RISK-BASED APPROACH VS HARM-BASED APPROACH

Is it at odds with fundamental rights that the protection is dependent on the risk of violation instead of harm?

Low risk of a data breach? > Less measures to prevent a data breach.

VS

Low harm with a data breach? Less measures to prevent a data breach.

SOLOVE’S PRIVACY THREATS

E.g. Threats to information privacy:

Information Collection
- Surveillance
- Interrogation

Information Processing
- Aggregation
- Identification
- Insecurity
- Secondary Use
- Exclusion

Information Dissemination
- Breach of Confidentiality
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion
- Invasion
- Intrusion
- Decisional Interference
**RISK MANAGEMENT TOOLS**

A risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood.

Risk management are coordinated activities to direct and control an organization with regard to risk.

Risk management translate a complex reality to a manageable set of issues.

What is law?

Translate a complex reality to a legal reality that is manageable for a wide range of issues.

Critique on existing impact assessment frameworks are:

1. narrow conceptions of legal notions that stem from computer security.
2. Data controller weigh legal duties against other interests. (Different starting point than fundamental rights)

**RISK-BASED LEGAL OBLIGATIONS**

Does not mean: do not risk any violation of a right.

It might be proportionate to carry out low risk activities.

>>balancing act of rights and objectives.

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well-defined components of risk management (e.g. ISO 3100026)

- establishing the context: “taking into account the nature, scope, context and purposes of the processing and the sources of the risk”;
- assessing the risks: “assess the particular likelihood and severity of the high risk”;
- treating the risks: “mitigating that risk” and “ensuring the protection of personal data”, and
“demonstrating compliance with this Regulation”

**ART. 35 GDPR**

- Data protection impact assessment
- Tool demonstrate compliance

**GOALS:**

- describe the processing
- assess its necessity and proportionality
- help manage the risks to the rights and by assessing them and determining the measures to address them.
RISK OF NO OR SLOPPY DPIA

- Administrative fine of up to 10M euro or up to 2% of the total worldwide annual turnover of the preceding financial year
  - whichever is higher.

A DPIA is required when the processing is “likely to result in a high risk to the rights and freedoms of natural persons”

The rights and freedoms primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

When no DPIA is carried out or is necessary the data controller still has to implement measures to appropriately manage risks.

BASIC PRINCIPLES

ONE OR MORE DPIA?

Single processing operation or multiple processing operations that are similar or a technology product

a DPIA should be continuously reviewed and regularly re-assessed.
EXAMPLES OF HIGH RISK
- a systematic and extensive evaluation of personal aspects
  - Profiling
  - Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences.
- Personal data of a highly personal value
  - personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.
- Matching or combining datasets
- Data concerning vulnerable data subjects
  - mentally ill persons, asylum seekers, or the elderly, patients, etc.

EXAMPLES OF HIGH RISK
- Large Scale
  - Absolute and relative number of data subjects
  - the volume of data and/or the range of different data items being processed;
  - the duration, or permanence, of the data processing activity;
  - the geographical extent of the processing activity.

EXAMPLES OF HIGH RISK
- a systematic monitoring of a publicly accessible area on a large scale.
  - This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

EXAMPLES OF HIGH RISK
- Innovative use or applying new technological or organisational solutions
  - accordance with the achieved state of technological knowledge
    - IoT
  - When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”
    - An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.
**LET’S DO A QUIZ!**

DPIA yes/no

---

**WHAT METHODOLOGY??**

It is up to the data controller to choose a methodology. (as long as it is compliant with the GDPR)

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller’s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

See hand-out

---

**BASIC PRACTICE FOR IMPACT ASSESSMENT**

- Systematic process/living instrument.
- PIA: societal concerns/DPIA: individual concerns
- Determine on the scope, nature, context and purpose
- Appropriate assessment method
- Possible solutions to address the concerns
- DPIA are best effort obligations
- The assessors should have sufficient now-how
- DPIA should be transparent for the DPA
- Deliberative internal and external stakeholders
- Inclusive of all roles and stakes
- Adaptive to the situation
- The controller is accountable
- Independence of assessor

---

**PIA IN PRACTICE. HOW TO AVOID THIS...**
### PIA WIV (2015/2016)
- PIA focus on improvement of legislation
- Privacy protection is not meant as unnecessary burden for intelligence agencies, it provides a framework that channels and checks the work of intelligence agencies.
- Broad competence is necessary, but not in all circumstances that competence should be used.

### PRIVACY RISKS WIV
- Mistakes in processing of data
- Mistakes in interpretation of data
- Data can be hacked or leaked
- Data can be shared with third parties. Loose control on use
- Data is used for different purposes
- Data can be used outside the context in automated analyses > risk false interpretation

### PRIVACY RISKS WIV
- Mistakes in exercise of competence
- Mission creep: competence used for different purpose
- Definitions are stretched
- Experiments in grey areas > codification of practices
- Sliding scale for privacy protection

### IDENTIFICATION OF WEAKNESSES IN WIV
- Technology neutral phrasing has its limits
  - Broadly phrased competences that become over inclusive
  - Balance between legal certainty and tech-neutrality
- False assumption that meta data is less privacy intrusive than content data
- False assumption that wired data and wireless data (radio frequency) have the same privacy assumptions.
- Proposal drafted with old-fashioned examples. Binoculars vs. Drones.
- Structure of the law complex
RECOMMENDATIONS
PIA WIV

- Structure of law should be more simple
- Missing provisions:
  - Open data and sources OSINT
  - Data protection by design and by default
- A selection of the unacceptable privacy risks:
  - Hacking a third party to get to a target
  - The definition of communication providers should not be extended to cloud providers because they resemble the old-fashioned drawer.
  - Sharing of bulk data with foreign partners
  - Old data should not be shared with partners

RECOMMENDATIONS
WIV PIA

Selection of risks that need safeguards:
- Shorter and better motivated retention of data
- Immediate deletion of non-selected data
- Limited retention periods
- Hacking a PC/smarterphone is the most severe privacy infringement: proper safeguards.