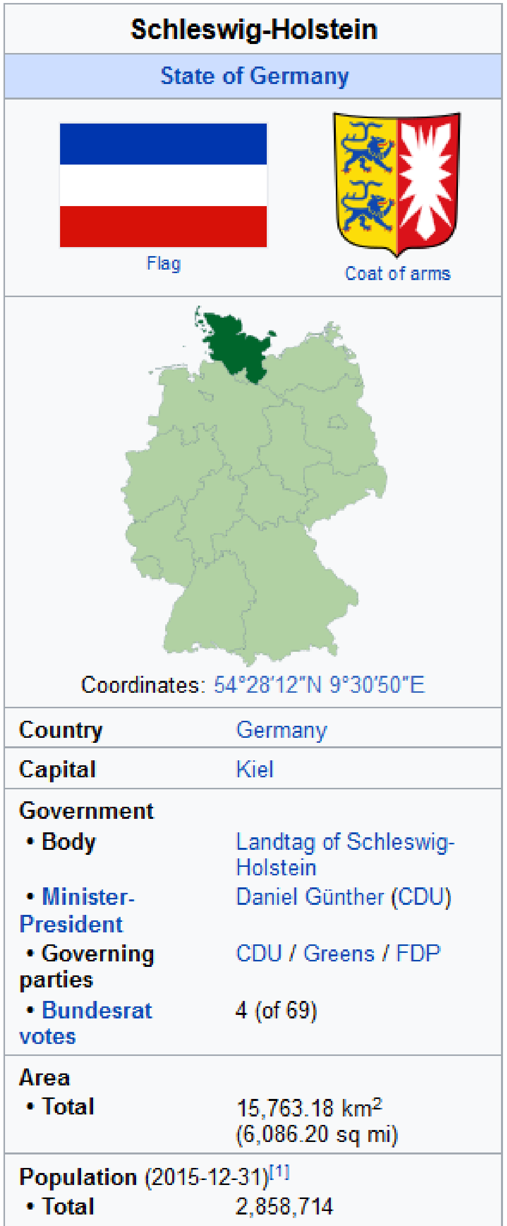
GDPR Risk Framework – Extending the Security Perspective

Felix Bieker & Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein, Germany

ENISA – Garante Workshop, Rome, 8 February 2018

Setting of ULD



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 km² (6,086.20 sq mi)
Population (2015-12-31)[1]	
• Total	2,858,714

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

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

DANMARK
Tønder
Sønderå
Sønderborg
Als(en)
Sylt
Niebüll
Flensburg
Flensburger Förde
Angeln
Nordfriesland
Föhr
Amrum
Bondenau
Langeneß
Halligen
Pelworm
Nordstrand
Husum
Treene
Schleswig
Schlei
Schwansen
Eckernförder Bucht
Eckernförde
Dänischer Wohld
Kieler Bucht
Kieler Förde
Fehmarn
Burg
Eiderstedt
Sorge
Eider
Rendsburg
Kanal
KIEL
Wagrien
Oldenburg
168 m
Bungsberg
Helgoland
35 km
Heide
Dithmarschen
Ostsee-
Holsteinische Schweiz
Plön
Eutin
Neustadt
Neumünster
Lübecker Bucht
Nord-
Itzehoe
B.Segeberg
Trave
Brunsbüttel
Stör
Lübeck
Cuxhaven
Glückstadt
Krückau
B.Oldesloe
Elmshorn
Ratzeburg
Pinnau
Alster
Elbe
Pinneberg
Mölln
Bremerhaven
Stade
HAMBURG
Elbe-Lübeck-Kanal
Buxtehude
MECKLENBURG-VORPOMMERN
NIEDERSACHSEN
km 50

CC SOME RIGHTS RESERVED

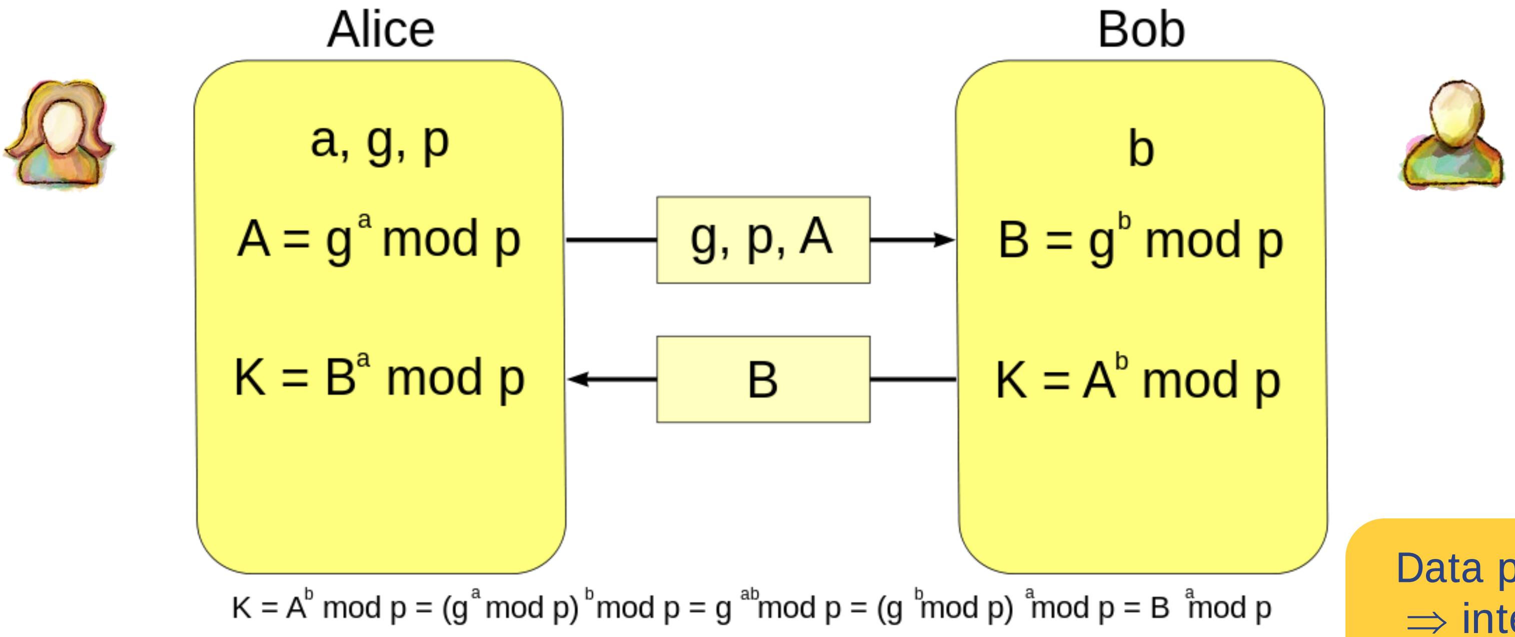
Source: www.maps-for-free.com

Imbalance
in power
⇨
data protection
necessary

Important:
Perspective of
the individual

Source: Marianne Bevis

Data protection: more than IT security



Alice

a, g, p

$A = g^a \bmod p$

$K = B^a \bmod p$

g, p, A

B

Bob

b

$B = g^b \bmod p$

$K = A^b \bmod p$

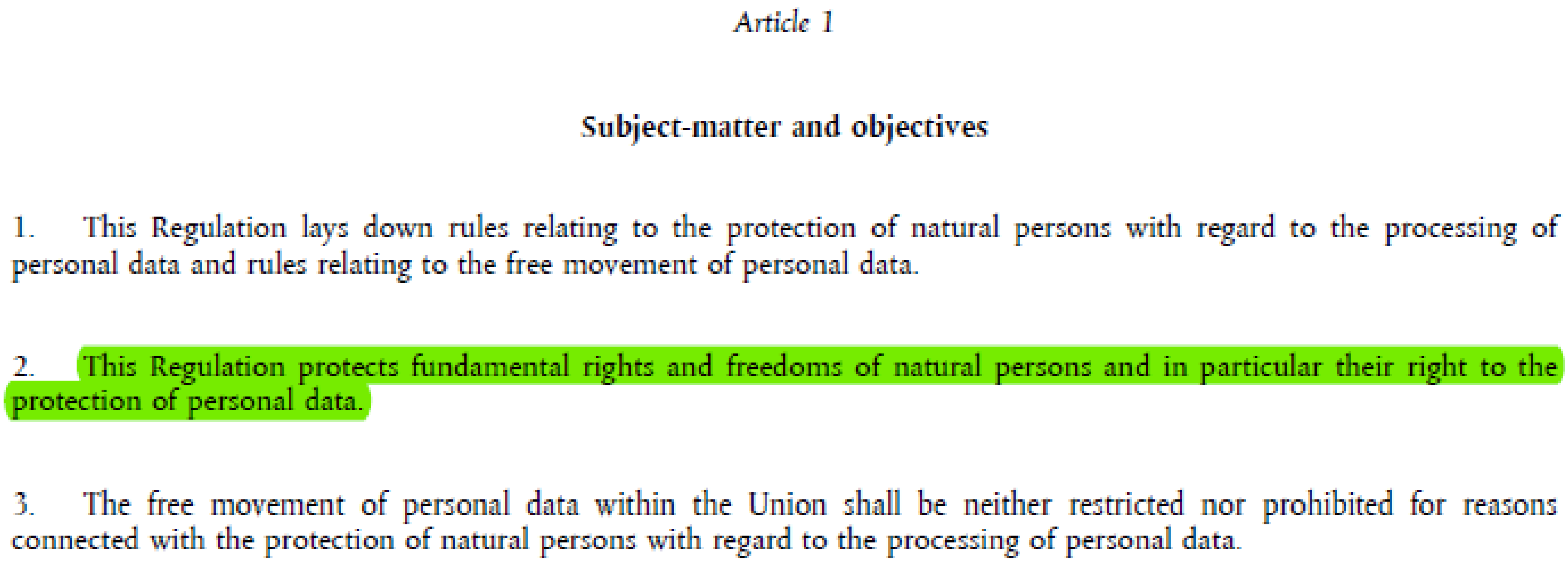
$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Data processing ⇒ interference with fundamental rights

IT security: The adversary is Eve (or Mallory).

Data protection: The adversary is Bob!
(Well, at least he is one of them.)

Data protection: rights of individuals



Article 1

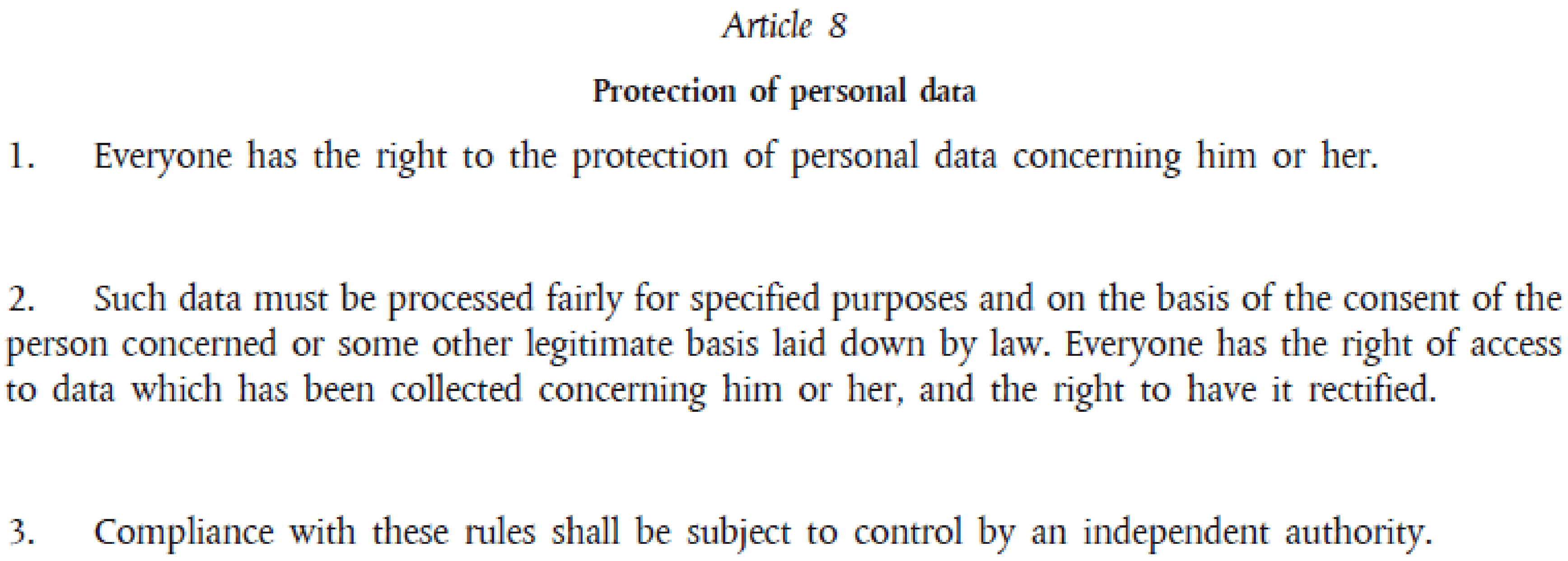
Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Data protection: rights of individuals



Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

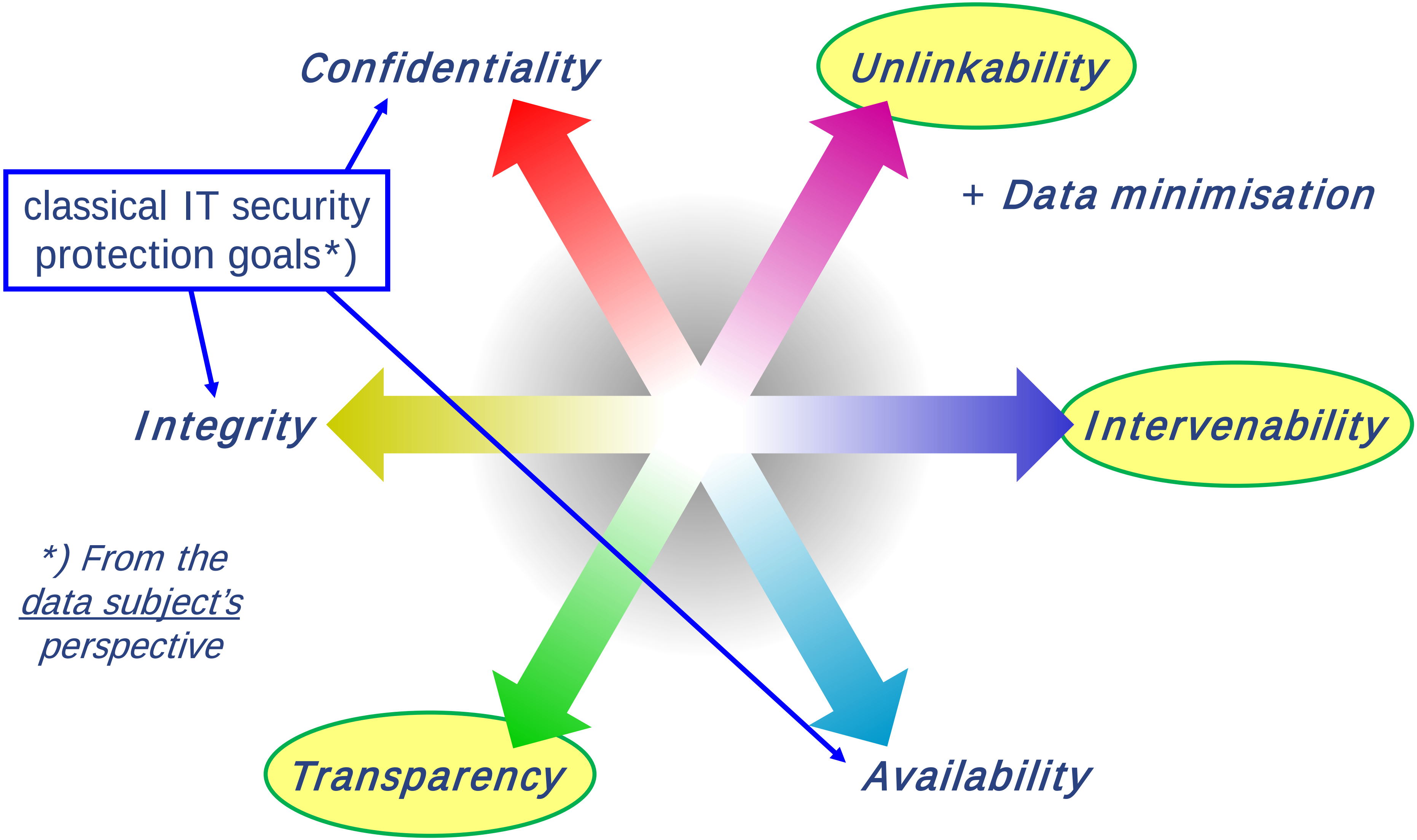
Right to data protection

- Not just privacy harms
- Protects all personal data
- Processing of data is interference
  - Must be justified
  - Interference must be as minimal as possible

And there are more

- Article 7: right to protection of private life (privacy)
- Article 11: freedom of speech
- Article 12: freedom of assembly
- Article 21: non-discrimination
- And others

Protection goals: more than IT security



Confidentiality

Unlinkability

+ Data minimisation

classical IT security protection goals*)

Integrity

Intervenability

Transparency

Availability

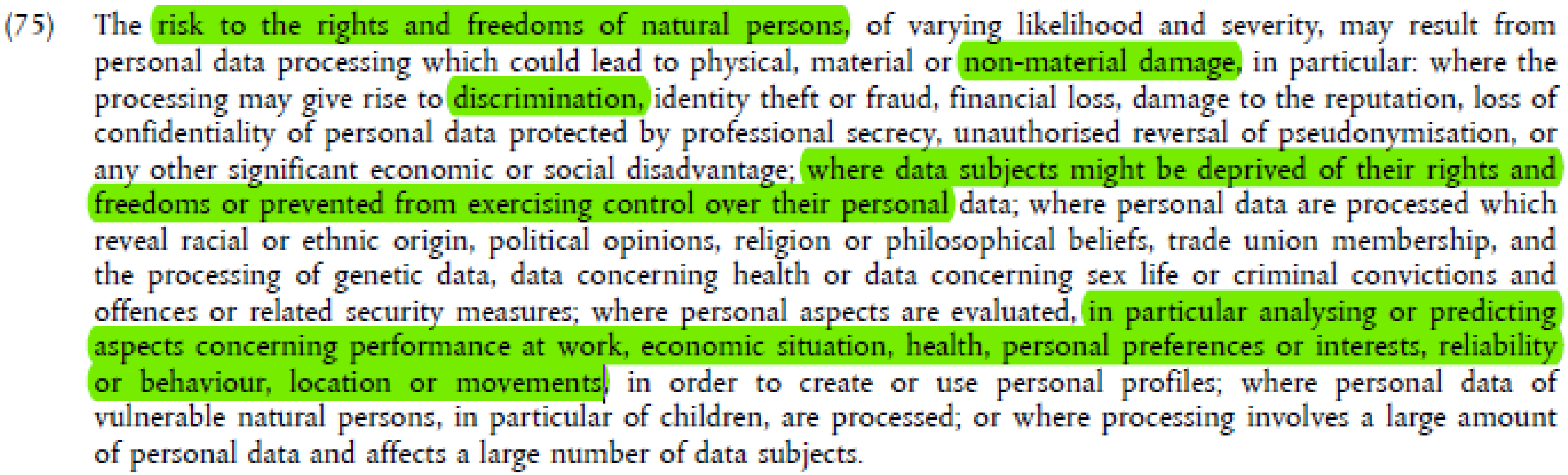
*) From the data subject's perspective

… more than IT security

- Availability + integrity guarantees may hinder erasure, possibly conflicting with data minimisation/unlinkability (purpose limitation) + intervenability (right to erasure, right to rectification)
  - E.g. blockchain implementation
  - E.g. redundancy by distributing various copies
  - E.g. logfiles with personal data

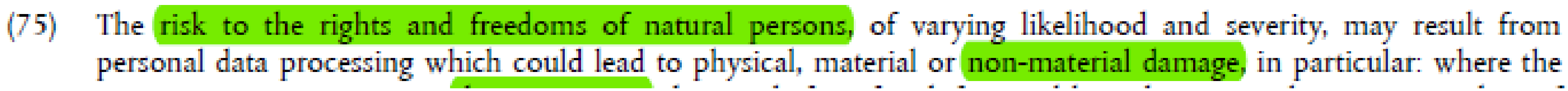
- Confidentiality guarantees may hinder transparency (information) + intervenability (right of access)
  - E.g. hidden data collection
  - E.g. price discrimination

Not just any risk

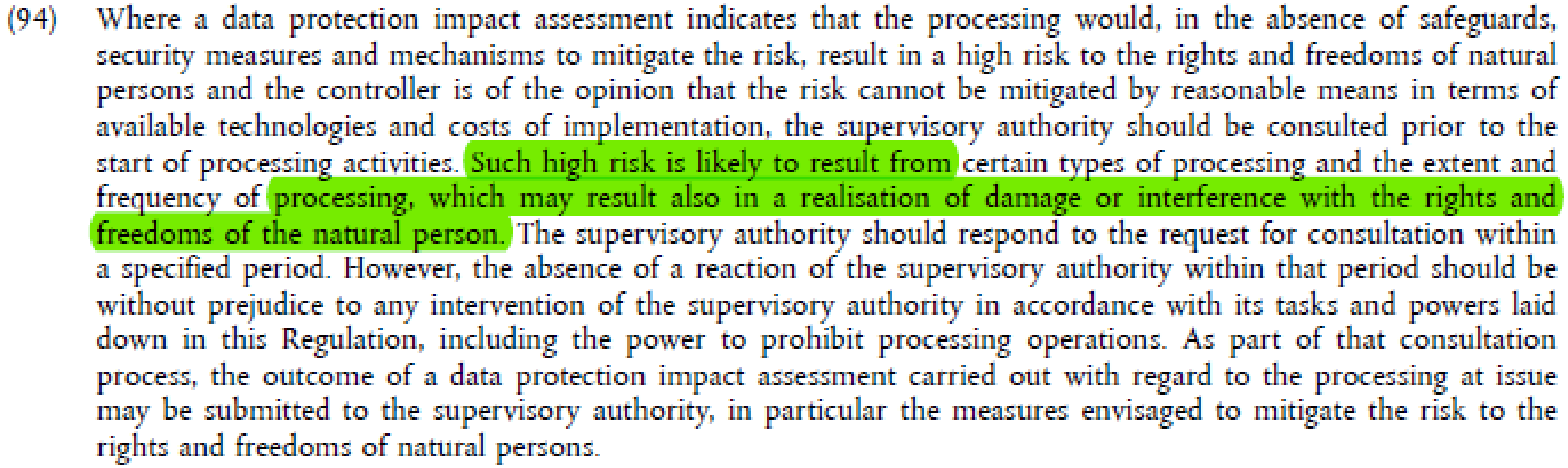


(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Not just any risk



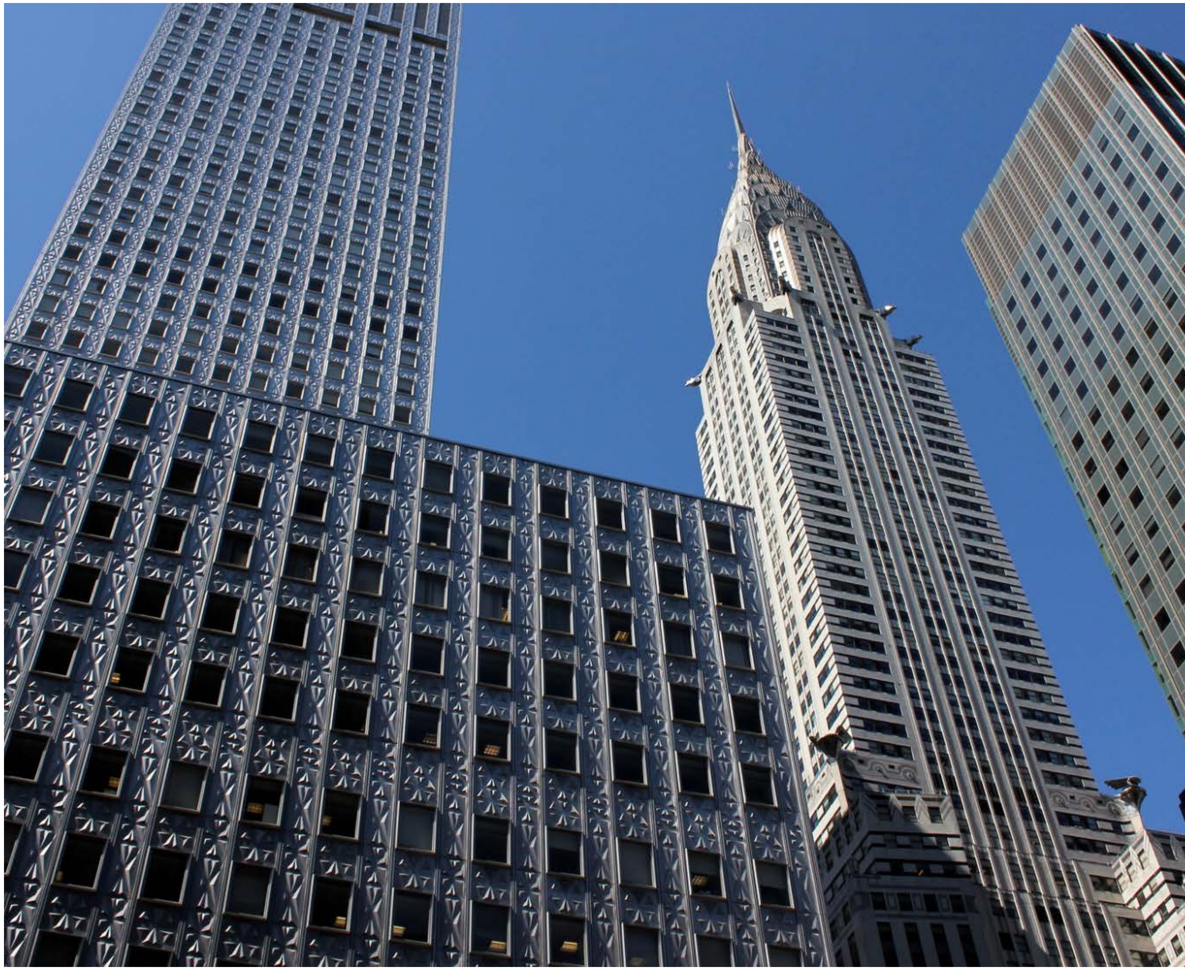
(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the



(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

GDPR risk framework

- Risk sources
  - processor/controller
  - third parties (IT security)
  - adverse events (safety)



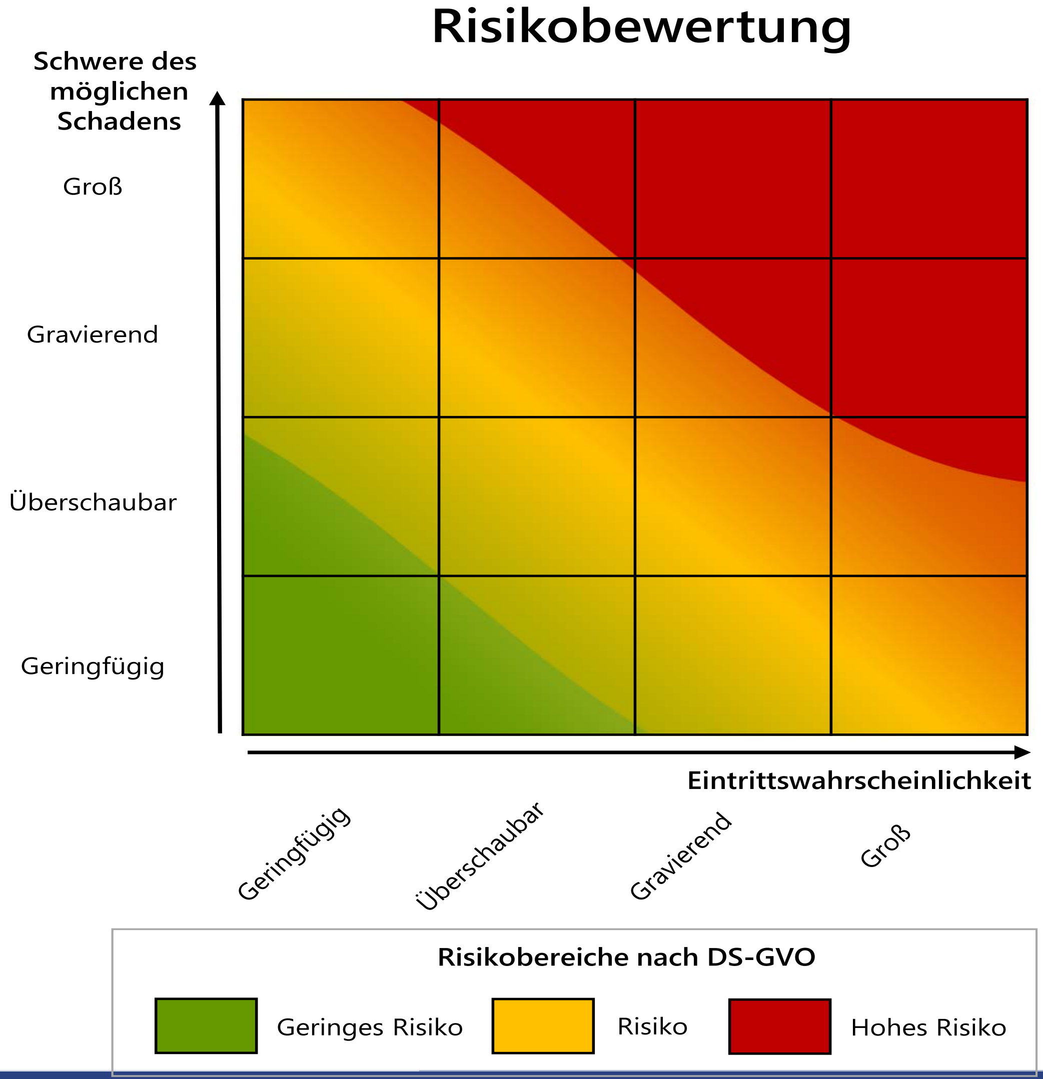
Source: Marianne Bevis

GDPR risk framework

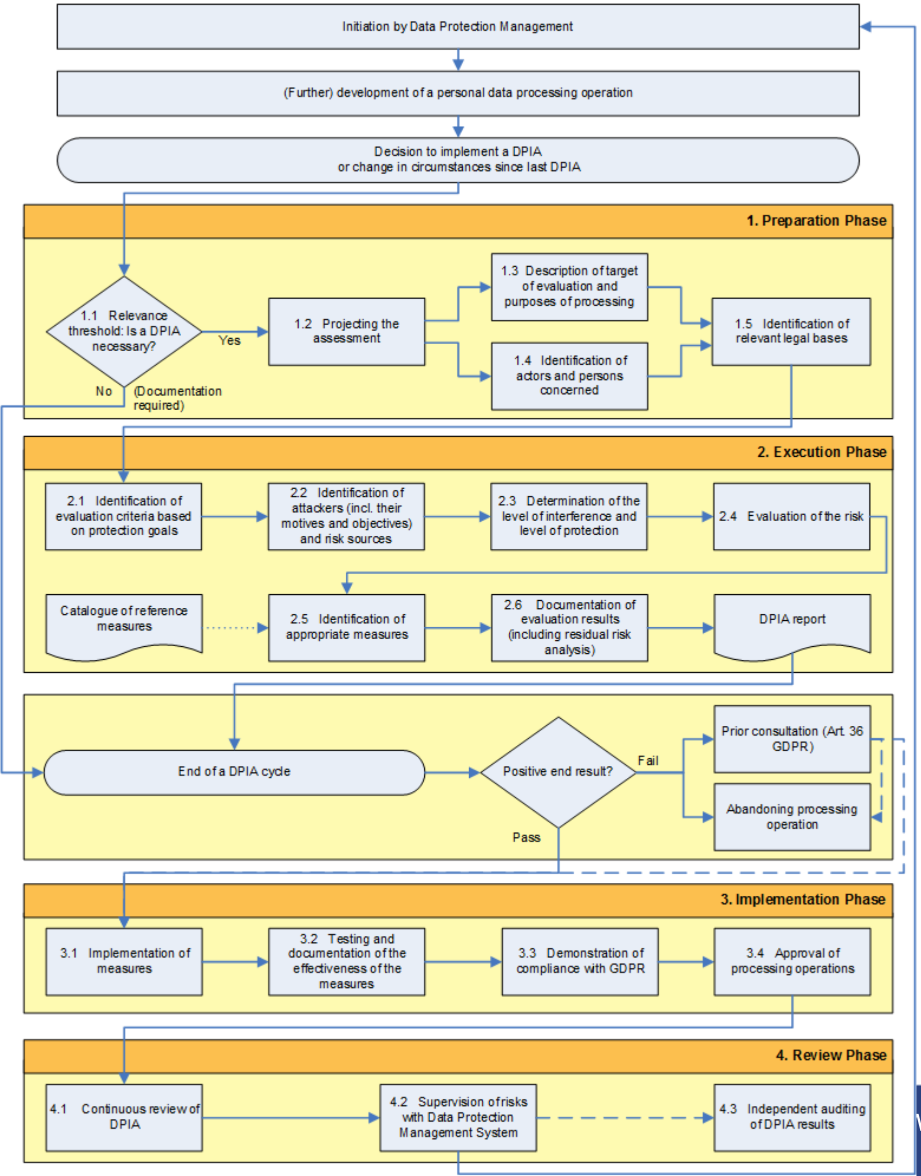
- Risk = severity of potential damage x likelihood
- But cannot be quantified
- Can be approximated objectively

- Risk for rights must be mitigated with technical and organisational measures, etc. to protect rights

→ Arts 24, 25, 32, 35 GDPR



Add-on: DPIA Framework



Initiation by Data Protection Management

(Further) development of a personal data processing operation

Decision to implement a DPIA
or change in circumstances since last DPIA

1. Preparation Phase

1.1 Relevance threshold: Is a DPIA necessary?

Yes

No

(Documentation required)

1.2 Projecting the assessment

1.3 Description of target of evaluation and purposes of processing

1.4 Identification of actors and persons concerned

1.5 Identification of relevant legal bases

2. Execution Phase

2.1 Identification of evaluation criteria based on protection goals

2.2 Identification of attackers (incl. their motives and objectives) and risk sources

2.3 Determination of the level of interference and level of protection

2.4 Evaluation of the risk

Catalogue of reference measures

2.5 Identification of appropriate measures

2.6 Documentation of evaluation results (including residual risk analysis)

DPIA report

End of a DPIA cycle

Positive end result?

Fail

Pass

Prior consultation (Art. 36 GDPR)

Abandoning processing operation

3. Implementation Phase

3.1 Implementation of measures

3.2 Testing and documentation of the effectiveness of the measures

3.3 Demonstration of compliance with GDPR

3.4 Approval of processing operations

4. Review Phase

4.1 Continuous review of DPIA

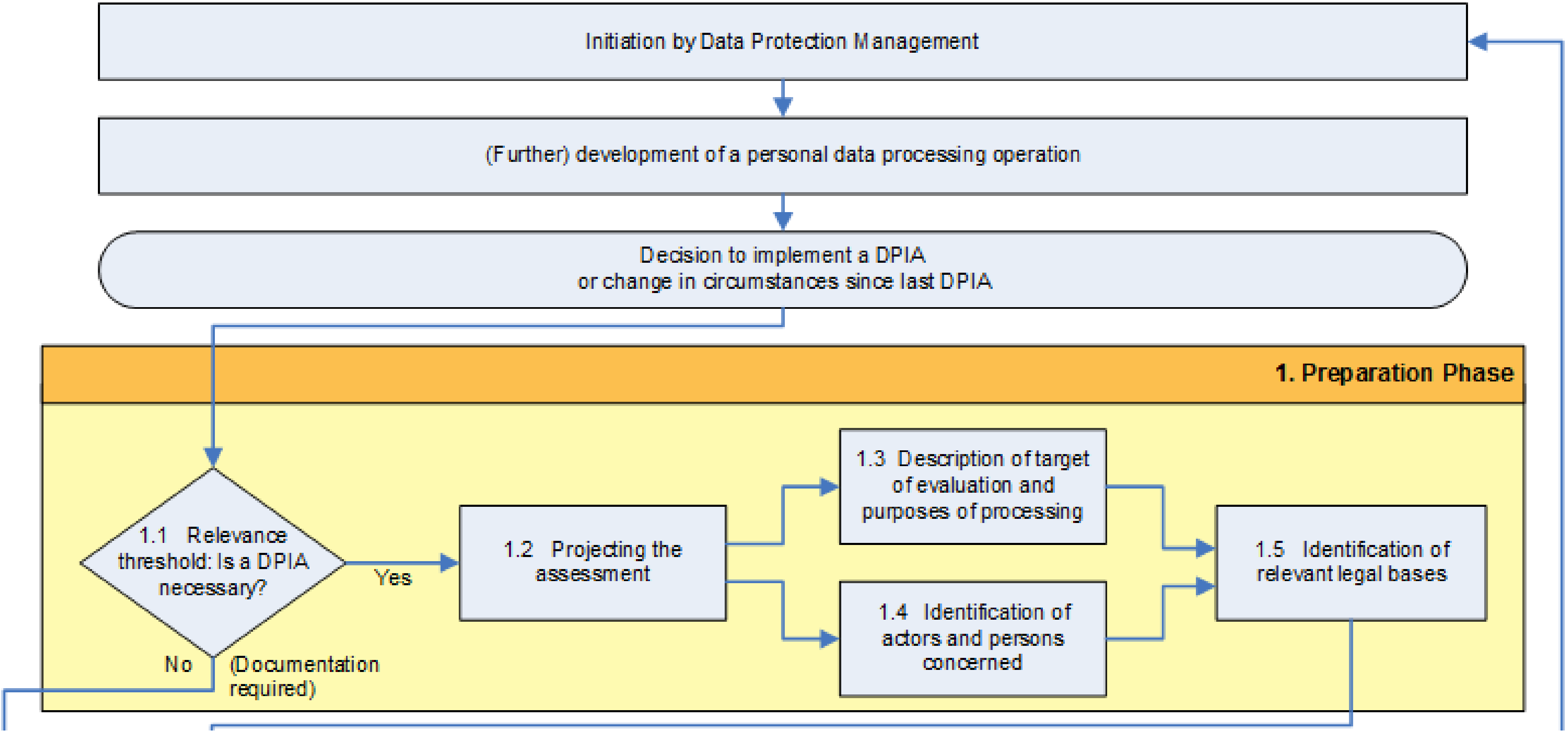
4.2 Supervision of risks with Data Protection Management System

4.3 Independent auditing of DPIA results

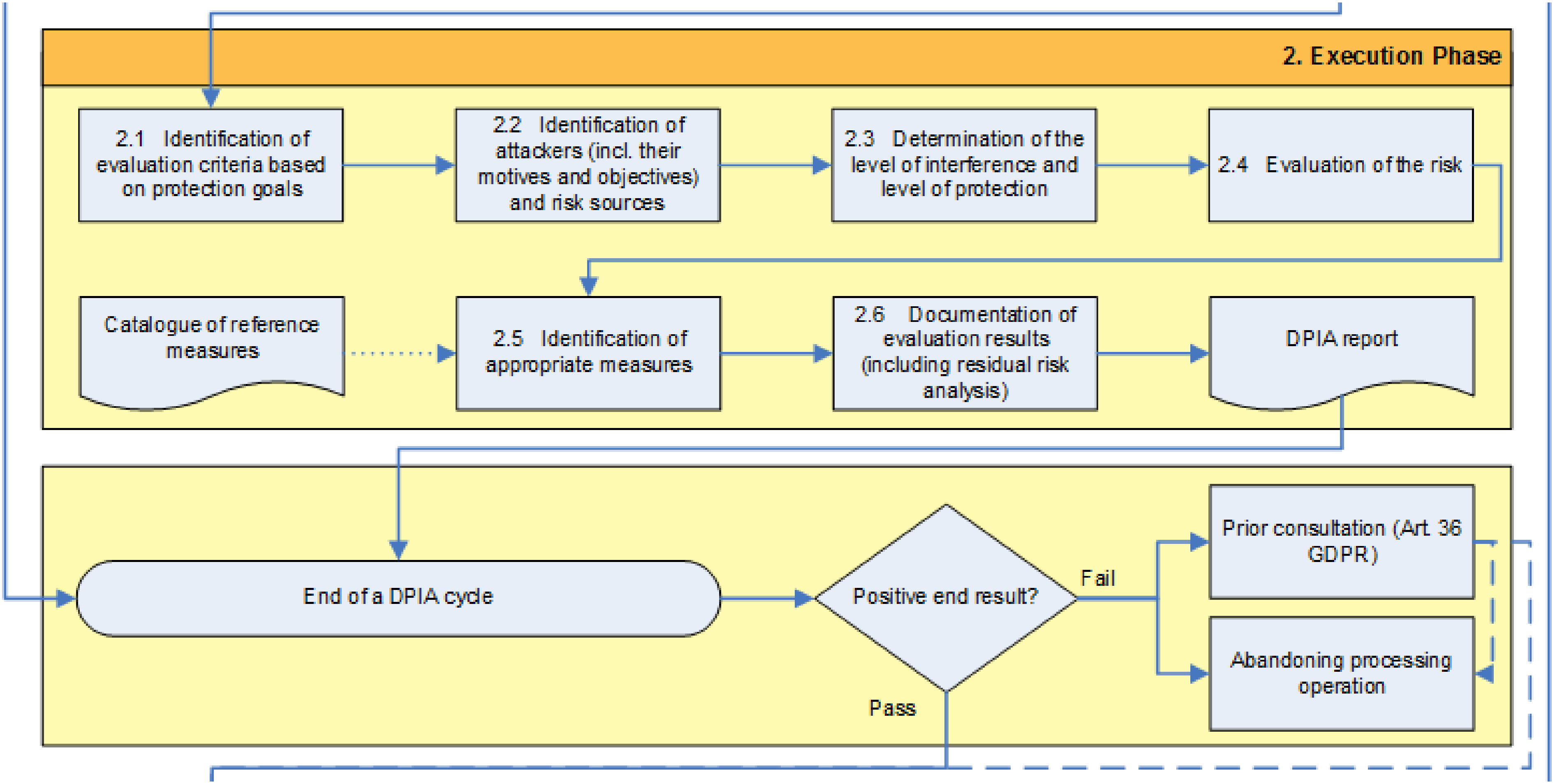
Translated version of framework from White Paper of Forum Privatheit (Privacy Forum)

Available at: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf

Add-on: DPIA Framework


Initiation by Data Protection Management
(Further) development of a personal data processing operation
Decision to implement a DPIA
or change in circumstances since last DPIA
1. Preparation Phase
1.1 Relevance threshold: Is a DPIA necessary?
Yes
No
(Documentation required)
1.2 Projecting the assessment
1.3 Description of target of evaluation and purposes of processing
1.4 Identification of actors and persons concerned
1.5 Identification of relevant legal bases

Add-on: DPIA Framework



2. Execution Phase

2.1 Identification of evaluation criteria based on protection goals

2.2 Identification of attackers (incl. their motives and objectives) and risk sources

2.3 Determination of the level of interference and level of protection

2.4 Evaluation of the risk

Catalogue of reference measures

2.5 Identification of appropriate measures

2.6 Documentation of evaluation results (including residual risk analysis)

DPIA report

End of a DPIA cycle

Positive end result?

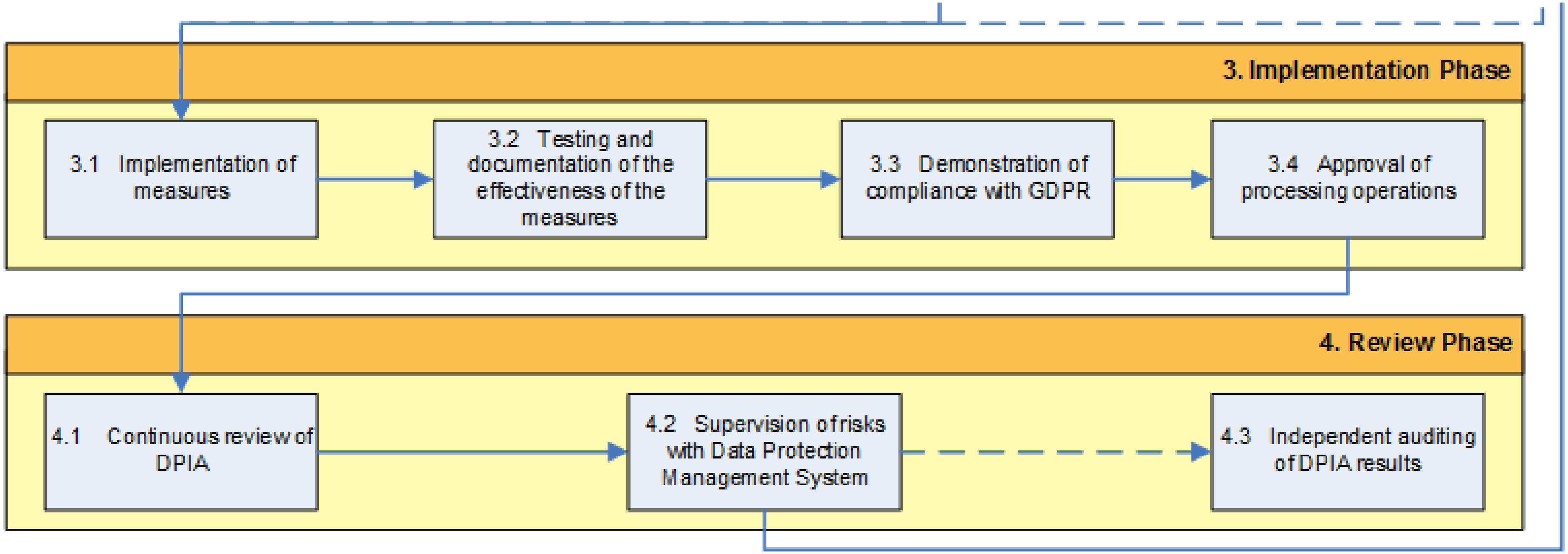
Fail

Pass

Prior consultation (Art. 36 GDPR)

Abandoning processing operation

Add-on: DPIA Framework


3. Implementation Phase

3.1 Implementation of measures

3.2 Testing and documentation of the effectiveness of the measures

3.3 Demonstration of compliance with GDPR

3.4 Approval of processing operations

4. Review Phase

4.1 Continuous review of DPIA

4.2 Supervision of risks with Data Protection Management System

4.3 Independent auditing of DPIA results

Standard Data Protection Model

- Determination of the necessary level of protection ("normal", "high", "very high")
- Identification of risks and proper safeguards
- Protection goals as structure + for same understanding

- Model recommended by the German DPAs; suitable for
  - Supervision
  - Audits
  - Data Protection Impact Assessment
  - Data Protection by Design and by Default

SDM

The Standard Data Protection Model

A concept for inspection and consultation on the basis of unified protection goals

V.1.0 – Trial version

Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

Content

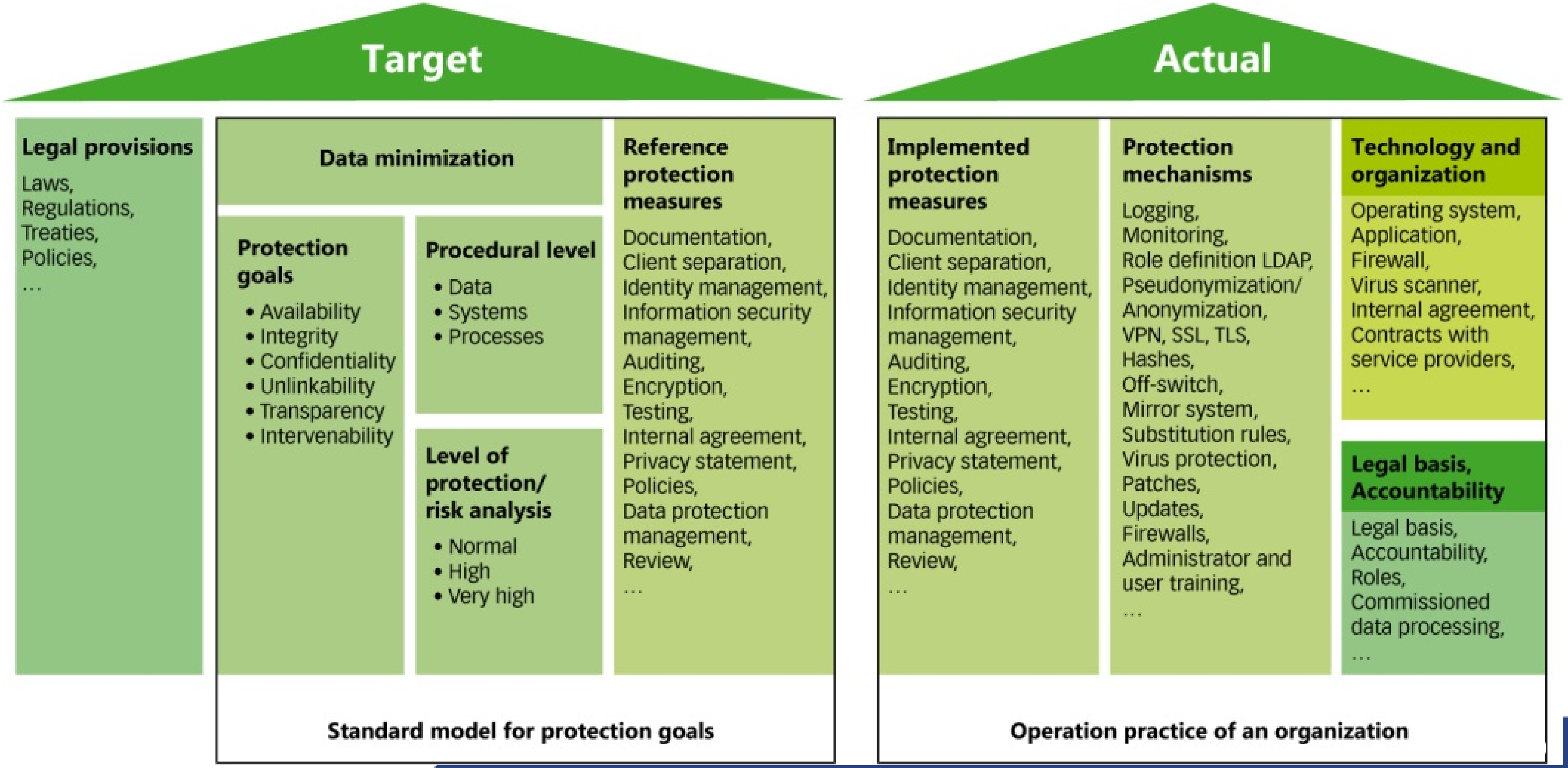
Page 1 of 48

https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methodology_V1_EN1.pdf

- Work for 2018++: catalogues of <u>reference protection measures</u>
- Envisioned: repositories with info on maturity, conditions etc.

Standard Data Protection Model

To be integrated in the Data Protection Management System of the controller



Target

Legal provisions

Laws,
Regulations,
Treaties,
Policies,
...

Data minimization

Protection goals

- Availability
- Integrity
- Confidentiality
- Unlinkability
- Transparency
- Intervenability

Procedural level

- Data
- Systems
- Processes

Level of protection/ risk analysis

- Normal
- High
- Very high

Reference protection measures

Documentation,
Client separation,
Identity management,
Information security management,
Auditing,
Encryption,
Testing,
Internal agreement,
Privacy statement,
Policies,
Data protection management,
Review,
...

Standard model for protection goals

Actual

Implemented protection measures

Documentation,
Client separation,
Identity management,
Information security management,
Auditing,
Encryption,
Testing,
Internal agreement,
Privacy statement,
Policies,
Data protection management,
Review,
...

Protection mechanisms

Logging,
Monitoring,
Role definition LDAP,
Pseudonymization/ Anonymization,
VPN, SSL, TLS,
Hashes,
Off-switch,
Mirror system,
Substitution rules,
Virus protection,
Patches,
Updates,
Firewalls,
Administrator and user training,
...

Technology and organization

Operating system,
Application,
Firewall,
Virus scanner,
Internal agreement,
Contracts with service providers,
...

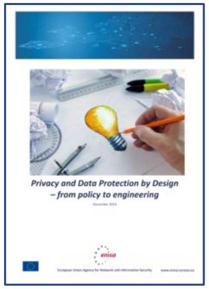
Legal basis, Accountability

Legal basis,
Accountability,
Roles,
Commissioned data processing,
...

Operation practice of an organization

References

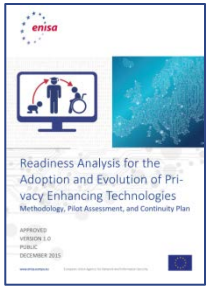
- https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (2015)
- https://www.enisa.europa.eu/publications/pets (2016)
- https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (2018)
- https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf (2016)
- Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015



Privacy and Data Protection by Design – from policy to engineering

December 2014

enisa



enisa

Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies

Methodology, Pilot Assessment, and Continuity Plan

APPROVED
VERSION 1.0
PUBLIC
DECEMBER 2015

enisa

Privacy and data protection in mobile applications

A study on the app development ecosystem and the technical implementation of GDPR

NOVEMBER 2017

SDM

The Standard Data Protection Model

A concept for inspection and consultation on the basis of unified protection goals

Protection Goals for Privacy Engineering

Thank you for your attention!

Felix Bieker, LL.M. (Edinburgh)
fbieker@datenschutzzentrum.de
0049 431 988 1226

https://www.datenschutzzentrum.de