byRisk

Issue 2 - November 2025

NEWSLETTER

Helping SMEs Identify and Analyze Data Protection and Privacy Risks

Raising Awareness of Data Protection and Privacy Risks Among SMEs and the General Public

The byRisk project is funded by the Citizens, Equality, Rights and Values Programme (CERV) of the European Union and is coordinated by the Hellenic Data Protection Authority.

The Partners

The byRisk Consortium is made up of three partners, each representing a different sector: regulatory, academic, and software industry. The project is coordinated by the Hellenic Data Protection Authority, with the other two partners being the University of Piraeus Research Center and ICT Abovo PC.

HELLENIC DATA PROTECTION AUTHORITY

ICT abovo Information & Communication Technologies

UNIVERSITY OF PIRAEUS RESEARCH CENTER

The project in brief

On December 1st, 2024, the Hellenic Data Protection Authority launched the project titled "**Driven by risk: Fostering data protection risk assessment for SMEs and raising risk awareness among the general public ('byRisk')**", following a successful proposal to the European Commission.

Visit the website of the project at
https://byrisk-project.eu/

The byRisk project is funded by the European Union's Citizens, Equality, Rights and Values Programme (CERV) under Grant Agreement No. 101193352.
It is coordinated by the Hellenic Data Protection Authority.

The project is scheduled for completion in November 2026.

The project's Goals

byRisk aims to achieve two strategic goals:

To assist SMEs to effectively identify and analyse all data protection and privacy risks associated with their data processing activities:

- **By developing a comprehensive taxonomy of data protection and privacy risks**, and identifying the most effective channels for communicating these risks to SMEs and data subjects.
- **By creating a Risk Assessment Tool** enabling intuitive identification and analysis of data protection and privacy risks, utilizing context-aware questionnaires.

To raise awareness of data protection and privacy risks among a wide range of stakeholders, including SMEs and the general public:

- **By developing a Risk Awareness Tool for the general public** that will be utilised for raising awareness of data protection and privacy risks through visualizations of potential harms, as well as recommended precautions and countermeasures.

⇨ Awareness-raising activities will also focus on specific groups, such as university students and ICT professionals, aiming to further increase awareness within the communities that design and operate ICT systems.

New Taxonomy and Tool Framework

Following the first newsletter, which outlined the project's initial steps, methodology, and key takeaways from the SME survey, this second edition focuses on the next stage of development and implementation. Throughout July 2025, significant progress was made in developing a new risk taxonomy and designing the framework and core functionalities of the risk assessment tool.

A new taxonomy of data protection and privacy risks

One of the main objectives of the byRisk project is to develop a **new taxonomy** for systematically characterizing risks to individuals' rights and freedoms arising from personal data processing.

The concept of risk is closely linked to the potential impact on individuals resulting from such processing.

The proposed taxonomy aims to provide a structured framework for classifying and analyzing these risks in terms of their relevant impacts, thereby supporting comprehensive risk assessment and promoting awareness.

Therefore, a **four-level taxonomy** is proposed, organized in a **top-down structure** as detailed below, starting from the identification of potential violations of fundamental rights and progressively moving towards more specific levels, including individual harms, related regulatory issues, and concrete risk sources:

Level 1: Violation of Fundamental Rights:
This level encompasses the specific fundamental rights that may ultimately be infringed if an event materializing a given risk source occurs.

Level 2: Harms to individuals:
This level encompasses the potential negative consequences or impacts on individuals, which may be linked to specific violations of fundamental rights.

Level 3: Regulatory issues:
This level describes specific legal issues arising from applicable legislation that may occur if an event materializing a given risk source takes place.

Level 4: Risk sources:
This level refers to specific situations or conditions that may lead to harms for individuals.

Developing an SME-Oriented Tool

Application of the risk taxonomy to SME contexts

The primary areas of concern for SMEs in relation to risky personal data processing pertain mainly to activities involving customers and employees. Although AI-based systems are not yet widely adopted by SMEs in Greece, credible indications suggest that their deployment is likely to increase in the near future.

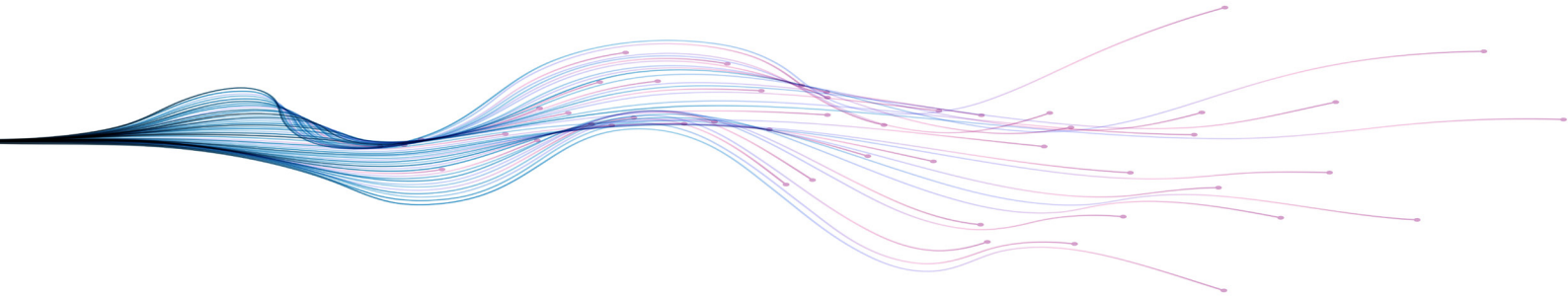
Taking the identified risk sources from the above taxonomy as a starting point, several representative real-world scenarios will be described, reflecting typical SME operations in which at least one such risk source may be instantiated.

Processes, Functionalities, and Expected Outcomes of the Tool

The processes and functionalities of the Risk Assessment Tool for SMEs must be clearly defined to guide its development. This includes documenting the functionalities to be integrated, the processes and interfaces to be implemented, the expected outcomes, and the manner in which SMEs will interact with the tool to obtain relevant information.

Requirements

In designing an effective method for communicating risks to SMEs, several **key requirements** have been identified to ensure usability, clarity, and accessibility. The Risk Assessment Tool should be **user-friendly**, featuring a simple and intuitive



interface that allows users to quickly access relevant information without having to complete excessive fields. Information should be presented in a layered manner, using **clear and accessible language**. The tool should be **platform-independent**, functioning seamlessly across different operating systems such as Windows and Android, without the need for additional software installations. Finally, it should enable the generation of comprehensive and easy-to-understand **output reports**, which can be conveniently saved as PDFs or printed for further use.

Core Functionalities

The risk assessment tool has been designed around a structured **sequence of phases**, each serving a distinct purpose in the evaluation process.

In the **Initial Phase**, users define the processing context, setting the foundation for a comprehensive understanding of the data environment. During the **Risk Identification Phase**, potential risks are identified and linked to applicable real-world scenarios, while each risk is associated with its potential sources. The **Impact Categorization Phase** then connects the identified risks to relevant regulatory considerations, ensuring alignment with applicable legal frameworks. Finally, the **Impact Assessment Phase** focuses on assessing potential harms to individuals and evaluating the implications for affected fundamental rights. A comprehensive downloadable output report will be generated.

Moreover, the tools will provide appropriate explanatory text to the user. To ensure simplicity, user input is required only during the first two phases. The subsequent phases use the provided information to execute assessments automatically.

Public Insight into Data Risks

Strategy to improve public understanding of risk

The web-based risk-awareness tool, freely accessible to the general public, aims to maximize the dissemination of information on personal data protection. Its introduction will include a brief explanation of the importance of safeguarding personal data and the potential harms that may arise from misuse.

Users will then be guided through practical examples of possible harms and the conditions under which they may occur. As these harms depend heavily on the context of data processing, users will first select a specific use case of interest. These use cases will represent typical data processing scenarios, informed by the HDPA's extensive experience in handling data protection complaints.

For each use case, the tool will present several real-world examples of improper practices by data controllers/data processors. By selecting one or more of these scenarios, users will receive feedback on the potential harms they may face and any possible legal violations committed by the data controller, accompanied by clear and accessible explanations.

While the risk awareness tool differs from the risk assessment tool designed for SMEs, it will nonetheless rely on the same underlying risk taxonomy.

Next steps

Looking ahead to the end of 2025, the project will focus on three key milestones. First, an **awareness raising strategy** will be developed to increase understanding of data protection risks among stakeholders. Next, a **first version of the risk awareness tool for the public** will be launched, providing accessible guidance and information. Finally, a **preliminary version of the risk assessment tool for SMEs** will be delivered for the pilot phase, allowing small and medium-sized enterprises to explore and test its functionalities.

byRisk

https://byrisk-project.eu/
Email: byRisk@byrisk-project.eu