Information
- Introduction to Privacy and Cloud services
- Privacy Analysis in Cloud Services & Research Topics
- Questions

# Chair

## Chair of Business Administration, especially Business Informatics, Mobile Business and Multilateral Security

Chair of Mobile Business & Multilateral Security

Theodor-W.-Adorno-Platz 4
Campus Westend
RuW, 2nd Floor

| | |
|---|---|
| Phone: | +49 69 798 34701 |
| Fax: | +49 69 798 35004 |
| eMail: | info@m-chair.de |

www.m-chair.de

# Team & External PhD Students

Kai
Rannenberg

Narges
Arastouei

Diana
Weiss

Sascha
Löbner

Atiyeh
Sadeghi

Ann-Kristin
Lieberknecht

Frédéric
Tronnier

Ahad
Niknia

Peter
Hamm

Tim
Schiller

Michael
Schmid

Christopher
Schmitz

# Selected Alumni

**Prof. Dr. Jan Muntermann**
*Göttingen University*

**Dr. Stefan Figge**
*BuyIn (Deutsche Telekom / Orange)*

**Dr. Mike Radmacher**
*Deutsche Telekom*

**Dr. Andreas Albers**
*Deutsche Telekom*

**Dr. Stefan Weiss**
*Swiss Re*

**Prof. Dr. Denis Royer**
*Ostfalia - Hochschule für angewandte Wissenschaften*

**Dr. Markus Tschersich**
*Continental*

**Dr. Ahmad Sabouri**
*Continental*

**Dr. Falk Wagner**
*EE*

**Dr. Christian Kahl**
*CyberSolutions GmbH*

**Dr. Gökhan Bal**
*Deutsche Bahn*

**Dr. André Deuker**
*KfW*

**Dr. Shuzhe Yang**
*GLS*

**Dr. Ahmed Yesuf**
*FARO*

**Dr. Welderufael Tesfay**
*Deutsche Telekom*

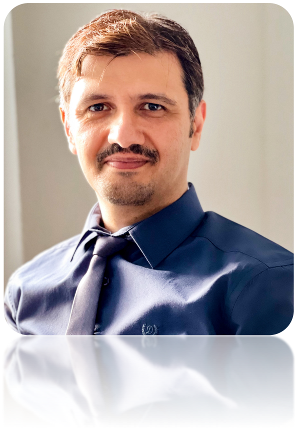
**Dr. Fatbardh Veseli**
*Capgemini Germany*

**Dr. Majid Hatamian**
*Google*

**Dr. habil. Sebastian Pape**
*Continental*

**Dr. *David Harborth***
*Capgemini Invent*

# Supervisor



**Dr. Ahad Niknia,**
Ph.D of Computer Science

**Research Interests**

- Cloud Privacy Analysis and Management
- Cloud Security and Dependability
- Cryptography and Applied Cryptography
- Security and Privacy
  - Domains
  - Emerging Applications
  - Standardization
  - Evaluation and certification

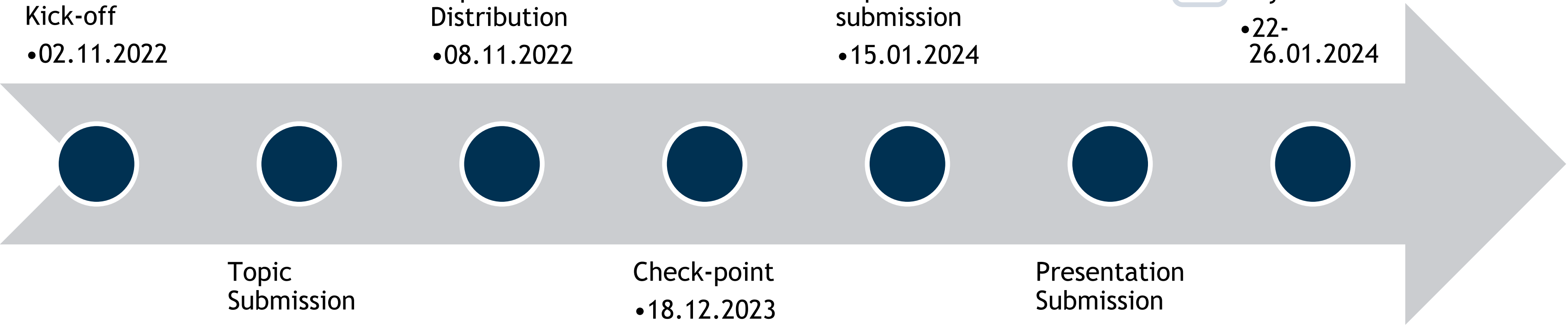
RuW Building, Office 2.232,
Email: ahad.niknia@m-chair.de

Contact: Seminar@m-chair.de

# Students

**Tell me abut Yourself ☺**

# Process



Kick-off
- 02.11.2022

Topic Submission
- 06.11.2022

Topic Distribution
- 08.11.2022

Check-point
- 18.12.2023 14:00

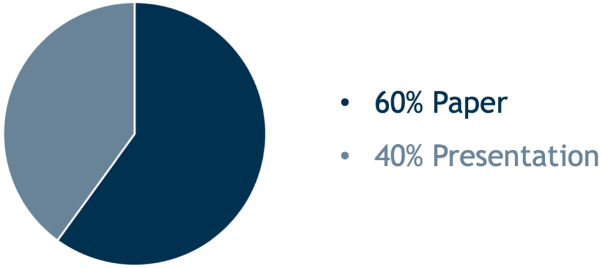
Paper submission
- 15.01.2024

Presentation Submission
- 19.01.2024

⚠ Presentation Days
- 22-26.01.2024

This seminar consists of two administrative parts:

- Participation in both parts is required for successful completion of Seminar.
- The work is evaluated on an individual basis.



# Formal requirements

- For the paper, the formal requirements of the chair apply.
  - Please use the provided word template (or LaTeX)
  - Use the APA American Psychology Association style for citations
  - 10 pages text are recommended (excluding cover, table of contents, references, etc.)

# Submission

- The seminar papers must be submitted in **electronic form** in the following format:
  - Ms-word/OpenOffive/LaTeX.zip AND
  - Adobe PDF (Make sure that the file can be opened with Adobe PDF Reader )

  via E-Mail to: seminar@m-chair.de

- The PDF file should include the statutory declaration with **your scanned signature**

- Submission until 15th Jan 2024

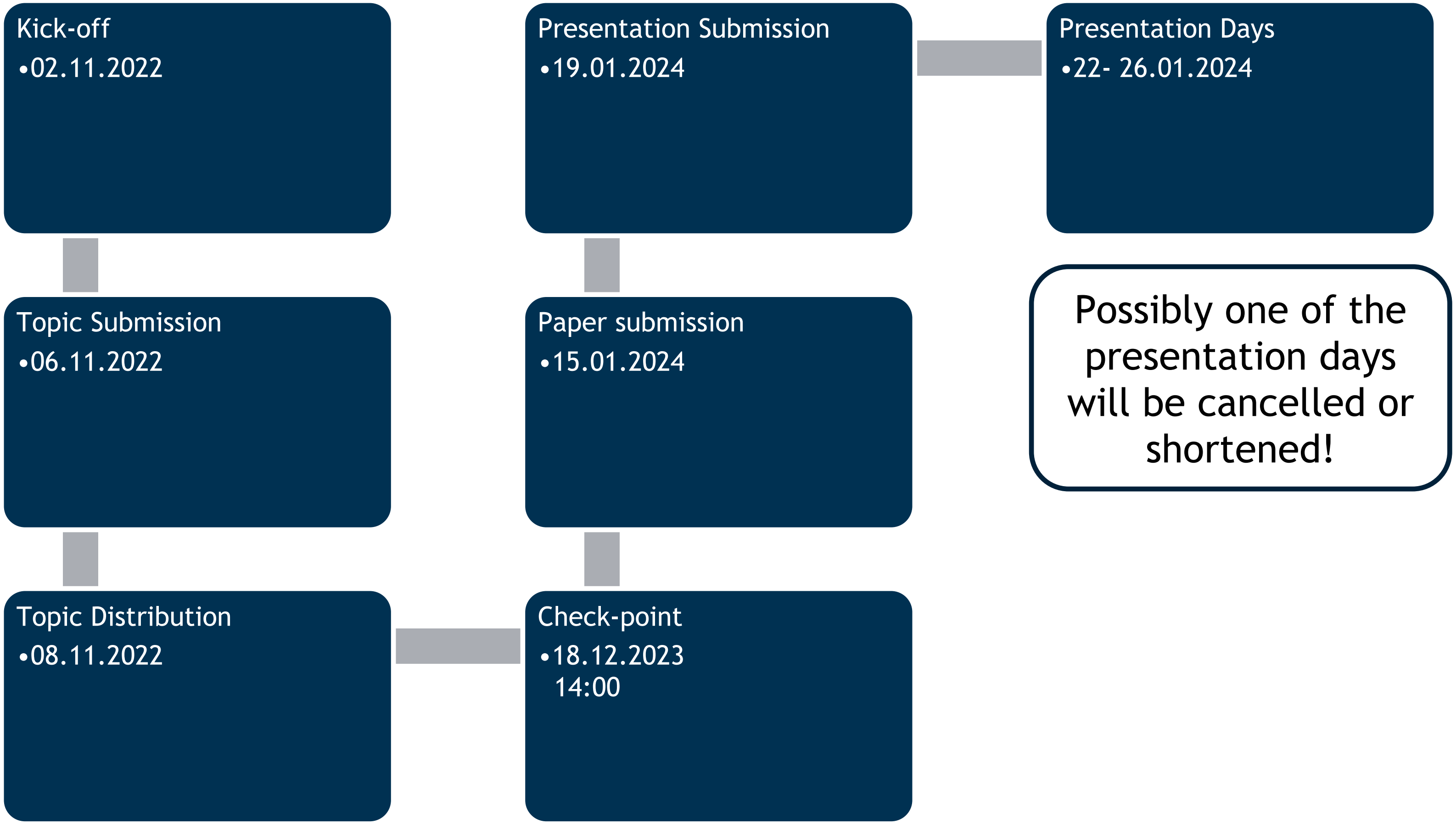
# Formal requirements for presentations

- Seminar presentation:
  - Duration: 15 min. at most
  - Following discussion: 15 min

- Each presentation is assigned a moderator
  - Responsible for the first question
  - Moderating the discussion

- Submission until 19th Jan 2024
  - PDF or PPTX
  - Email to seminar@m-chair.de

# Important dates



Kick-off
- 02.11.2022

Topic Submission
- 06.11.2022

Topic Distribution
- 08.11.2022

Check-point
- 18.12.2023
  14:00

Paper submission
- 15.01.2024

Presentation Submission
- 19.01.2024

Presentation Days
- 22- 26.01.2024

Possibly one of the presentation days will be cancelled or shortened!

# Contact

In case of any questions or problems arise during the seminar you can contact: seminar@m-chair.de

For comprehensive questions please make an appointment for your topic: (send questions/topics beforehand)

- Ahad.niknia@m-chair.de

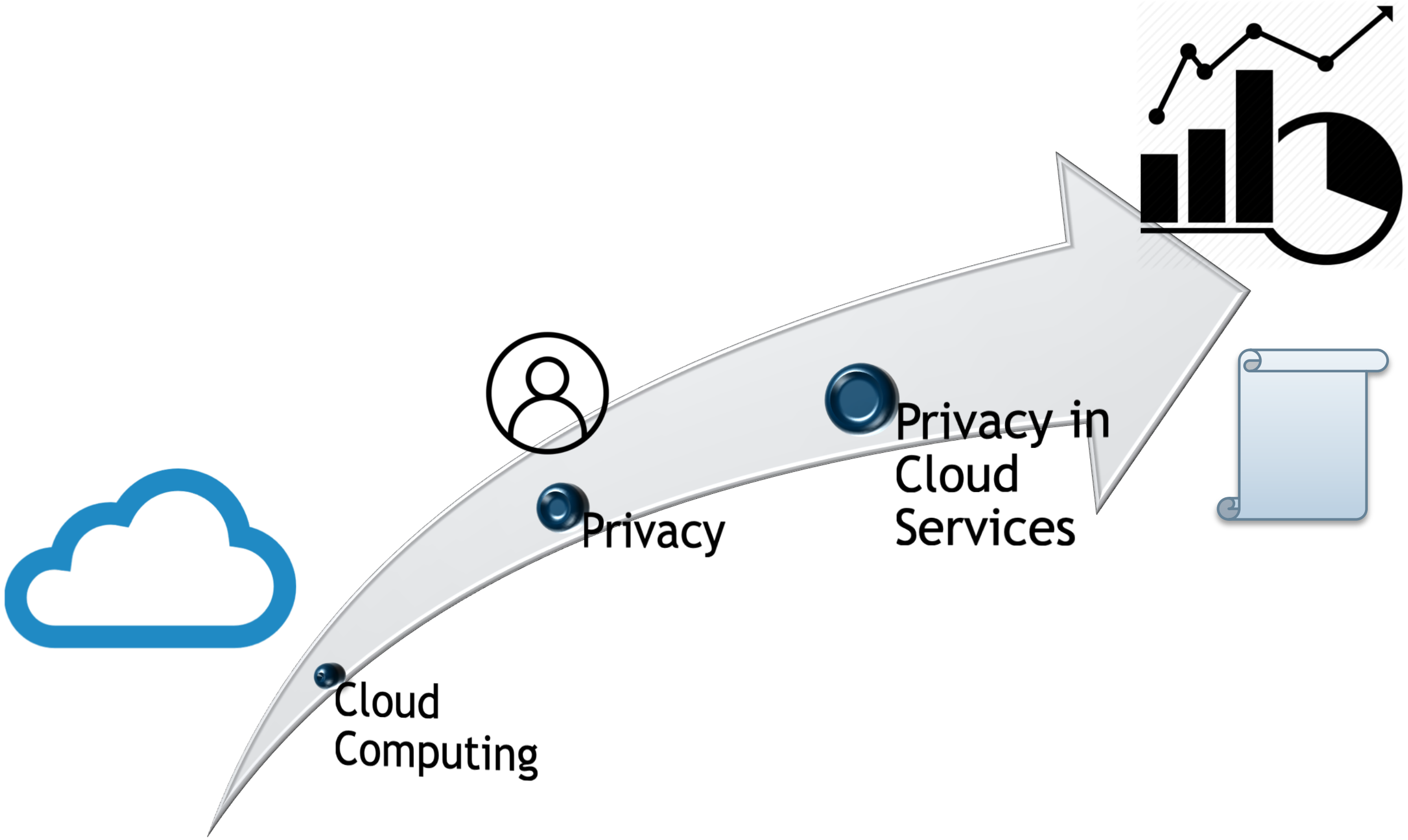
# Agenda

- Organizational Information
- Introduction to Privacy and Cloud Services
  - Outline
  - Motivation
  - Privacy & Cloud Services
- Privacy Analysis in Cloud Services & Research Topics
- Questions

# Cloud Services and Privacy

Introduction to Privacy and Cloud services

Outline



Cloud Computing

Privacy

Privacy in Cloud Services

# Cloud Services and Privacy

Introduction to Privacy and Cloud services

1- Cloud Computing, some examples

| | |
|---|---|
| **Applications** | Docs Sheets Slides<br>ZOHO Work · Online<br>EVERNOTE |
| **Storage** | Your stuff, anywhere<br>box |
| **Computing** | amazon web services<br>rackspace the open cloud company |
| **Development platform** | Windows Azure<br>salesforce force.com |

[1]

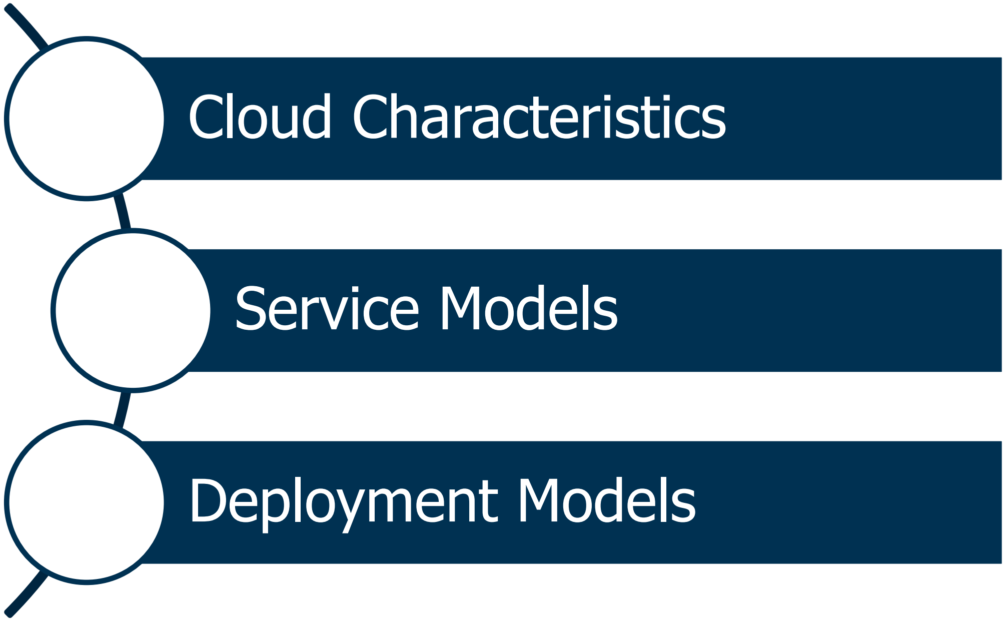
# Cloud Services and Privacy

## Introduction to Privacy and Cloud services

## 1- Cloud Computing, basics

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services).

[10,11]



Cloud Characteristics

Service Models

Deployment Models

# Cloud Services and Privacy

## Introduction to Privacy and Cloud services

### 1- Cloud Computing, basics

**Cloud Characteristics**

- On-Demand Self Service
- Broad Network Access
- Resource Pooling
- Measured Service
- rapid elasticity or expansion

[11]

# Cloud Services and Privacy

Introduction to Privacy and Cloud services
1- Cloud Computing, basics

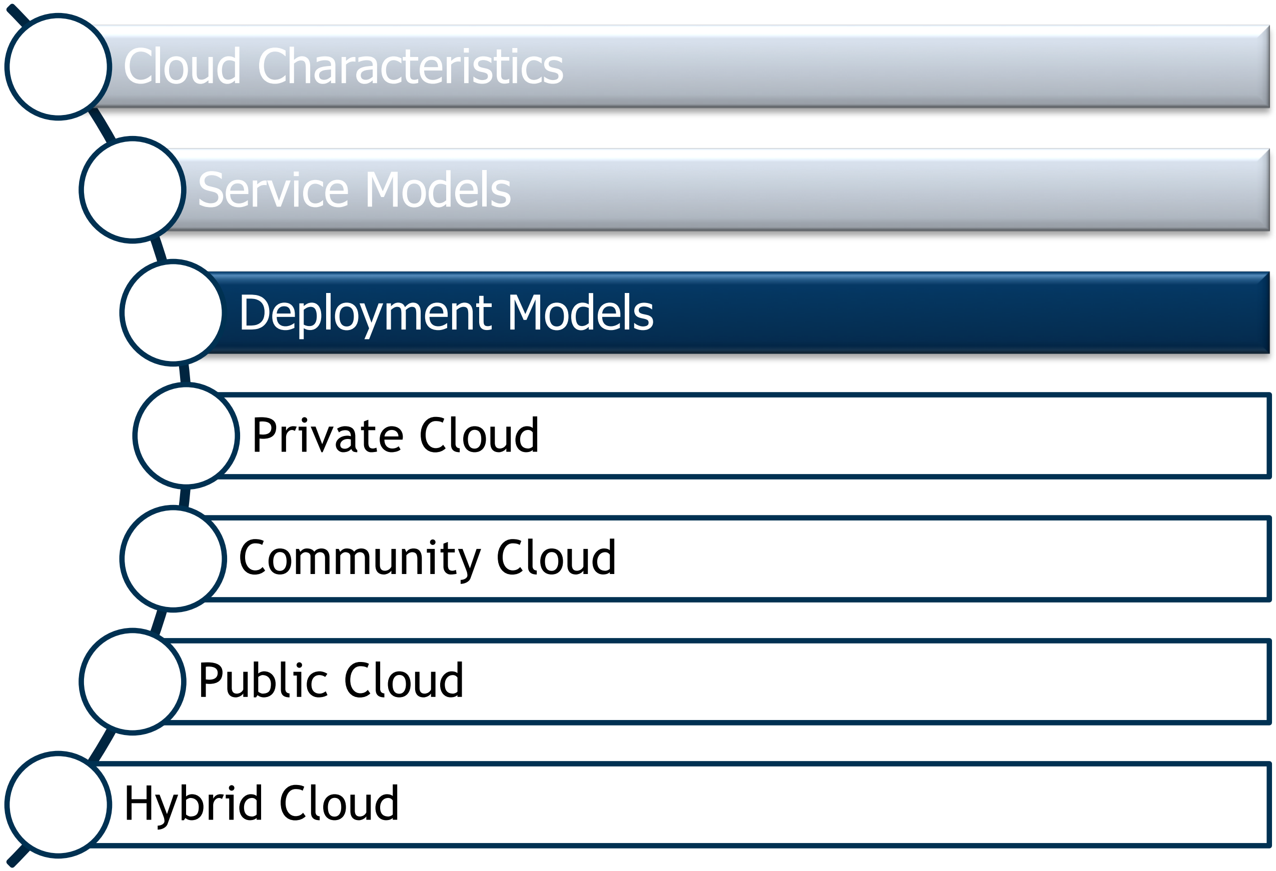
- Cloud Characteristics
- **Service Models**
  - Software as a Service (**SaaS**)
  - Platform as a Service (**PaaS**)
  - Infrastructure as a Service (**IaaS**)
- Deployment Models

[11]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud services

### 1- Cloud Computing, basics



Cloud Characteristics

Service Models

Deployment Models

Private Cloud

Community Cloud

Public Cloud

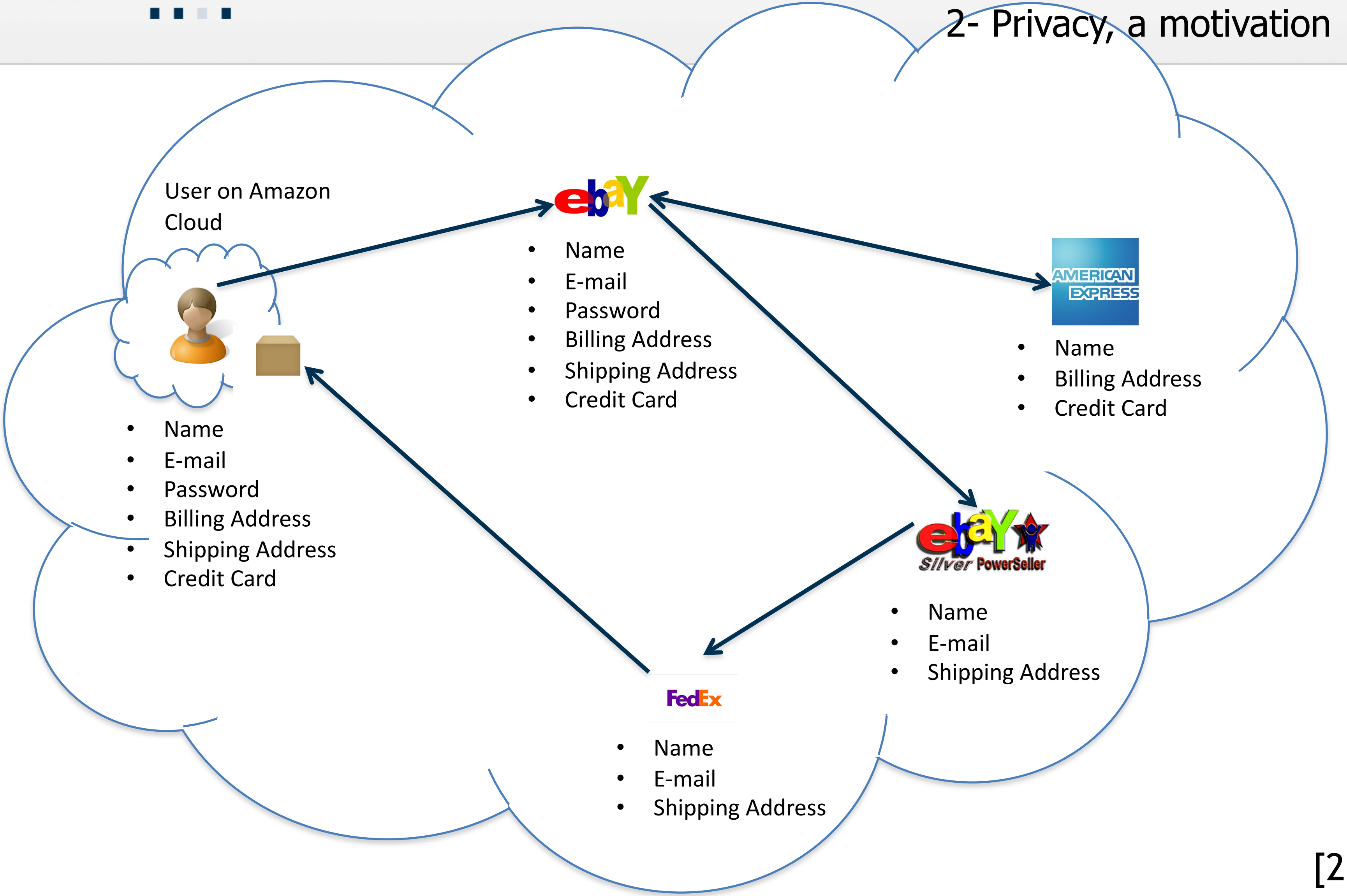
Hybrid Cloud

[11]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud services

## 2- Privacy, a motivation



User on Amazon Cloud

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- Name
- Billing Address
- Credit Card

- Name
- E-mail
- Shipping Address

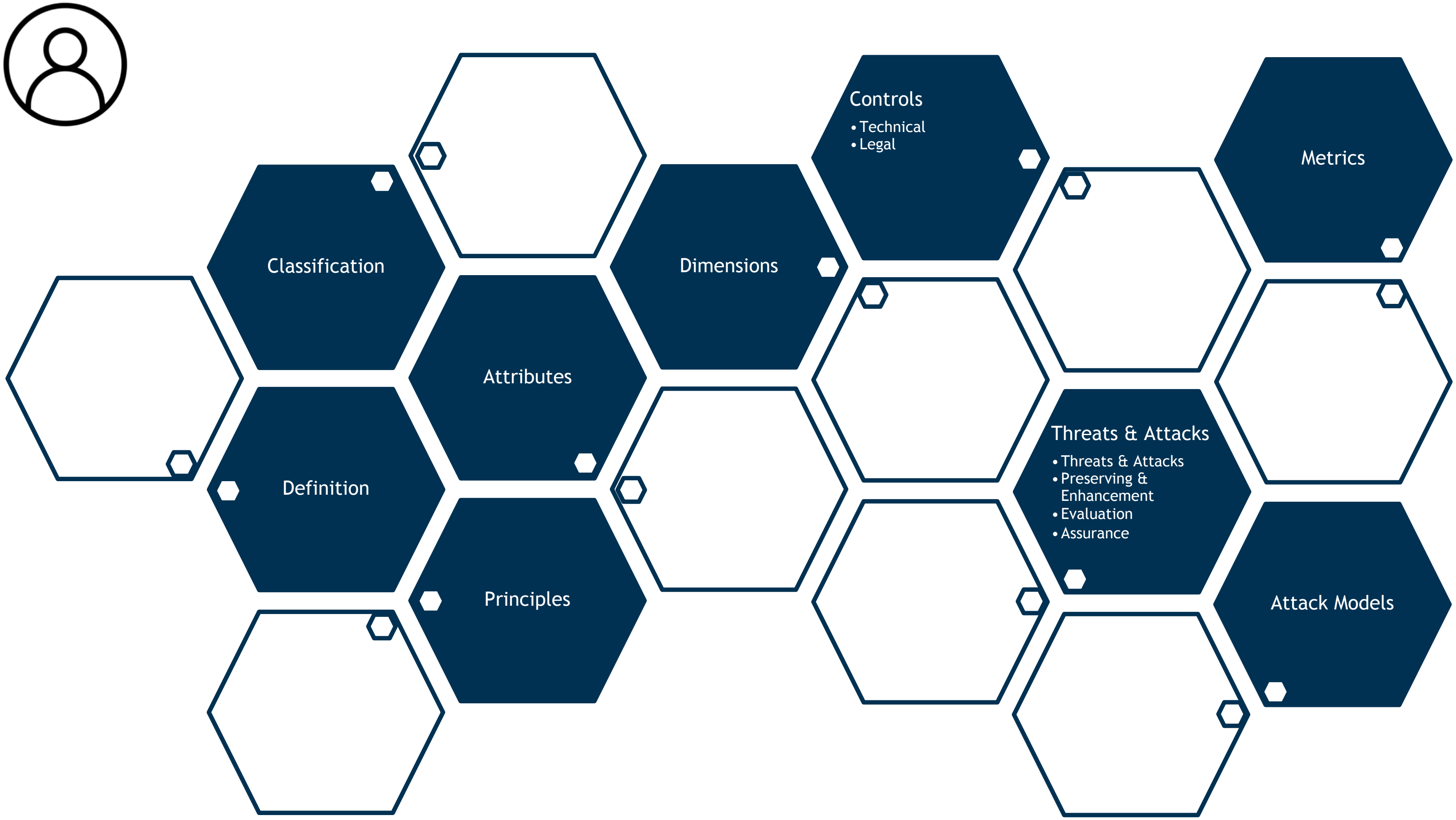
- Name
- E-mail
- Shipping Address

[2]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud services

## 2- Privacy

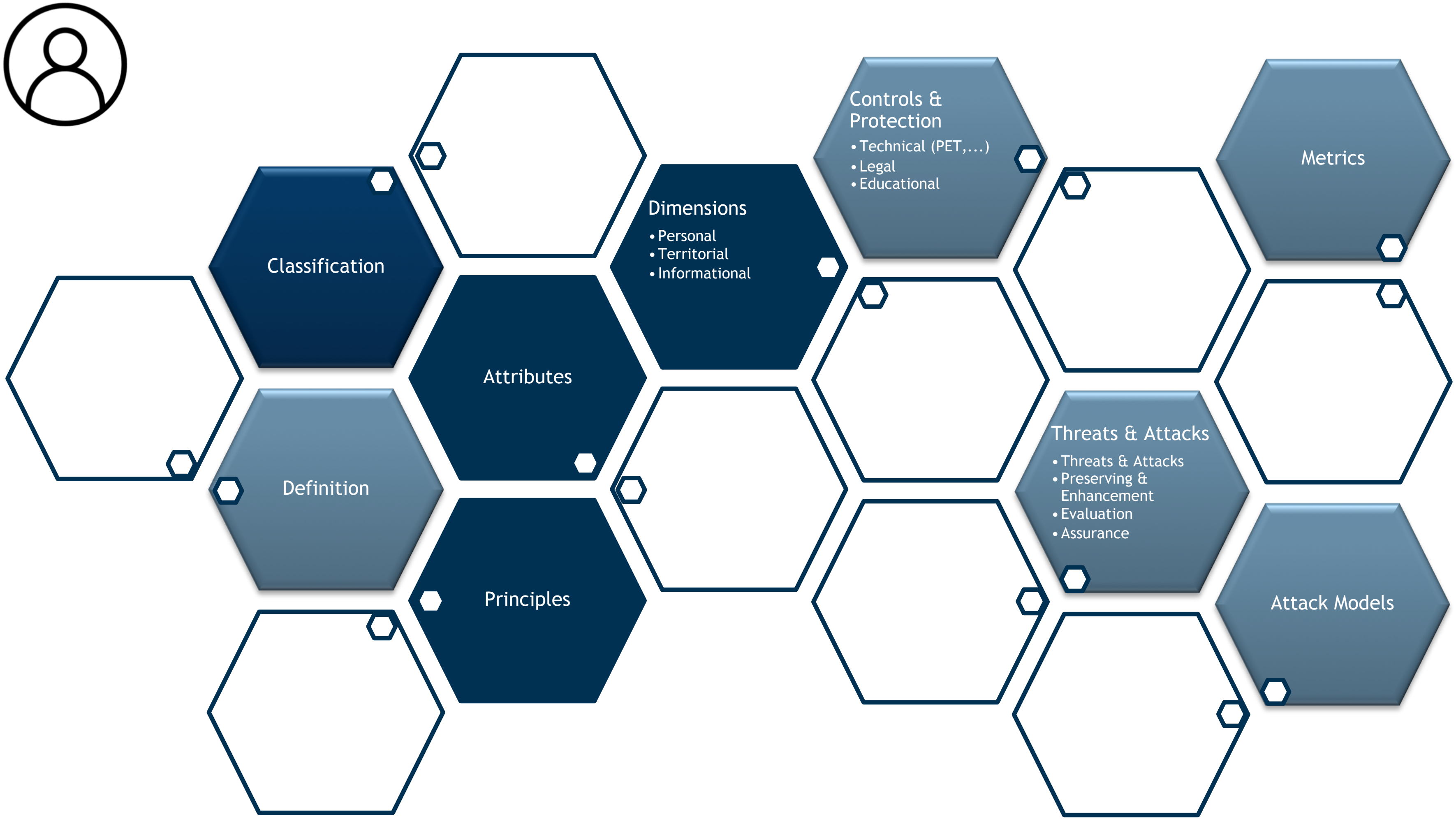


[2,3,4,5]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services



Controls & Protection

- Technical (PET,...)
- Legal
- Educational

Metrics

Classification

Dimensions

- Personal
- Territorial
- Informational

Attributes

Threats & Attacks

- Threats & Attacks
- Preserving & Enhancement
- Evaluation
- Assurance

Definition

Principles

Attack Models

[2,3,4,5]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services

the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others

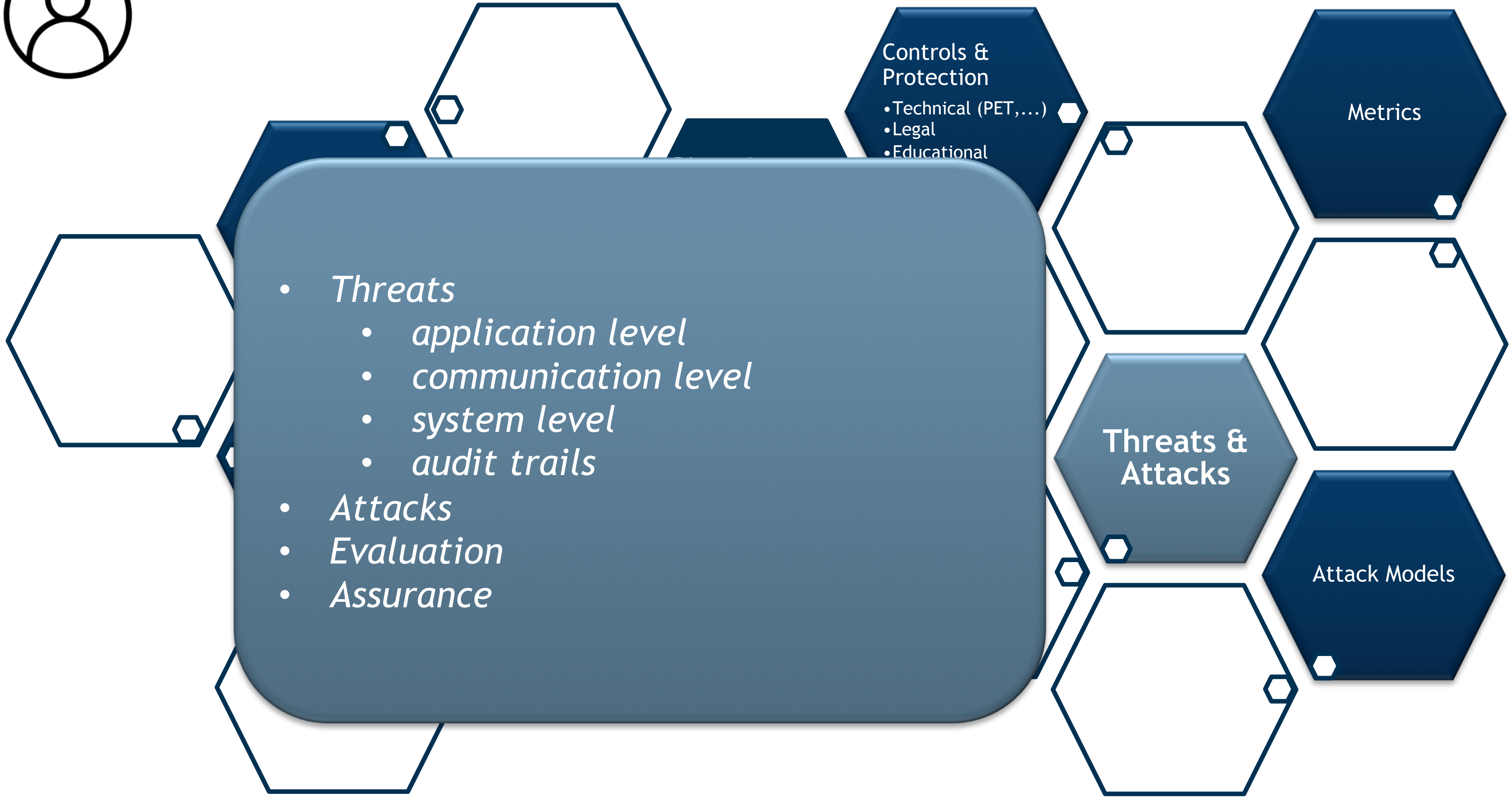
*International Organization for Standardization* (ISO), defines an attack as an ‘‘attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of anything that has value’’

[2,3,4,5,6]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services



Controls & Protection
- Technical (PET,...)
- Legal
- Educational

Metrics

Threats & Attacks

Attack Models

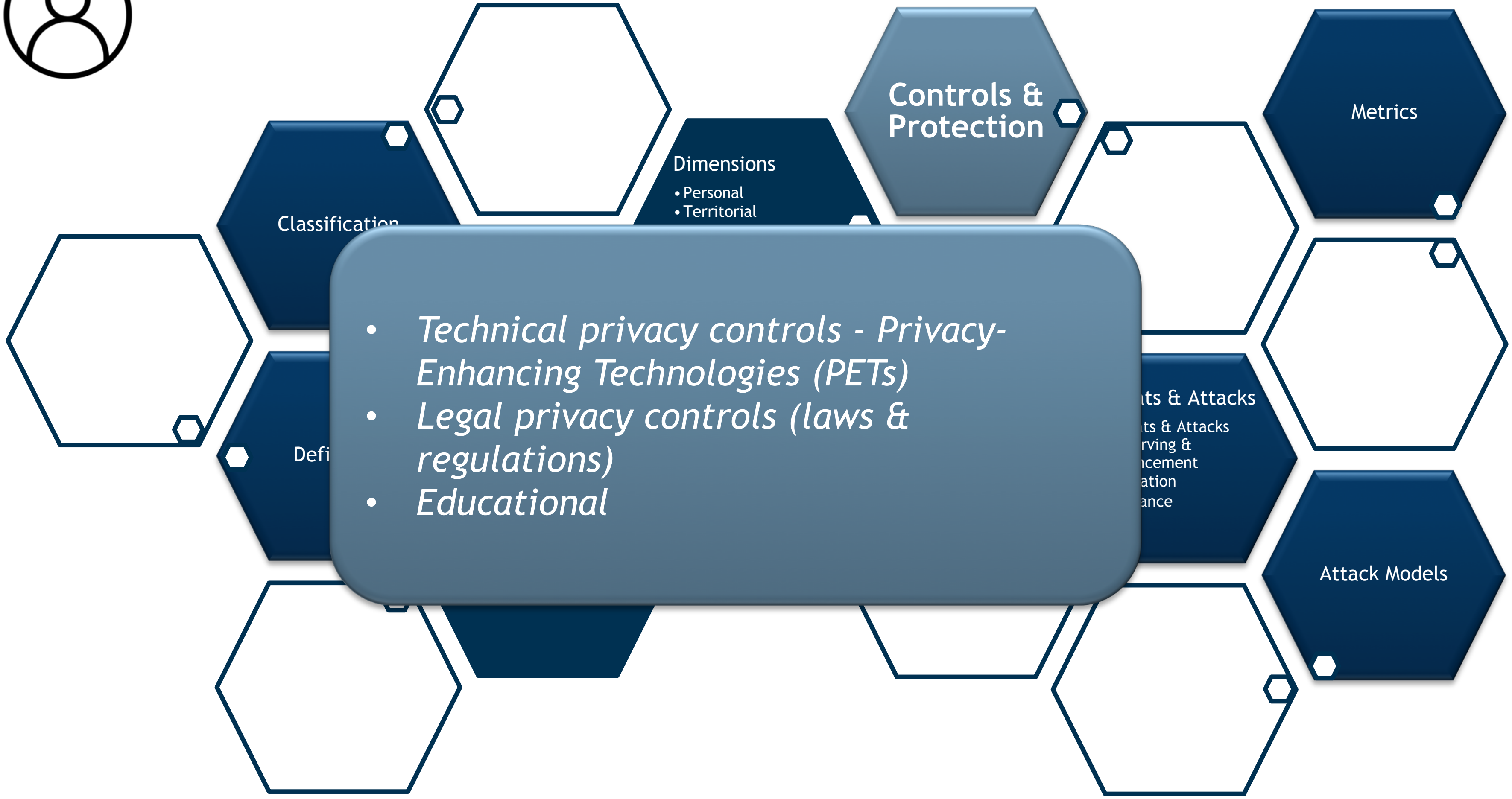
- *Threats*
  - *application level*
  - *communication level*
  - *system level*
  - *audit trails*
- *Attacks*
- *Evaluation*
- *Assurance*

[2,3,4,5]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services



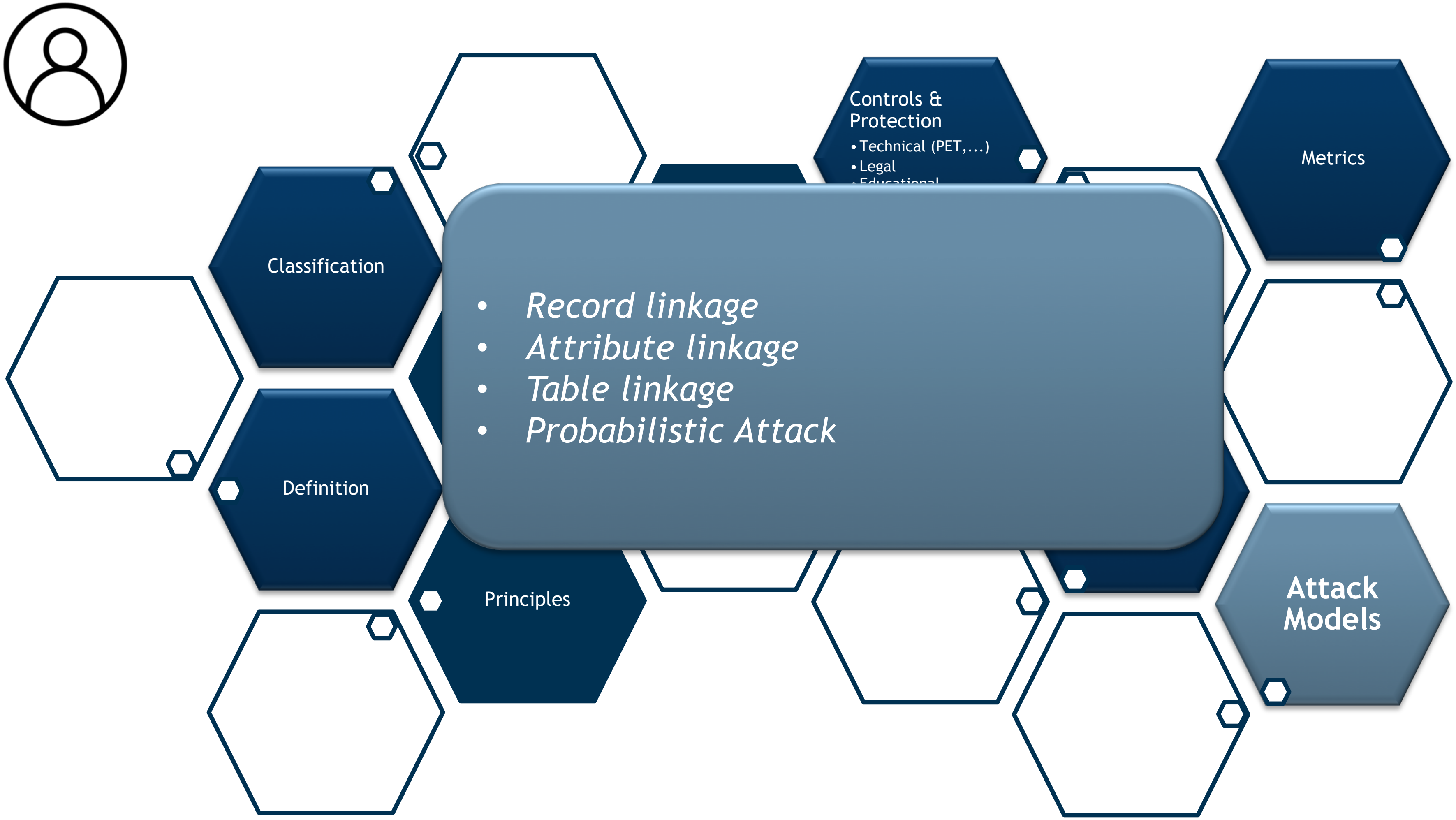
- *Technical privacy controls - Privacy-Enhancing Technologies (PETs)*
- *Legal privacy controls (laws & regulations)*
- *Educational*

[2,3,4,5]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services



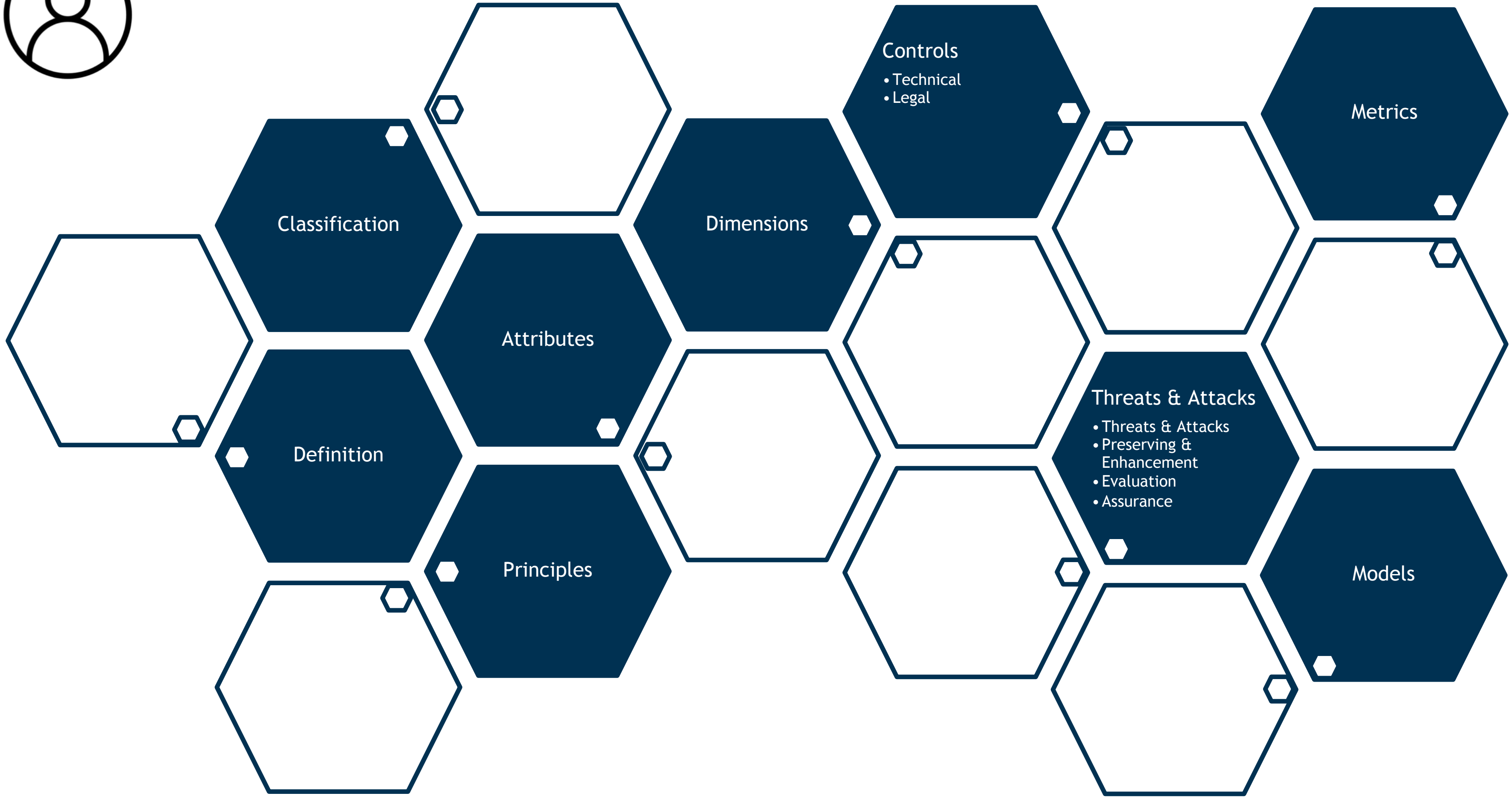
- *Record linkage*
- *Attribute linkage*
- *Table linkage*
- *Probabilistic Attack*

[2,3,4,5,8,9]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy, Attack & Cloud Services

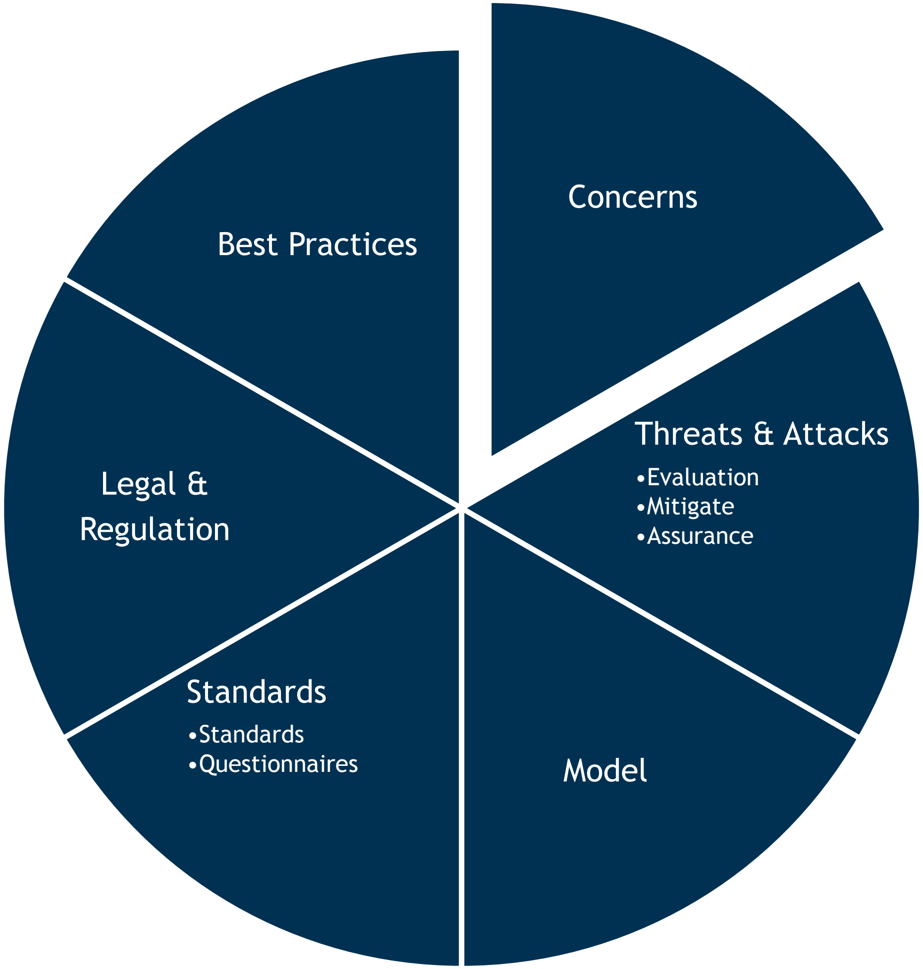


[2,3,4,5]

# Cloud Services and Privacy

## Introduction to Privacy and Cloud Services

## 3- Privacy & Cloud Services, our point of view



# Agenda

- Organizational Information
- Introduction to Privacy and Cloud services
- **Privacy Analysis in Cloud Services & Research Topics**
- Questions

# Prospective Research Areas

Standards and methods
Regulations

Privacy preserving & Enhancement

Assurance methods

Privacy threats

Best practices

Privacy concerns

Privacy evaluation

Economic incentives

# Seminar Topics

I. Literature review on “data privacy; definitions, principles and standards (with respect to the cloud services)”
II. Review on privacy analysis, measuring and evaluation methods
III. Literature review on the cloud data models
IV. Literature review on “Privacy concerns in cloud services”
V. Literature review on privacy threats and risks modelling with respect to the cloud systems
VI. Systematic review on “Privacy-preserving and enhancement methods (with respect to the cloud services)”
VII. Systematic review on “Privacy by design in cloud services”
VIII. Literature review on the “assurance methods for privacy threats”
IX. Privacy in cloud service providers’ regulations, a review and best practices

Please check our website for more and updated information…

Send list of your preferred topics (2-3 topic) by the end of 06.11.2022.

# Agenda

- Organizational Information
- Privacy Analysis in Cloud Services & Research Areas
- Questions ?

Link

# References

[1] Rao A., (2013). Security and Privacy in the Age of Cloud Computing (lecture slides)

[2] Ranchal R,, Bhargava B., Angin P., Singh N., Othmane L.B., & Lilien L. (2017). Privacy and Identity Management in Cloud (lecture slides)

[3] Bhargava B.,Zhong Y., & Lilien L. (2015). Introduction to Privacy in Computing (lecture slides)

[4] Simone Fischer-Hübner, "IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms", Springer Scientific Publishers, Lecture Notes of Computer Science, LNCS 1958, May 2001, ISBN 3-540-42142-4.

[5] Simone Fischer-Hübner, "Privacy Enhancing Technologies, PhD course," Session 1 and 2, Department of Computer Science, Karlstad University, Winter/Spring 2003

[6] Plastics—Determination of Fracture Toughness—Linear Elastic Fracture Mechanics (LEFM) Approach, International Organization for Standardization, Geneva, CH, Standard, Sep. 2009. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO _IE%C_27000_2009.zip

[7] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," ACM Comput. Surv., vol. 51, no. 3, pp. 1–38, Jun. 2018, doi: 10.1145/3168389.

[8] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Comput. Surv., vol. 42, no. 4, pp. 14:1–14:53, Jun. 2010, doi: 10.1145/1749603.1749605

[9] SILVA P., MONTEIRO E., and SIMÕES P. (2021). Privacy in the Cloud: A Survey of Existing Solutions and Research Challenges, (IEE Access, 2021, pp. 10473-10497

[10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. (2009).

[11] P. Mell, and T. Grance. 800-145. National Institute of Standards and Technology (NIST), Gaithersburg, MD, (September 2011)

# Supporting Information
# Data Protection and Privacy

## 1 Introduction to Privacy and Data Protection

- Introduction
- Legal aspects
- User aspects
- Technical aspects

# Data Protection and Privacy

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
  - Data protection is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - Privacy is the right to be left alone, e.g. to be unwatched or anonymous [WaBr1980]

# Introduction I

- Early day definitions: “The right to be let alone” Warren and Brandeis, 1890, Harvard Law Review: “The right to privacy” [WaBr1890]
- Beginning of information age: “The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Westin, 1967.

- Westin’s index
  - Privacy fundamentalists
  - Privacy pragmatists
  - Privacy unconcerned

Source: https://pixabay.com/es/de-distancia-junction-direcci%C3%B3n-1020088/

# Introduction II

- Contemporary: **It is complex.**
  - "The ability of the individual to protect information about [herself]" Goldberg et. al 1997

- Personal information: "Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly "

Source: https://pixabay.com/es/icono-la-cabeza-ver-el-perfil-1247948/

# Supporting Information
# Data Protection and Privacy

1

## Introduction to Privacy and Data Protection

- Introduction
- Legal aspects
- User aspects
- Technical aspects

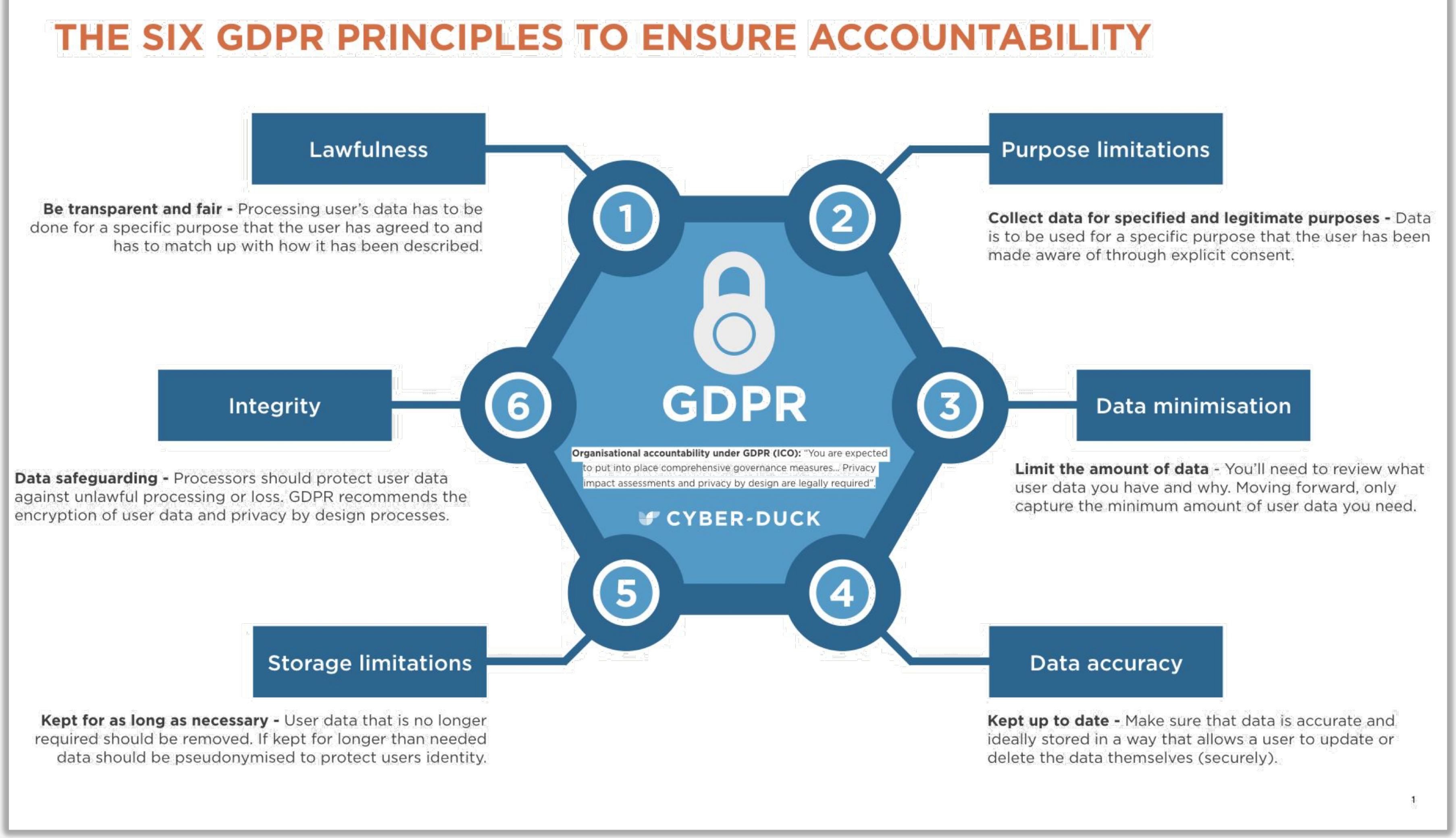
# General Data Protection Regulation (GDPR)

- Entered into force on 24 May 2016 and applies since 25 May 2018.

- The European Commission says that the recently approved regulation “puts the citizens back in control of their data, notably through”:
  - **A right to be forgotten** - Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - **Data security:** Personal data that is “any information relating to an identified or identifiable natural person” (GDPR article 4) has to be protected against loss, damage and unauthorized processing

[GDPR 2016]

# General Data Protection Regulation (GDPR)



## THE SIX GDPR PRINCIPLES TO ENSURE ACCOUNTABILITY

**Lawfulness**

**Be transparent and fair -** Processing user's data has to be done for a specific purpose that the user has agreed to and has to match up with how it has been described.

**Purpose limitations**

**Collect data for specified and legitimate purposes -** Data is to be used for a specific purpose that the user has been made aware of through explicit consent.

**Data minimisation**

**Limit the amount of data** - You'll need to review what user data you have and why. Moving forward, only capture the minimum amount of user data you need.

**Data accuracy**

**Kept up to date -** Make sure that data is accurate and ideally stored in a way that allows a user to update or delete the data themselves (securely).

**Storage limitations**

**Kept for as long as necessary -** User data that is no longer required should be removed. If kept for longer than needed data should be pseudonymised to protect users identity.

**Integrity**

**Data safeguarding -** Processors should protect user data against unlawful processing or loss. GDPR recommends the encryption of user data and privacy by design processes.

**Organisational accountability under GDPR (ICO):** "You are expected to put into place comprehensive governance measures... Privacy impact assessments and privacy by design are legally required".

1

# Law Alone is not Sufficient

- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of 'privacy' policy (e.g. selling privacy for "peanuts").

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

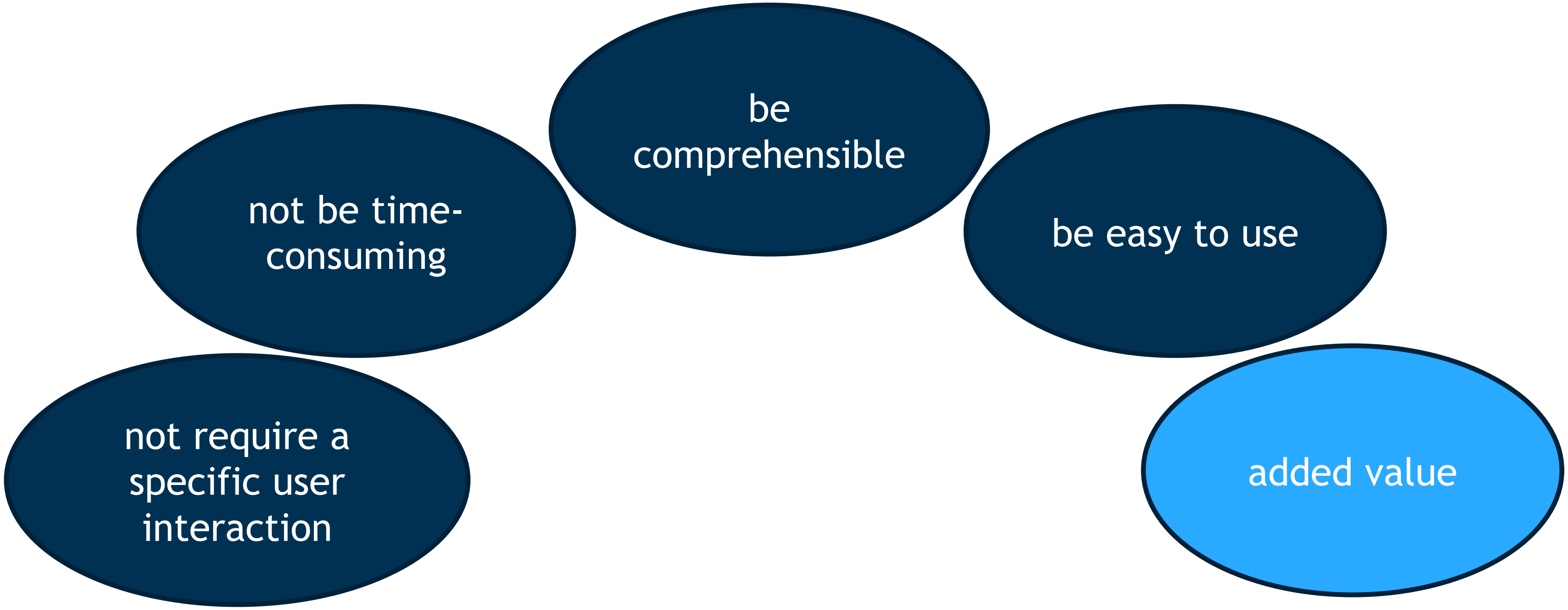
# Supporting Information Data Protection and Privacy

## 1 Introduction to Privacy and Data Protection

- Introduction
- Legal aspects
- User aspects
- Technical aspects

# User awareness

- User awareness (transparency)
- Solution should:



be comprehensible

not be time-consuming

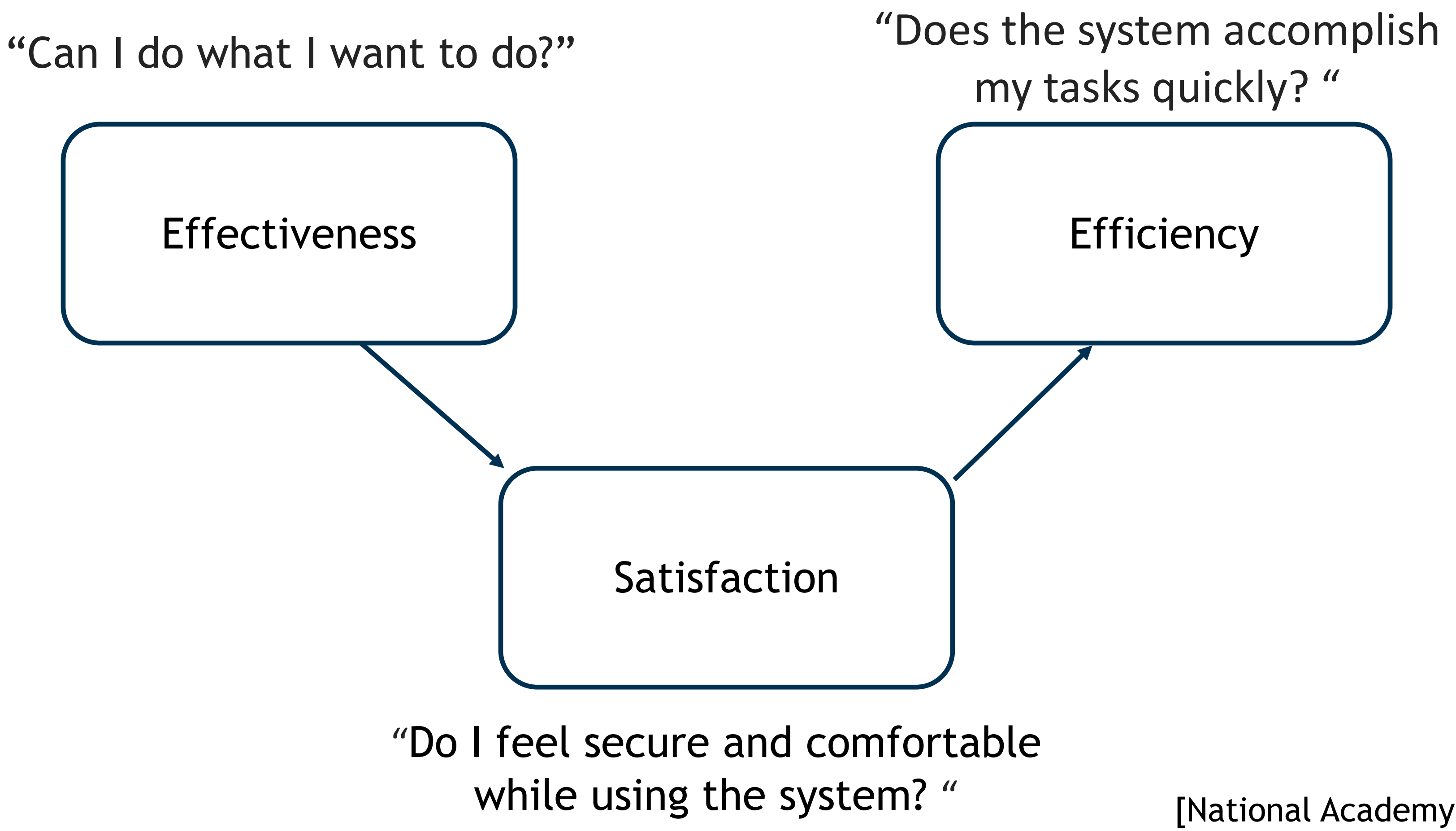
be easy to use

not require a specific user interaction

added value

[Danezis2014]

# Usability


“Can I do what I want to do?”
Effectiveness
“Does the system accomplish my tasks quickly? “
Efficiency
Satisfaction
“Do I feel secure and comfortable while using the system? “

[National Academy2010]

# Supporting Information
# Data Protection and Privacy

## 1 Introduction to Privacy and Data Protection

- Introduction
- Legal aspects
- User aspects
- Technical aspects

# Technical Aspects of Privacy

A. Privacy by design

B. Privacy engineering

C. Privacy enhancing technologies

Source: https://pixabay.com/es/humanos-siluetas-redes-internet-1157116/

# A. Privacy by design

- Refers to the notion of embedding privacy directly into the design of ITs and systems
- Adopted as one essential principle in the GDPR.

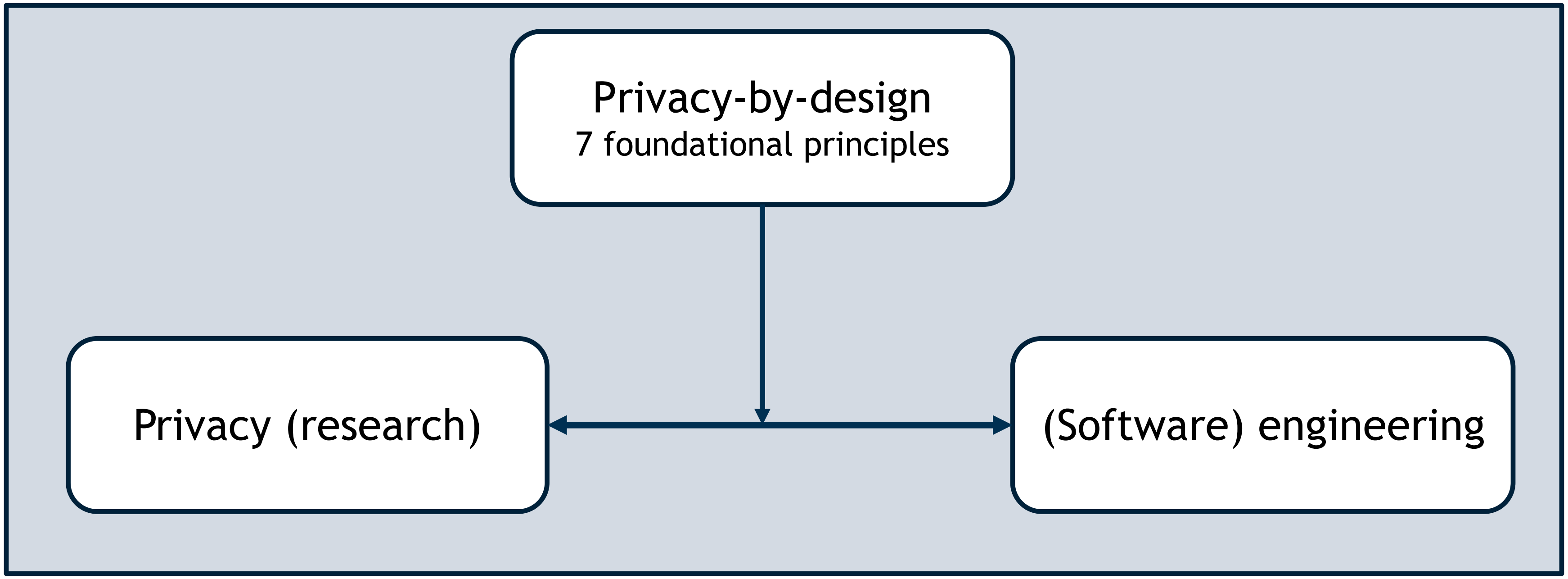
[Cavoukian2010]

## 7 foundational principles

- Proactive not reactive
- Privacy as the Default setting
- Privacy Embedded into the Design
- Full Functionality
- End-to-End Security
- Visibility and Transparency
- Respect for User Privacy

# B. Privacy engineering I

- Connection between research and practice (privacy and software engineering)



Privacy-by-design
7 foundational principles

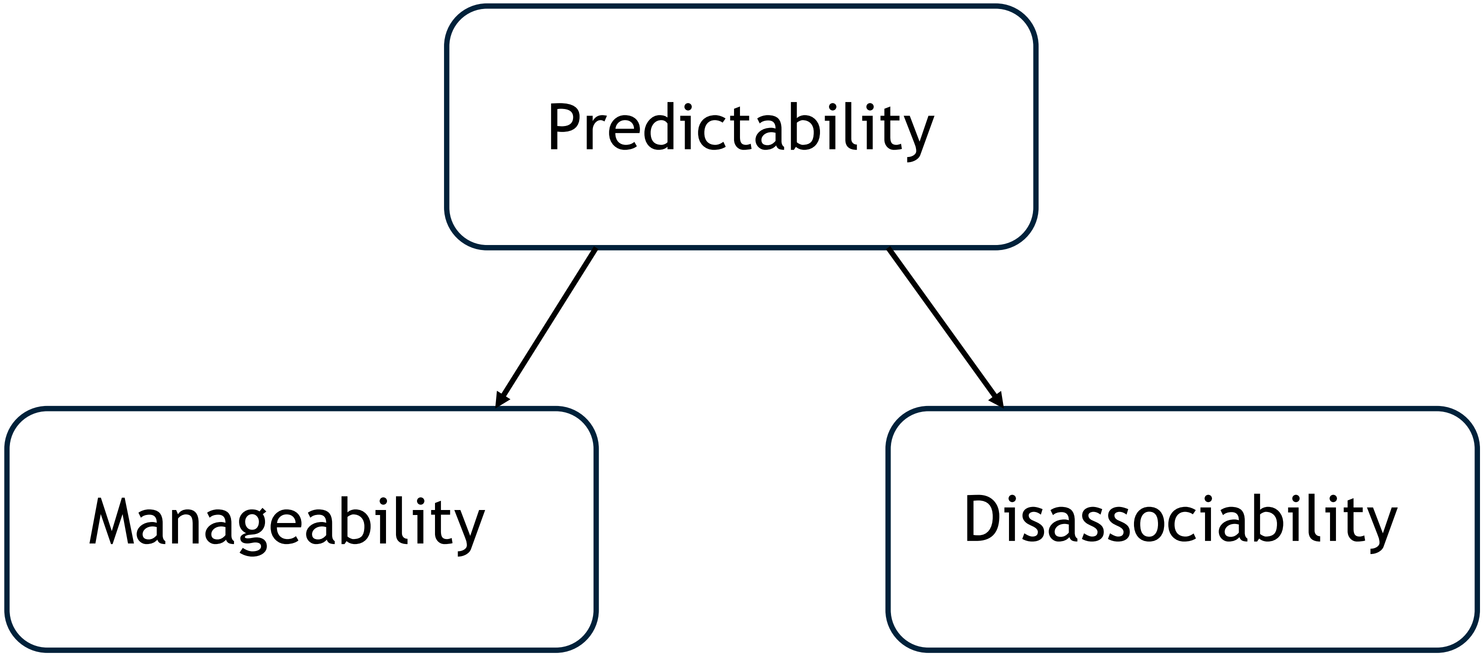
Privacy (research)

(Software) engineering

[Gürses2016]

# B. Privacy engineering II

- Three main goals:



[NIST2014]

# C. Privacy enhancing technologies

- Privacy Enhancing Technologies (PETs)
  - It refers to the category of technologies that minimise the processing of personal data

- Examples
  - Automatic anonymisation (e.g. Anonymizer, iPrivacy)
  - Encryption tools (e.g. SSL)
  - Policy Tools (e.g., P3P, TRUSTe)
  - PPML (e.g. Federated Learning, Homomorphic Encryption)

[Danezis2014]

# Supporting References

- [Cavoukian2010]: Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, 2010.
- [D' Acquisto2015]: Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics.
- [Gürses2016]: Privacy Engineering: Shaping an Emerging Field of Research and Practice IEEE Security and Privacy, 14:2, pp. 40-46, 2016.
- [NIST2014]: NIST Privacy Engineering Objectives and Risk Model Discussion Draft. Introduction, 2014.
- [Danezis2014]: Privacy and Data Protection by Design – from policy to engineering, 2014.
- [National Academy2010]: Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop
- [Europe2006] European Parliament and the Council: Directive 2006/24/EC of the European Parliament and if the council; www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf
- [EC2014] Progress on EU data protection reform now irreversible following European Parliament vote. Accessed at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm on 12.11.2014.
- [EC-Prot-2014] European Commission: Protection of personal data: http://ec.europa.eu/justice/data-protection/index_en.htm
- [WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, Harvard Law Review; Vol. IV; December 15, 1890, No. 5; http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- [Bishop2006] Bishop, C. M. (2006). Pattern recognition and machine learning. springer.
- [Goodfellow2016] Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1, No. 2). Cambridge: MIT press.
- [Kelleher2015] Kelleher, J. D., Namee, B. M., & D’Arcy, A. (2015). Machine learning for predictive data analytics. Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies, 1-19.
- [Al-Rubaie2019] Al-Rubaie, M., & Chang, J. M. (2019). Privacy-preserving machine learning: Threats and solutions. IEEE Security & Privacy, 17(2), 49-58.
- [Zheng2019] Zheng, M., Xu, D., Jiang, L., Gu, C., Tan, R., & Cheng, P. (2019, November). Challenges of privacy-preserving machine learning in IoT. In Proceedings of the First International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things (pp. 1-7).

mobile business

## Chair of Mobile Business & Multilateral Security

**Dr. Ahad Niknia**
Goethe University Frankfurt
E-Mail: ahad.niknia@m-chair.de
WWW: www.m-chair.de

GOETHE UNIVERSITÄT FRANKFURT AM MAIN