

Issue 1 - May 2025

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.

Views and opinions expressed are however those of the project partners only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.



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.











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 <u>https://byrisk-project.eu/</u>

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.

byRisk Newsletter



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.



Fisrt steps Identifying data protection risks

Risks are closely linked to various fundamental rights and freedoms of individuals, extending beyond just data protection concerns. Within the context of data protection, the broader definition of what constitutes a risk has yet to be fully explored.

The following outlines the initial actions taken within the project:

- Firstly, the data protection requirements set out in the **current national and European legal and regulatory frameworks** — including those applicable to the byRisk project — were thoroughly examined.
- Secondly, a literature review was necessary in order to examine existing data protection taxonomies and methodologies for assessing risks, along with tools for risk management. It highlighted several distinct types of data protection taxonomies, with particular emphasis on the risks associated with AI systems, which represent a unique category of risks with distinct characteristics.
- Lastly, the **methodology employed**, which was based on a structured **questionnaire**, aimed to gather **direct feedback from SMEs** regarding their needs in order to effectively identify the risks associated with their data processing activities.





To achieve the desired objectives, an appropriate questionnaire was drafted and delivered through an electronic survey, which was distributed to SMEs across Greece.

This approach enabled respondents to provide their answers conveniently while ensuring anonymity. The questions were carefully curated based on the HDPA's prior knowledge and experience regarding what constitutes a risk and which areas may be less understood by SMEs.

The primary objective of the survey was to identify, to the greatest extent possible, the needs of Greek SMEs in accurately identifying data protection risks, as well as to assess whether they are using or plan to use AI systems. To achieve this, the HDPA pinpointed specific sectors where data protection activities are particularly critical due to the associated risks. These sectors play a vital role in the Greek economy and include the following:

- Hotels and Tourism
- Education (both for minors and adults)
- Retail (physical and online)
- Food Services
- Healthcare
- IT Services



Key Takeaways

The **key conclusions** drawn from the survey are summarized as follows:

- There is no commonly agreed definition of what exactly constitutes a data protection risk.
- Users' perceptions of risk often differ from those held by organizations.
- There is a limited number of available tools for risk assessment. Most SMEs in Greece do not currently use these tools, although the vast majority express interest in having access to one.
- SMEs in Greece appear to focus primarily on security-related risks.
- According to SMEs, the processes that pose the highest risks to personal data protection are those involved in managing customer/service relationships (e.g. customer data).
- SMEs in Greece currently do not use AI tools and are generally unaware of the associated risks.
- It is essential to provide clear guidance to both SMEs and the public on how data processing activities can impact human rights, extending beyond privacy and personal data protection.
- This guidance should specifically address the threats and risks emerging from the evolving AI systems ecosystem.
- Developing an effective tool to assist SMEs in accurately identifying all relevant risks is of paramount importance.
- To enable precise risk identification for SMEs and the public, a clear and welldefined risk taxonomy must be established as a foundational step.



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