Cybersecurity, EU data protection law and risk assessment in the eHealth sector

Cyberwatching.eu Webinar
‘Cybersecurity for Healthcare: Human and Legal Perspectives’
26 September 2019

Eva Schlehahn
Senior legal researcher and consultant at Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
uld67@datenschutzzentrum.de

CANVAS

Constructing an Alliance for Value-driven Cybersecurity

What is CANVAS about?

Informing stakeholders how cybersecurity can be aligned with European values and fundamental rights.

(H2020 Coordination and Support Action)

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Cybersecurity and data protection: Both matter in the eHealth sector

What Caused the Breach? An
Use of Information
Health Data

and Conclusions

Even with the increasing use of IT in healthcare, the vast majority of data breaches affecting individuals appear to be the result of theft and loss, not hacking or IT incidents. A huge cost is associated with data breaches in organizations; estimates suggest that on average, each lost or exposed customer record costs the organization $202.[19] In fact, data breaches are estimated to cost the US healthcare industry a whopping $6.5 billion on average annually, which would be enough to fund 216 million flu vaccinations or hire 81,000 registered nurses.[20] Unauthorized access or disclosure accounted for only a small percentage of the breaches affecting individuals but played a much greater role in the number of breaches in covered entities and business associates, suggesting the need for stricter controls (physical

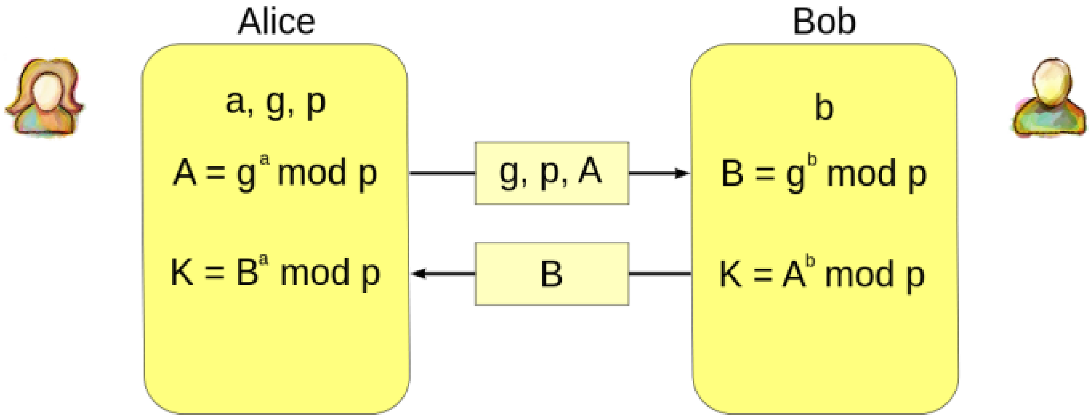
Core reason: Poor baseline security

Different perspectives of IT security and data protection

IT Security: Any **person** can be an attacker

Data protection: Any **organisation** can be an attacker
→ addressing power asymetries

For cryptologists: Esp. Bob is the attacker, not Eve or Mallory



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

Controller obligations

Valid legal ground & enabling data subject‘s rights

Technical & organizational measures

Being able to demonstrate compliance

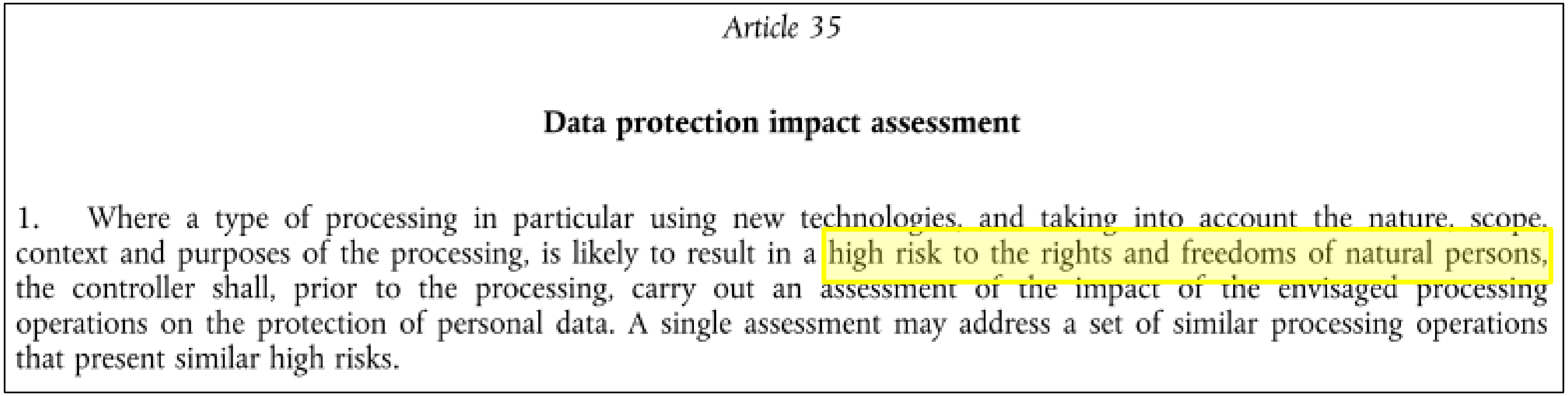
Data protection by design and default

Records of processing activites

Security of processing

Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment
Art. 35 GDPR



Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

EDPB criteria (WP248rev.01 pp. 9 f.) for high risk:

1. Evaluation or scoring, including profiling and predicting (e.g. by credit rating systems of banks)
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring (of persons, e.g. in networks or public areas)
4. Sensitive data or data of a highly personal nature involved (Art. 9 data + context-dependent)
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects (e.g. children, mentally ill people, patients..)
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Article 22 and recital 91).

The term ‘risk’ in data protection

Any personal data processing = infringement on the right to data protection

-> Thus, already **any processing is a risk occured**!

This applies **even if** the processing is

- covered by a legal ground (thus legimized) and
- verifiable secure IT is being used

Goal of a DPIA:

Determine the needed necessary technical & organizational measures to reduce the risk as far as possible

CANVAS

So what is ‘risk’ from data protection view?

The possibility of the occurrence of an event that in itself is damage or that can lead to further damage to one or more individuals

Damage can be physical, material or immaterial (including unjustified interference with fundamental rights)

Steps of a risk assessment

1. Identification of Risks
    - What damage can occur?
    - What events may lead to damage?
    - Which actions/factors can lead to events?

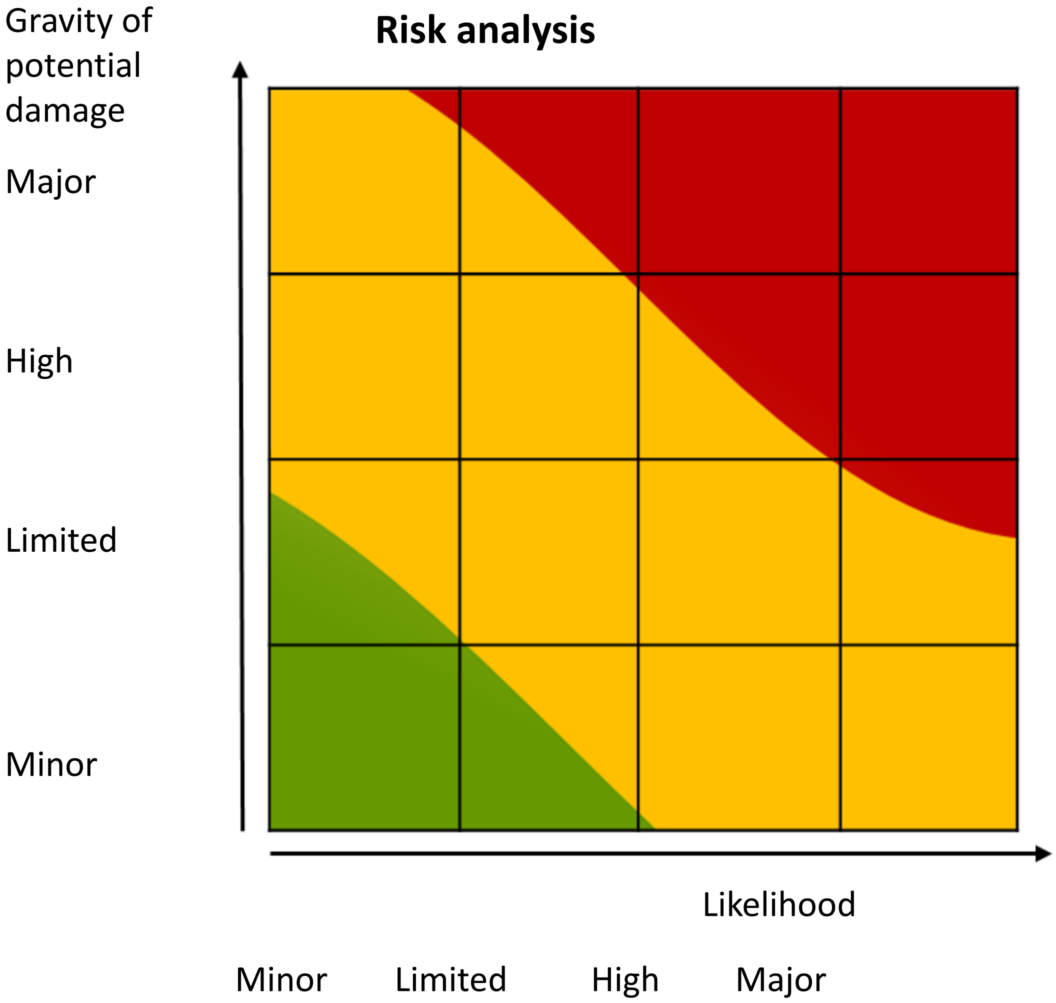
2. Assessment of
    - Gravity of (potential) damage
    - Likelihood of realisation

3. Categorization of Risk

Two dimensions:

- Severity of potential damage
- Likelihood of occurrence

But can’t be quantified, just approximated objectively



Typical risks in data protection

Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
An organisation facilitates an **illegitimate personal data processing operation.**	The **severity of fundamental rights infringement** caused by a legitimate personal data processing is **either not at all or wrongly determined**; the legal ground was not or not sufficiently identified, the assumption of responsibility/accountability is unclear.	An organisation facilitates an in principle legitimate processing operation, but illegitimately **extends or changes the processing purpose** (data retention, Big Data).	An organisation **fails to implement sufficiently effective measures for IT security.**	An organisation facilitates measures **for IT security, but not in conformity with fundamental rights** (clash security/data protection).	The **attacker model is incorrect or sub-complex** (e.g. processing organisation doesn't have itself as attacker on the radar; the same applies for authorized entities, such as security agencies)	The **processing operation is not sufficiently audited and evaluated.**

How to use synergies between IT security and data protection?

In IT security, protection goals are widely known to address risks:

- **Confidentiality**
- **Integrity**
- **Availability**

Suggestion:
Use the operative solution of data protection known in Germany for DPIA‘s
-> Standard-Datenschutz-Modell (SDM, Standard Data Protection Model)

It extends the classic IT security goals by <u>three complementing goals</u>:

- **Unlinkability**
- **Transparency**
- **Intervenability**

The SDM is one of the DPIA frameworks mentioned by the by Art. 29 WP in working paper 248 in April 2017.

More information and learning material

White Papers

- Extensive scientific background material
- Generates an integrative view on existing data and knowledge related to cybersecurity from ethical, legal and technical viewpoints

Briefing Packages

- Concise and comprehensive summaries of CANVAS results for European and national policy makers

Reference Curriculum

- Integrating the value perspective into cybersecurity training and education

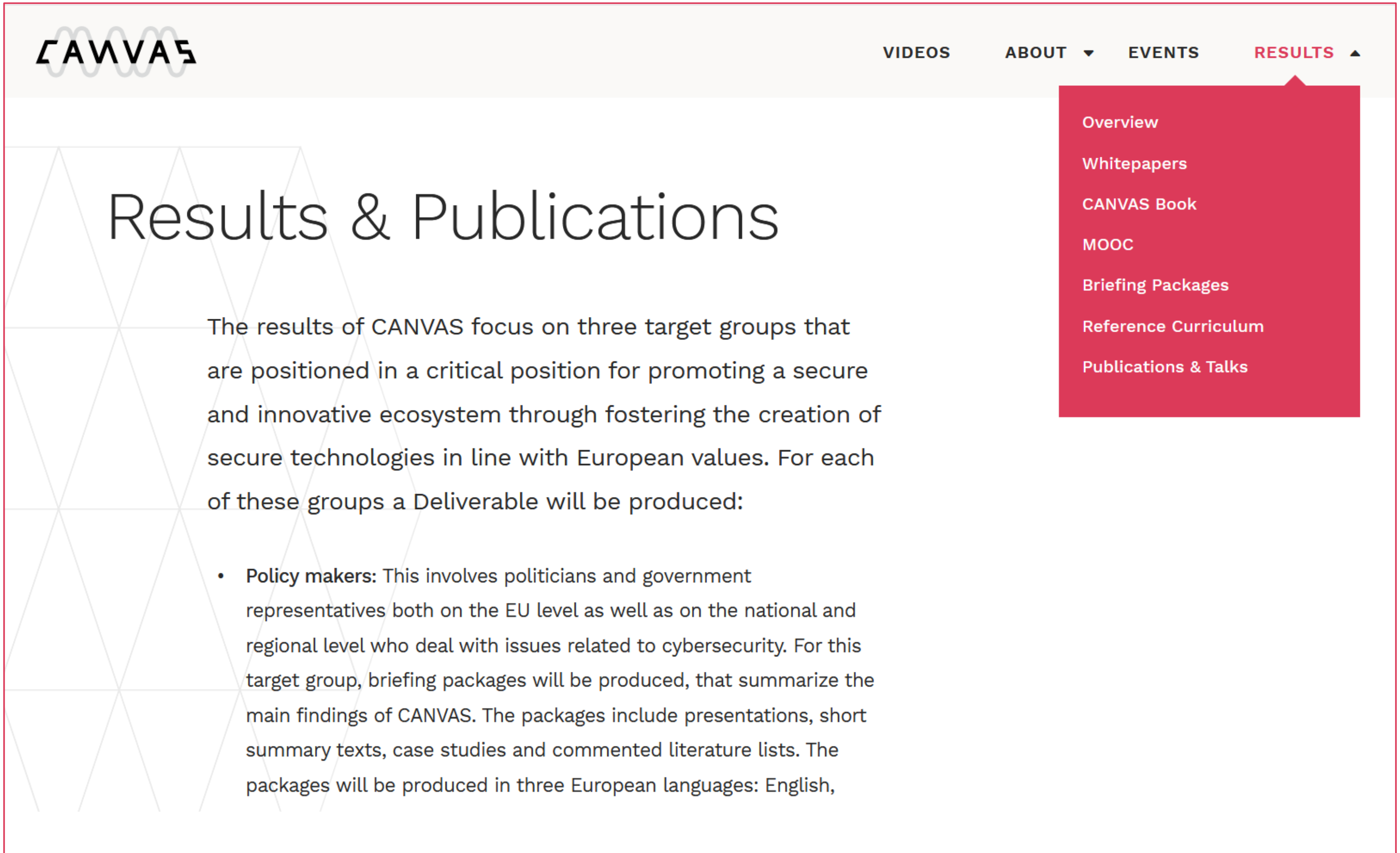
MOOC

- Massive Open Online Course

Upcoming: CANVAS book

Where to find the CANVAS materials

- **Project website: https://canvas-project.eu/**

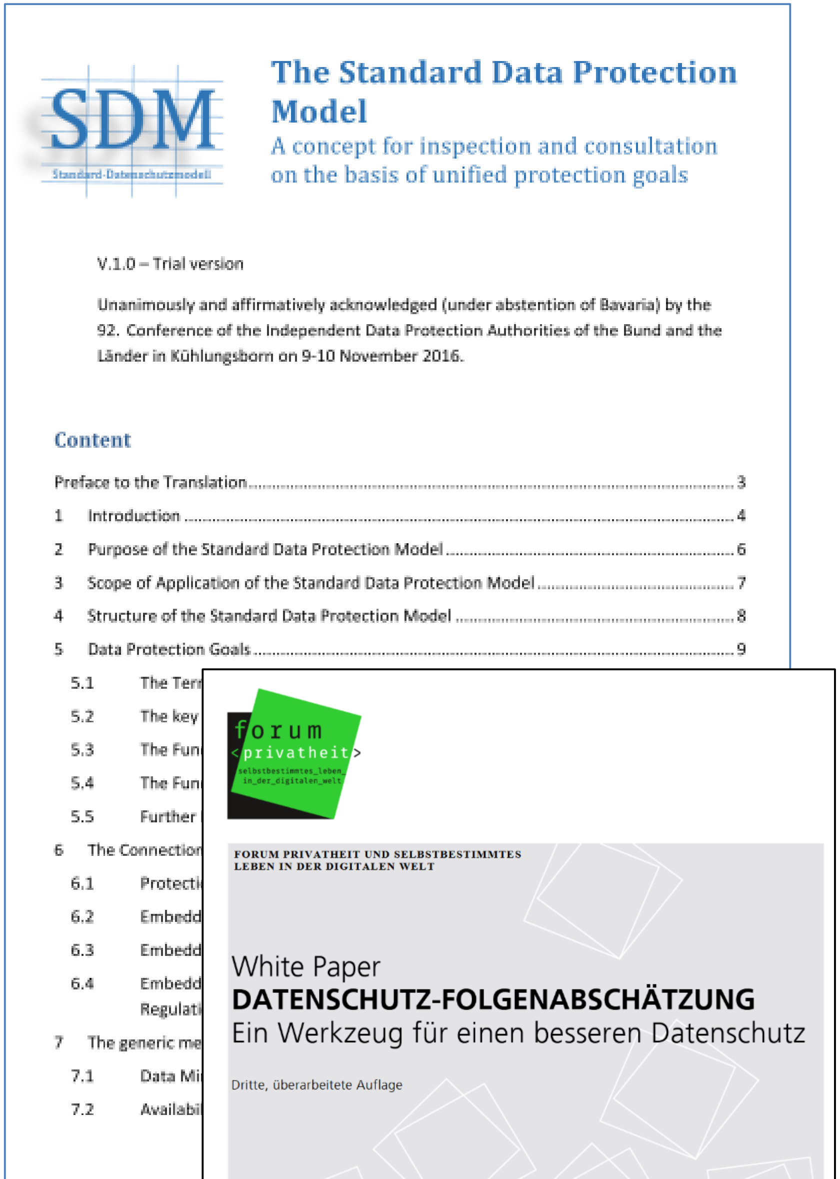


Results & Publications

The results of CANVAS focus on three target groups that are positioned in a critical position for promoting a secure and innovative ecosystem through fostering the creation of secure technologies in line with European values. For each of these groups a Deliverable will be produced:

- **Policy makers:** This involves politicians and government representatives both on the EU level as well as on the national and regional level who deal with issues related to cybersecurity. For this target group, briefing packages will be produced, that summarize the main findings of CANVAS. The packages include presentations, short summary texts, case studies and commented literature lists. The packages will be produced in three European languages: English,

References



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

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Ein Werkzeug für einen besseren Datenschutz

Dritte, überarbeitete Auflage

Input & feedback on slides: Martin Rost, Felix Bieker, Benjamin Bremert (all ULD)

Friedewald, M.; Bieker, F.; Obersteller, H.; Nebel, M.; Martin, N.; Rost, M., Hansen, M.: ‘*White Paper - Datenschutz-Folgenabschätzung, ein Werkzeug für einen besseren Datenschutz*’, Project Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt, 3rd Edition, November 2017

Available at: https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf

Hansen, M.; Jensen, M.; Rost, M:

‘*Protection Goals for Privacy Engineering*’

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163220

‘*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*’

V.1.0 – Trial version 9-10 November 2016

92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn

Initial English version available at:

https://www.datenschutzzentrum.de/sdm/ (2nd and improved English version is currently in progress)