ELISE action
Webinar Series

ELISE guidance on Location Data Privacy

Massimo PEDROLI, Deloitte IT
Gabriele Di NILLO, Deloitte IT
Ilenia Pia VICECONTI, Deloitte IT
Lorena HERNANDEZ, European Commission JRC
Simon VREČAR, European Commission JRC (Consultant)
Ray BOGUSLAWSKI (Consultant)

2020, October 22

European Location Interoperability Solutions for e-Government

Enabling Digital Government through Geospatial and Location Intelligence

ISA²

ISA² Programme & ELISE action

European Interoperability Programme

cross-border *and* ***cross-sector*** *Interoperability solutions*

for ***public administrations, businesses*** *and* ***citizens***

54 different actions tackling **interoperability** from different angles

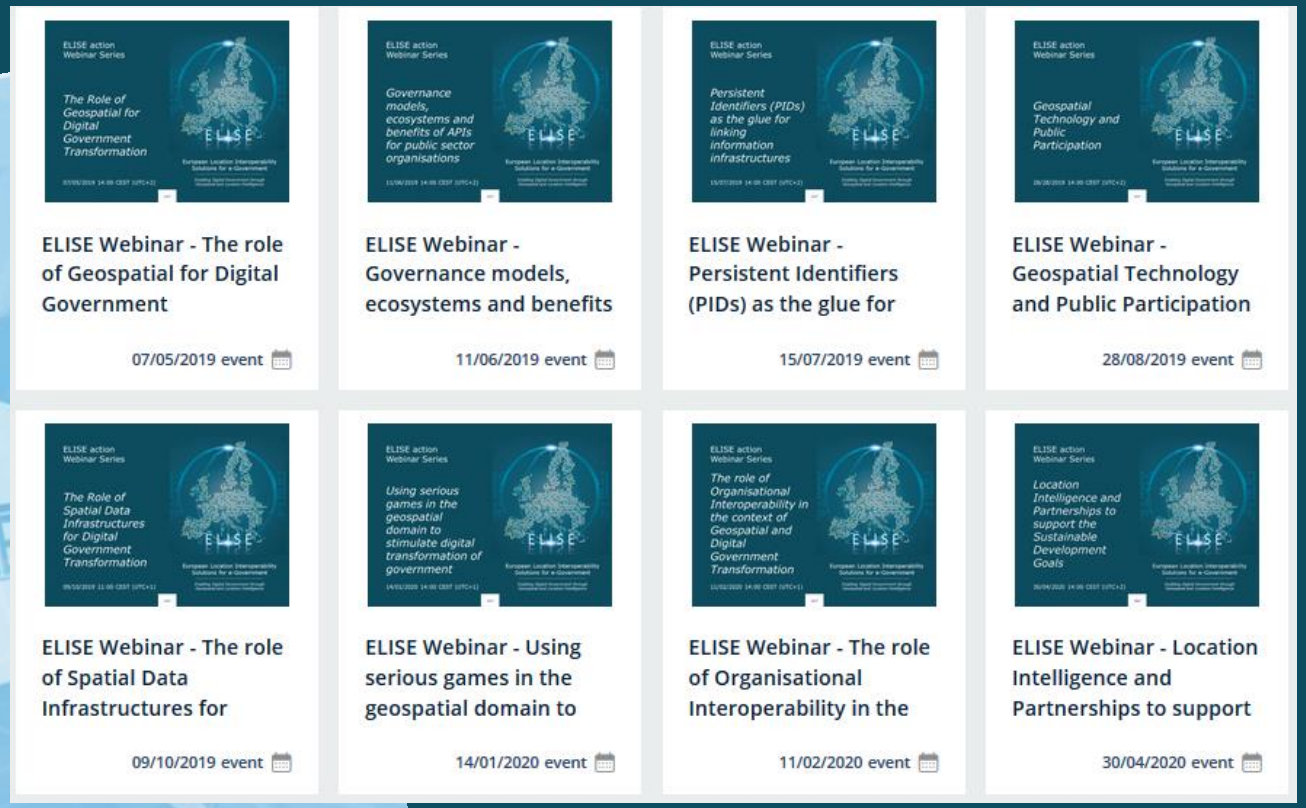
ELISE action is the **only** action focusing on the **location dimension**

European Location Interoperability Solutions for e-Government

Enabling Digital Government through Geospatial and Location Intelligence

ISA²

Welcome to the ELISE webinar series



ELISE **Knowledge Transfer** activities

Purpose:

- Engage in **an agile way**
- with **topics** of relevance to the **Digital Transformation**
- **by harnessing the use of spatial data and technology.**
- **Share** the results **of ELISE activities.**

https://europa.eu/!nP74ph

Our speakers

Massimo PEDROLI

Senior consultant in Public Sector

Deloitte.

Gabriele Di NILLO

Senior expert in Location Data Privacy

Deloitte.

Ilenia Pia VICECONTI

Senior expert in Location Data Privacy

Deloitte.

The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

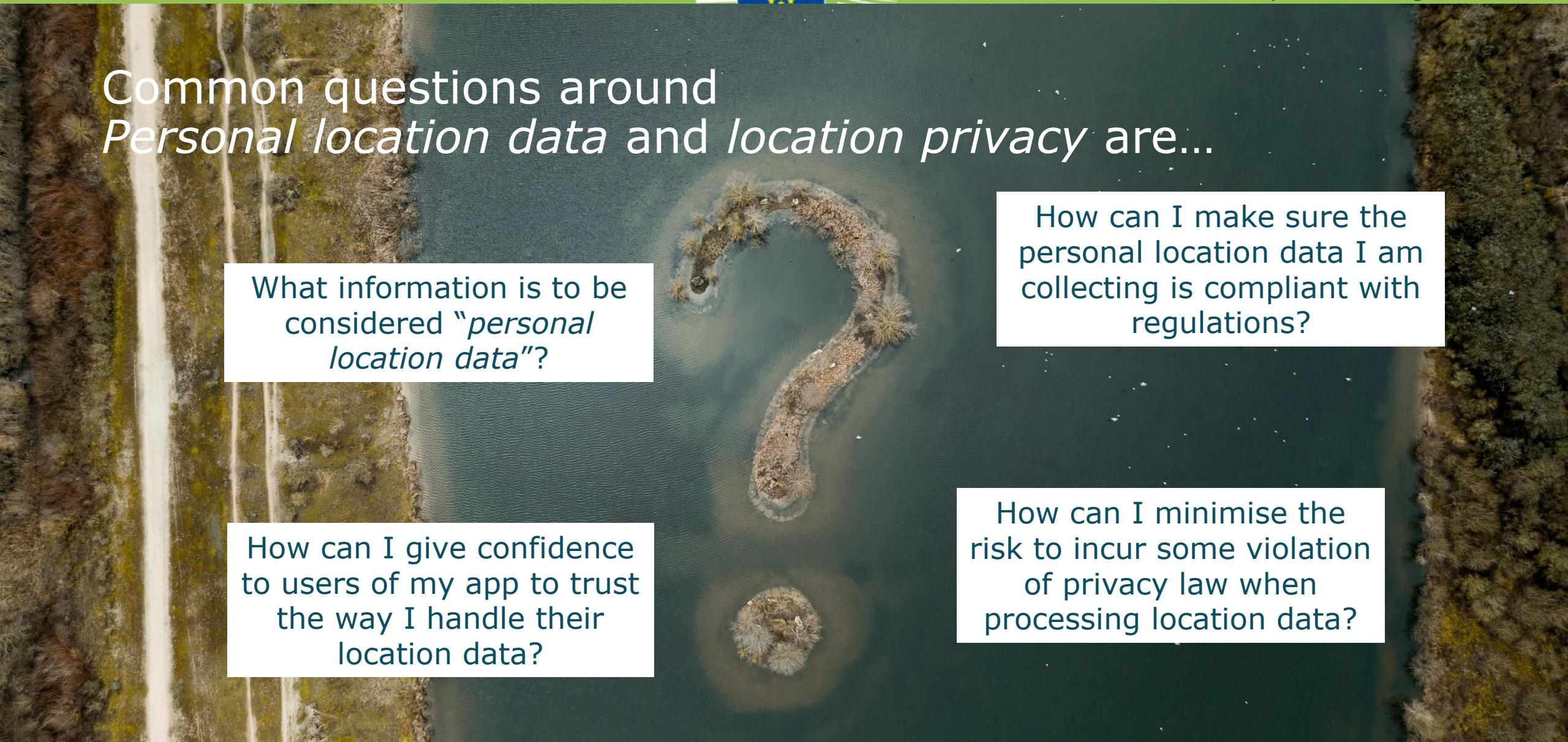
What we will cover today

1. What is "personal location data" and how does it relate to "location data privacy"?
2. Why is location data privacy important for me? User journeys
3. ELISE guidance on Location Data Privacy
4. Conclusions and main take-aways
5. Q&A

1

What is "*personal location data*" and how does it relate to "*location data privacy*"?

Common questions around *Personal location data* and *location privacy* are…



What information is to be considered "*personal location data*"?

How can I make sure the personal location data I am collecting is compliant with regulations?

How can I give confidence to users of my app to trust the way I handle their location data?

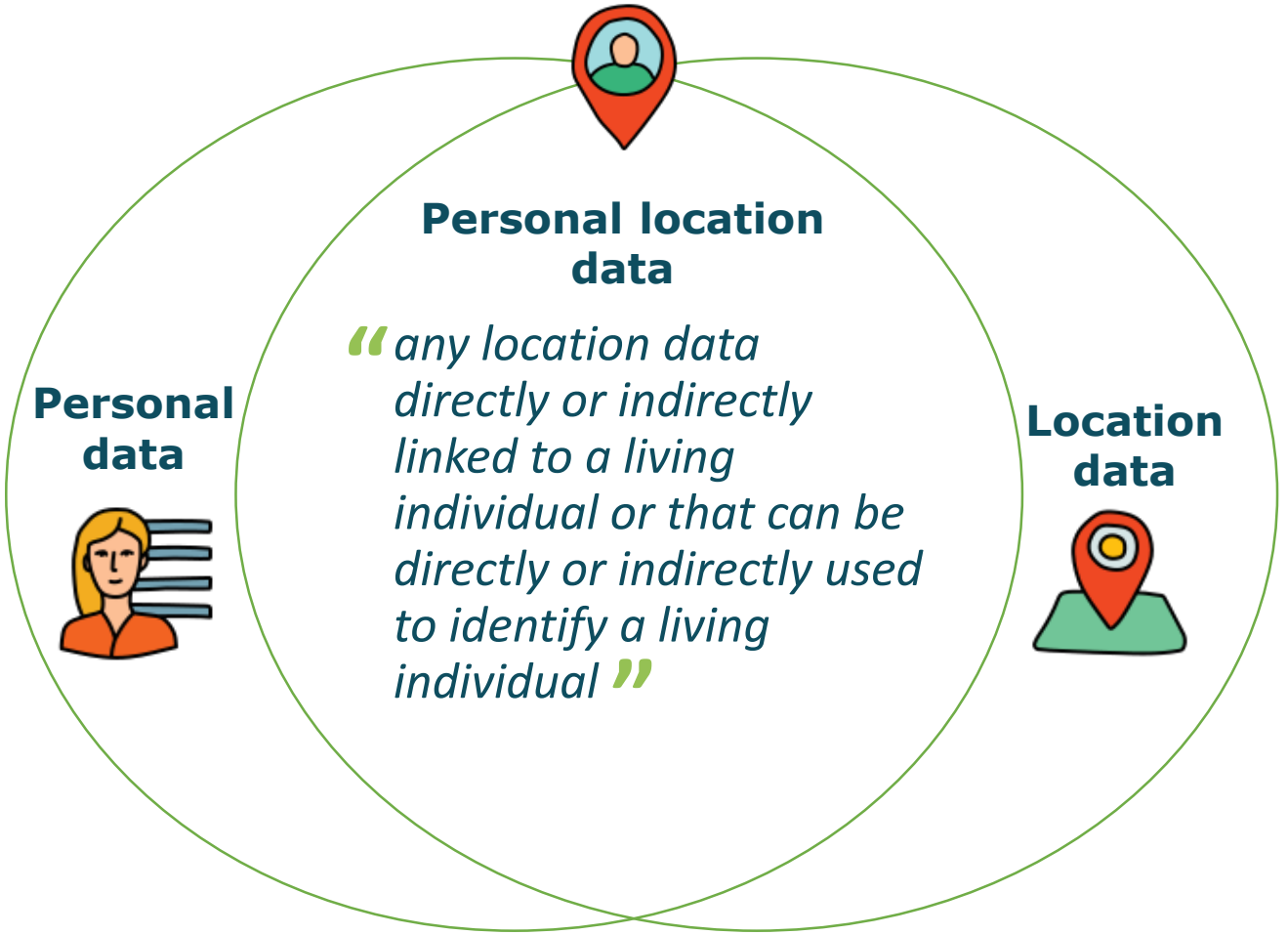
How can I minimise the risk to incur some violation of privacy law when processing location data?

GDPR: a gamechanger for *Personal Location Data*

- General Data Protection Regulation (2016/679) is the **first** piece of EU data protection regulation to mention location data explicitly

but with no clear-cut definition of Personal Location Data

- Location data publishers, re-users and individuals (data subjects) sharing their location data with public and private sector organisations are all impacted by GDPR



Source: Guidelines for public administrations on location privacy

How privacy protection takes into account "*Personal Location Data*"?

"Location Data Privacy is the individual's right not to be subjected to unauthorised collection, aggregation, processing and distribution (including selling) of his location data. It is the right to be protected by the ability to conceal information of whereabouts, which can be derived from personal location data"

Source: *Guidelines for public administrations on location privacy (2020)*

When does location data become "*Personal Location Data*"?

Personal data 	Location data 	Personal location data 
Telephone subscription account information linked to the smart phone	GPS coordinates of the location of a smart phone	By combining the two data sources, the location of the individual can be identified.
Internet subscription account information	Public IP address	
Realty owner information	Cadastral information about a realty	
Licence plate owner information	Traffic camera footage on a specific location	

Source: ***Guidelines for public administrations on location privacy (2020)***

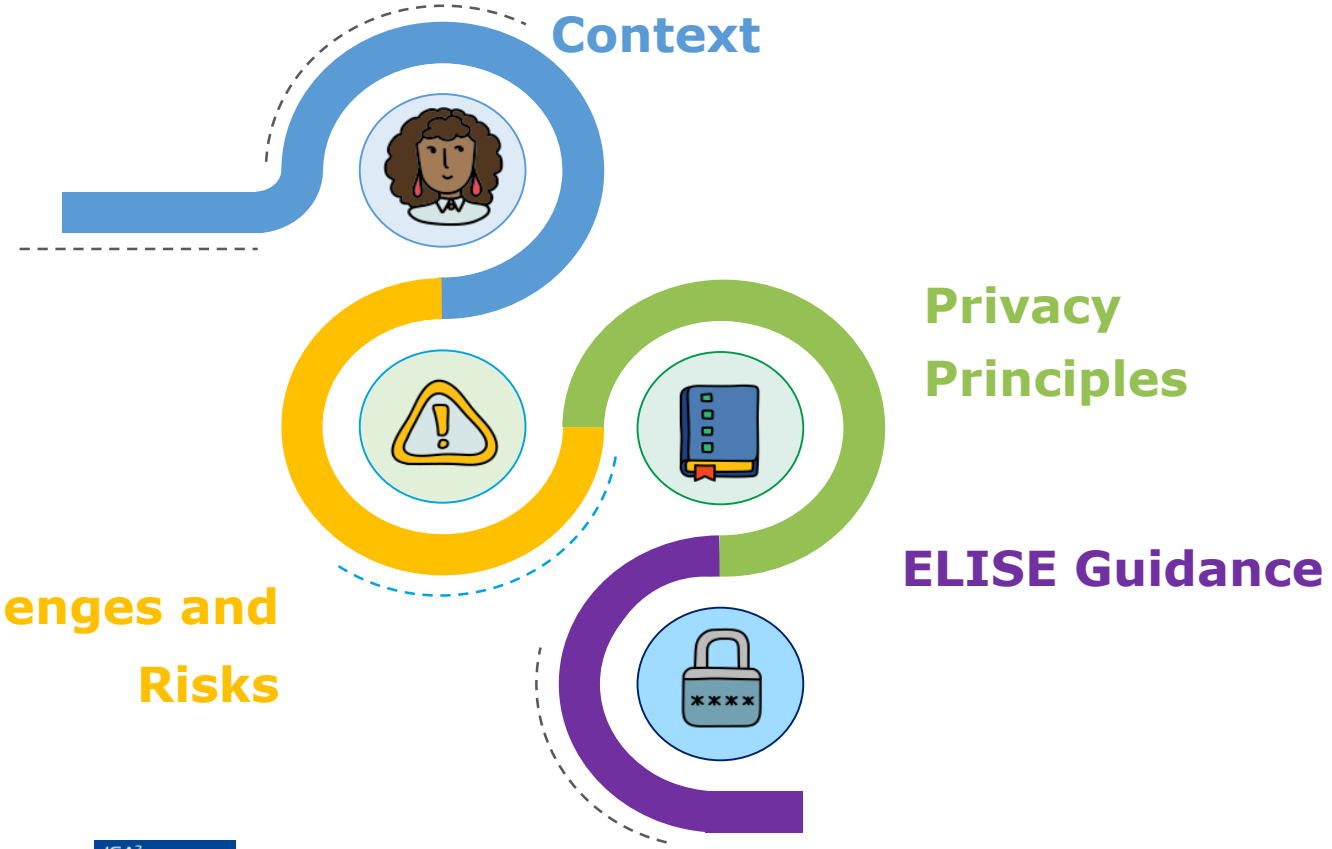
2

Why is *location data privacy* important for me?

User journeys

The "*User journey approach*", tackling **real needs** of

- Citizens
- Public administrations
- Businesses



Location Data Privacy seen by different "*personas*"

Hanna

National Statistician

Margot

Public Local Administration Officer

Tom

Passenger

Martin

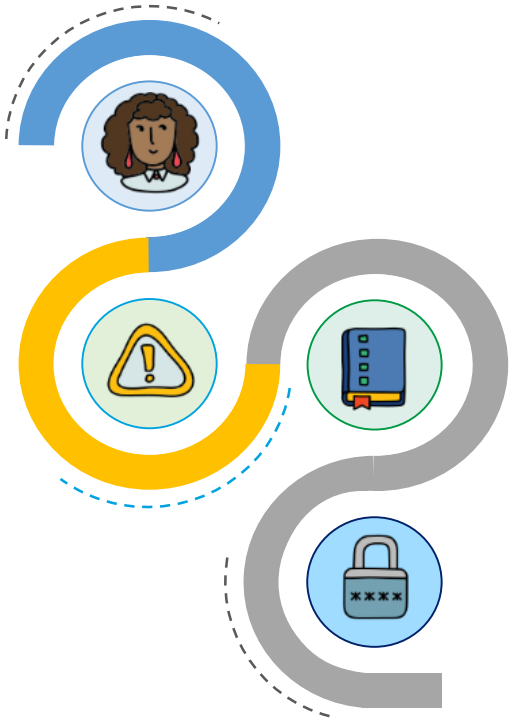
CEO of bus service provider

Hanna

National Statistician

Context

Hanna's Unit decides to **subject all collected personal location data to business intelligence processing**, with the **support of some external experts**



Challenges and Risks

- Data usage **out of their original scope**
- **Unlawful use** of the data
- Risk of **re-identifying individuals**

Hanna

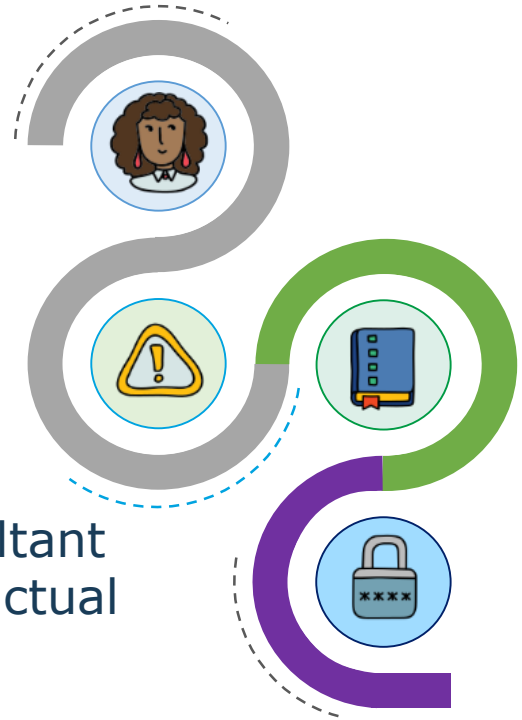
National Statistician

Privacy Principles

- Apply **data minimisation**
- **Secure data processing** activities

ELISE Guidance

- Investigate the **purpose** of data usage
- **Minimise** the amount of data for external consultant
- Correct **technical controls** and contractual agreements
- Considering data **anonymisation**.
- Reduce the precision of **geographical areas**

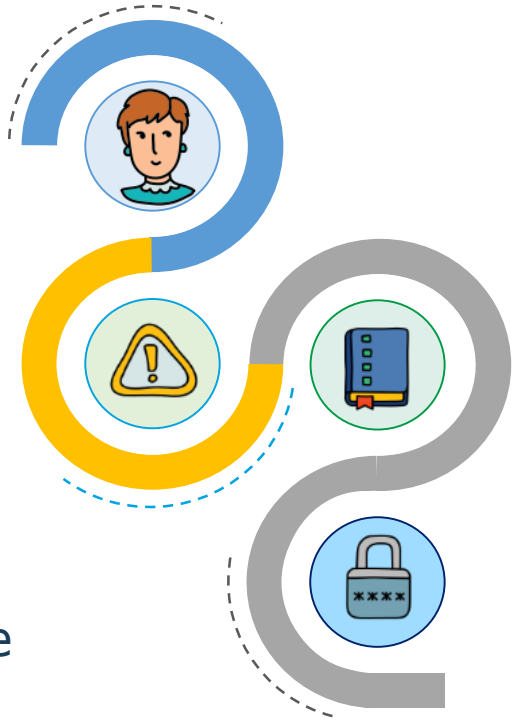


Margot

Public Administration Officer

Context

Margot's office plans to **promote a new service, sending out personalised information brochures to its citizens**



Challenges and Risks

- **Respect** all applicable laws and regulations
- **Re-use of data** collected for a different purpose

Margot

Public Administration Officer

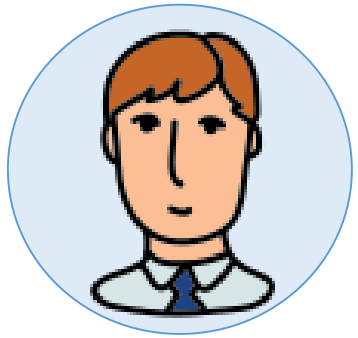
Privacy Principles

- Achieve **lawful processing** of personal location data (see *Guidelines*)
- **Comply** with the data subject's rights (see *Guidelines*)

ELISE Guidance

- Build **trust** being clear about the intended use of data through self-explanatory **privacy notice**
- Public administrations **must explicitly ask for consent** if data is not collected under specific legal provision
- Implement a **personal location data protection programme** as part of a general data protection programme

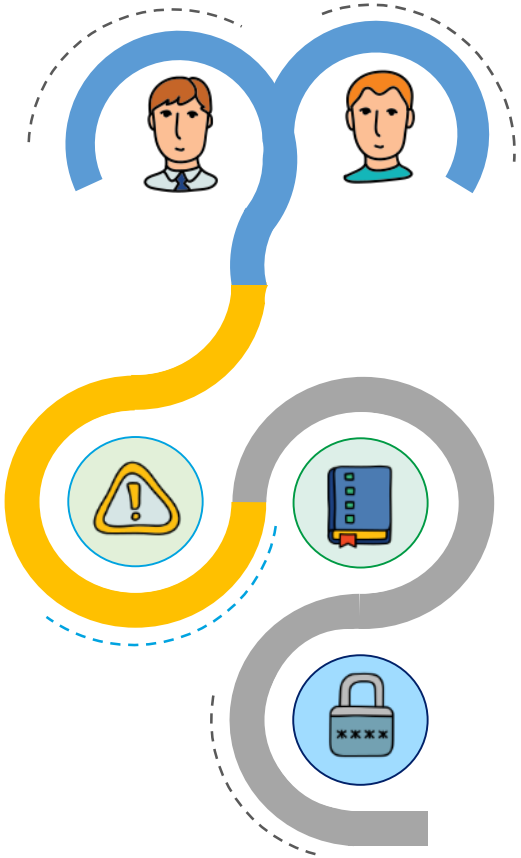
Martin



CEO
bus service
provider
(data controller)

Context

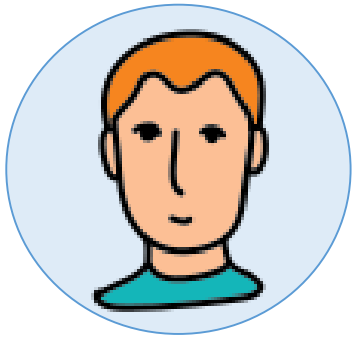
Martin offers an app, developed and managed by a third party, to plan trips and get updates on bus status using GPS. He plans to **add new functionality**: **integration with social media** to save personal information and favourite trips across all users' connected devices



Challenges and Risks

- End users' **trust**
- **Inadequacy of data and service quality**
- **Privacy risk** assessment

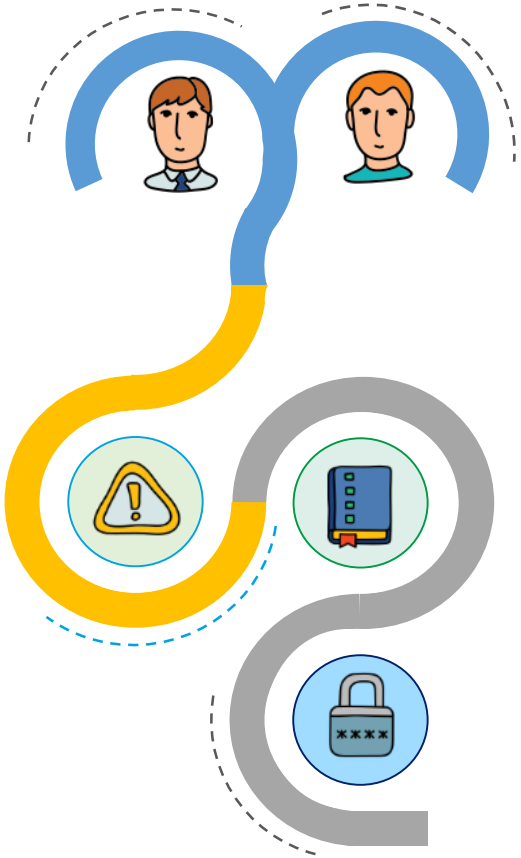
Tom



Passenger
(data owner)

Context

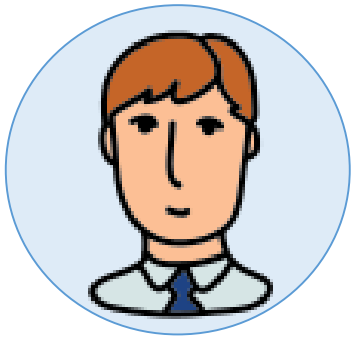
Tom is considering downloading a mobile app to receive **real-time updates** on the status of the buses and to be **notified** when he needs to **get off the bus**



Challenges and Risks

- **Inappropriate use** of personal location data, use out of scope, transfer to third parties

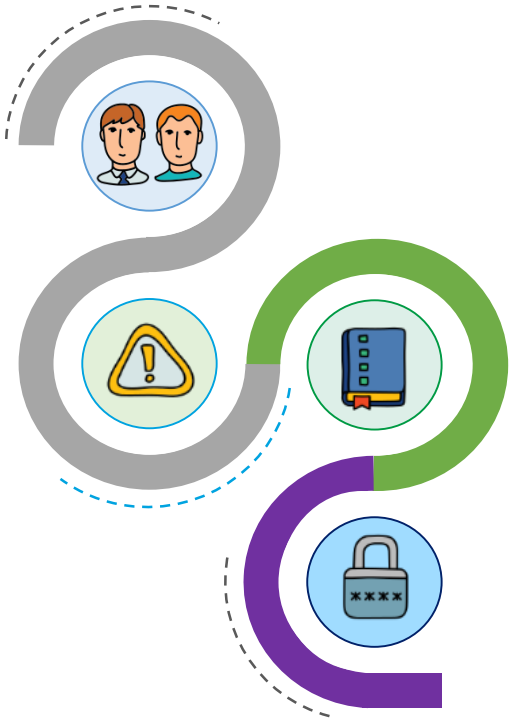
Martin



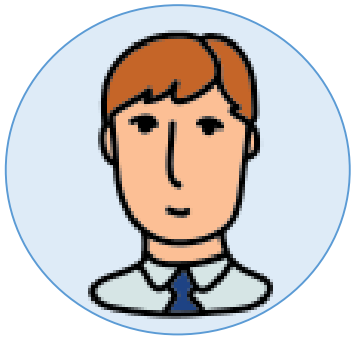
Tom

Privacy Principles

- **Lawful processing** of personal location data (see *Guidelines*)
- Data protection **by design and default** (see *Guidelines*)
- Data **minimisation** (see *Guidelines*)
- **Data subjects** are also **data owners** (see *Guidelines*)
- Build **trust** (see *EULF Blueprint*)



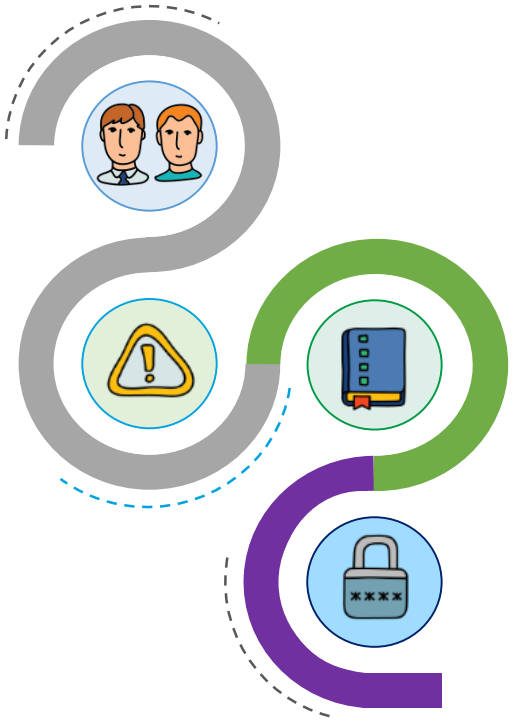
Martin



Tom

ELISE Guidance

- **Permission** for data collection
- Be clear, **go simple**
- Apply data protection **by design and default**
- Publish a **privacy notice**
- Apply **data minimisation**
- **Privacy risk assessment** for the connection to social media, **limiting the purpose** of use of social media information
- **Opt-in or opt-out**

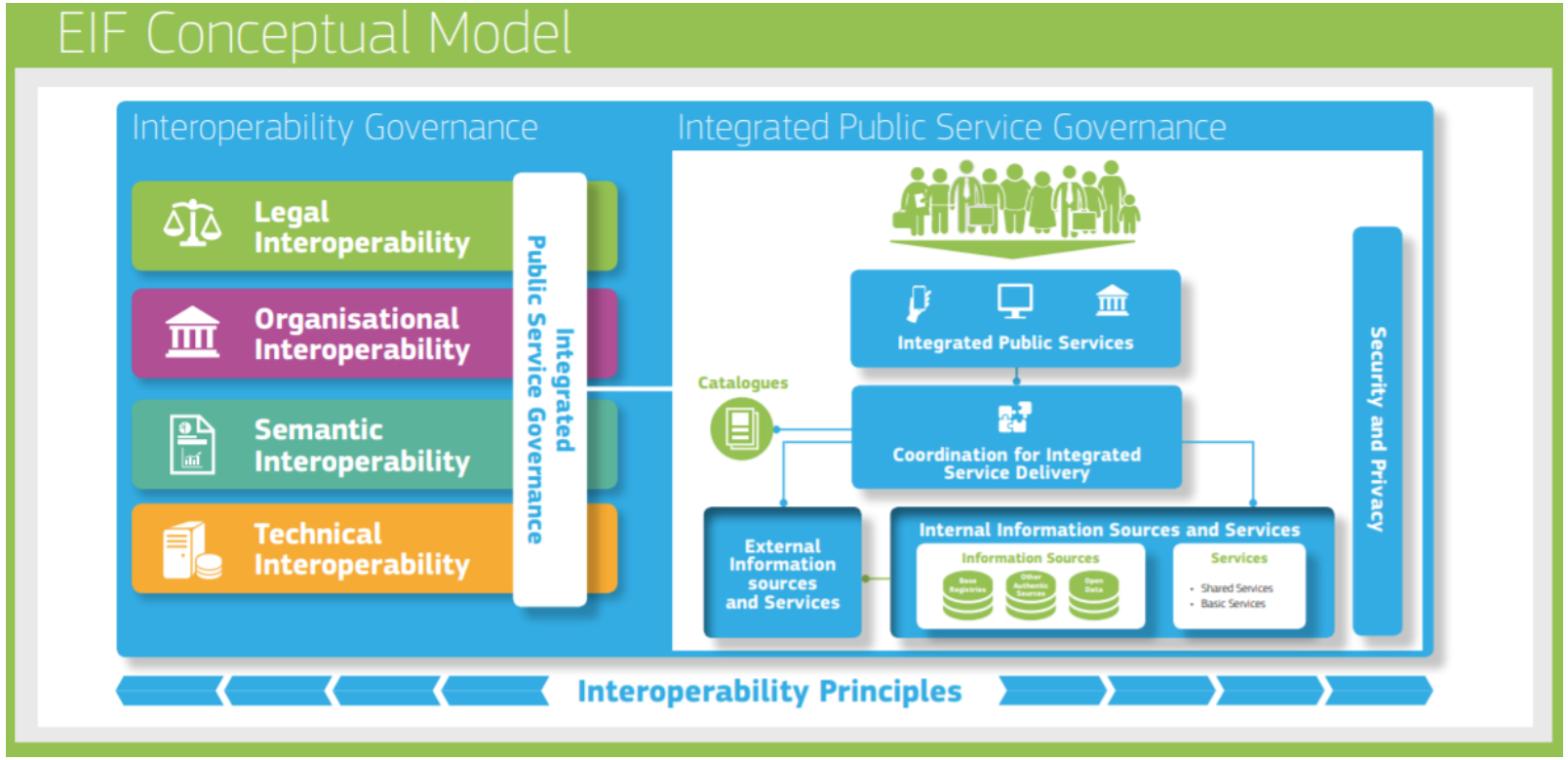


3

ELISE guidance on Location Data Privacy

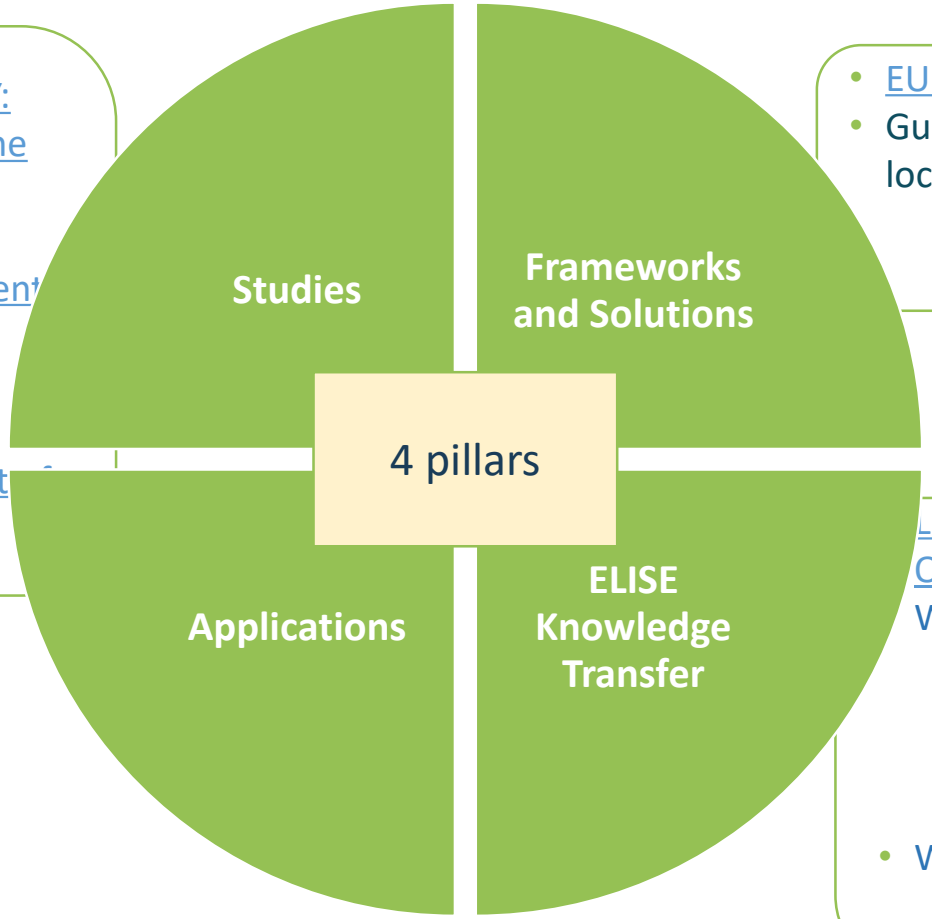
ELISE and the European Interoperability Framework (EIF)

As the central focus of the ELISE action is on "Location interoperability", the alignment with the ISA² *European Interoperability Framework* (EIF) is of high relevance



ELISE guidance on *Location data privacy*

- World Geospatial Industry Council, GEOSPATIAL INFORMATION AND PRIVACY: Policy Perspectives and Imperatives for the Geospatial Industry, 2020
- Assessing the impacts of digital government transformation in the EU
- AI Watch Artificial Intelligence in public services - Overview of the use and impact of AI in public services in the EU



- EULF Blueprint
- Guidelines for public administrations on location privacy:
  - Version 1 (2018)
  - Version 2 (2020)

Location Interoperability Framework Observatory

Workshop
- "General Data Protection Regulation (GDPR): *Trusting the use of your personal location data*", 22/09/2018
- Nordic GDPR workshop 07/06/18

- Webinars:
  - GDPR, 24/04/18
- ELISE Joinup page on Location Data Privacy

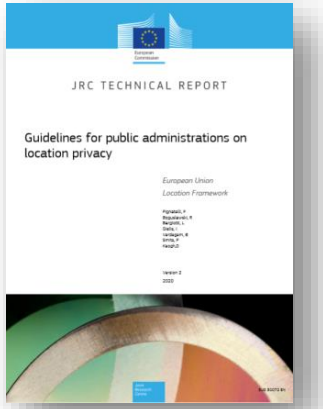
EULF Blueprint & *Location data privacy*

EULF Blueprint

- **Policy and Strategy Alignment**
- Digital Government Integration
- Standardisation and Reuse
- Return on Investment
- Governance Partnerships and Capabilities

Recommendation 3:
"Ensure all measures are in place, consistent with legal requirements, to protect personal privacy when processing location data"
Why, How, Challenges and Best Practices

- Guidelines for public administrations on location privacy
- LIFO



Aligned with EIF

- Principle 8 Security and Privacy (Rec 15)
- Organisational interoperability (Rec 28/29)
- Semantic interoperability (Rec 30)
- Integrated public service governance conceptual model (Rec 46)

Guidelines for public administrations on location privacy

to outline the key obligations that public administrations should comply with when handling personal location data

to raise awareness about the importance of location data privacy

Location Interoperability Framework

LIFO

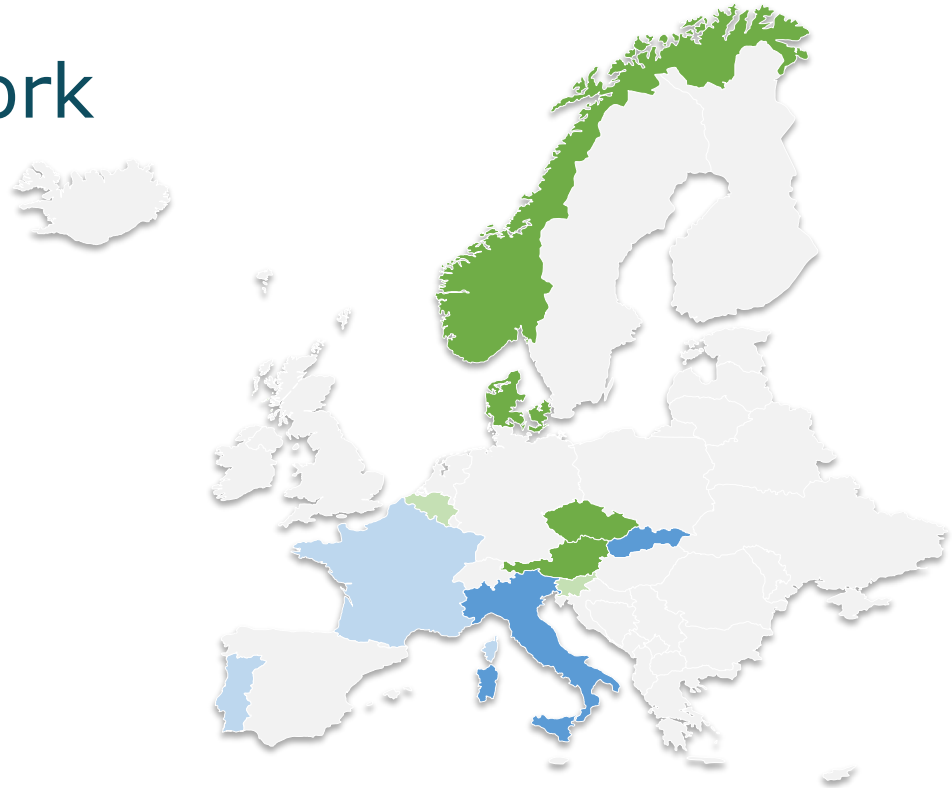
LIFO monitors the alignment of countries participating to the ISA² programme with the EULF Blueprint through a series of *questions* and related *indicators*

Question 3.1

How well-prepared are controllers and processors of public sector location data in your country for GDPR, including awareness of potential location data privacy issues and processes in place to comply with the rights of data subjects?

- 4 out of 10 countries (Austria, Czech Republic, Denmark and Norway) are fully prepared
- Recommendation index at 0.5 indicates need for progress in GDPR implementation

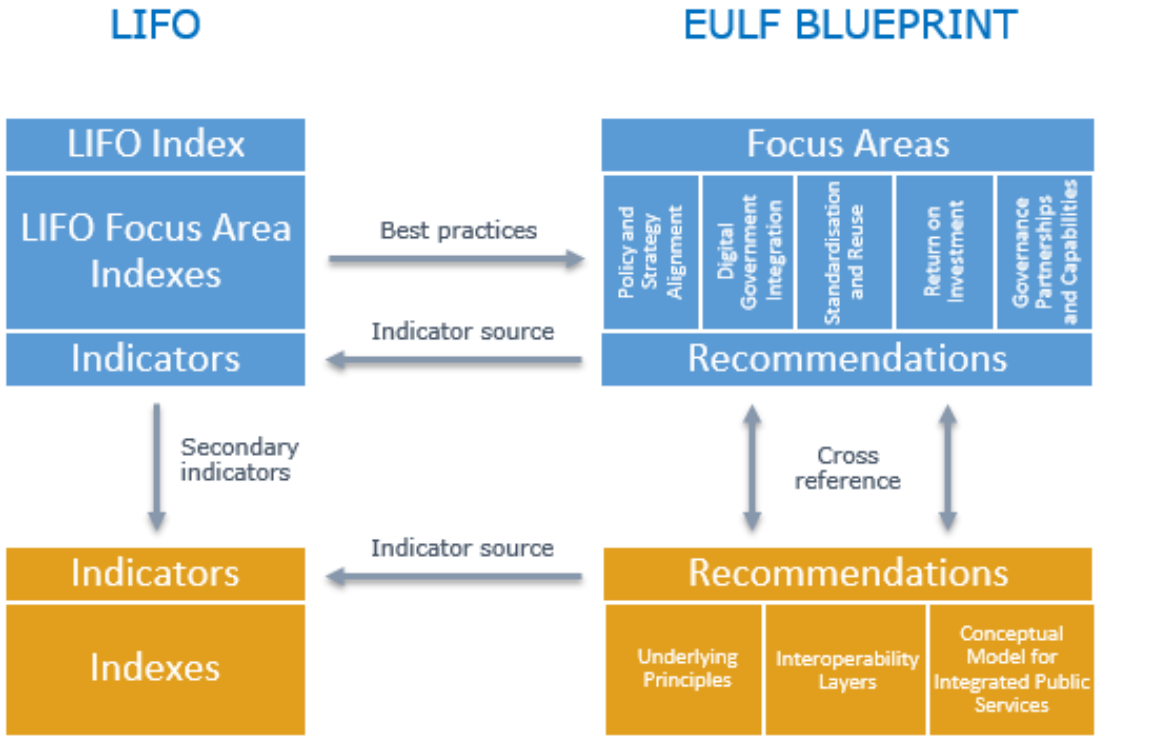
(Focus Area: *Policy and Strategy Alignment*)



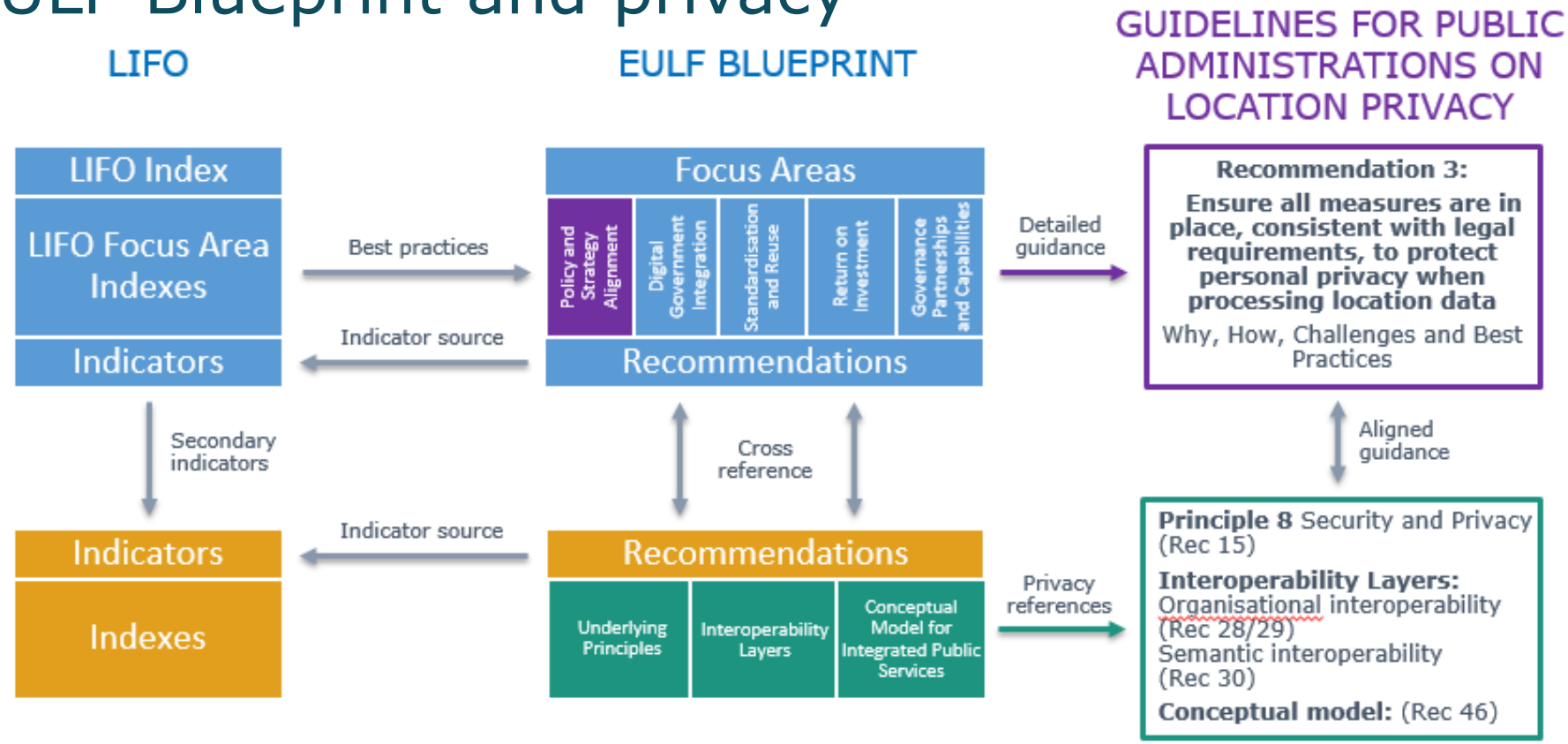
LIFO: Location Interoperability Framework Observatory - Presentation to ISA² Working Group

- Most organisations fully prepared
- Some organisations fully prepared
- Some significant gaps in preparations, little awareness or preparedness
- N/A

EIF, EULF Blueprint and …



EIF, EULF Blueprint and privacy



Location Data Privacy & Digital Government Transformation

An original **conceptual framework for assessing the impacts of Digital Government transformation in the public sector** and the impacts they have at social, economic and political levels, including several use cases

Technical Report

Germany / Spain

Case Studies

Search for **legitimacy** and **trust** can represent a significant **barrier to digital transformation** but can also be one of the potential **positive effects** that new technologies can produce

Lack of citizens' trust can affect **private** data processors as well as **governments**

AI implementations are particularly critical from a trust perspective and must rely upon **consultations** and **communication**

Citizens are rather **unwilling to trade off data privacy** against receiving services

Distrust can lead to new forms of **digital divide**

AI Watch - Artificial Intelligence in public services

Gather information on **EU Member States' initiatives on the use of AI in public services** and develop a methodology to identify risks and opportunities, drivers and barriers of the use AI in public services.

Monitor the development, uptake and impact of Artificial Intelligence (AI) in Europe

Privacy may be at risk due to the fact that many **devices and services gather data without the user's full understanding** of what is done with it afterwards

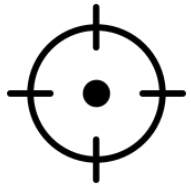
Potentially disruptive innovation may be limited by **citizens not appreciating governments' pervasiveness** for privacy concerns

AI governance as an **extension of data protection and competition regulations** to update and make them more effective

Ethical codes as the most diffused solution **to steer the development and use of AI**

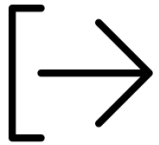
ELISE's *Location Data Privacy* page on Joinup

A repository for privacy and geospatial



Background and scope

Overview of location data privacy concept and relevance

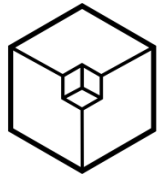


Outputs

Guidelines for public administrations on location privacy

WGIC Geospatial Information and Privacy

Events



Additional resources

EULF Blueprint

Location Interoperability Framework Observatory (LIFO)

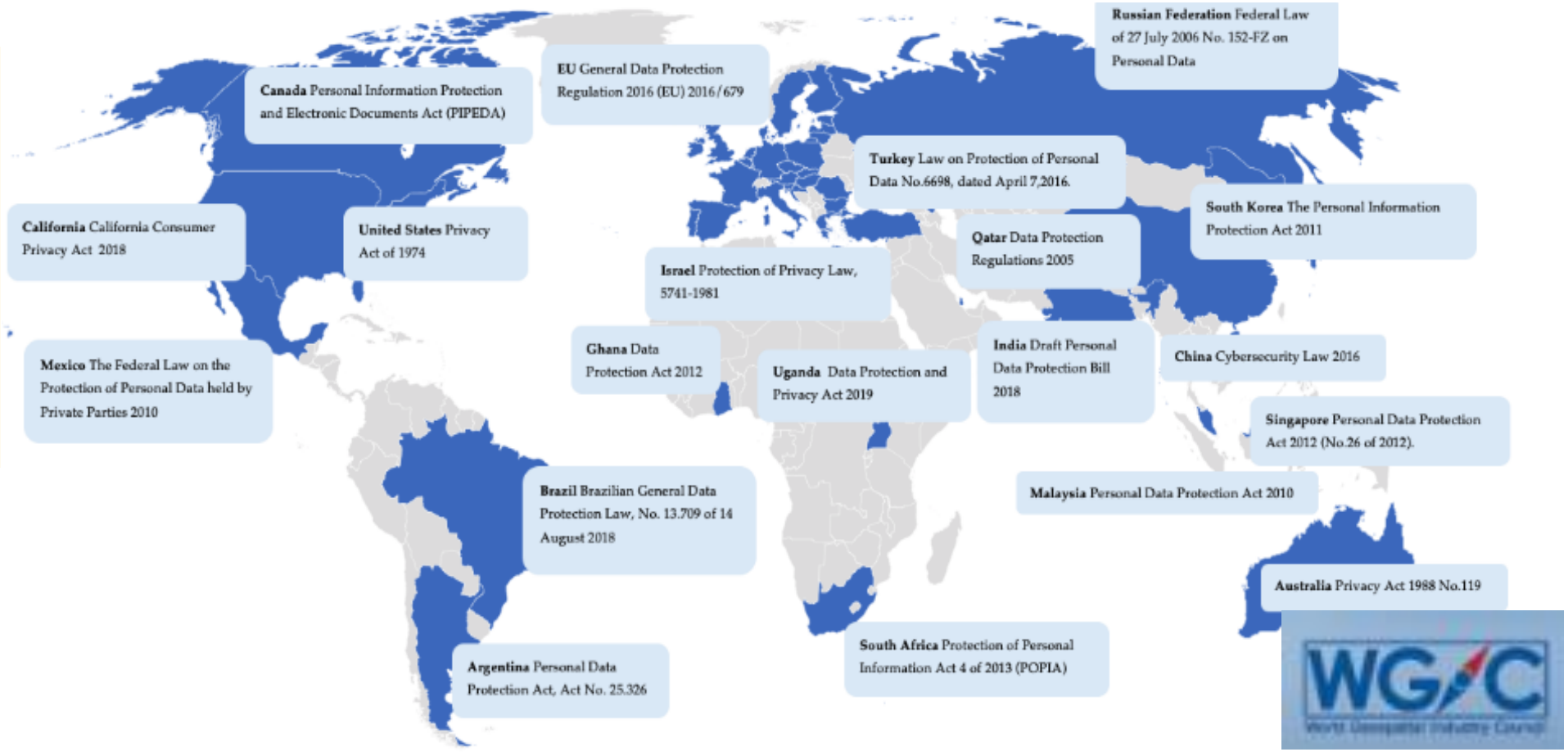
European Commission

Impact: WGIC policy report

GEOSPATIAL INFORMATION AND PRIVACY:
Policy Perspectives and Imperatives for the Geospatial Industry

ELISE contributed to the methodological framework for mapping of requirements under data protection and privacy legislation

Review of data protection regimes throughout the world



Impact: Citations

The Guidelines for Public Administrations on Location Privacy have been cited in several scholarly publications and presentations, to name a few:

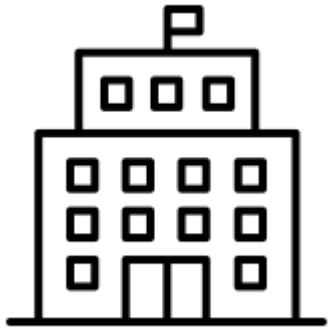
- Mehmaz Ataei, ***Location Data Privacy : Principles to Practice***, doctoral dissertation, Westfälische Wilhelms-Universität Münster, 2018
- Mehmaz Ataei, ***Privacy theory in practice: designing a user interface for managing location privacy on mobile devices***, Journal of Location Based Services, 2018
- Mehrnaz Ataei, Auriol Degbelo, Christian Kray, Vitor Santos, ***Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services***, 2018
- Rose Yorke Barber, ***Towards a methodology to estimate carbon emissions savings from local mode shift initiatives: a review of challenges and emerging technologies***, 2019
- Tanja Masson-Zwaan, Mahulena Hofmann, ***Introduction to Space Law***, 2019
- Peta Mitchell, ***Databodies in and through locative digital media***, presentation, American Association of Geographers Annual meeting, 2018
- Michelle Riedlinger, Chantal Chapman, Peta Mitchell, ***Location awareness and geodata sharing practices of Australian smartphone users***, 2019
- Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou, Konstantinos E. Psannis, ***GDPR Interference With Next Generation 5G and IoT Networks***, 2020

4

Conclusions and main take-aways

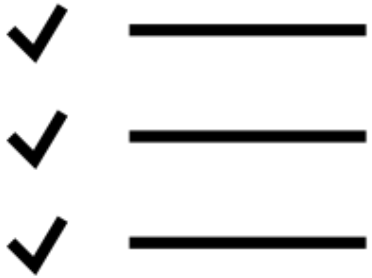
Key messages

Common European data spaces require **trust** in personal data usage

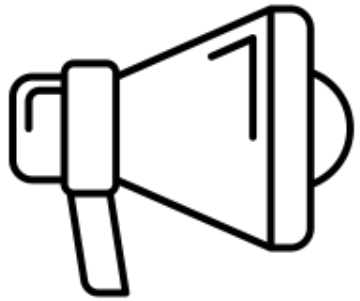


(Location) data privacy is and will remain **central in all European initiatives**

Technological innovations must be assessed under their **compliance with data protection legislation**

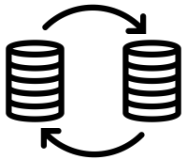


For better uptake GDPR and location data privacy require simple **guidelines and concrete use cases**, complemented by **awareness raising** on use of location data



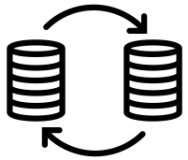
Ethical issues and **social impacts** of location data use go beyond sheer compliance with regulations

Challenges 1/2



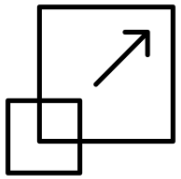
Peculiarities of location data privacy

Characteristics of personal location data determine particular risks



Data stewardship and GDPR

GDPR pushes from data ownership towards data stewardship building on users' trust



Detail level, scale and linkability of data

Trade-off between granularity/linkability and level of utilisation of data

Inter-reliant nature of public bodies on the private sector

Public services depending on privately sourced technologies and potentially affected by trust issues related to them

Policymaking and geospatial information

Increasing difficulties for lawmakers to keep pace with technological developments linked to the versatility of geospatial information

Awareness of public service providers

Possible lack of awareness of the collection/ processing of personal location data and when embedded within the overall process

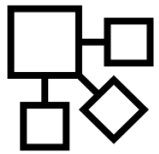
Challenges 2/2

Location data privacy in local and regional administrations

Smart cities and regional public services require increasing amounts of personal location information

Level of implementation

GDPR places particular implementation burdens on new technologies



Location data privacy implications for business and commercial data ecosystems

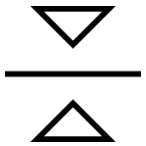
Increasing and possibly infringing use of location data for customer profiling

Big Data and GDPR

Big Data to be carefully managed to avoid unauthorised data profiling (for which location data constitute critical information)

Citizen generated and volunteered data in GDPR

Make sure that the purpose for which data provided by citizens are used is lawful and explicitly authorised



Alignment of EU legal framework

Transfer of data between different Member States must take into account possibly diverging national data protection laws

The legacy of ELISE for the Digital Europe Programme

Allowing citizens' trust in the use of their personal location data to support the implementation of the "*Clean, sustainable and smart communities and mobility*" initiative of the Digital Europe Programme (DEP)

Developing and deploying of interoperable, transparent, secure, and cross-border solutions deployed at a large scale to a large number of cities

Leveraging citizens' and businesses' trust to build Spatial Data Infrastructures (SDIs) capable of supporting self-sustainable, interoperable and cross-border data ecosystems

Location privacy awareness raising based on real examples and tools to assess location privacy risk and mitigate potential exposures (e.g. anonymisation techniques)

5 References

Bibliography 1/2

- Boguslawski R., Van Gansen K., Valayer C., Pignatelli F., European Union Location Framework Blueprint, Luxembourg, 2020
- Joint Research Centre, LIFO: Location Interoperability Framework Observatory - 2019 State of Play Report, 2020
- Misuraca, G., and van Noordt, C.., Overview of the use and impact of AI in public services in the EU, EUR 30255 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19540-5, doi:10.2760/039619, JRC120399
- Pignatelli, F., Boguslawski, R., Bargiotti, L., Gielis, I., Verdegem, B., Smits, P. and Keogh, D., Guidelines for public administrations on location privacy , EUR 30070 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-10225-0, doi:10.2760/546158, JRC119398
- Codagnone, C. et al., Assessing the impacts of digital government transformation in the EU, Misuraca, G. editor(s), EUR 30230 EN, , Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19005-9 (online), doi:10.2760/40285 (online), JRC120865
- World Geospatial Industry Council, GEOSPATIAL INFORMATION AND PRIVACY: Policy Perspectives and Imperatives for the Geospatial Industry, 2020

Bibliography 2/2

Reference legislation and guidelines:

- Directive 95/46/EC
- Regulation (EC) No 45/2001
- Decision No 1247/2002/EC
- Directive 2002/58/EC
- Council Framework Decision 2008/977/JHA
- Directive 2009/136/EC
- Regulation (EU) 2016/679
- Regulation (EU) 2016/679
- Regulation (EU) 2018/1725

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Council of Europe Convention No. 108 on data protection
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29100.

Q&A

Thank you

Stay tuned

Join the *ELISE* community in JoinUp

@eu_location

eulocation@ec.europa.eu

ELISE playlist