Data Protection by Design – how to fulfil European demands and provide trustworthy services

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

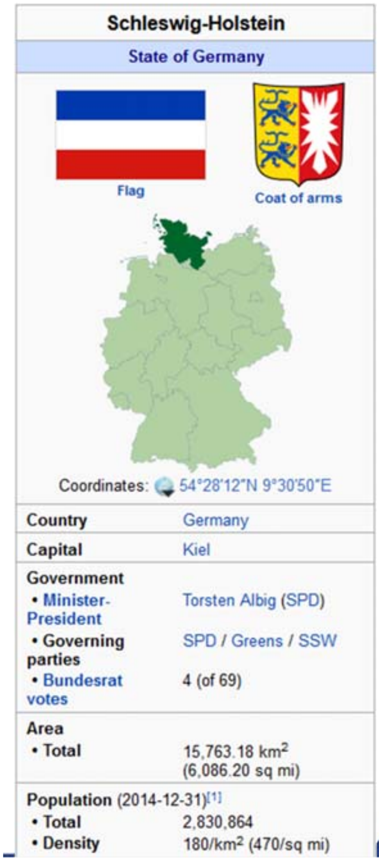
Datasikkerhedskonference 2017
Copenhagen, 21 March 2017

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

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



Schleswig-Holstein

State of Germany

Coordinates: 54°28′12″N 9°30′50″E

Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)
Population (2014-12-31)[1]	
• Total	2,830,864
• Density	180/km² (470/sq mi)

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

Source: www.maps-for-free.com

Overview

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion

Data Protection is mainly about ~~data~~

Photo: Ashtyn Renee

human beings with their rights

Questions to consider in system design:

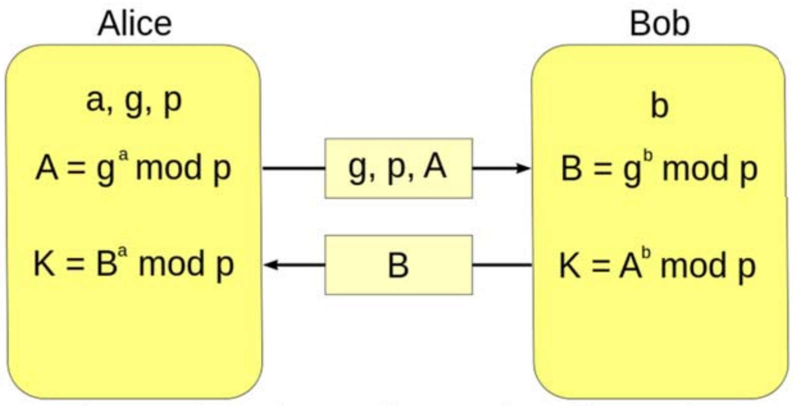
- Effects on individuals?
- Effects on society?

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.)

Overview

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion

Regulation (EU) 2016/679

EU General Data Protection Regulation – A game changer

Source: Johan Aulin

- Market location principle (Art. 3 GDPR)
- Data protection by design (Art. 25(1) GDPR)
- Data protection by default (Art. 25(2) GDPR)
- Data protection impact assessment (Art. 35 GDPR – “rights and freedoms of natural persons”)
- Certification (Art. 42+43 GDPR)
- Fines & sanctions (Art. 83+84 GDPR)
- Courts

Powerful toolbox, but only as good as its implementation

GDPR: Importance of "design"

Recital 4

The processing of personal data should be designed to serve mankind. […]

Overview

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers + data processors
- Producers of IT systems "should be encouraged" (Rec. 78)

Art. 25 Data Protection by Design and by Default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, [...]

- Objective: to design systems + services from early on, for the full lifecycle ...
  a) ... in a data-minimising way
  b) ... with the most data protection-friendly pre-settings

Data protection by design

Article 25 Data protection by design and by default

(1) Taking into account

the state of the art,

the cost of implementation and

the nature, scope, context and purposes of processing as well as

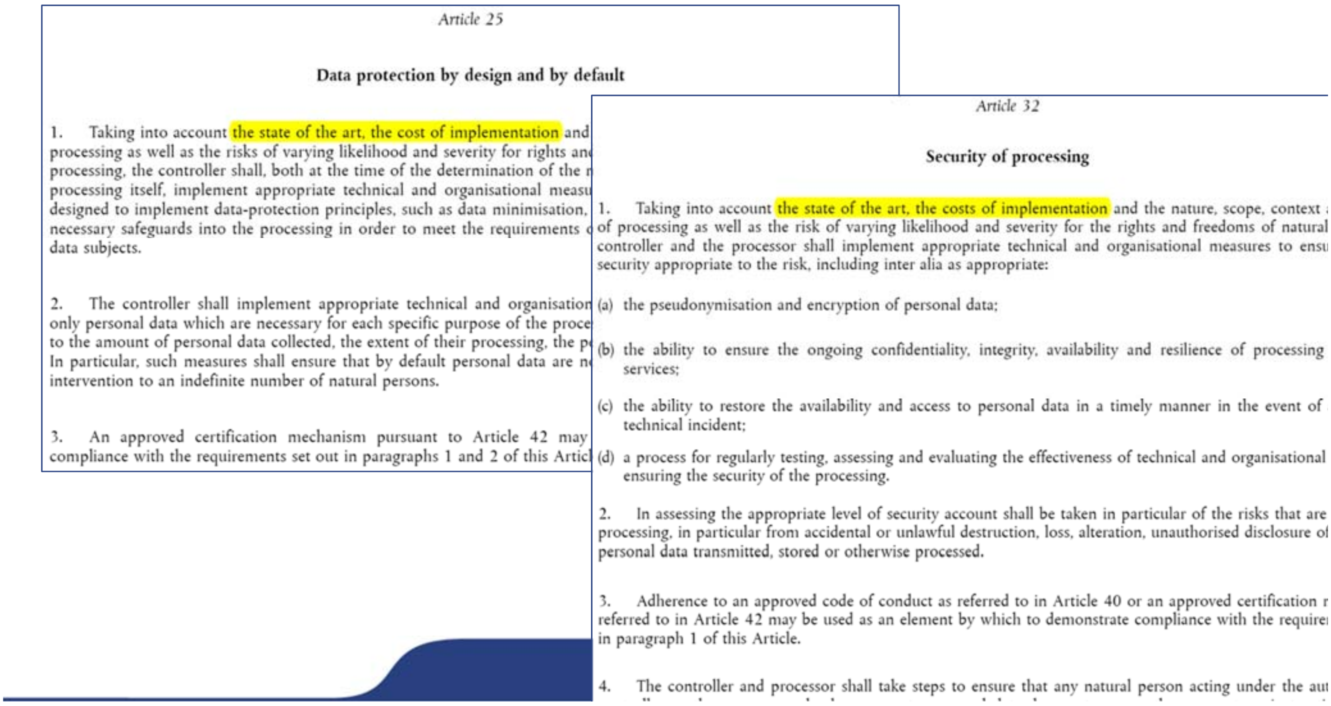
the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing,

Several potentially limiting conditions

the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Conditions “state of the art” and “the cost of implementation”?

Identical wording in Art. 32 “Security of processing”



Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and
processing as well as the risks of varying likelihood and severity for rights an
processing, the controller shall, both at the time of the determination of the r
processing itself, implement appropriate technical and organisational measu
designed to implement data-protection principles, such as data minimisation,
necessary safeguards into the processing in order to meet the requirements c
data subjects.

2. The controller shall implement appropriate technical and organisation
only personal data which are necessary for each specific purpose of the proce
to the amount of personal data collected, the extent of their processing, the p
In particular, such measures shall ensure that by default personal data are n
intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may
compliance with the requirements set out in paragraphs 1 and 2 of this Articl

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context
of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural
controller and the processor shall implement appropriate technical and organisational measures to ensu
security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing
services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of
technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational
ensuring the security of the processing.

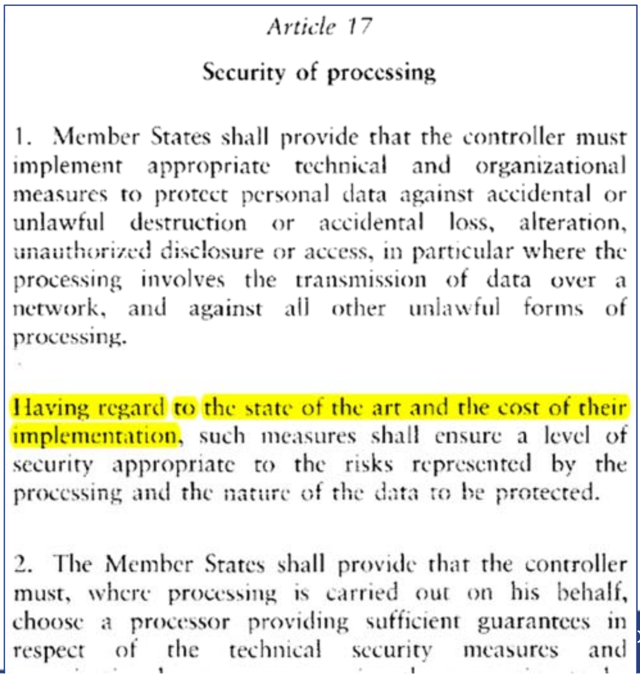
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are
processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of
personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification r
referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirei
in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the aut

Conditions “state of the art” and “the cost of implementation”?

On EU level nothing new, see Data Protection Directive 95/46/EC



Article 17

Security of processing

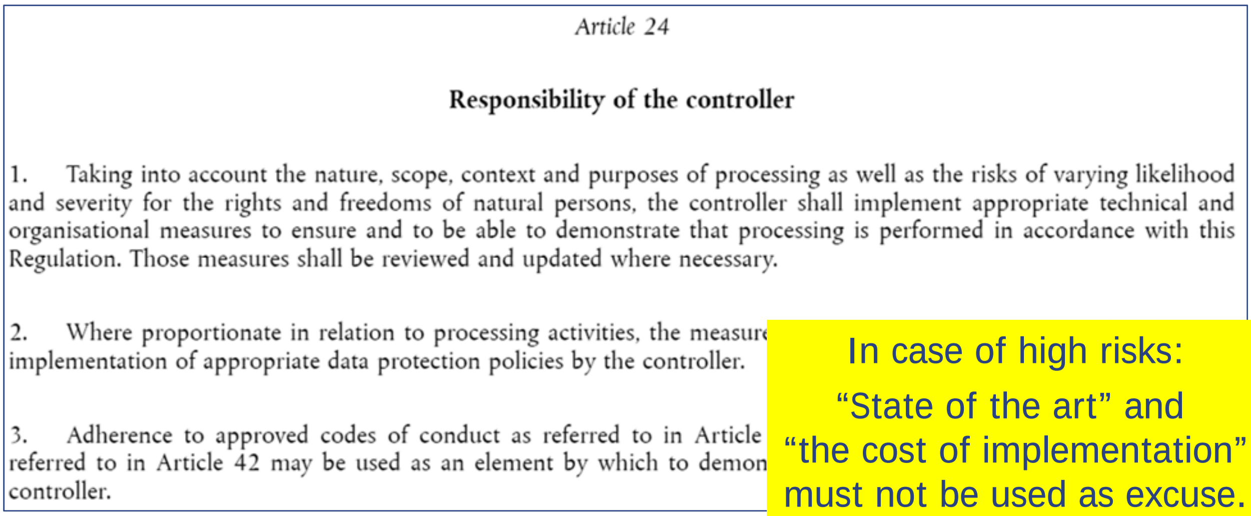
1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and

Conditions “state of the art” and “the cost of implementation”?

Not contained in Art. 24 GDPR: responsibility



Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measure implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article referred to in Article 42 may be used as an element by which to demon controller.

In case of high risks:

“State of the art” and “the cost of implementation” must not be used as excuse.

(see Art. 36 Prior Consultation)

Data protection by default

Article 25 Data protection by design and by default

Related to the “purpose limitation” principle (Art. 5)

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Social network clause

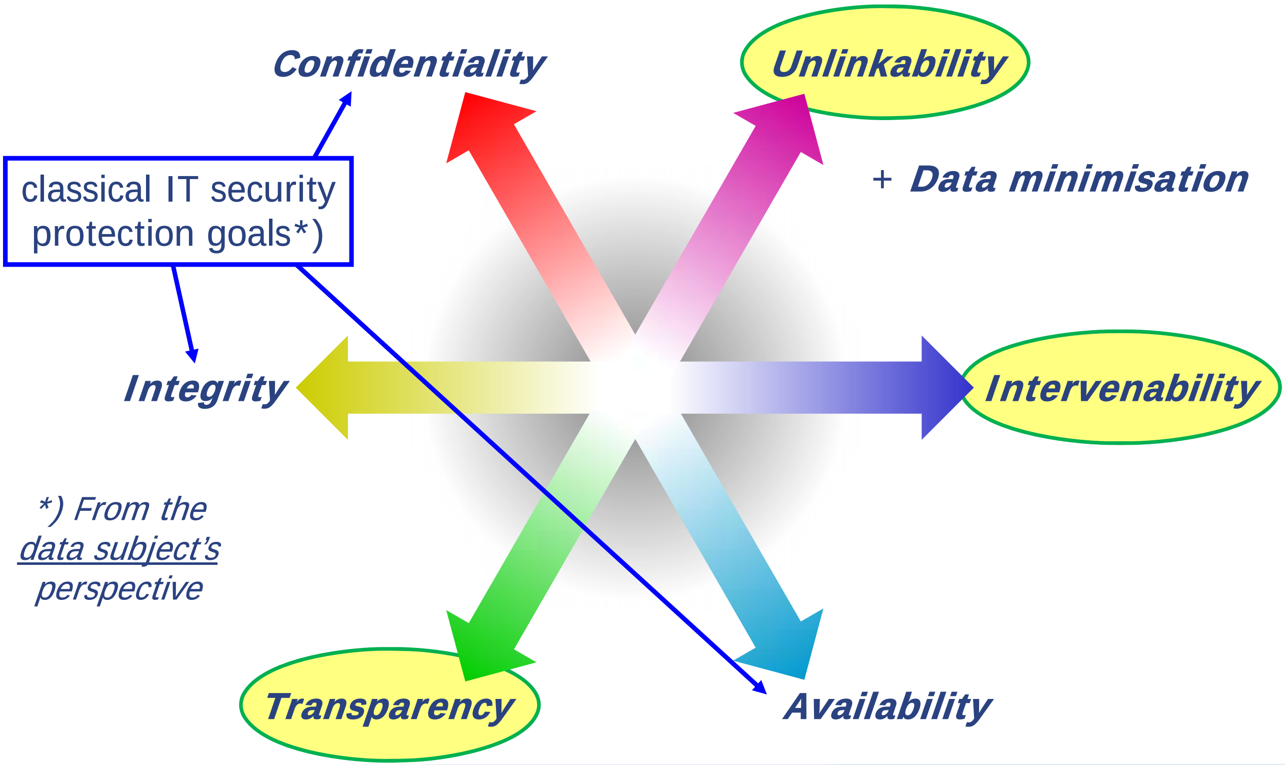
How? – Some hints in Recital 78

- Goal: to demonstrate compliance with the GDPR
- Adopting internal policies and implementing measures for data protection by design & by default
- Data minimisation
- Early pseudonymisation
- Transparency
- Monitoring of data processing by the data subject
- Expandable security – not “one size fits all”
- Data protection by design & by default in public tenders
- If Art. 25 (+ Art. 32) is ignored, administrative fines possible
  (Art. 83 GDPR: up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover)

Overview

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion

Protection goals: more than IT security



*) From the data subject's perspective

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

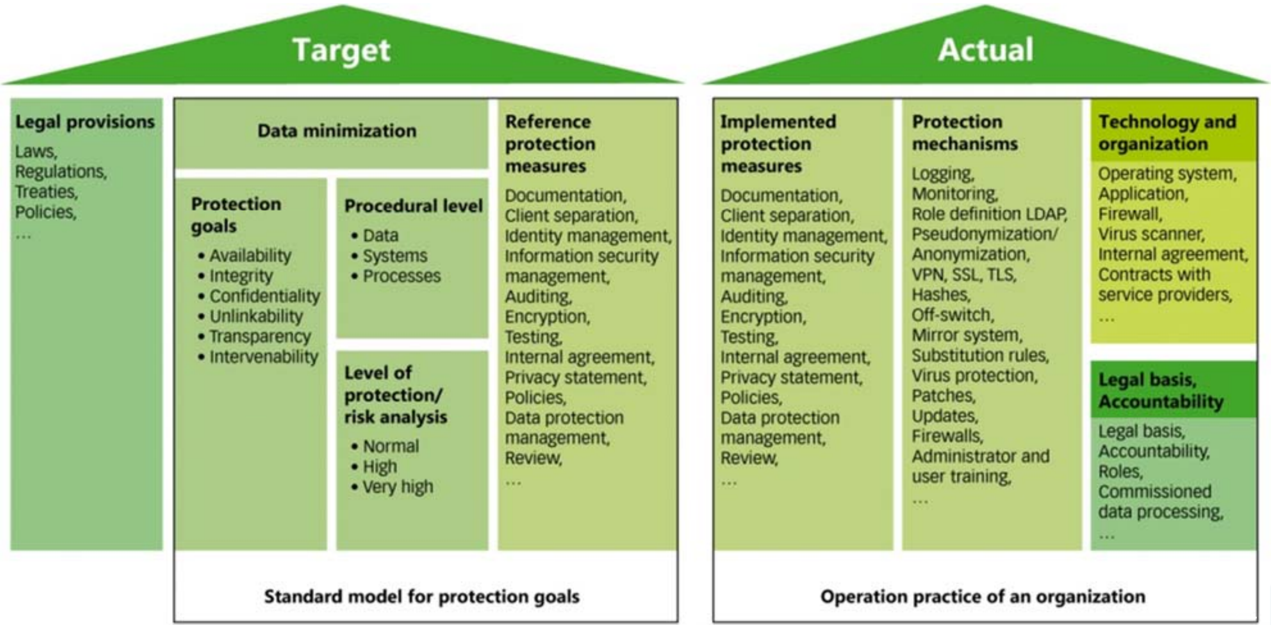
A concept for inspection and consultation on the basis of unified protection goals

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

- Work for 2017++: catalogues of reference protection measures
- 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

Data protection by design – controller's perspective in 2017

Photo: Martin Cox

Minimum:

- Low-key interpretation of the legal rules
- Documentation of internal policies and measures
- Awaiting requirements of supervisory bodies
- Awareness of responsibility (CEO; at best supported by Data Protection Officer)

For "optimum" on top:

Photo: Paul B

- Acting proactively
- Knowing and extending solution space
- Striving for certification
- Implementing a data protection management system for entire lifecycle
- Interacting with other actors and disciplines for improving technologies <u>and</u> workflows

BTW: All translations are equivalent, aren’t they?

- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen
- [DA] Artikel 25: Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger
- [SV] Artikel 25: Inbyggt dataskydd och dataskydd som standard
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Overview

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion

Conclusion

- Data protection by design and by default
  - Demanded by the General Data Protection Regulation
  - With focus on the perspective of the individuals
  - Necessary for trustworthy systems

Privacy Enhancing Technologies
protect your online privacy

enisa

Time to adopt PETs!

Privacy Enhancing Technologies (PETs) help to protect online privacy following the simple approach "reduce, protect, detect". The future starts now: make it a habit, adopt PETs.

- For controllers:
  - Be risk-aware
  - Be compliant
  - Re-think your concepts, processes & implementations
  - Demand the same from your processors

- "Privacy by disaster" is not an option – get help: Data Protection Officers + Commissioners

Data Protection Management Systems

Tak for opmærksomheden!

Marit Hansen

ULD, Holstenstr. 98, 24103 Kiel, Germany
marit.hansen@datenschutzzentrum.de

References

- https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design (2014)

Privacy and Data Protection by Design – from policy to engineering

- https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets (2015)

Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies

Methodology, Pilot Assessment, and Continuity Plan

- https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methodology_V1_EN1.pdf (2016)

SDM

The Standard Data Protection Model

- Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015

Protection Goals for Privacy Engineering