Data Protection in Scientific Projects – Dos and Don'ts

Dr. h.c. Marit Hansen

State Data Protection Commissioner
of Schleswig-Holstein, Germany

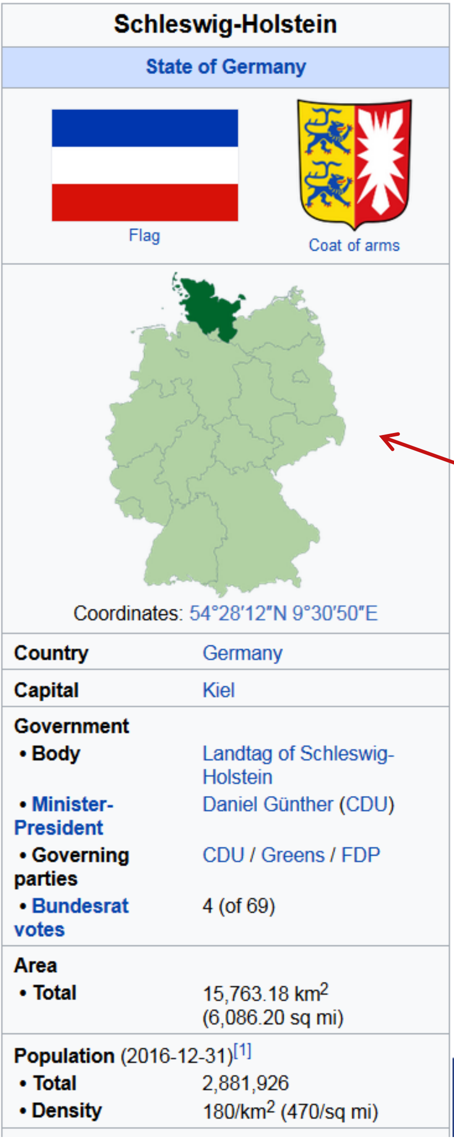
Bonn, 1 February 2024

Plattform Privatheit

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Setting of ULD

- State Data Protection Authority (DPA) for both the public and private sector
- Located in Kiel, Germany



Schleswig-Holstein

State of Germany

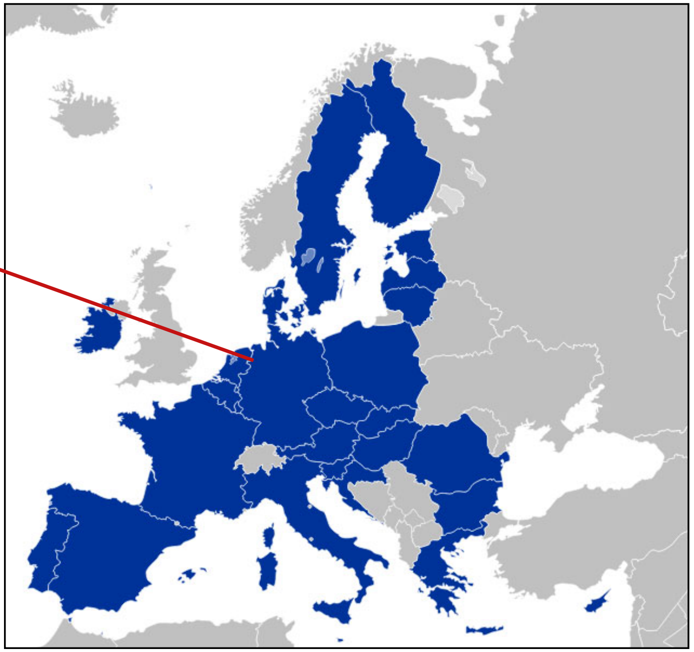
Flag

Coat of arms

Coordinates: 54°28′12″N 9°30′50″E

Country	Germany
Capital	Kiel
Government	
• **Body**	Landtag of Schleswig-Holstein
• **Minister-President**	Daniel Günther (CDU)
• **Governing parties**	CDU / Greens / FDP
• **Bundesrat votes**	4 (of 69)
Area	
• **Total**	15,763.18 km^2 (6,086.20 sq mi)
Population (2016-12-31)[1]	
• **Total**	2,881,926
• **Density**	180/km^2 (470/sq mi)

Source: en.wikipedia.org/wiki/Schleswig-Holstein



Source: Kolja21 via Wikimedia

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Imbalance in power ⇨ data protection necessary

GDPR: Obligations for controllers and processors

Important: Perspective of the individual

More than security of personal data

Image: beludise via Pixabay

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

General Data Protection Regulation = GDPR

Powerful toolbox
if applied appropriately

- Market location principle (Art. 3 GDPR)
- Responsibility (Art. 24 GDPR)
- Data protection by design (Art. 25(1) GDPR)
- Data protection by default (Art. 25(2) GDPR)
- Security (Art. 32 GDPR)
- Data protection impact assessment (Art. 35 GDPR – "Rights and freedoms of natural persons")
- Certification (Art. 42+43 GDPR)
- Fines & sanctions by Data Protection Commissioners (Art. 83+84 GDPR)
- Courts

Image: Astryd_MAD via Pixabay

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Data Protection Principles

Art. 5 GDPR – Principles relating to processing of personal data

Design requirements

(1)

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimisation
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (~ security)

(2) Accountability

Precondition: diligent analysis of responsibilities and legal basis

Image: Pete Linforth via Pixabay

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

GDPR demand: risk mitigation

High risk – design with technical and organisational measures necessary

Trustworthiness through appropriate measures and checkability

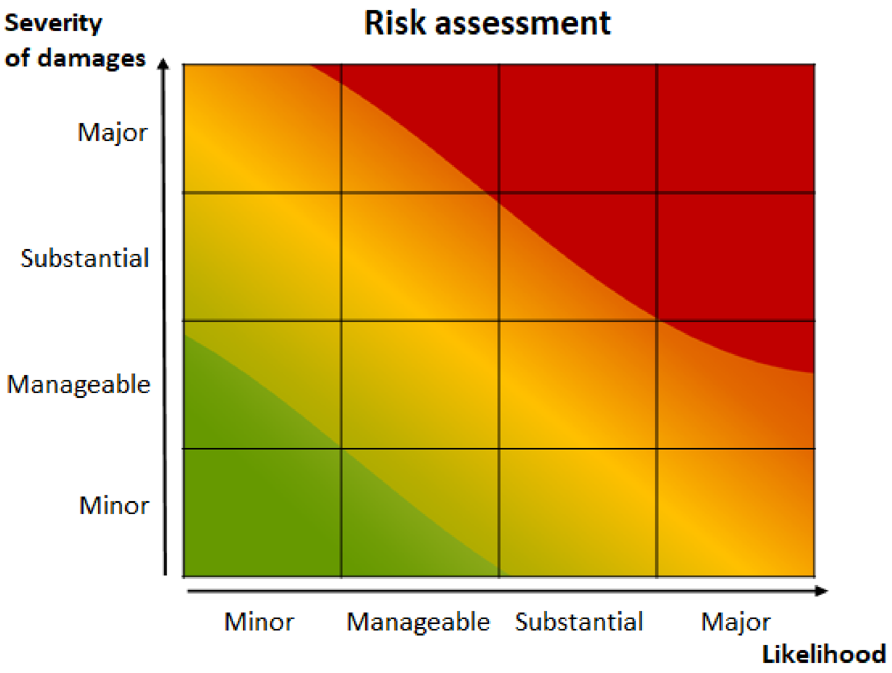
Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

The notion of risk in the GDPR

- Risk = severity of potential damage x likelihood
- Focus: rights and freedoms of natural persons – see Charter of Fundamental Rights
- Risk must be mitigated with technical and organisational measures (TOM) to protect rights

→ Articles 24, 25, 32, 33, 34, 35, 36 GDPR



Matrix: own translation from DSK-Kurzpapier Nr. 18 „Risiko", Datenschutzkonferenz [License www.govdata.de/dl-de/by-2-0], https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Mistakes

Image: Gerd Altmann via Pixabay

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Mistakes

Mistake 1: nobody feels responsible

- Controller – determines the purposes and means of the processing of personal data – alone or jointly
- Clarity about persons in charge and about processes

Mistake 2: forgetting about purposes

- Purposes: lawful, clearly defined
- Only necessary personal data
- Constraints when usage for other purposes desired

Mistake 3: no clear legal basis

- Consent? Legitimate interests? [to come: EDPB Guidelines]
- Caveat: data transfer outside EU/EEA

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Mistakes

Mistake 4: forgetting about data subjects

- Needed: proper information and …
- … processes for rights to access, rectification, erasure, portability

Mistake 5: security deficiencies

- Needed: professional information security …
- … including a process for handling data breaches

Mistake 6: problematic risk assessment

- Needed: perspective of the data subjects …
- … and, if high risk probable, Data Protection Impact Assessment prior to data processing

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Mistakes

Mistake 7: shortsighted planning, assuming static properties

- Needed: taking into account the full lifecycle and …
- … an iterative process (data protection management) for checking for necessary changes and dynamic adaptations

Mistake 8: anonymization not properly done

- Often tried: escape from the GDPR by processing anonymous data
- But: the anonymization has to work properly to prevent the risk of (re-)identification
- Otherwise: not anonymous, but personal data
- Way out: data minimization within the GPDP, especially through pseudonymization

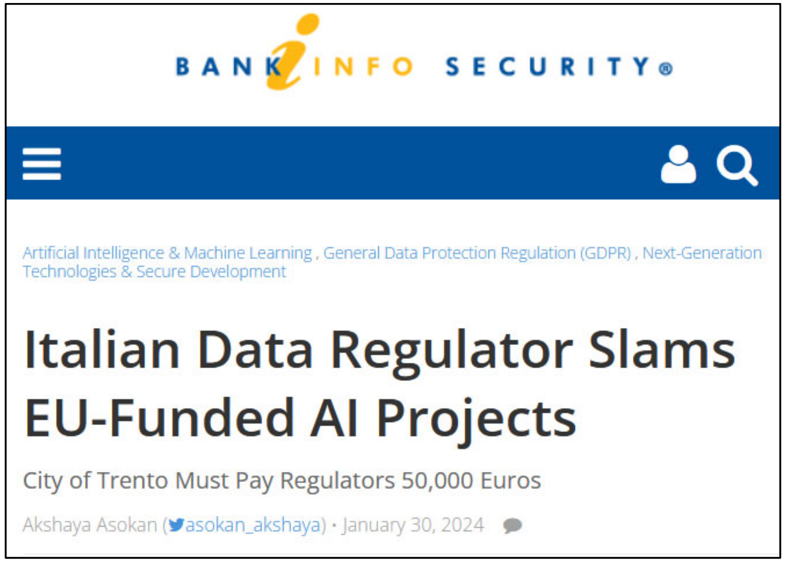
Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

https://www.bankinfosecurity.com/eu-funded-ai-projects-slammed-by-italian-data-regulator-a-24218

EU funding for unlawful projects?

- "The Italian data protection regulator fined a midsize northern city 50,000 euros for deploying a pilot artificial intelligence public safety project financed by the European Union."
- Projects MARVEL, PROTECTOR and PRECRISIS
- AI usage to process audiovisual data to detect threats
- Training on public data sets and contained features such as movement and object detection and clustering methodologies to identify anomalies in movements



BANK INFO SECURITY®

Artificial Intelligence & Machine Learning , General Data Protection Regulation (GDPR) , Next-Generation Technologies & Secure Development

Italian Data Regulator Slams EU-Funded AI Projects

City of Trento Must Pay Regulators 50,000 Euros

Akshaya Asokan (asokan_akshaya) • January 30, 2024

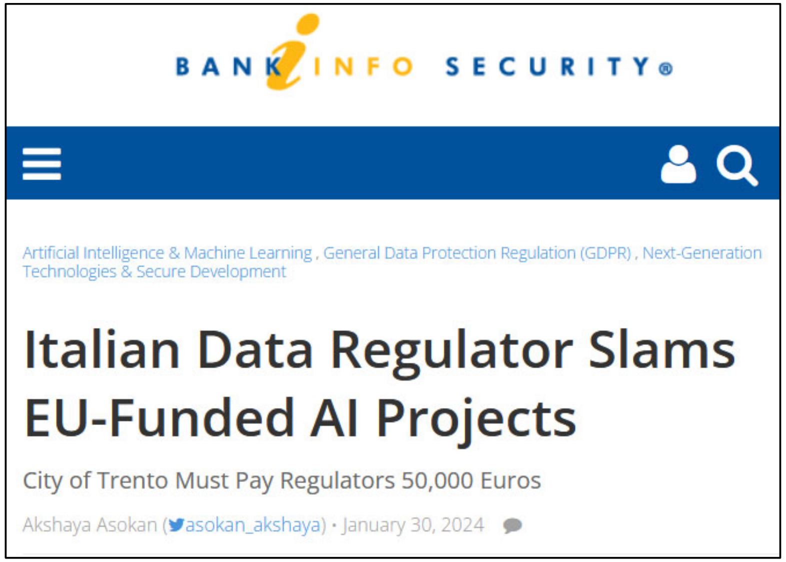
Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

EU funding for unlawful projects?

Italian Data Protection Authority:

- Surveillance of public spaces
- Risk: modify behaviour of people, affect the exercise of democratic freedoms
- No justification of the city
- No Data Protection Impact Assessment in advance
- No information of the residents about cameras and microphones
- Sharing the data with third parties (researchers, police, other countries' law enforcement agencies)



BANK INFO SECURITY®

Artificial Intelligence & Machine Learning , General Data Protection Regulation (GDPR) , Next-Generation Technologies & Secure Development

Italian Data Regulator Slams EU-Funded AI Projects

City of Trento Must Pay Regulators 50,000 Euros

Akshaya Asokan (asokan_akshaya) • January 30, 2024

https://www.bankinfosecurity.com/eu-funded-ai-projects-slammed-by-italian-data-regulator-a-24218

Overview

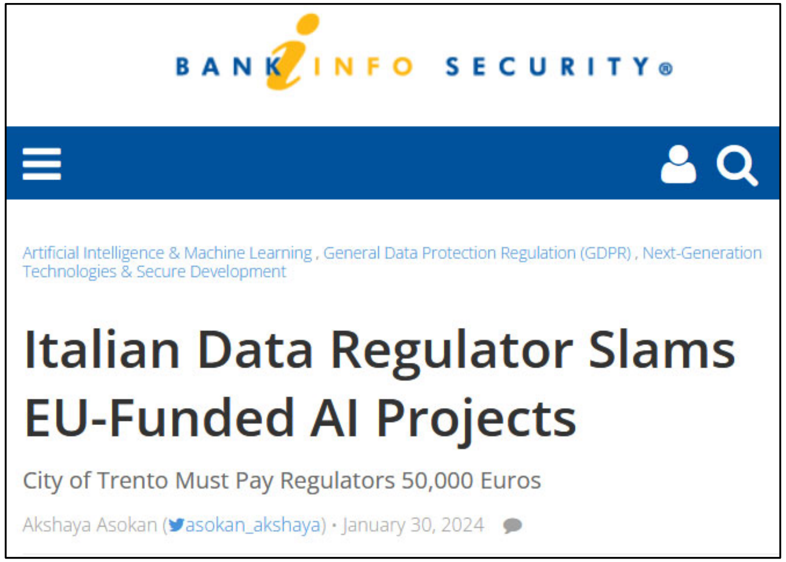
1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

EU funding for unlawful projects?

Italian Data Protection Authority:

- No proper anonymization: "removing user names and URLs, as well as blurring faces and license plates" not sufficient, because still voice capturing from microphones, identification from clothing or body morphology
- Wrong risk estimation ("low")

- Stop of data processing reduced the fine from 20 million Euro to 50.000 Euro



BANK INFO SECURITY®

Artificial Intelligence & Machine Learning , General Data Protection Regulation (GDPR) , Next-Generation Technologies & Secure Development

Italian Data Regulator Slams EU-Funded AI Projects

City of Trento Must Pay Regulators 50,000 Euros

Akshaya Asokan (asokan_akshaya) • January 30, 2024

https://www.bankinfosecurity.com/eu-funded-ai-projects-slammed-by-italian-data-regulator-a-24218

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Summary & outlook

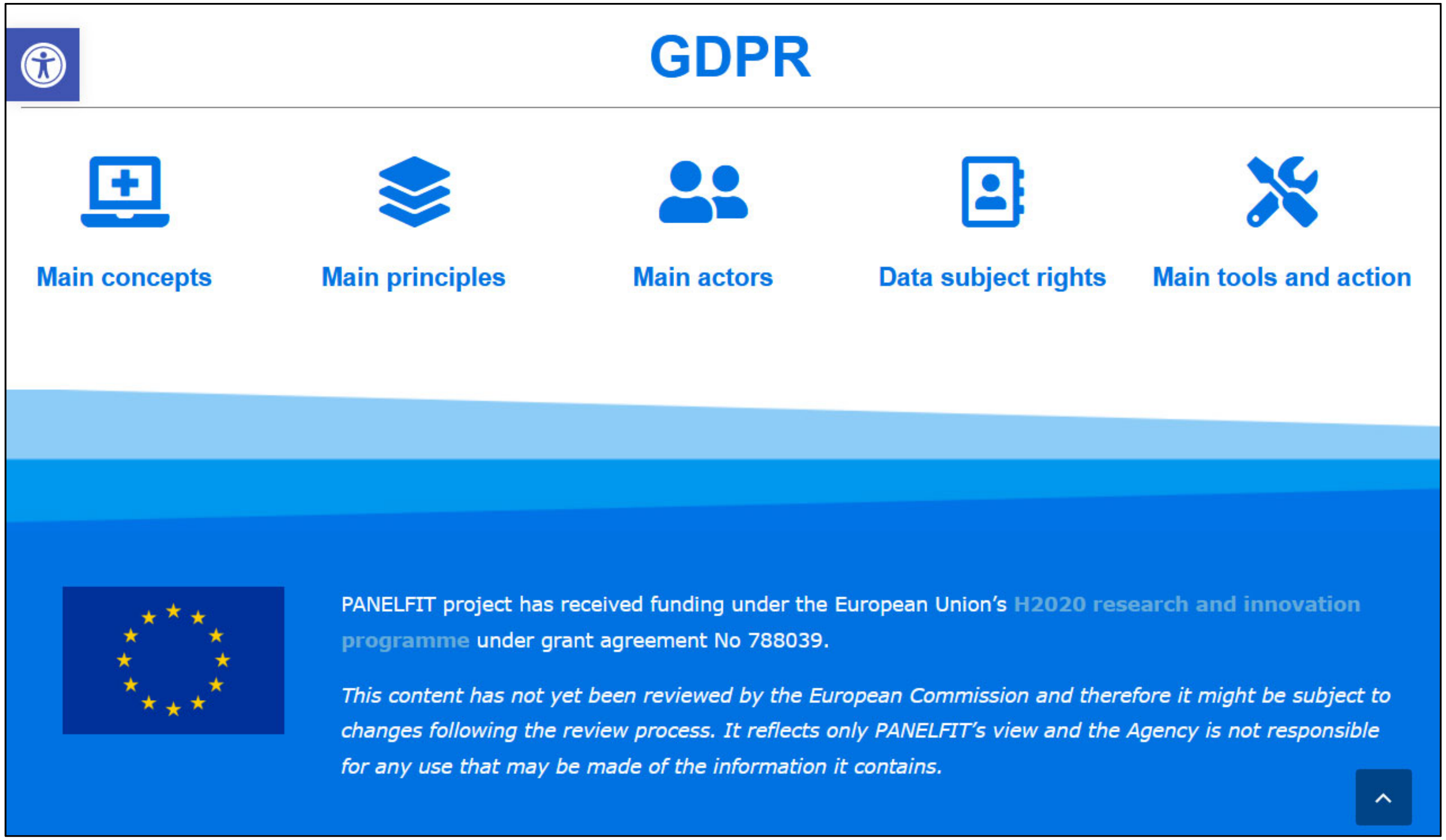
- Data protection in scientific projects is a challenge
  - Collaboration of partners: defining the relationship (joint controllership?), different cultures, different legal regimes
  - Usually time limitations for project employees, no means for establishing a professional infrastructure for data protection
- Advice: discuss with the data protection officers of your organisation
- Stability through thorough planning of processing of personal data:
  - Who is (joint) controller?
  - What is the purpose? What is necessary to achieve the purpose?
  - What is the legal basis?
  - What is the risk? How to mitigate it?
  - If risk not too high: design the system including TOM, otherwise no processing
- Taking the perspective of the data subjects:
  - Both users/citizens and employees

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Participatory Approaches to a New Ethical and Legal Framework for ICT

PANELFIT



GDPR

Main concepts

Main principles

Main actors

Data subject rights

Main tools and action

PANELFIT project has received funding under the European Union's H2020 research and innovation programme under grant agreement No 788039.

This content has not yet been reviewed by the European Commission and therefore it might be subject to changes following the review process. It reflects only PANELFIT's view and the Agency is not responsible for any use that may be made of the information it contains.

https://www.panelfit.eu/

Overview

1. What is data protection?
2. GDPR Principles
3. Standard Data Protection Model
4. Mistakes
5. Summary
6. Links

Links

- DSK: The Standard Data Protection Model Version 3.0a (English version), 2022, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf
- PANELFIT: Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation. THE GDPR – MAIN CONCEPTS, 2022, https://guidelines.panelfit.eu/wp-content/uploads/2022/07/Guidelines-The-GDPR-Main-Concepts.pdf
- SHERPA – Shaping the Ethical Dimensions of Smart Information Systems, https://www.project-sherpa.eu/