The wide notion of risk – A new risk taxonomy

Dr Konstantinos Limniotis

ICT Specialist, Head of Research & Studies

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Overview

- Understanding data protection risk under the GDPR
- Existing risk assessment approaches and challenges
- The byRisk approach
  - Review of existing methodologies, frameworks and taxonomies
  - Development of new risk taxonomy
  - Risk sources -> Regulatory issues -> Possible Harms to individuals -> Fundamental rights potentially affected
  - Application to everyday personal data processing activities

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

What is “data protection risk”?

- The notion of (data protection) risk is not explicitly defined in the GDPR.
  - Despite the fact that the GDPR has a general “risk-based” flavor
- Two commonly distinguished perspectives:
  - **Vernacular notion of risk:** Risk refers to a possible future event that may have **negative consequences** (i.e., a potential danger).
  - **Technical notion of risk:** Risk combines the **likelihood** of an event occurring with its **potential impact**.
- Therefore, risk is associated with:
  - the possible future event itself that is being considered,
  - the impact that we will get in case that this event happens,
  - how this event could be materialized (related to the likelihood)

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Revisiting the risk under the GDPR

- Recital 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 (…)*"
- **Risk impact under the GDPR** primarily concerns harm to individuals (physical, material, or non-material)
  - E.g., Discrimination, financial loss, reputational damage, etc.
- Most importantly, these rights and freedoms being mentioned in the GDPR not only concern the rights to privacy and personal data protection, but include other fundamental rights *[WP29, Guidelines on DPIA, 2017]*

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Data Protection Risk Assessment: Current Approaches and Challenges

- Focus on GDPR compliance rather than actual harm
  - Risks are often defined simply in terms of violations of GDPR principles.
    - E.g. risk of violation of data minimization
- The risk may coincide with the threat
  - E.g. Risk of being victim of a phishing attack
- Overemphasis on information security
  - Existing approaches frequently prioritise security-related risks, paying less attention to other data protection risks.
- Limited suitability for SMEs
  - Many methodologies focus on DPIAs, which are not always required for SMEs and may be too complex for their everyday needs.
- Additional challenges introduced by AI
  - Identifying AI-related risks is particularly difficult, especially for SMEs since they may have limited knowledge of the underlying AI systems/models.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The approach in the byRisk project

- A systematic, “rights-oriented” approach:
  - Develop a comprehensive taxonomy to identify and analyse data protection risks, going beyond information security and regulatory compliance.
- Starting from everyday activities:
  - Consider typical real-world personal data processing activities, particularly those undertaken by SMEs.
- Identifying potential harms:
  - Examine the actual negative consequences that individuals may experience as a result of improper personal data processing.
- Considering fundamental rights:
  - Identify how such harms may adversely affect individuals' fundamental rights and freedoms, apart from privacy and data protection.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The approach in the byRisk project

- A systematic, “rights-oriented” approach:
  - Develop a comprehensive taxonomy to identify and analyse data protection risks, going beyond information security and regulatory compliance.
- Starting from everyday activities:
  - Consider typical real-world personal data processing activities, particularly those undertaken by SMEs.
- Identifying potential harms:
  - Examine the actual negative consequences that individuals may experience as a result of improper personal data processing.
- Considering fundamental rights:
  - Identify how such harms may adversely affect individuals' fundamental rights and freedoms, apart from privacy and data protection.

A common foundation for practical tools:
Support risk assessment by SMEs and raise awareness of data protection risks among the general public.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The byRisk methodological steps: Review of existing approaches

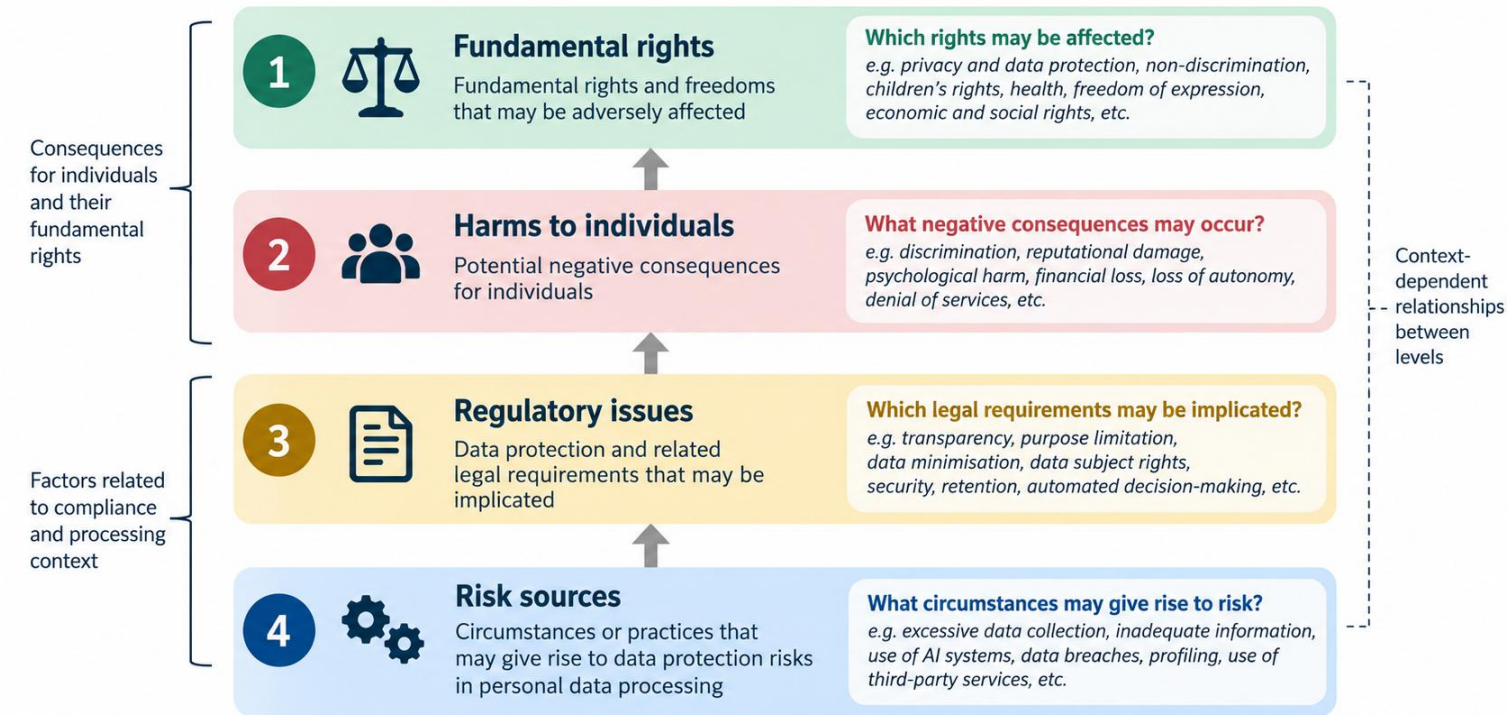
- Legal and regulatory analysis: Examination of the GDPR, AI Act and EU Charter of Fundamental Rights
- Extensive literature review: Examination of existing data protection, privacy, cybersecurity and AI risk assessment methodologies, tools and taxonomies.
- Data Protection Authorities: Review of approaches developed by supervisory authorities, including CNIL (France), AEPD (Spain), IDPC (Malta) and ICO (UK).
- Established risk assessment methodologies: Examination of approaches such as CNIL's PIA methodology, and relevant NIST frameworks.
- AI risk management frameworks: Analysis of the NIST AI Risk Management Framework (AI RMF), including its AI trustworthiness characteristics.
- AI-specific risk taxonomies and research: Review of the MIT AI Risk Repository, PLOT4AI, and academic classifications of AI risks, including risks related to fairness, transparency, privacy, robustness and fundamental rights.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The byRisk Data Protection Risk Taxonomy

- Drawing on an extensive review and synthesis of existing literature, methodologies and risk taxonomies, byRisk developed a new taxonomy to systematically identify and characterise data protection risks arising from personal data processing.

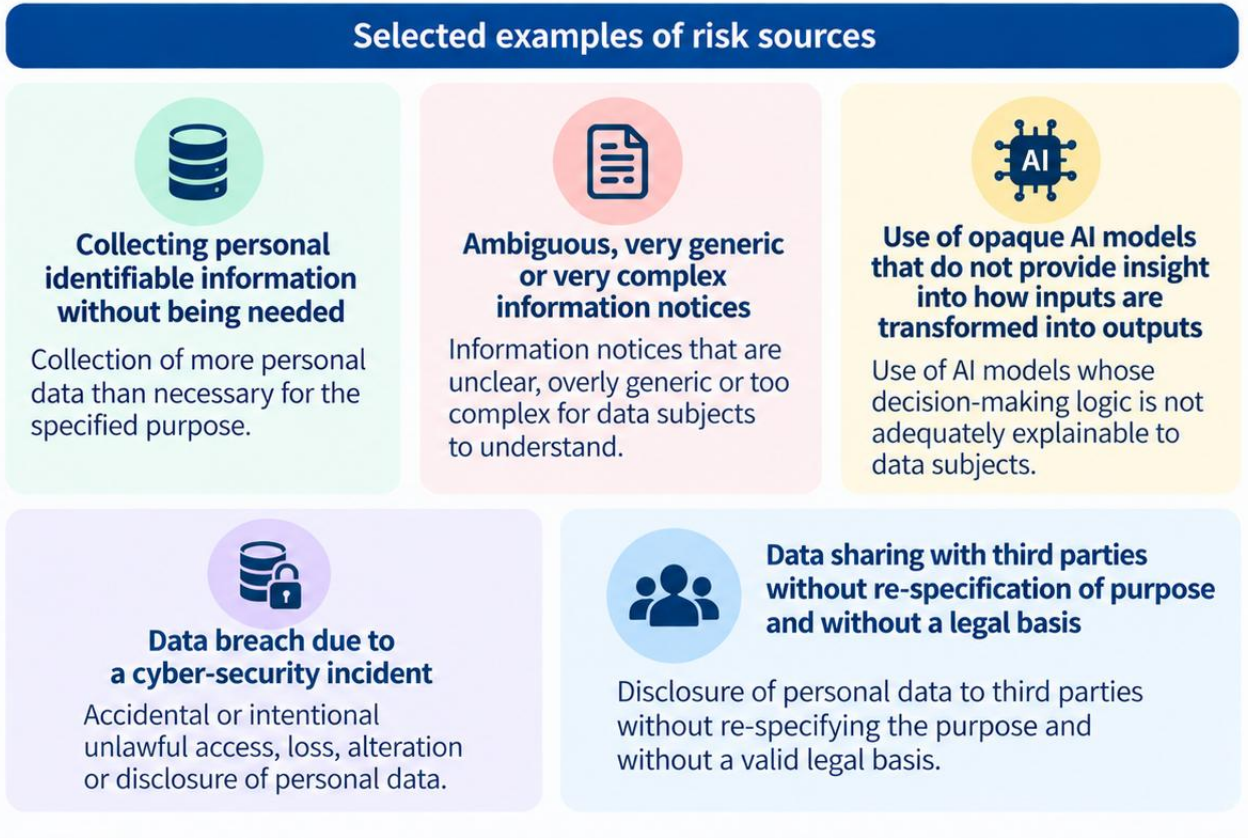


Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 4: Risk Sources

- Risk sources represent situations or practices that may give rise to adverse consequences for individuals.
- They cover a broad range of data protection concerns, extending beyond information security.
- Their relevance depends on the particular processing activity and business context.
- The byRisk taxonomy identifies 40 general risk sources, including sources associated with the use of AI systems.



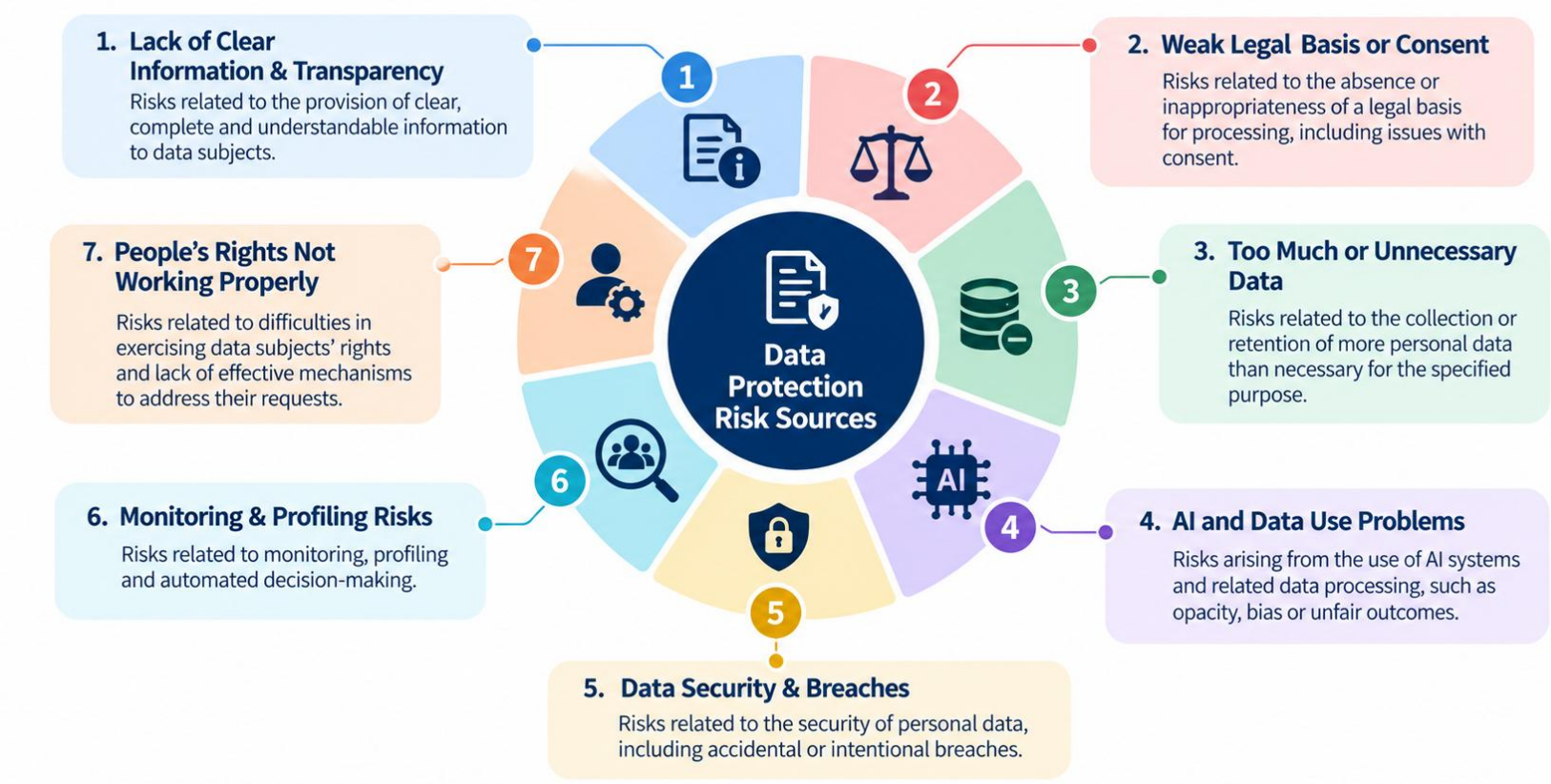
Each risk source could be instantiated by several common (or less common) real-world scenarios

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 4: Grouping risk sources

- The 40 risk sources can be grouped into the following categories



Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 3: Regulatory issues

- Risk sources may be associated with the non-fulfilment of specific data protection requirements.
- The taxonomy identifies 9 categories of regulatory issues

#	Regulatory Issue
1	Lack of transparency
2	Function creep / Lack of purpose limitation
3	Unlawful or excessive data retention
4	Collection of excessive personal data / Inferring excessive personal data
5	Loss of confidentiality / integrity / accuracy
6	Lack of informed consent
7	Users' rights are not sufficiently satisfied
8	Unlawful profiling and/or automated decision-making
9	Lack of accuracy / robustness / fairness of AI systems*

* Only applicable where AI systems are used.

Regulatory issues connect risk sources with relevant legal requirements, but without replacing a comprehensive legal compliance assessment.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 2: Harms to individuals

- Data protection risks should be examined in terms of their potential negative consequences for individuals.
- The taxonomy identifies 11 types of potential harms

#	Harm	Description
1	Physical harm	Physical injury or risk to physical safety.
2	Psychological harm – Anxiety	Negative impact on mental health, in particular anxiety (e.g. stress, fear, emotional distress).
3	(Cyber-)bullying	Harassment, intimidation or humiliation through digital means.
4	Lack of autonomy, manipulation and influence (including disinformation)	Reduced ability to make free and independent decisions due to manipulation, influence or exposure to disinformation.
5	Chilling effect	Deterrence from exercising rights or engaging in lawful activities due to the processing of personal data.
6	Unwanted privacy intrusion (beyond user's expectations)	Unwanted or excessive intrusion into an individual's private life beyond their reasonable expectations.
7	Sense of loss of control of personal data	Reduced ability to control how personal data are collected, used or shared.
8	Damage to the Reputation	Harm to an individual's reputation or social standing.
9	Discrimination	Unfair or unequal treatment of individuals or groups.
10	Denial of rights/services	Being denied access to rights, services, benefits or opportunities.
11	Financial harm	Direct or indirect financial loss.

Data protection risk assessment must consider what may actually happen to individuals, rather than focusing exclusively on GDPR compliance.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 1: Fundamental Rights

- The taxonomy considers 9 categories of fundamental rights
  - Drawing on the EU Charter of Fundamental Rights

#		Fundamental right
1		Right to Human Dignity
2		Right to Privacy & Data Protection
3		Freedom of Expression and Information
4		Freedom of Assembly & Association
5		Right to Property
6		Rights to Non-Discrimination & Equality (including persons with disabilities)
7		Right of child
8		Right to Health
9		Economic & Social Rights (e.g., work, housing, education)

- We focus on rights most likely to be affected by improper personal data processing
- Grouped into high-level categories, for convenience

The same type of risk source and/or harm may have different implications for fundamental rights, depending on the circumstances and the context of the processing

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Level 1: Fundamental Rights

#		Fundamental right	Description (relevant Articles of the Charter)
1		Right to Human Dignity	Refers to Article 1 (Human Dignity) and Article 3 (Right to the integrity of the person) of the EU Charter of Fundamental Rights.
2		Right to Privacy & Data Protection	Covers Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the EU Charter of Fundamental Rights. These rights are essential in any assessment of risks related to the mishandling of personal data.
3		Freedom of Expression and Information	Refers to Article 11 of the EU Charter of Fundamental Rights, which includes the freedom to hold opinions and to receive and impart information and ideas without interference.
4		Freedom of Assembly & Association	Refers to Article 12 of the EU Charter of Fundamental Rights, which includes the freedom of peaceful assembly and the freedom of association at all levels, including political, trade union and civic matters.
5		Right to Property	Refers to Article 17 of the EU Charter of Fundamental Rights, which guarantees lawful ownership, use and inheritance of possessions.
6		Rights to Non-Discrimination & Equality (including persons with disabilities)	Encompasses Article 21 (non-discrimination), Article 23 (equality between men and women), Article 25 (rights of the elderly) and Article 26 (integration of persons with disabilities) of the EU Charter of Fundamental Rights.
7		Right of child	Refers to Article 24 of the EU Charter of Fundamental Rights, which provides for the protection and care of children, their best interests as a primary consideration, and their right to express their views freely, with due regard to their age and maturity.
8		Right to Health	Refers to Article 35 of the EU Charter of Fundamental Rights, covering the right to access preventive health care and to benefit from medical treatment under the conditions established by national laws and practices.
9		Economic & Social Rights (e.g., work, housing, education)	Encompasses Articles 31 (fair and just working conditions), 27 (workers' right to information and consultation), 33 (family and professional life) and 14 (right to education) of the EU Charter of Fundamental Rights.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The byRisk taxonomy in practice – An example

- Let us consider the following scenario:

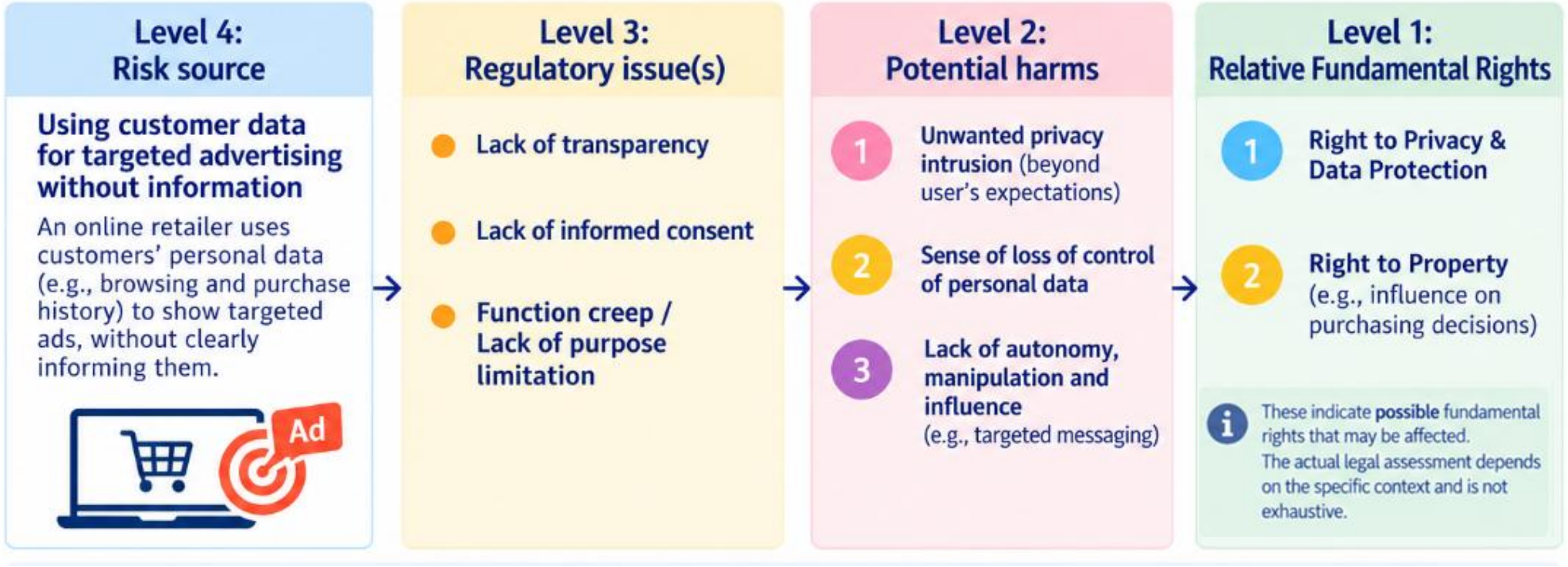


- How to identify/understand the risk, according to the byRisk taxonomy?

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The byRisk taxonomy in practice – An example



- A single risk source may lead to multiple harms and affect several fundamental rights, depending on the processing context.
- Note that even a routine business practice may create risks to individuals' rights and freedoms, even in the absence of a security breach.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

From the taxonomy to real-world scenarios

- The byRisk taxonomy provides a common framework for systematically identifying data protection risks.
- Real-world scenarios translate general risk sources into situations arising from everyday processing activities.
- These scenarios are tailored to specific processing contexts.
- The resulting associations provide the foundation for the two byRisk tools:
  - Risk awareness for the general public
  - Risk assessment for SMEs

See next…

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Thank you for your attention



Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.