# “Demonstration of the (by)Risk Assessment Tool for the SMEs”

Georgia Panagopoulou

ICT Specialist, Head of Audits and Security Department

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.

# Roadmap

01 Methodology adopted

02 The questionnaire for SMEs

03 Analysis of responses

04 Conclusions

05 SMEs Risk Assessment Tool: two practical examples

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.

# Methodology adopted

## QUESTIONNAIRE

- Anonymous electronic questionnaire
- Designed and distributed via the secure EU Survey platform
- Questions informed by the HDPA's experience
- Focus on key risks and areas where SMEs may lack awareness or understanding

## TARGET SECTORS

- **Hotels & tourism**
- **Education**
- **Retail (physical & online)**
- **Food service**
- **Healthcare • IT services**

## DISSEMINATION

- Through SME associations to maximise outreach
- Direct contact with SMEs previously engaged with the HDPA, including through ByDefault project

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 questionnaire for SMEs (1/3)

## SME Profile & Personal Data Processing

### SME PROFILE

- Company size (number of employees)
- Sector of activity

### PERSONAL DATA PROCESSING ACTIVITIES

- Customer relationships and marketing
- Employee management and recruitment
- Security and operational efficiency (e.g. CCTV, GPS)
- Supplier relationship management

### RISK PRIORITIZATION

- Processing activities perceived as posing the highest data protection risks

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 questionnaire for SMEs (2/3)

## Data Protection Risk Identification & Assessment

### HIGH-RISK PROCESSING STAGES

- Collection, storage, use, sharing, deletion or anonymisation

### RISKS TO INDIVIDUAL RIGHTS AND FREEDOMS

- Financial or physical harm, discrimination, manipulation, harassment, loss of control

### RISK ASSESSMENT TOOLS

- Use of established methodologies, such as ISO/IEC 29134:2017 and the CNIL Risk Assessment Tool.
- Identification of other tools used or lack of experience with risk assessment

### POTENTIAL SOURCES OF RISK

- Cyberattacks, human error, software failures, inadequate training, and insufficient oversight of external contractors

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 questionnaire for SMEs (3/3)

## AI Adoption & Needs for a Risk Identification Tool

### AI ADOPTION

- Current use or planned adoption of AI systems.
- Identification of the purposes

### AI RELATED DATA PROTECTION RISKS

- Inappropriate processing of personal data through AI chatbots.
- Inaccurate, misleading, or biased outputs.
- Unfair decisions in recruitment.
- Unauthorized access to data or use of personal data for AI training without users' awareness.
- Lack of transparency, explainability, human intervention, and effective exercise of GDPR rights.

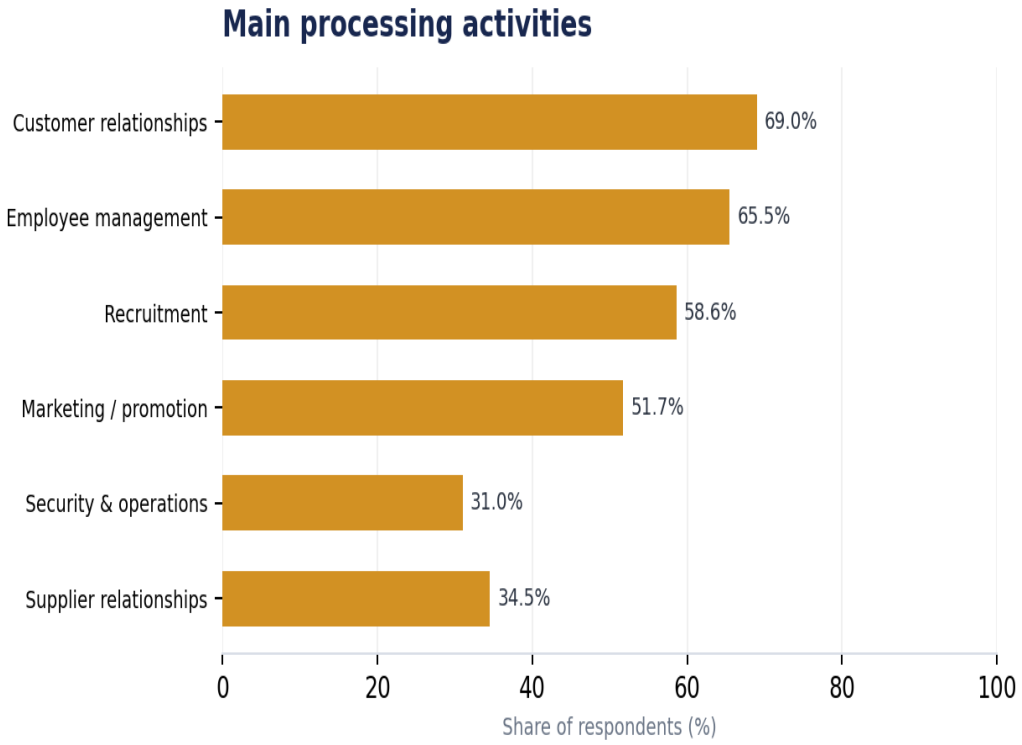
### EXPECTED FEATURES OF A RISK IDENTIFICATION TOOL

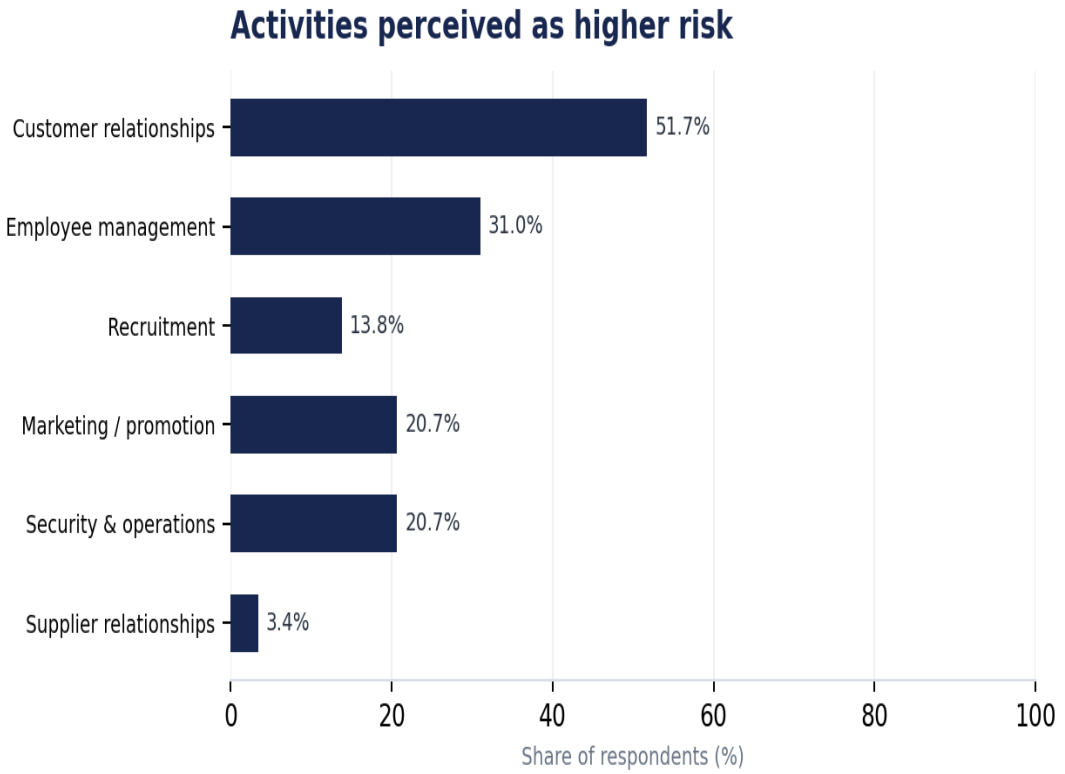
- Dynamic identification and prioritization of risks.
- Consideration of legal obligations, data sensitivity, and potential impacts on individuals.
- Coverage of risks to rights and freedoms, beyond information security.
- Applicability to all types of personal data processing.

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.

# Analysis of responses (1/4)



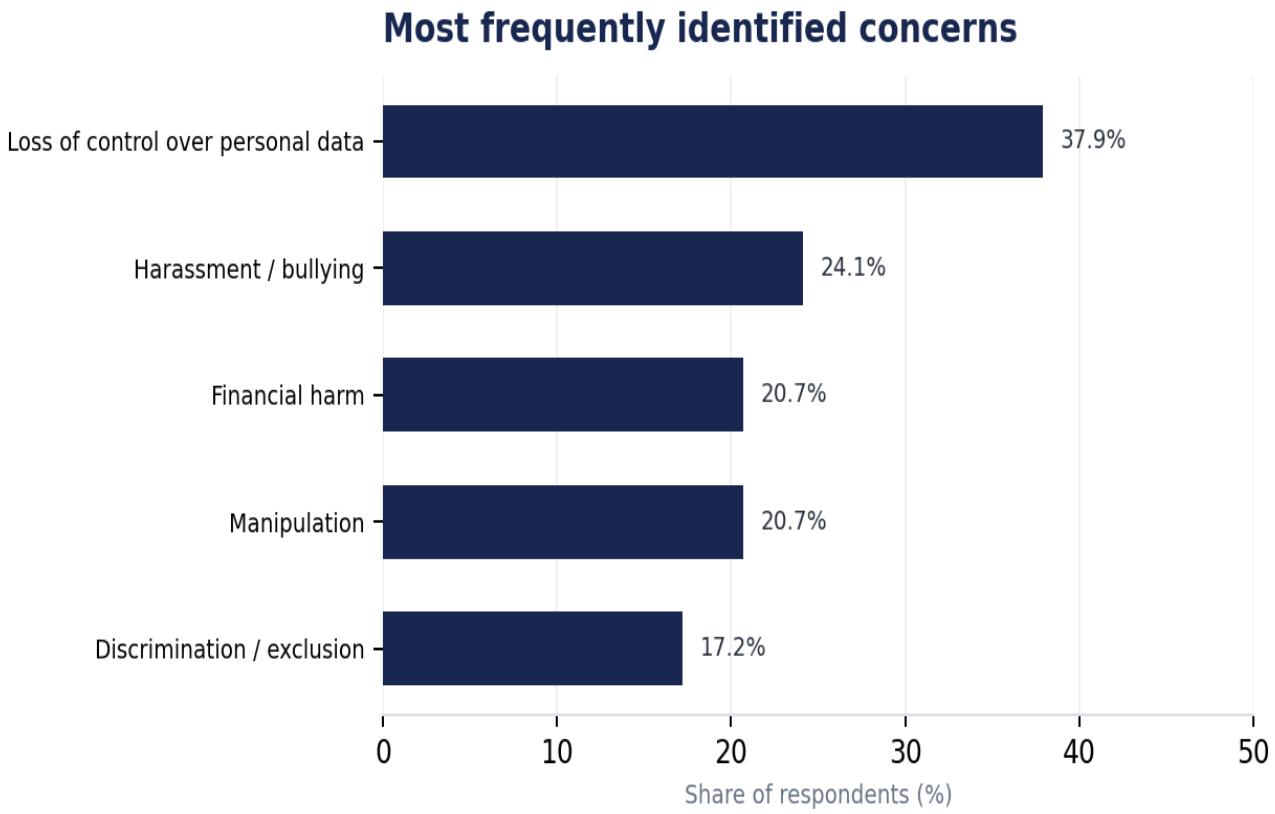




**Customer and employee-related processing features prominently in both charts.**

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.

# Analysis of responses (2/4)




**USE OF RISK ASSESSMENT TOOLS**

**69.0%** no tool

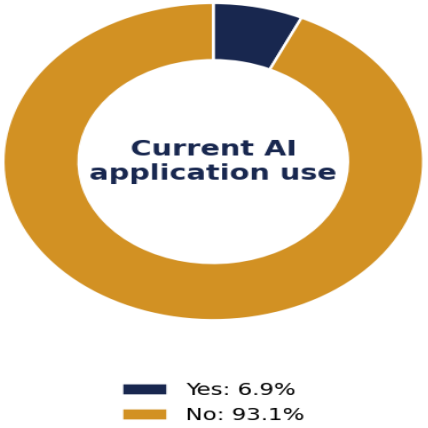
13.8% CNIL tool • 3.4% ISO/IEC 29134:2017

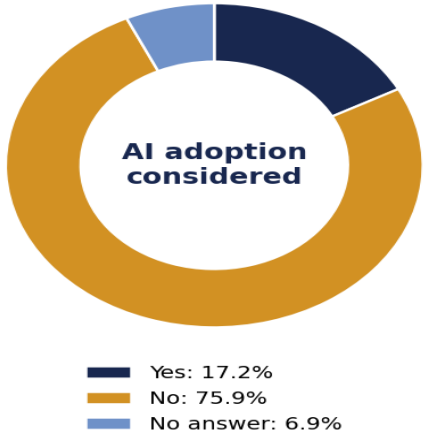
17.2% other tools

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.

# Analysis of responses (3/4)




**≈40%** — **Accuracy of AI outputs**

Concern about the accuracy of information provided by AI systems

**≈35%** — **Access to a human**

When users cannot be served or dispute an AI outcome

**≈25%** — **Biased or unfair decisions**

Risk of decisions that may be biased or unfair

**≈28%** — **Data extraction & inference**

Risk from poor implementation and/or protection of AI systems

**≈33%** — **AI training with personal data**

Use of personal data to train AI without users' awareness

**≈38%** — **Ability to exercise GDPR rights**

Whether AI applications enable users to exercise their data-protection rights

**≈33%** — **Personal data entered into AI chatbots**

Improper or unclear processing of users' personal data

**≈33%** — **Transparency & explainability**

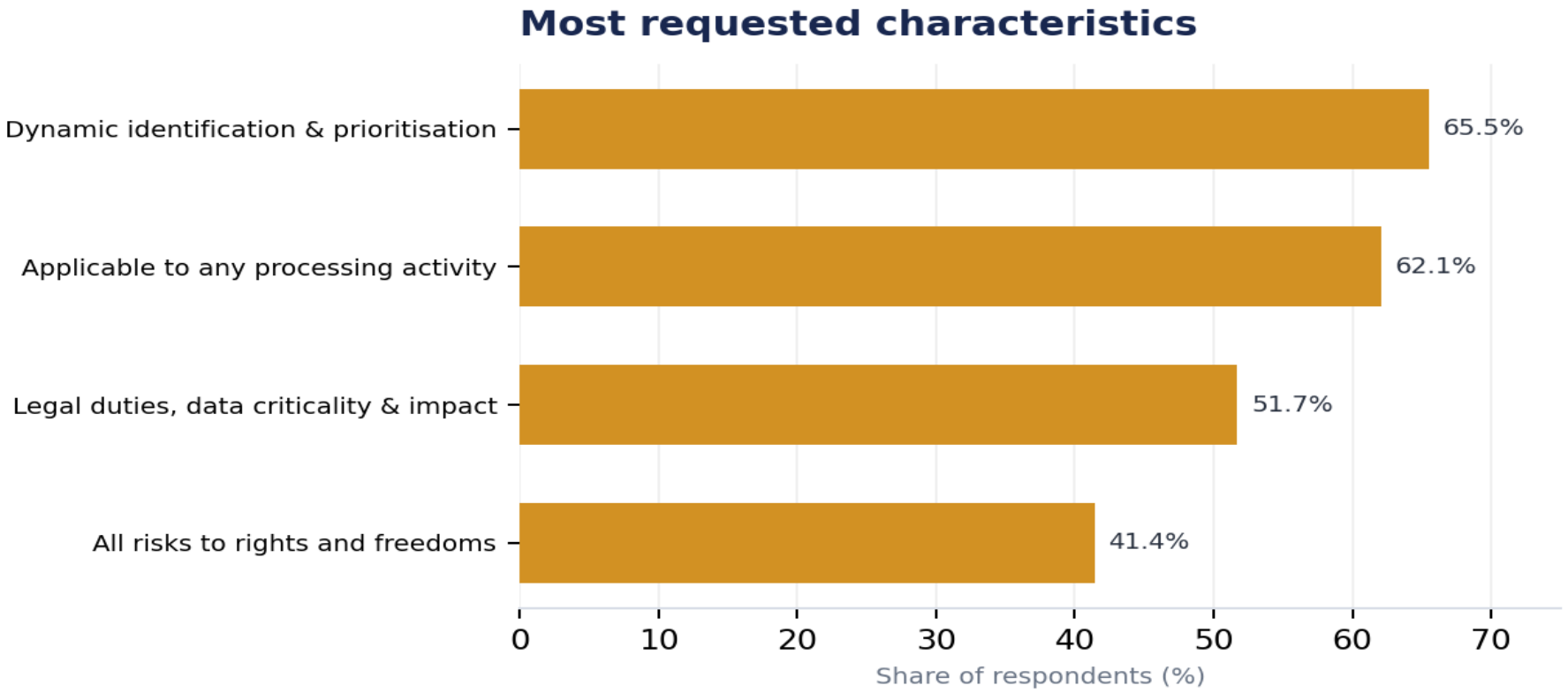
Informing users and explaining how AI applications function

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.

# Analysis of responses (4/4)

## What SMEs expect from a risk identification tool




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.

# Conclusions

- It is important to provide guidance, to both SMEs and to the public, of how data processing operations may actually affect human rights (beyond the rights to privacy and personal data protection).
- The guidance should cover the threats and risks associated with the new AI systems ecosystem
- An efficient tool to support SMEs in properly identifying all the relevant risks is of high importance.

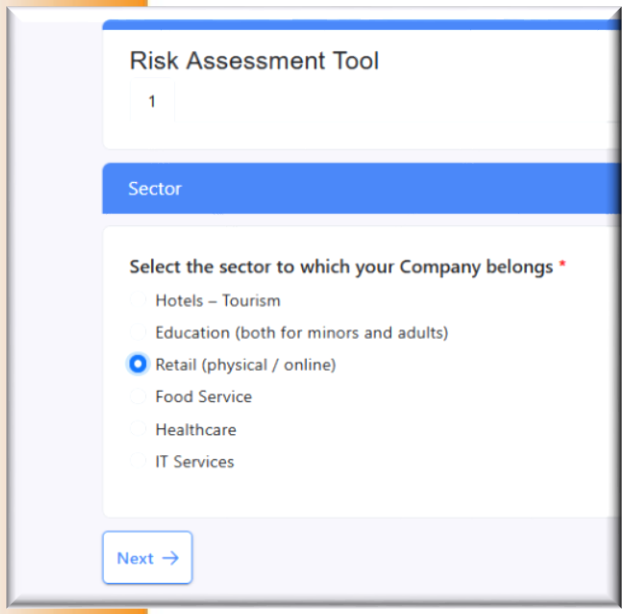
Funded by the European Union

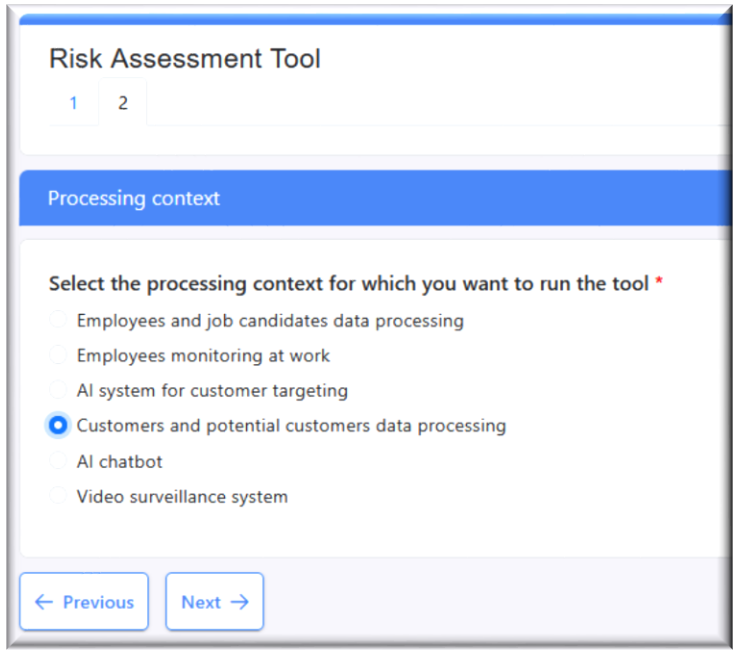
The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting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

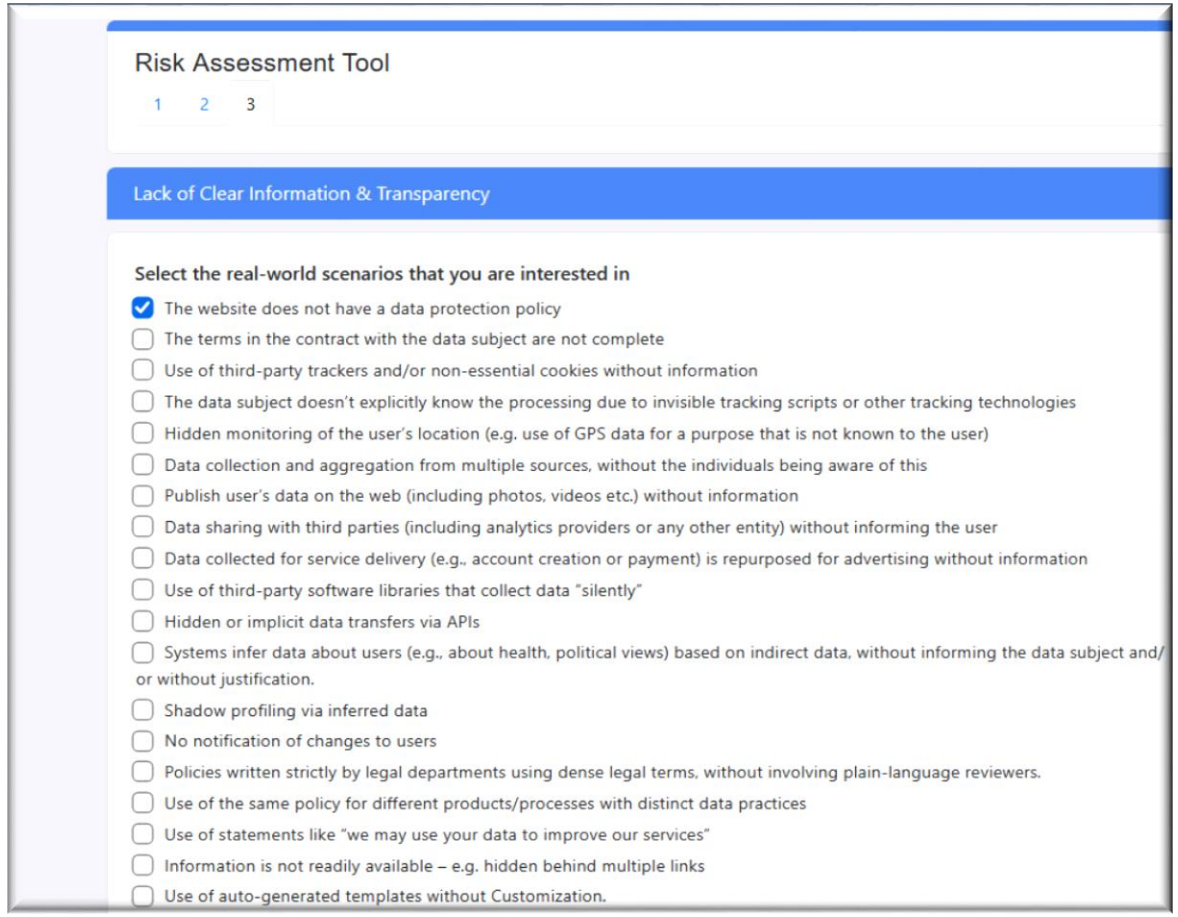
# SMEs Risk Assessment Tool Examples

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.




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.

# SMEs Risk Assessment Tool

## 1. Example Report | 1/4 · Risk profile

SECTOR

**Retail (physical / online)**

PROCESSING CONTEXT

**Customers and potential customers data processing**

## Risk sources

1. **No (properly) communicating to the data subjects information about their rights**
2. **Non-existing information concerning personal data processes**

SELECTED REAL-WORLD SCENARIO

**The website does not have a data protection policy**

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

# SMEs Risk Assessment Tool



## Key regulatory issues identified in this example

### 1 Users' rights are not (sufficiently) satisfied

STEMS FROM RISK SOURCE

No (properly) communicating to the data subjects information about their rights

### 2 Lack of transparency

STEMS FROM RISK SOURCES

- Non-existing information concerning personal data processes
- No (properly) communicating to the data subjects information about their rights

Two regulatory concerns are linked to the same underlying transparency and communication gaps.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

## Possible harms for the individuals

### 1 Sense of loss of control of personal data

When customers and potential customers are not informed in a clear and transparent way which personal data is collected and how such data is used or shared, possibly for different purposes than their initial collection, individuals feel they no longer control their personal information, leading to feelings of vulnerability and diminished trust in the retail company.

### 2 Unwanted privacy intrusion (beyond user's expectations)

When retailers use unclear, complex or hidden policies, customers and potential customers (such as website guests), including app users, may be unaware of how extensively their personal information is accessed or shared or used in a way they did not expect of agree to (including their physical movements in a shop or browsing habits online). This can lead to unwanted privacy intrusions, where the customers feel their private lives are exposed without consent or awareness.

### 3 Denial of rights/services

When retailers fail to provide clear and accessible information about how customer data is collected, used, or shared, customers may not fully understand their data rights or how to exercise them. Customers/ potential customers are not able to request data deletion (for example deletion of their purchase history, correct inaccuracies, or object to profiling). As a result, they may lose control over their information or even miss deadlines or procedures for raising concerns or complaints. In some cases, the processing of inaccurate data may lead to denial of properly customized services. This can lead to undermining fairness and accountability in commerce (including digital commerce).


**Funded by the European Union**

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

# Fundamental Rights that may be violated

## 1 Rights to Non-Discrimination & Equality (including persons with disabilities)

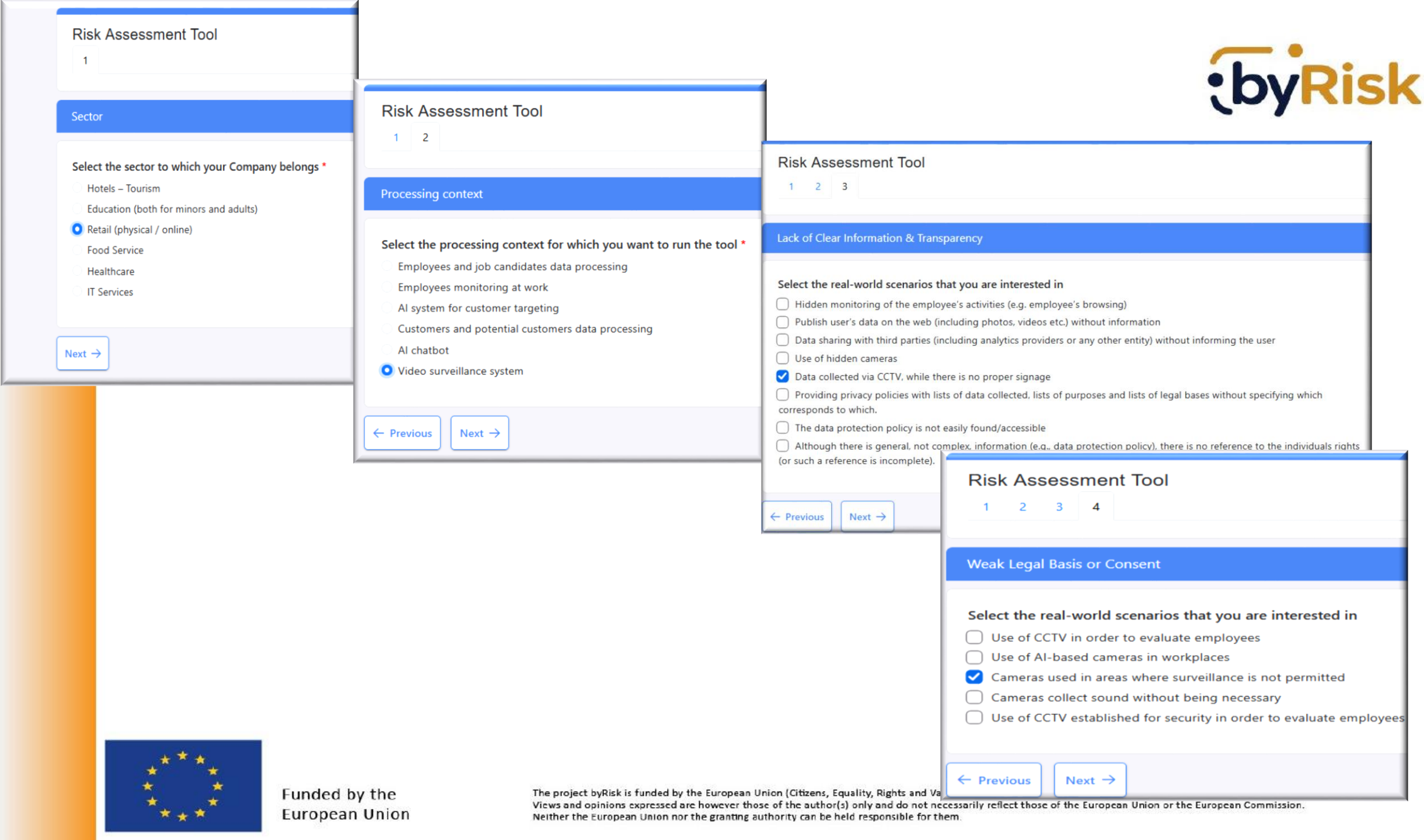
Violations of the Right to Non-Discrimination and Equality occur when processes such as profiling, automated decision-making, or unjustified data inference create or reinforce unfair treatment among customers/potential customers. These violations undermine equality of opportunity, including pricing, offers, customer support, or access to services.

## 2 Right to Privacy & Data Protection

Harms such as loss of control, privacy intrusion, denial of rights, financial harm, and anxiety are main violations of the Right to Privacy and Data Protection, resulting from unlawful, non-transparent, or processing without security safeguards or data minimization. These failures not only fail to uphold legal obligations but also undermine user trust, fairness, and autonomy especially in digital environments.

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.




byRisk

Funded by the European Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Va
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.

# SMEs Risk Assessment Tool

## 2. Example Report | 1/6 · Risk profile

SECTOR

**Retail (physical / online)**

PROCESSING CONTEXT

**Video surveillance system**

## Risk sources

### 1 Non-existing information concerning personal data processes

Scenario: Data collected via CCTV, while there is no proper signage

### 2 Lack of Purpose-Specific Data Collection Design

Scenario: Cameras used in areas where surveillance is not permitted

CASE IN FOCUS

**CCTV use without proper signage and cameras in areas where surveillance is not permitted**

**Funded by the\nEuropean Union**

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

# SMEs Risk Assessment Tool



## Two regulatory issues emerge from the CCTV risk sources

### 1 Lack of transparency

STEMS FROM RISK SOURCE

Non-existing information concerning personal data processes

### 2 Collection of excessive personal data – Inferring excessive personal data

STEMS FROM RISK SOURCE

Lack of Purpose-Specific Data Collection Design

Funded by the\nEuropean Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

## Possible harms for the individuals

### 1 Denial of rights/services

If customers and staff are not clearly informed about CCTV use, they may not know how to exercise rights such as requesting footage (e.g., for theft disputes, incidents, or complaints), correction, or objection, limiting their ability to protect their personal data.

### 2 Lack of autonomy, manipulation and influence (including disinformation)

CCTV footage in retail settings may be reused beyond security purposes (e.g., customer profiling, employee performance evaluation, behavioural analytics) without a valid legal basis, influencing both customer behaviour and employee conduct without clear awareness.

### 3 Chilling effect

Lack of transparency may discourage natural behaviour in retail environments (e.g., asking questions, trying products, or raising complaints) due to fear that actions are being recorded and reviewed.

### 4 Psychological harm – Anxiety

Shoppers, employees, and visitors may feel uncertain or uneasy about being monitored during shopping or working activities, particularly if surveillance coverage and purposes are unclear, creating discomfort in an environment expected to be routine and low-pressure. Customers, staff, and visitors may feel increased stress or discomfort if surveillance extends beyond theft prevention or operational security, especially if they are unsure whether footage is used for performance monitoring or behavioural tracking.


**Funded by the European Union**

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

## Possible harms for the individuals

### 5 Unwanted privacy intrusion (beyond user's expectations)

Poorly communicated surveillance in retail spaces may create a feeling of being constantly observed beyond reasonable expectations, especially in areas like fitting rooms entrances, checkout queues, or self-service zones where customers expect limited observation. Installing cameras in areas such as, e.g., near fitting rooms, cashier areas, staff-only zones, or detailed customer tracking zones or using audio recording without necessity may exceed what customers and employees reasonably expect in retail environments.

### 6 Sense of loss of control of personal data

If CCTV cameras in retail environments (e.g., shop floors, entrances, checkout areas, fitting rooms nearby) are not clearly signposted or explained, customers, employees, and visitors may not understand who is being recorded, for what purpose, how long footage is stored, or who can access it. This creates a loss of perceived and actual control over personal data in a shopping context. Individuals lose control over how their recorded data is used when CCTV is repurposed for secondary objectives such as employee evaluation, customer behavior analysis, queue tracking, or dispute resolution without proper legal justification.


**Funded by the\nEuropean Union**

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

## Fundamental Rights that may be violated

### 1 Right to Privacy & Data Protection

The use of CCTV systems in retail environments (e.g., clothing stores, market places etc.) may interfere with privacy and data protection when customers or staff are recorded without clear notice, when surveillance extends into semi-private or expectation-sensitive retail areas (e.g., fitting room entrances, checkout queues, staff-only areas), or when footage is retained excessively or reused for secondary purposes such as employee evaluation, customer profiling or behavioural scoring. This right is engaged through multiple harms including unwanted privacy intrusion, loss of control over personal data, psychological harm (anxiety), and manipulation or behavioural influence. In a retail context, individuals expect short-term, transaction-focused interactions, and continuous or poorly explained surveillance—especially when combined with analytics or integrated systems across store networks—can undermine trust and conflict with core principles of transparency, purpose limitation, and data minimisation.

### 2 Freedom of Expression and Information

In retail environments, customers and staff may alter their natural behaviour if they are aware or suspect that they are being continuously recorded, particularly in sensitive interaction points such as customer service desks, checkout areas, or complaint situations. Customers may avoid raising concerns, asking questions, or engaging in open communication with staff, while employees may adjust their service behaviour, communication style, or workplace interactions due to perceived surveillance and performance monitoring.


Funded by the\nEuropean Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission can be held responsible for them.

## Fundamental Rights that may be violated

### 3 Economic & Social Rights (e.g., work, housing, education)

CCTV monitoring and profiling in the retail sector may affect economic and social rights by influencing employment conditions for retail staff, including performance evaluation, disciplinary decisions, and workplace monitoring practices that may not always be transparent or proportionate. For customers, excessive or intrusive surveillance may affect willingness to shop in certain stores or use retail services, indirectly impacting access to goods and everyday consumer services.

### 4 Rights to Non-Discrimination & Equality (including persons with disabilities)

CCTV systems in retail environments may result in discriminatory outcomes when surveillance is combined with profiling, behavioural analysis, or subjective interpretation of recorded behaviour. This may lead to unequal treatment of customers (e.g., differential service attention) or biased evaluation of employees' performance based on recorded behavior.

Funded by the\nEuropean Union

The project byRisk is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV). The 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 European Commission 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.