

Conducting an Overview of Privacy Legislation, Regulation and Standards as a Means to Improve Education on Data Privacy Compliance

Master's Thesis Kick-Off Presentation, Ali Asaf Polat

15 May, 2023

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
www.matthes.in.tum.de

Introduction

- Motivation
- Goals

Research Questions

Methodology

Initial Results

Next Steps

- Data Privacy is getting more important with increasing data gathering from the user.
- There are different data privacy regulations based on the location.(GDPR, CCPA, PIPEDA)
- Legal regulations look overwhelming and there is no comprehensive overview. So, this makes it difficult for practitioners to understand and comply with the laws.



- Investigate existing legal regulations, and present a structured and curated collection of topics that is easy to understand for practitioners.
- By doing that, practitioners can gain a better understanding of the legal regulations and design their systems and business models accordingly.



Introduction

- Motivation
- Goals

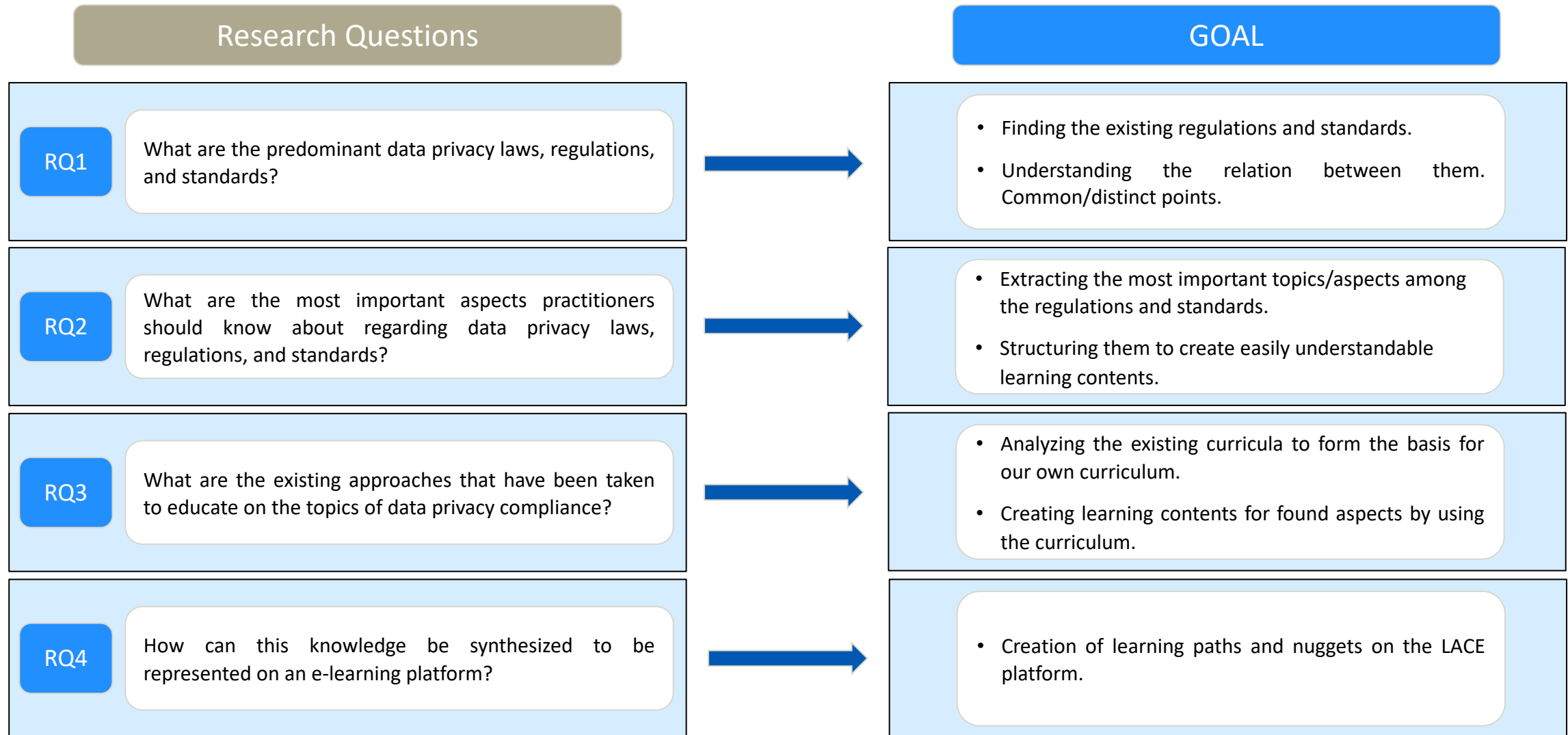
Research Questions

Methodology

Initial Results

Next Steps

Research Questions



Outline

Introduction

- Motivation
- Goals

Research Questions

Methodology

Initial Results

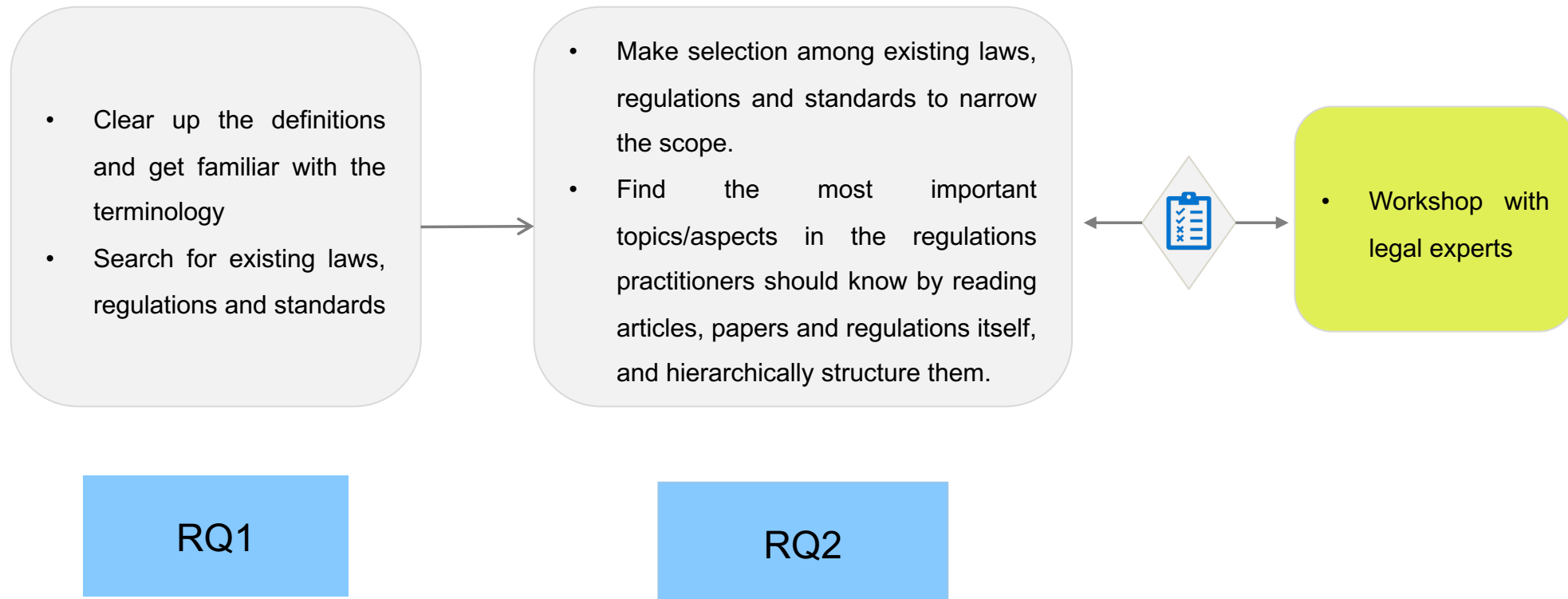
Next Steps

RQ1

What are the predominant data privacy laws, regulations, and standards?

RQ2

What are the most important aspects practitioners should know about regarding data privacy laws, regulations, and standards?

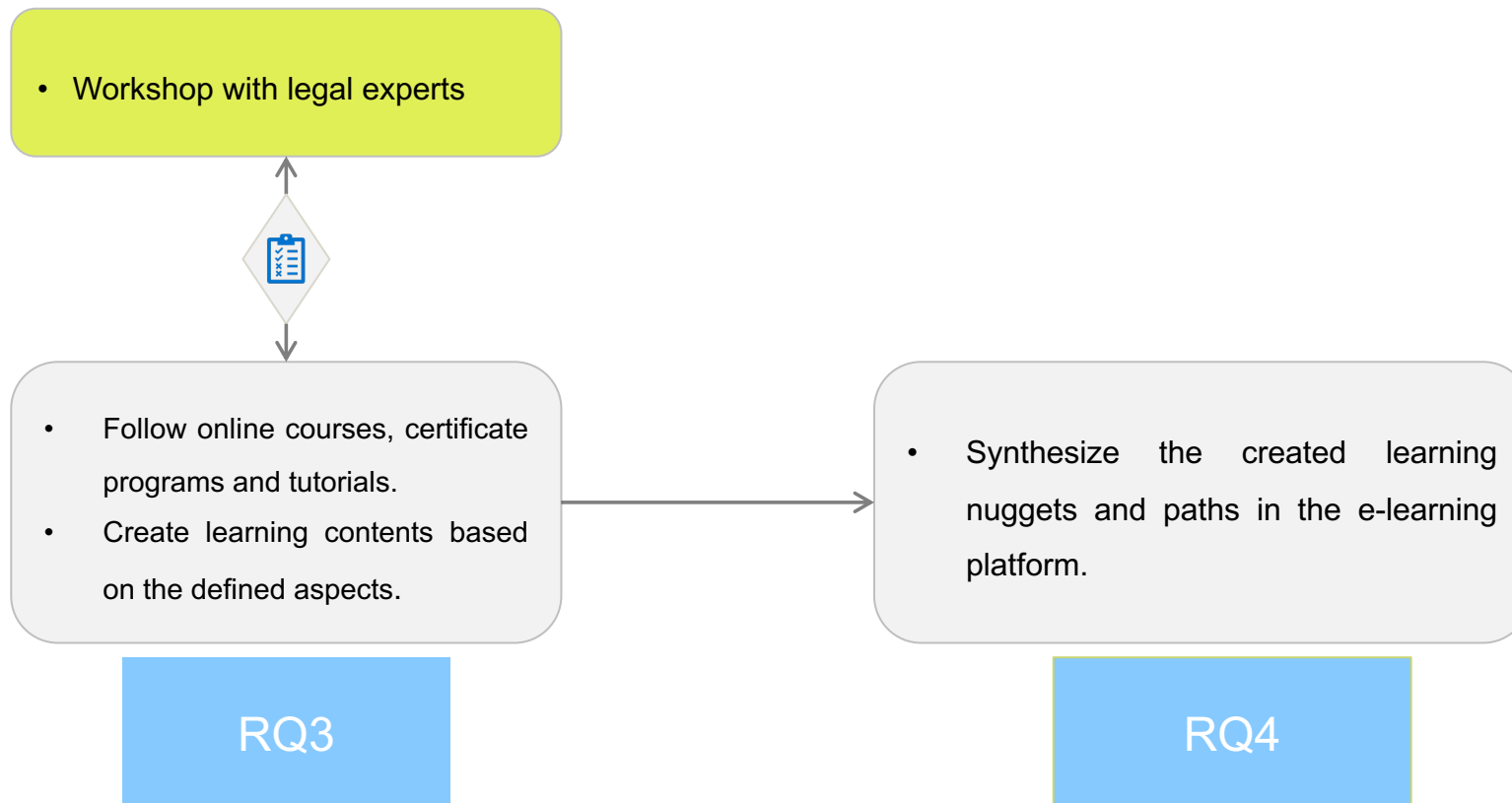


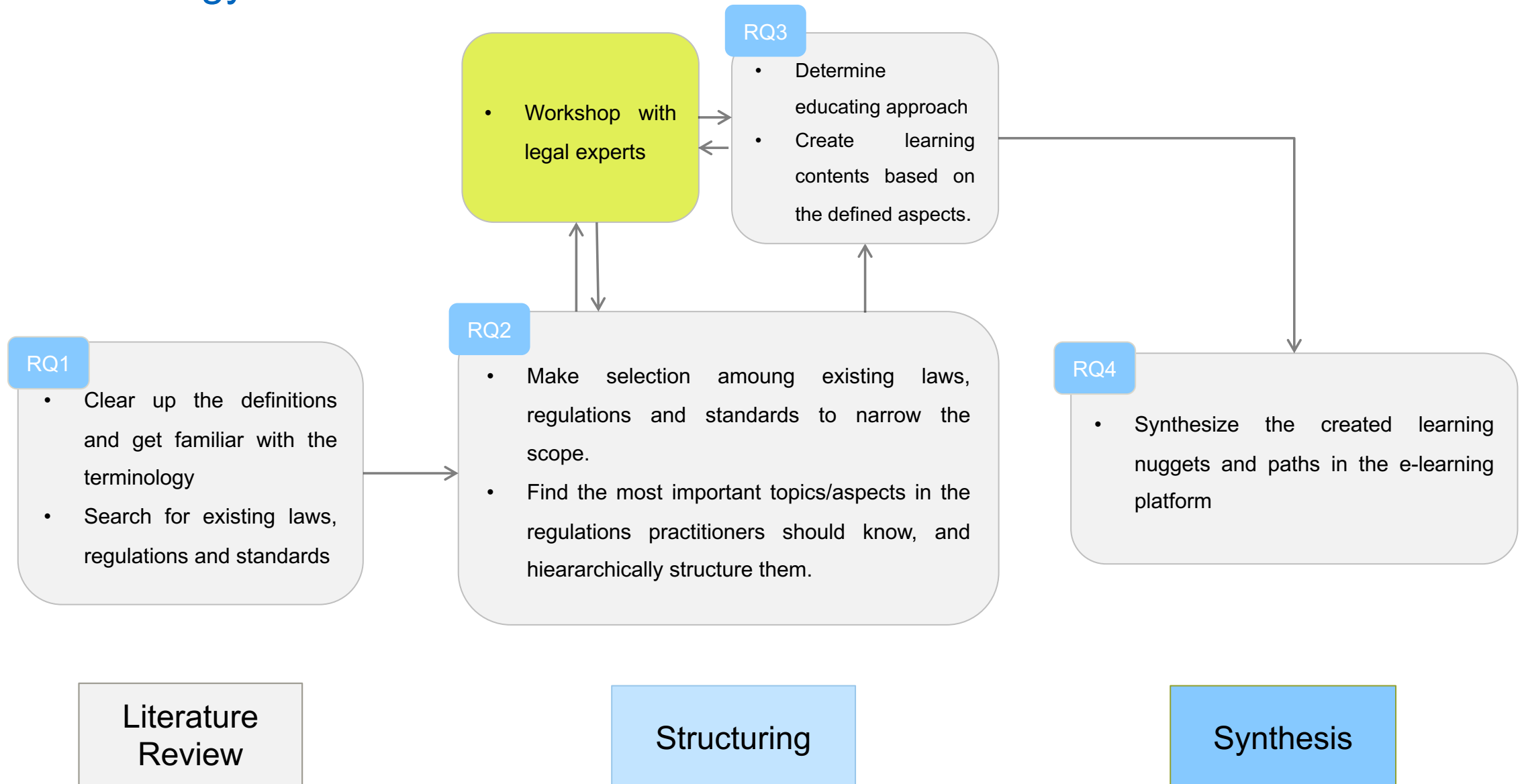
RQ3

What are the existing approaches that have been taken to educate on the topics of data privacy compliance?

RQ4

How can this knowledge be synthesized to be represented on an e-learning platform?





Outline

Introduction

- Motivation
- Goals

Research Questions

Methodology

Initial Results

Next Steps

RQ1

What are the predominant data privacy laws, regulations, and standards?

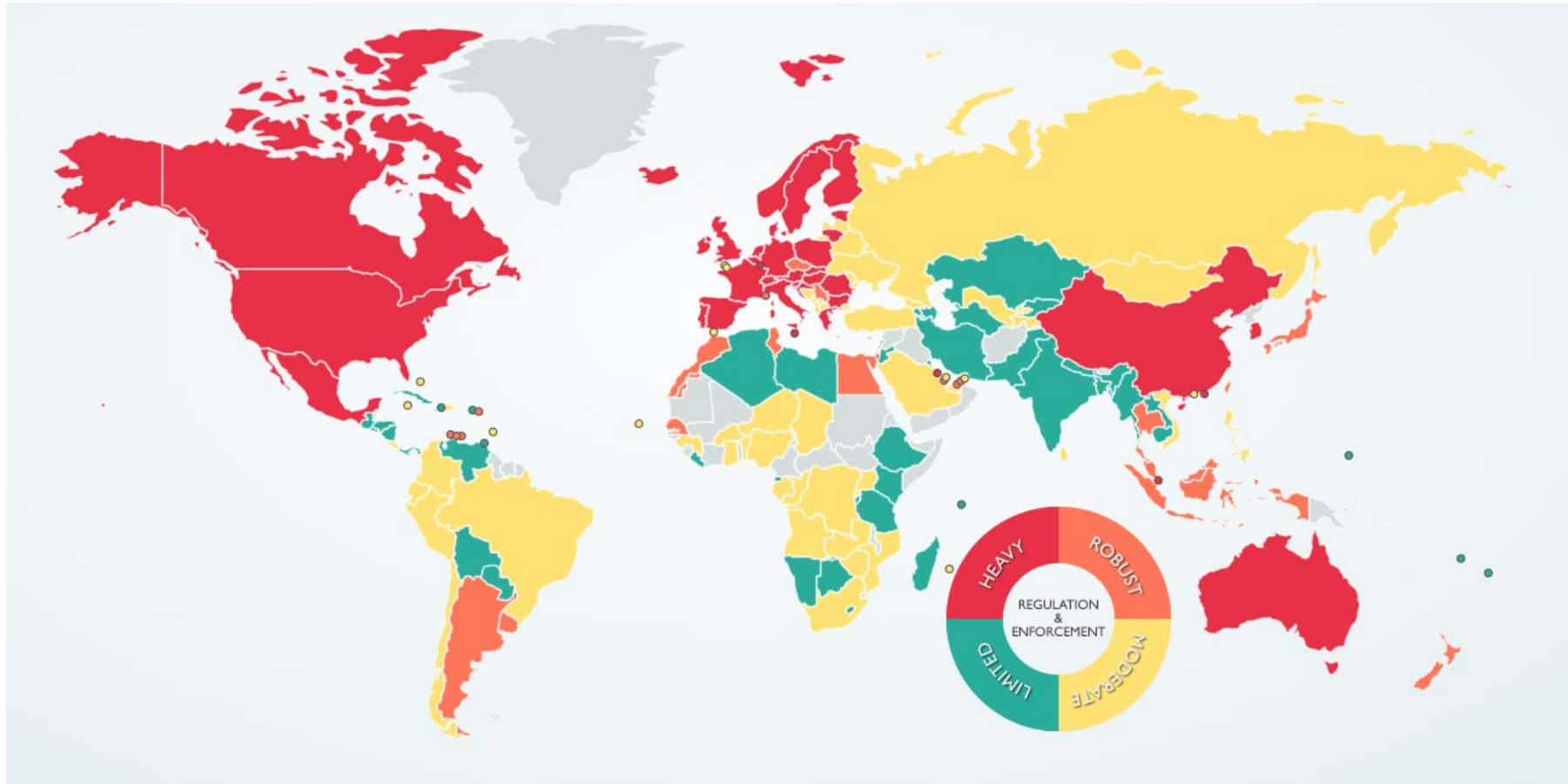
- Getting familiar with the terminology.
- Clarifying definitions and finding relations between the terms.

Aspects	Legislation	Regulation	Standard
Authority	Legislation branch, the parliament	Agencies, boards, and commissions	Committees from industry, governments, academia and the public interest
Scope	Apply to society as a whole	More specific areas, industries or sectors	More specific areas, industries or sectors
Flexibility	Complex legislative process to change	Relatively easy to change by public comments	Accumulation of best practices
Enforcement	Judicial system, courts	Agencies, boards, and commissions that has power to subject to fines	No enforcement but creates reliability

Initial Results/ Selected Countries

RQ1

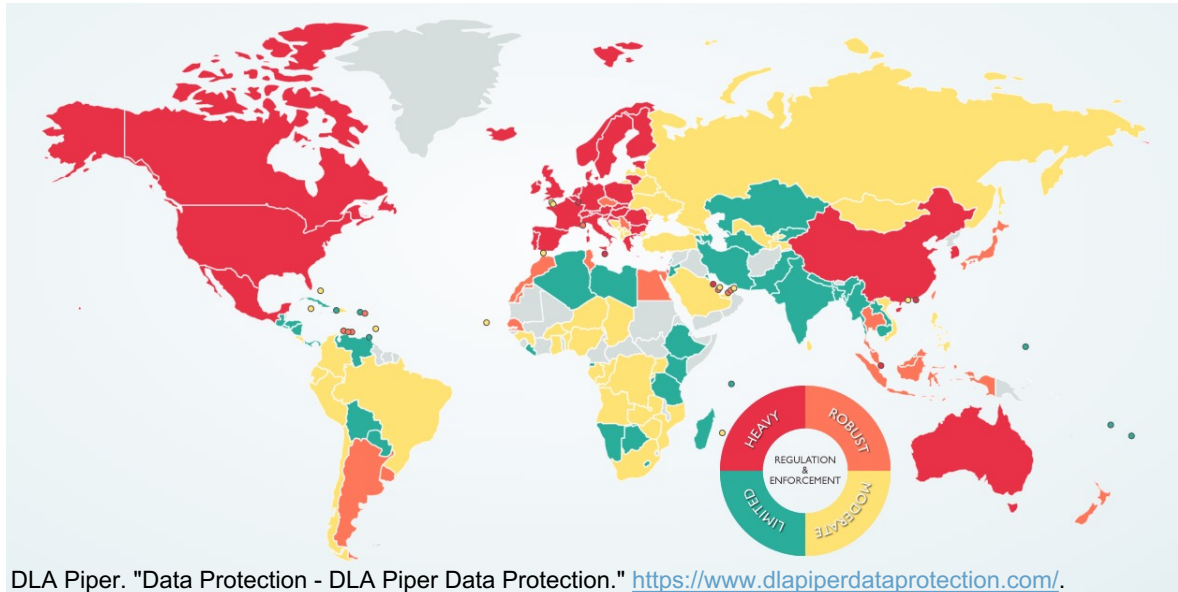
What are the predominant data privacy laws, regulations, and standards?



DLA Piper. "Data Protection - DLA Piper Data Protection." <https://www.dlapiperdataprotection.com/>.

RQ1

What are the predominant data privacy laws, regulations, and standards?



Selected Countries

- European Data Protection Area
- USA
- Canada
- China
- Bahrein
- Mexico
- Australia
- South Korea
- Singapore

How are those countries classified as having heavy regulations?

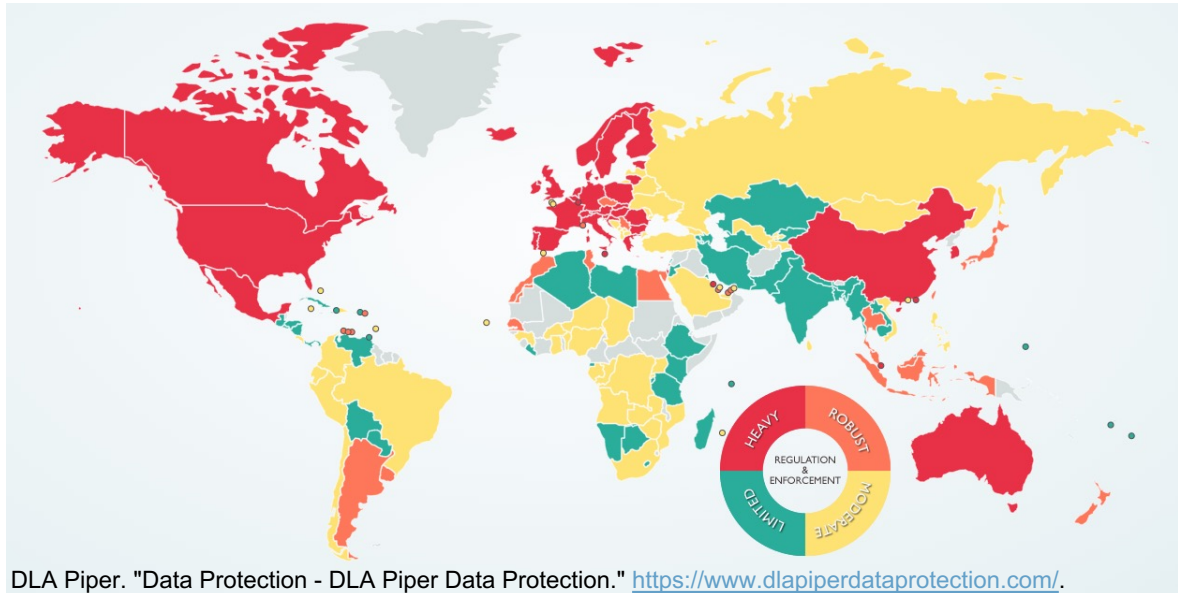
✉ From: *****n@dlapiper.com

“...We base the assessment on questions that local counsel in the relevant jurisdictions answers, mainly around (1) **the level of legislation** (e.g., omnibus laws, comprehensive laws, or sectoral/sector specific, or no legislation at all), (2) **the level of sanctions associated with non-compliance** and (3) **the practical/actual enforcement by regulatory authorities, or where it exists though a private right of action etc.** They **rate** each of these categories and sub-questions that sit under that category on a scale from 1-5...”

Initial Results/ Selected Countries

RQ1

What are the predominant data privacy laws, regulations, and standards?



Selected Countries

- European Data Protection Area
- USA
- Canada
- China
- ~~Bahrain~~
- ~~Mexico~~
- Australia
- South Korea
- Singapore
- **Brazil**
- **Japan**

How are those countries classified as having heavy regulations?

✉ From: *****n@dlapiper.com

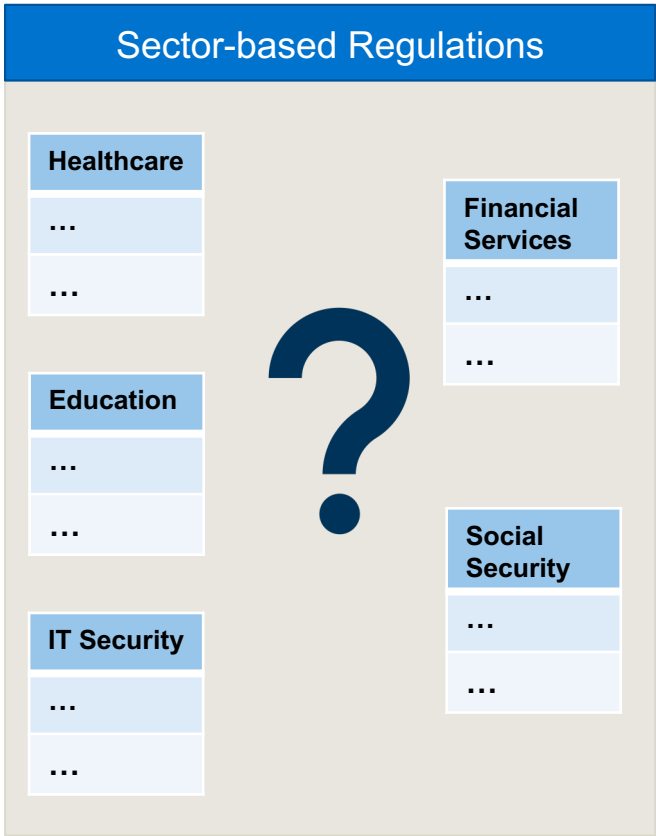
“...We base the assessment on questions that local counsel in the relevant jurisdictions answers, mainly around (1) **the level of legislation** (e.g., omnibus laws, comprehensive laws, or sectoral/sector specific, or no legislation at all), (2) **the level of sanctions associated with non-compliance** and (3) **the practical/actual enforcement by regulatory authorities, or where it exists though a private right of action etc.** They **rate** each of these categories and sub-questions that sit under that category on a scale from 1-5...”

RQ1

What are the predominant data privacy laws, regulations, and standards?

- Finding data privacy related legislations and regulations for selected countries.
- There are also sector-based regulations which have provisions for data privacy.

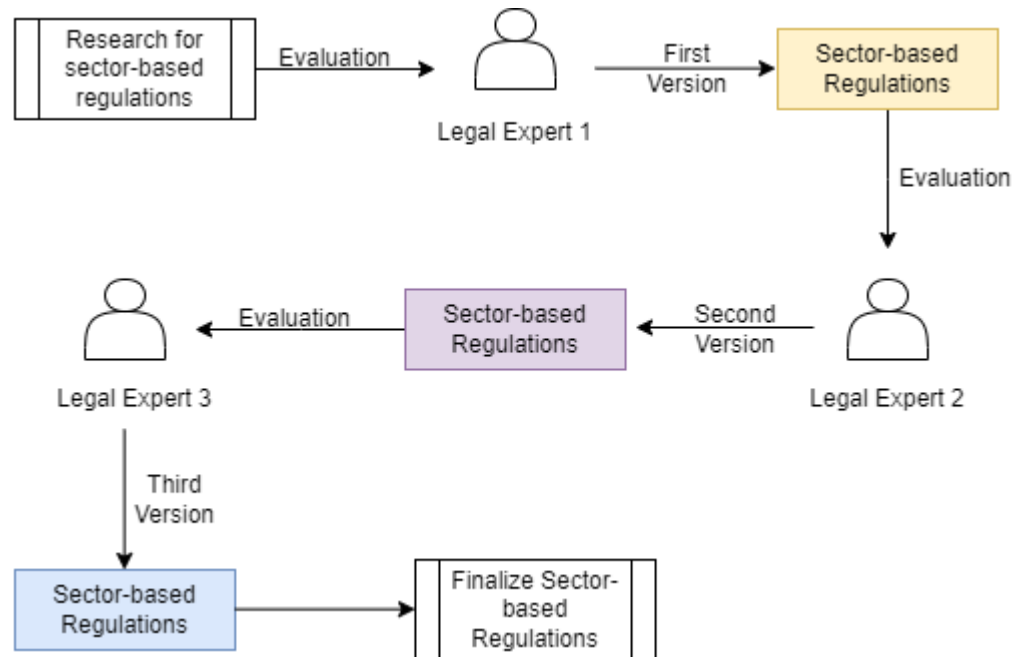
Data Privacy, Data Protection Regulations	
Regulation	Country/Region
General Data Protection Regulation(GDPR)	European Data Protection Area
California Consumer Privacy Act(CCPA)	California/USA
Virginia Consumer Data Protection Act(VCDPA)	Virginia/USA
The China Personal Information Protection Law (PIPL)	China
Brazilian General Data Protection Law (LGPD)	Brazil



Initial Results/Sector-based Regulations

RQ1

What are the predominant data privacy laws, regulations, and standards?



Financial Services

- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act
- Dodd-Frank Act



Healthcare

- Health Insurance Portability and Accountability Act(HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)



Education

- Family Education Rights and Privacy Act(FERPA)



Specific Consumer Protection

- California Consumer Privacy Act(CCPA)
- Telephone Consumer Protection Act(TCPA)
- Telemarketing Sales Rule



Immigration and Crime Prevention

- The Criminal Justice Act
- The Migration Act



IT Security for Critical Infrastructure

- German IT Security Act
- Critical Infrastructure Protection Act
- Cybersecurity Information Sharing Act



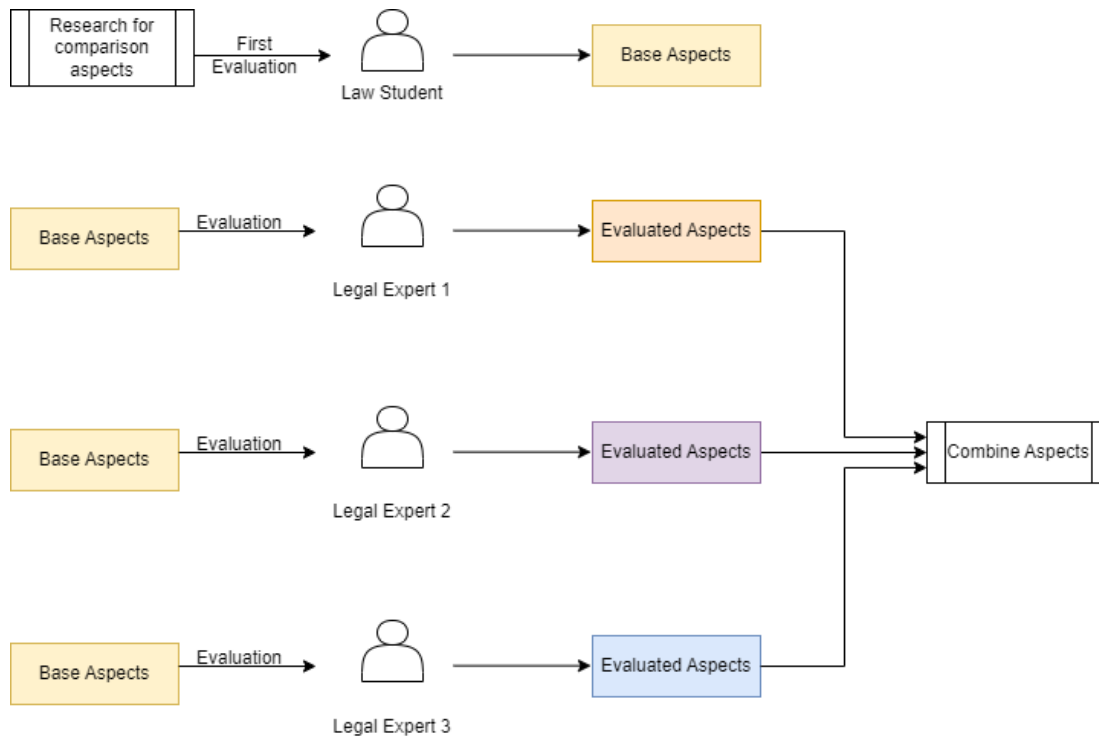
Social Security

- Social Code in Germany (Sozialgesetzbuch)
- Social Security Administration Act

Initial Results : Important Topics / Comparison Aspects

RQ2

What are the most important aspects practitioners should know about regarding data privacy laws, regulations, and standards?



Principles

- Lawfulness
- Fairness
- Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity, Confidentiality and Availability
- Accountability

Legal Basis

- Consent
- Legitimate Interest
- Performance of Contract
- Legal Obligation
- Vital Interest
- Public Interest

Enforcement

- Administrative Supervisory Authority and Enforcement
- Administrative Fines in case of non-compliance
- Personal Liability
- Private Right of Action

Privacy by Design

Privacy by Default

Controller and Processor

- Define Data Controller or synonyms
- Define Data Processor or synonyms
- Assigning a DPO or synonyms in certain circumstances
- Binding contract between Controller and Processor
- Keep record of data processing activities
- Data Breach Notifications
- Recognize accountability
- Provide Safeguards for International Data Transfer
- Conducting DPIA for High Risk Activities
- Security Requirements

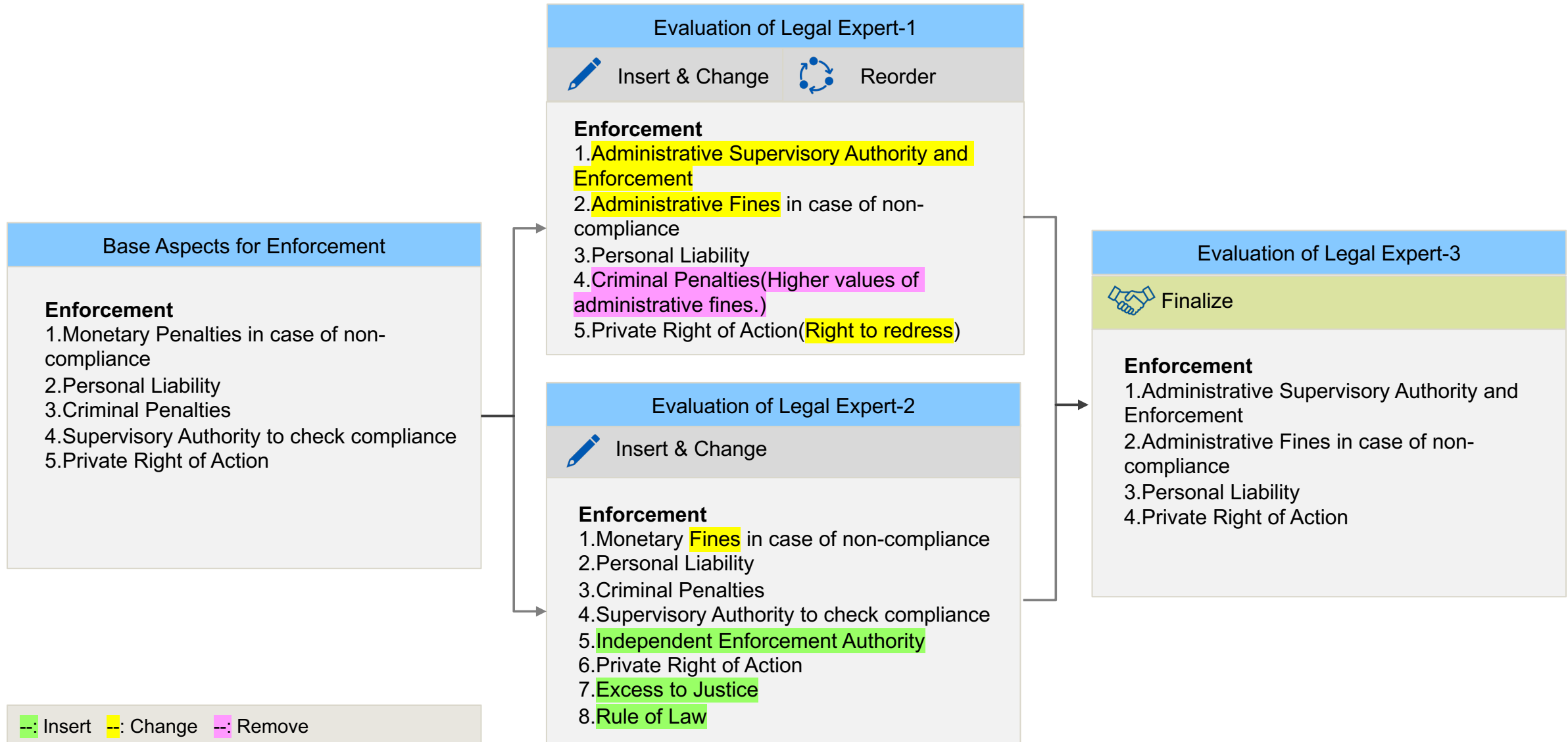
Right of Data Subject

- Right to opt out specific or all processing
- Right to Access
- Right to Erasure
- Right to Data Portability
- Right against automated decision making
- Right to Correct(or Rectification)
- Age-based opt-in right
- Right to Redress

Thresholds

- Compliance requirements based on thresholds

Initial Results: Evaluation of Comparison Aspects with Legal Experts



Outline



Introduction

- Motivation
- Goals

Research Questions

Methodology

Expected Results

Next Steps

RQ1

What are the predominant data privacy laws, regulations, and standards?

- Structure researched **standards**

RQ2

What are the most important aspects practitioners should know about regarding data privacy laws, regulations, and standards?

- Extract **the most important aspects** practitioners should know from existing **standards**
- **Compare regulations** based on **specified aspects**

RQ3

What are the existing approaches that have been taken to educate on the topics of data privacy compliance?

- Research existing approaches from different platforms and tutorials
- Create **learning contents** for found aspects by applying educating approach

RQ4

How can this knowledge be synthesized to be represented on an e-learning platform?

- **Represent** created contents on an **e-learning platform** by creating learning paths and nuggets

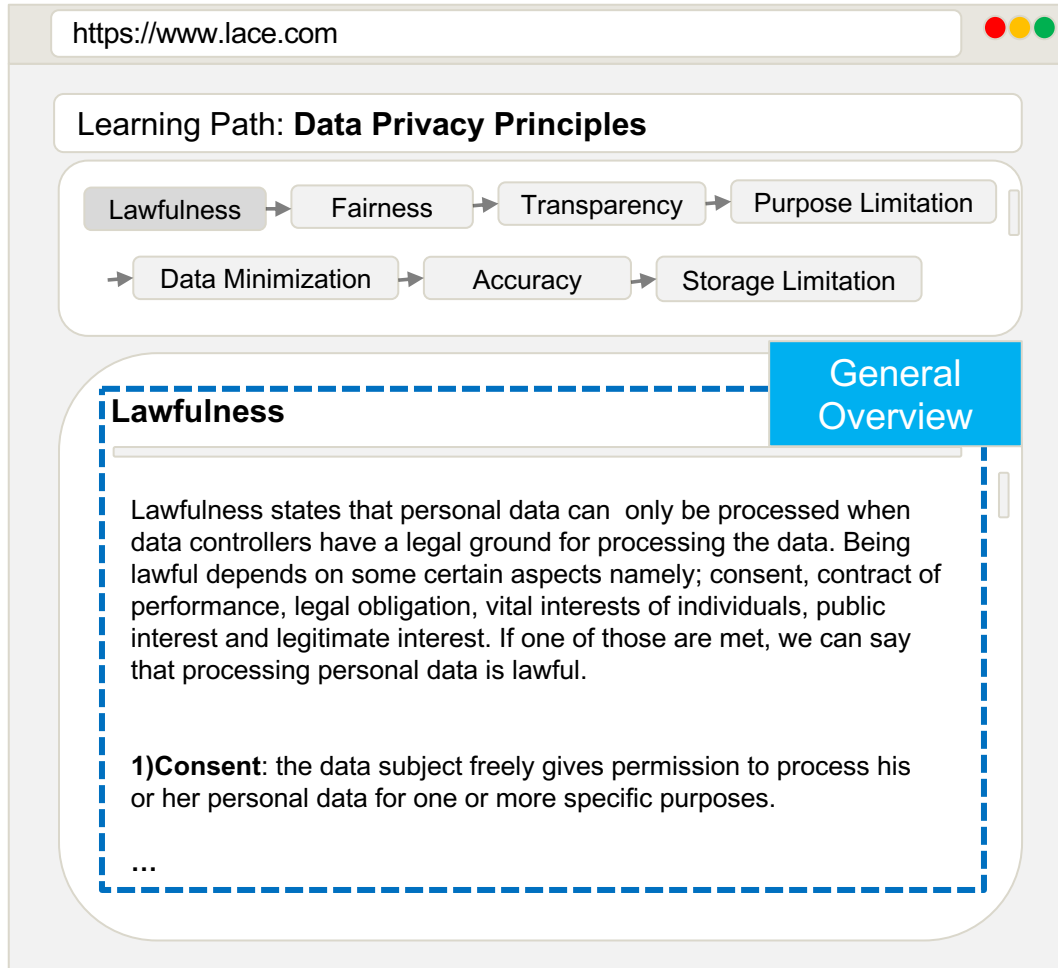
Next Steps

- Finishing comparison table based on the found aspects and selected countries

Comparison Aspects	GDPR	CCPA	PIPL	...
Principles				
Lawfulness	Being lawful depends on consent, contract of performance, legal obligation, vital interests of individuals, public interest and legitimate interest.		...	...
Fairness	The data subject must be informed about the processing operation and its purposes, existence of profiling and the consequences of such profiling	The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared.	...	...
Transparency	Individuals must be informed which personal data is collecting from them, why it is collected and how they will be used.	The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared.	...	...
Purpose Limitation	Personal data must be collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	A business shall not collect additional categories of personal data or use personal data collected for additional purposes without providing the consumer with notice consistent with this section.	...	...
Data Minimization	Personal data can be collected in adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed		...	...
...	...	...	...	...

Next Steps

- Creating learning contents and representing them on an e-learning platform



https://www.lace.com

Learning Path: **Data Privacy Principles**

Lawfulness → Fairness → Transparency → Purpose Limitation

→ Data Minimization → Accuracy → Storage Limitation

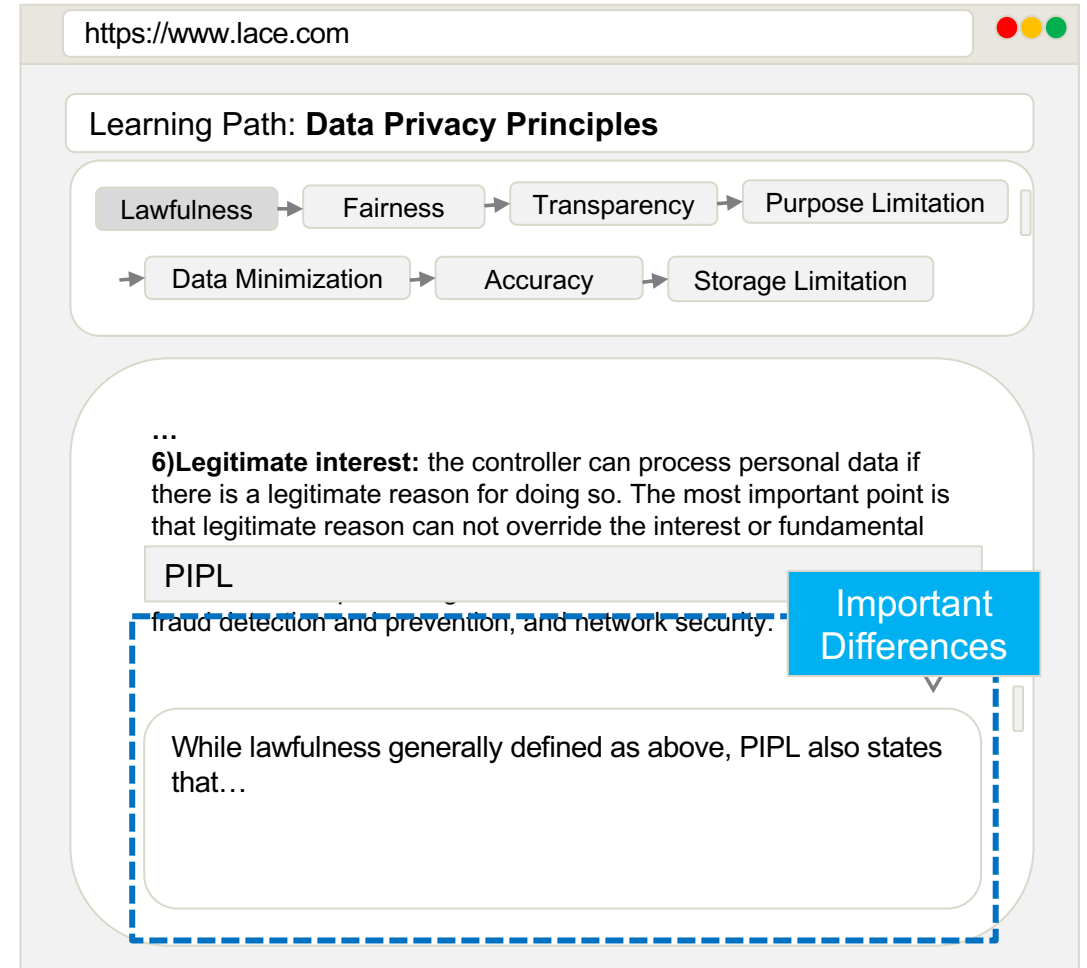
Lawfulness

Lawfulness states that personal data can only be processed when data controllers have a legal ground for processing the data. Being lawful depends on some certain aspects namely; consent, contract of performance, legal obligation, vital interests of individuals, public interest and legitimate interest. If one of those are met, we can say that processing personal data is lawful.

1)Consent: the data subject freely gives permission to process his or her personal data for one or more specific purposes.

...

General Overview



https://www.lace.com

Learning Path: **Data Privacy Principles**

Lawfulness → Fairness → Transparency → Purpose Limitation

→ Data Minimization → Accuracy → Storage Limitation

...

6)Legitimate interest: the controller can process personal data if there is a legitimate reason for doing so. The most important point is that legitimate reason can not override the interest or fundamental

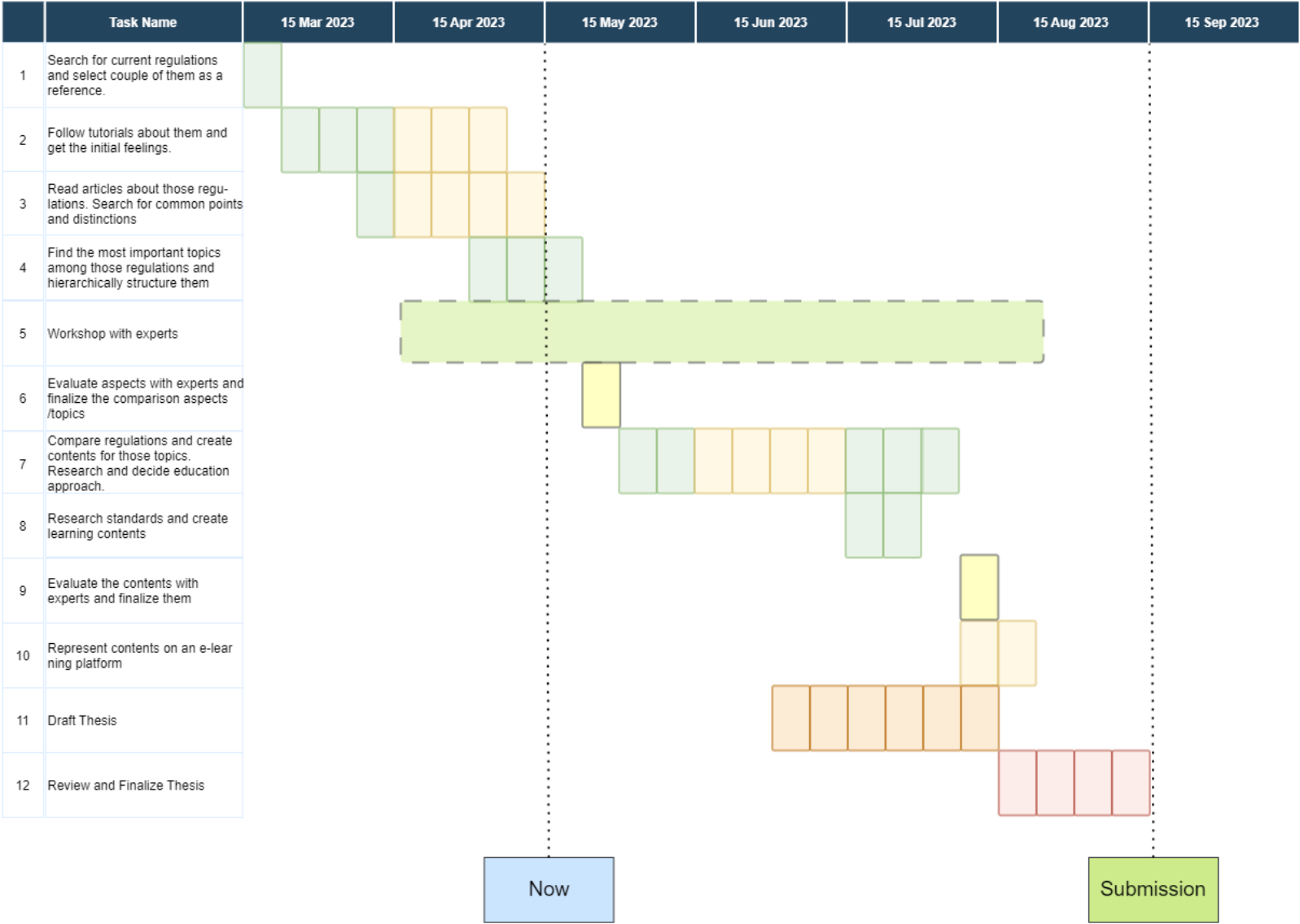
PIPL

fraud detection and prevention, and network security.

While lawfulness generally defined as above, PIPL also states that...

Important Differences

Timeline





Ali Asaf Polat

aliasafpolat@hotmail.com

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business
Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

