SENTINEL

Bridging the security, privacy, and data protection gap for smaller enterprises in Europe

D7.6 - Ecosystem building and SMEs engagement report – final version

This work is part of the SENTINEL project. SENTINEL has received funding from the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

Project Information

Grant Agreement Number	**101021659**
Project Acronym	SENTINEL
Project Full Title	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
Starting Date	1st June 2021
Duration	36 months
Call Identifier	H2020-SU-DS-2020
Topic	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Project Website	https://www.sentinel-project.eu/
Project Coordinator	Dr. George Bravos
Organisation	Information Technology for Market Leadership (ITML)
Email	gebravos@itml.gr

Document Information

Work Package	Work Package 7
Deliverable Title	D7.6 - Ecosystem building and SMEs engagement report - final version
Version	1.5
Date of Submission	29/05/2024
Main Editor(s)	Ruben Costa (UNINOVA), Cláudio Côrrea (UNINOVA)
Contributor(s)	-
Reviewer(s)	Marinos Tsantekidis (AEGIS), Eleni-Maria Kalogeraki (FP), Siranush Akarmazyan (ITML)

Document Classification							
Draft		**Final**	X	**Confidential**		**Public**	X

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	29/03/2024	Draft	Confidential
1.1	30/04/2024	Review conducted by ITML	Confidential
1.2	30/04/2024	Review conducted by AEGIS	Confidential
1.3	02/05/2024	Review conducted by FP	Confidential
1.4	22/05/2024	Reviewers’ comments addressed	Confidential
1.5	29/05/2024	Final version ready	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	**Explanation**
EDIH	European Digital Innovation Hub
GDPR	General Data Protection Regulation
SMEs/MEs	Small, Medium Enterprises/Micro Enterprises
MVP	Minimum Viable Product
OTMs	Organization and Technical Measures
PDP	Personal Data Protection
WP	Work Package

Executive Summary

Deliverable D7.6 “Ecosystem building and SMEs engagement report – final version” is produced within Work Package 7 (Ecosystem building, Exploitation and sustainability management) of the SENTINEL Project, under Task 7.4 “SENTINEL ecosystem building: Continuous engagement of technology providers, SMEs/MEs”.

This document aims to report on the activities carried out during the last 18 months of the project (M19-M36), within Task 7.4. It follows SENTINEL Dissemination Strategy in which the SENTINEL stakeholders’ engagement activities are to be reported.

The document presents the efforts of the SENTINEL project, towards continuous community building and an ecosystem around the project’s results. The report presented establishes a solid SENTINEL stakeholder engagement strategy and time plan to outline the stakeholder communication activities for the entire project period. In particular, it includes the ongoing work on networking and liaisons with technical- and domain-specific communities. Furthermore, it describes the activities organized for potential end-users and stakeholders to promote the project’s technologies and impact assessment outcomes for future transferability to other domains and thus sustainability. As part of this strategy and aiming to create awareness and interest of primary stakeholders, insights from the stakeholder analysis are illustrated in this report based on the 4th and 5th SME-centric workshop questionnaires released according to the stakeholder engagement plan.

1. Introduction

1.1 Purpose of the document

1.1.1 Scope

The ecosystem building and SMEs engagement report – final version (D7.6), builds a community and an ecosystem around the project's results during the project period, including networking and liaisons with technical- and domain-specific communities. This process is split into two (2) main phases: i) engaging potential end users of the SENTINEL platform (that is, processing sensitive data or dealing with cybersecurity aspects); and ii) identifying potential technology providers to enhance the SENTINEL offerings further.

The main purpose of this document is to showcase the progress of the work in T7.4 conducted in the second half of the project which was presented in previous deliverable (D7.5).

1.1.2 Contribution to WP7 and project objectives

This deliverable has been composed within the context of *WP7 "Ecosystem building, Exploitation and sustainability management".* It focuses on ensuring that the outcomes of the project are widely disseminated to the appropriate target group, at the appropriate time and via appropriate methods. Furthermore, it aims at identifying stakeholders who can contribute to the development, evaluation and uptake of the project outcomes and encouraged them to participate in the project's current and future actions.

The main objectives of WP7 are:

- Develop the project's visual identity.
- Raise awareness about the project concept, developments and findings to all key actors.
- Develop the dissemination and communication strategy of the project.
- Develop the SENTINEL business model and strategies for incentivizing/promoting project adoption.
- Create a marketing strategy that focuses on commercialization.

1.1.3 Relation to other WPs and deliverables

This deliverable is the updated version of deliverable D7.5 "Ecosystem building and SMEs engagement report – interim version". This document reports on the ecosystem-building and SMEs engagement activities conducted during the last 18 months of the project (M19-M36). The report details the continuous efforts to build a community and ecosystem around the project's results, focusing on engaging potential end-users and technology providers to enhance SENTINEL's offerings. It is very closely related and aligned with the developments in the Work Package 6 "Real-life experiment evaluations: SENTINEL pilots", namely through the activities reported in:

- D6.1: SENTINEL Demonstration - initial execution and evaluation
- D6.2: SENTINEL Demonstration - final execution
- D6.3: Assessment report and impact analysis

1.2 Structure of the document

This document is structured in the following way:

- Section 2 describes the SENTINEL strategy followed for ecosystem building and SMEs engagement.
- Section 3 highlights the SME's engagement activities performed after M19 until M36.
- Section 4 provides a detailed analysis of the 4th and 5th SME-centric workshops.
- Section 5 presents key takeaways of all SME-centric workshops and illustrates overall insights obtained from all five SME engagement questionnaires.
- Section 6 concludes the report with final remarks.

The results of the work reported here are crucial for the project's exploitation activities that have been taking place in parallel, under WP7. Such findings enabled us to gather feedback on the SENTINEL platform and assess the willingness of SMEs to invest in such solutions.

1.3 Intended readership

This document is intended for both consortium members and external to the project stakeholders, by illustrating the SENTINEL strategy and the stakeholder engagement activities performed between the 19th month and 36th month of the project.

2. Review on SENTINEL Ecosystem Building and SMEs Engagement Strategy

2.1 Objectives

The SENTINEL ecosystem building and SMEs engagement focus on establishing a community and an ecosystem around the project's results. This work includes networking and liaisons with technical- and domain-specific communities, focusing on potential end-users and interested stakeholders to promote the project's technologies and impact assessment outcomes for future transferability to other domains and thus sustainability. Towards this direction, special focus has been given to Digital Innovation Hubs. Based on UNINOVA's direct involvement with in NOVA4TECH hub and other hubs, and also their strong connection with the Madan Parque incubator, this task formed a solid basis for the SENTINEL ecosystem in two directions: First, by engaging with potential end users of the SENTINEL platform (that is, SMEs/MEs processing sensitive data or dealing with cybersecurity aspects); Second, by identifying potential technology providers to further and continuously enhance the SENTINEL offerings. This also includes networking with relevant associations, liaising with standardisation bodies, organizing stakeholders' workshops, linking with other H2020 projects, and participating in conferences, fairs and exhibitions.

2.2 Ecosystem building phases

The SENTINEL ecosystem building process is divided into 3 main phases: (i) Networking and Liaison; (ii) Sustainability building; and (iii) Market outreach.

The first phase “Networking and Liaison” started in M1 and finished in M12. This phase was related to the organization of workshops for engaging stakeholders, starting to liaise with other H2020 projects, defining what are the project's main offerings and also the production of stakeholder questionnaires.

The second phase “Sustainability building”, started in M13 and finished in M24. The main objectives were to analyse the results from the previous phase, to set a clear definition of the SENTINEL offerings and value proposition, and to boost engagement with key stakeholders through workshops and questionnaires.

The third and last phase “Market outreach”, started in M25 and finished in M36. The main objectives here were to study the early adopters per use case and organize early-adopters targeted events.

2.3 SMEs analysis and mapping

In order to continue the stakeholder engagement activities, the SENTINEL consortium has organised two additional SME-centric workshops within M19-M36 period. The main objective was to continuously raise awareness of SENTINEL offerings and engage SMEs as future end users of the SENTINEL services. Both workshops focused on testing and validating the platform in different SME contexts. The events were accompanied by a questionnaire that helped the consortium better understand the SMEs' needs, challenges, current OTMs, infrastructure and awareness of GDPR compliance obligations [1].

SENTINEL has also engaged different DIHs, at the national and EU level. The aim was to compile the analysis and technical results to address a much wider perspective and information for the Exploitation phase.

Besides the EDIHs engaged in the first period (INNOVA4TECH, Digital Manufacturing Innovation of Wales, INNOV TOURISM DIH, idD Portugal Defense, CONNECT5 and Madeira Digital Innovation Hub, Produtech, DIH4CPS, DIHWorld, DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH), SENTINEL was able to engage with ATTRACT EDIH, Südwestfalen EDIH and AIP (Associação Industrial Portuguesa), although the last one is not an EDIH, we consider relevant to engage with AIP mainly because it represents the Portuguese SME ecosystem, with more than 6.000 associates. Such contacts enabled us to recruit additional SMEs for using and validating the SENTINEL offerings throughout the several SME-centric workshops organized.

2.4 SME engagement methods

For initial SME engagement activities, SENTINEL focused on collecting data to profile the context of SMEs and to understand the gaps related to non-compliance with GDPR and mechanisms for addressing personal data protection. For the 1st and 2nd SME engagement workshops, the questionnaires used to collect data were sent after workshops while for the 3rd workshop, the feedback was collected through a live survey campaign facilitated via a QR code.

In the second phase of workshops, during the 4th and 5th SME-Centric Workshop, SENTINEL aimed to enhance awareness among participants and evaluate their engagement with the platform’s offerings. These workshops were crucial for understanding the participants' perceptions of the SENTINEL offerings and evaluating their willingness to invest in the platform. Through targeted discussions and feedback sessions, we collected valuable insights on the engagement of SMEs, participants’ familiarity with GDPR and personal data management procedures and how do they feel that SENTINEL offering can bring value added to their business.

The main objective of organizing such workshops was to gain perspective directly from the SMEs, continuing the discussions around cybersecurity, data protection and bringing the real experience with GDPR compliance obligations. To fulfill such objectives and have a substantial impact on SMEs, SENTINEL has also produced more content, such as the podcasts and the platform demo videos[1].

2.5 Stakeholder engagement time plan

The SENTINEL stakeholder engagement time plan methodology consists of four phases (shown in Figure 1) which are aligned with the SENTINEL overall methodology and time-plan.

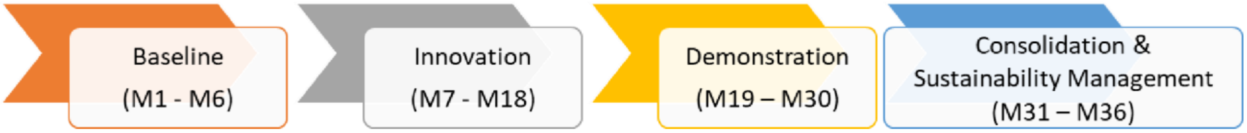

Figure 1. Stakeholder Engagement Time Plan

[1] https://www.youtube.com/@SentinelH

The Baseline Phase (M1-M6) is where SENTINEL triggered awareness within SMEs about SENTINEL's motivations, objectives and offerings. The 1st SME-centric workshop was held in M4, where SENTINEL was presented to a manufacturing ecosystem of SMEs. In this workshop a consultation to the SMEs present at the workshop was held through questionnaires, with the objective of understating the level of maturity of SMEs with regards to PDP and GDPR compliance and also, the usage of cybersecurity tools.

The Innovation Phase (M7-M18) comprehends the period related with the technical development of the SENTINEL's MVP and FFV. In this phase, two (2) more SME-centric workshops were organized, one in M12 and another one in M17, in this last one, a preview of SENTINEL's MVP hands-on was presented. During the workshop, a questionnaire was addressed to all attendees, aiming to consolidate reviews about the first impression of SENTINEL's MVP. Besides these two (2) SME-centric workshops organized, webinars and attendance at recognized events (IoT week, FIC Forum) had also taken place. Such dissemination events, where also good opportunities to engage different SMEs to SENTINEL's offerings.

The Demonstration Phase (M19-M30) had a strong focus on dissemination and communication activities, aiming to enlarge the number of SMEs engaged with SENTINEL's offering. These activities also addressed different DIHs and incubators, that facilitated raising awareness among SMEs, for example the 4th SME-centric workshop already mentioned in this deliverable. Such activities (e.g., workshops, open demonstrations, webinars and seminars) have been used to promote the SENTINEL platform and its offerings to all stakeholders, focusing mainly on SMEs/MEs operating on any field related with needs on data privacy and compliance, technology providers, and policy makers. All members of the consortium have been engaged in promoting such events in industrial and scientific communities (via their web-based dissemination channels) and inviting participants. In addition, the Demonstration Phase aimed at demonstrating the SENTINEL Full-Featured Version (FFV) to SMEs/MEs enabling the testing and validation of the platform under real-life conditions in the context of the SENTINEL Pilots (cf. D6.2 [2]).

The Consolidation & Sustainability Management Phase (M31-M36) focused on design and describing the best practices for maintaining and operating the system in the long-term. This included, collecting feedback from SMEs regarding the final SENTINEL platform, an example of this feedback, were the activities conducted under the 5th SME-centric workshop, but also creating adequate support channels to SMEs that are interested in adopting the SENTINEL platform in a long-term, this included, the production of a well-documented end-user guide for installing, deploying and using the SENTINEL and its components. This phase validated the utility of the proposed solution on a larger scale, within the wider European business community.

3. SENTINEL's SMEs Engagement Activities M19-M36

3.1 4th SME-centric Workshop

The 4th SME-centric workshop occurred in conjunction with the third pilot demonstration event on September 25th, 2023. The SENTINEL partners organized the SME-centric workshop, with the main scope of demonstrating the SENTINEL platform within the third pilot of the project. The SMEs which attended the workshop, have been engaged through the EDIHs (European Digital Innovation Hubs) as part of Task 7.4 activities.

The workshop took place virtually via Microsoft Teams, with the participation of 24 diverse SMEs. A full guide of instructions has been shared to the participants to proceed correctly with the evaluation and trial of the platform.

The external SMEs have been kindly invited to validate the Full Featured Version (FFV) of the SENTINEL platform from a twofold perspective. Firstly, to test the available functionalities of SENTINEL FFV under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trial along with other validation criteria, such as usability, performance, user satisfaction, user interface (UI), etc. In this regard, the participants of each SME were kindly requested to create their organisation profiles and follow all the instructions in order to validate all the features of the SENTINEL platform. And secondly, to assess the way that SENTINEL FFV addresses privacy, personal data protection, and cybersecurity requirements of different processing activities utilised by SMEs in their daily business.

During the event, the SMEs were invited to leave feedback through an interactive questionnaire (see Appendix-I: SENTINEL Interactive Questionnaire Part I: Participants Introduction) to collect data about the user level of awareness with regards to GDPR and PDP, for understanding the participants' perceptions of the SENTINEL offerings and evaluating their willingness to invest in the platform.

The results of the questionnaire can be found in Section 4.1. The Platform Demonstration video recorded during the event is available on SENTINEL's YouTube Channel[2].

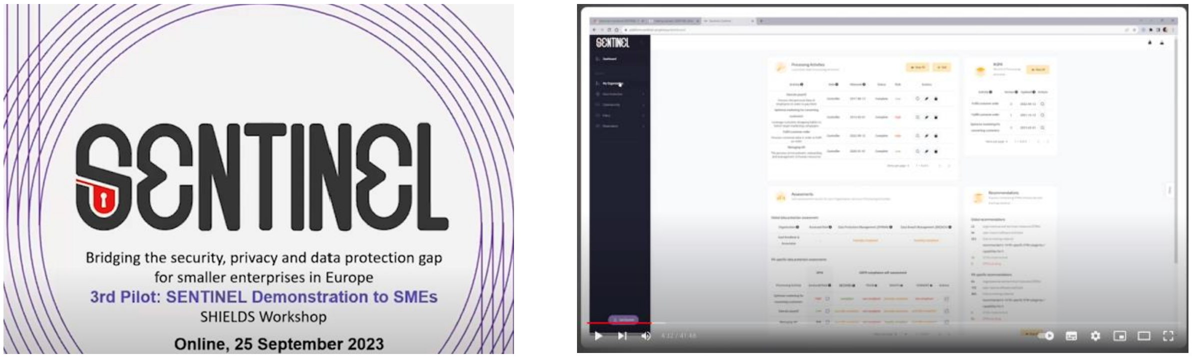
SENTINEL
Bridging the security, privacy and data protection gap
for smaller enterprises in Europe
3rd Pilot: SENTINEL Demonstration to SMEs
SHIELDS Workshop
Online, 25 September 2023

Figure 2. 4th SME-Centric Workshop

[2] https://www.youtube.com/watch?v=E9K67qc9Gx4&t=28s

3.2 5th SME-centric Workshop

The final SME-centric workshop was held in Athens, Greece, on the 27th of February during the 2nd day of the 7th SENTINEL plenary meeting. The event aimed: i) to present the main achievements reached within the scope of the project, demonstrate the SENTINEL platform and elaborate on the innovation capacities of the project (Task 7.4 objective, addressed in this report), ii) to allow different types of SMEs to test and validate the SENTINEL platform (Task 6.4 objective, cf. D6.3). It covered topics related to GDPR, personal data protection and cyber security and how these aspects can affect the SMEs' core business activities.

The Final SENTINEL platform was presented to the audience highlighting its innovation capacities, and how an SME can utilize them to leverage its privacy and cybersecurity. The workshop welcomed 11 companies from the private sector, small and medium-sized enterprises (SMEs), startups, and Small Business Entities, without any sector restrictions. Moreover, it was dedicated to business owners, company CEOs, decision-makers and managers, data, privacy, and cybersecurity experts.

Likewise, the 4th SME-centric workshop, during the event, the SMEs were invited to contribute and answer an interactive questionnaire (see Appendix-I: SENTINEL Interactive Questionnaire Part I: Participants Introduction) to collect data on their awareness of GDPR and Personal Data Protection (PDP), their perceptions of the SENTINEL offerings, and their willingness to invest in the platform. The SENTINEL External Advisory Board members also had the possibility to test and validate the platform during the workshop. The results of the questionnaire can be found in Section 4.2.

SENTINEL
SENTINEL FINAL SME-CENTRIC
WORKSHOP
Bridging the gap in personal data protection and cybersecurity for SMEs

Figure 3. 5th SME-centric Workshop

4. Insights from the SENTINEL's 4th and 5th SME-centric workshops

4.1 Analysis of the 4th SME-centric questionnaire

Before analysing the results of the 4th and 5th SME engagement questionnaires, it is worth to mention that questions were aiming to:

- First, to understand who our participants are and conduct a profiling of the SMEs being represented in the workshop.
- Secondly, to understand their existing resources, whether they use any GDPR related solutions and understand the level of maturity with regards to the adoption and investment in PDP and GDPR compliance assessment tools.
- Thirdly, understand SMEs needs/expectation and collect feedback about SENTINEL offerings.

As previously mentioned in the 3.1 section, the 4th SME engagement workshop was held online on the 25th of September 2023. Organized by UNINOVA, this workshop gathers 24 external SMEs. For more information about the organization process of this workshop, please refer to D6.2 "SENTINEL Demonstration - final execution".

During the event, the SMEs were invited to contribute and answer the interactive questionnaire, prepared as part of T7.4 "SENTINEL ecosystem building: Continuous engagement of technology providers, SMEs/MEs" to collect data about users profiling, their level of knowledge and relevance of GDPR related tools/services as well as their perception on the SENTINEL platform and willingness to invest in solutions similar to SENTINEL.

The questionnaire was aimed at profiling end-users and identifying further personas to build a community ecosystem around the project's results. It aimed at understanding the level of maturity with regards to the adoption and investment in PDP and GDPR compliance assessment tools. As well as evaluating the attendee's experience with the SENTINEL Platform.

The following subsections provide an in-depth analysis of the results of the questionaries addressed within SME-centric workshops 4th and 5th. The analysis is made according to the different questions categories mentioned previously: (i) Profiling; (ii) Existing Solutions and resources; and (iii) Needs and expectation.

4.1.1 Profiling

According to the responses depicted in Figure 4, it's evident that the majority, accounting for 61% of the workshop attendees, hailed from the IT/Technology, and Engineering sectors.

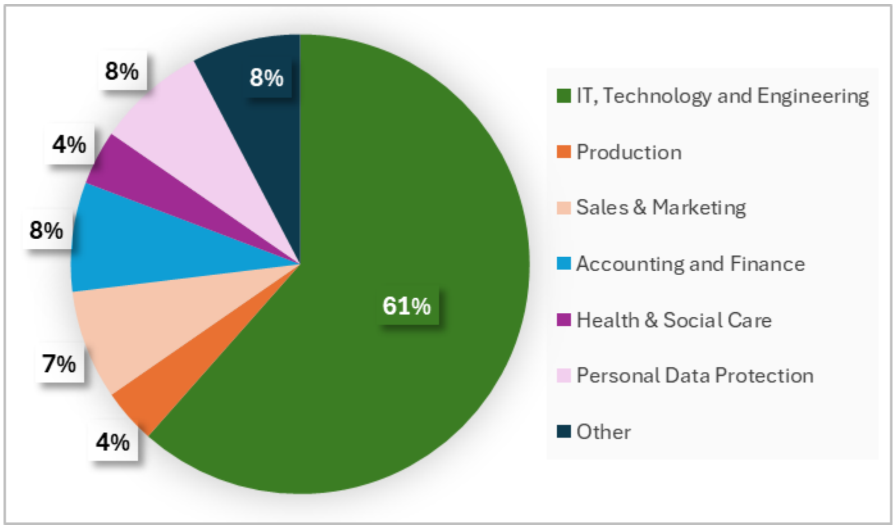

Figure 4. 4th questionnaire: What is your area of expertise?

This demographic insight is invaluable for tailoring the workshop discourse, enabling the speaker to enhance the user experience during their initial interaction with the platform.

In addition, as shown in Figure 5, it was revealed that the majority of the SMEs are processing customer related data (44%), followed by employee and industrial related data (36% and 16% respectively).

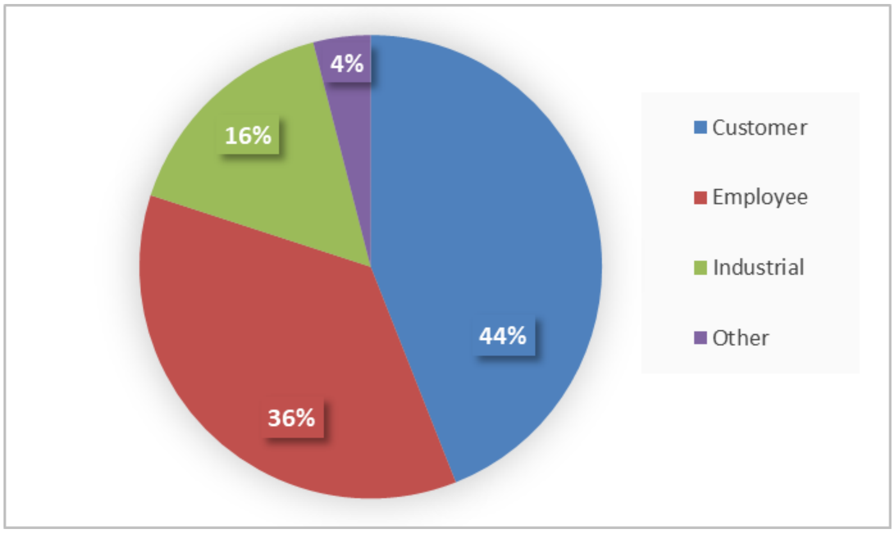

Figure 5. 4th questionnaire: What type of data does your organization process?

Analysing the GDPR knowledge level (Figure 6), we revealed that regardless the technological background of the respondents, most participants indicated possessing either basic or intermediate knowledge of Data Protection and GDPR. Also to highlight almost half of the SMEs representatives are considered beginners in terms of knowledge in personal data protection and EU GDPR. By cross-referencing the two previously collected pieces of information, we can consider that the topic of data protection and GDPR still needs to be disseminated among technology professionals and that awareness levels can be increased with relevant information tailored to this type of professional.

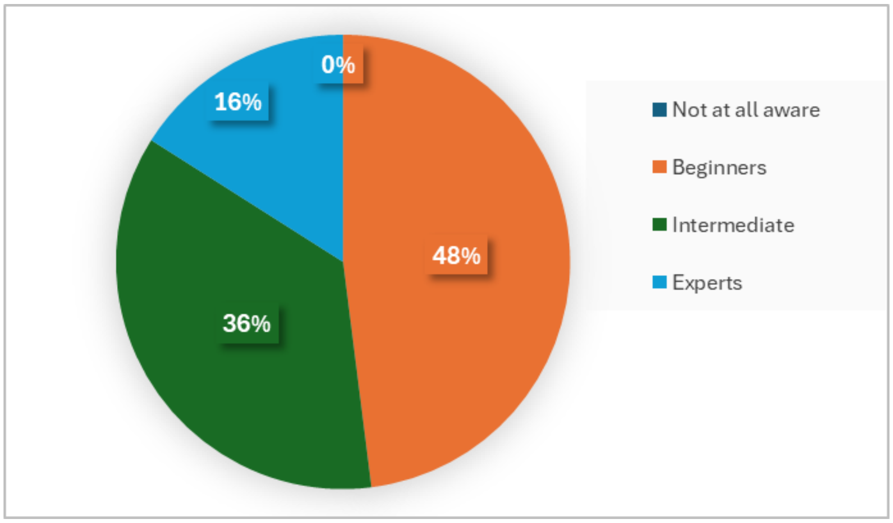

Figure 6. 4th questionnaire: Please identify your level of knowledge regarding personal data protection and EU GDPR

Subsequently, inquiries extended to gauging interest in receiving assistance for GDPR compliance. A noteworthy 59% expressed uncertainty, underscoring the need for further information, while 25% expressed a keen interest in attaining support to achieve GDPR compliance and fortify their data protection measures.

4.1.2 Existing solutions and resources

Exploring further, inquiries delved into investment patterns regarding GDPR compliance and data protection solutions. Strikingly, around 50% of participants disclosed the absence of any dedicated software or external services within their companies while the other half declared leveraging either software services or external consulting services (Figure 7).

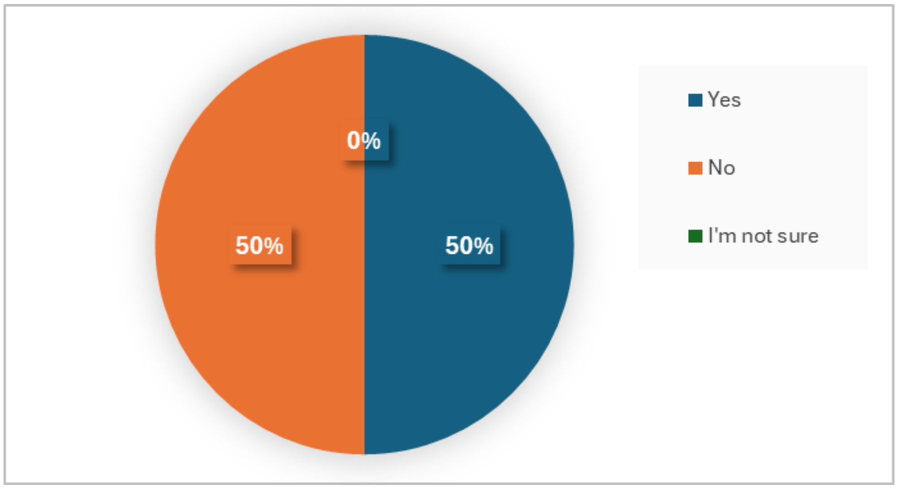

Figure 7. 4th questionnaire: Does your organisation employ any tools or services for privacy assessment to estimate and/or support its GDPR compliance?

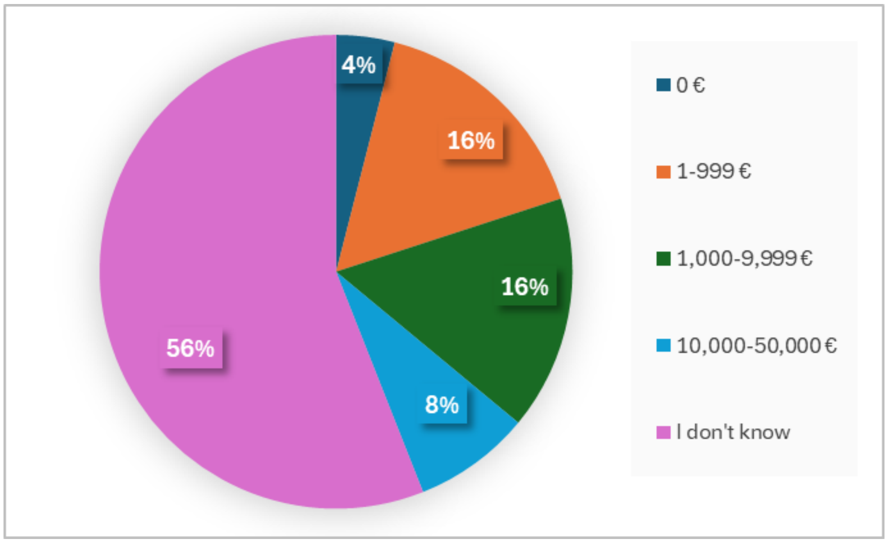

Figure 8. 4th questionnaire: If you employ services for privacy assessment, what are your annual expenses, approximately?

Furthermore, insights into annual investment allocations unveiled a spectrum, with 56% unable to specify, 8% investing €10,000 to €50,000, 16% allocating €1,000 to €9,999, and another 16% spending up to €999 annually. These revelations serve as valuable market research, informing pricing strategies for the service and platform development (Figure 8).

4.1.3 Needs and expectation

In the concluding segment, respondents' feedback regarding the potential adoption and investment in the SENTINEL platform was examined. Notably, 60% regarded it as a potential solution, with 20% expressing affirmative intent and the remaining 20% showing reluctance.

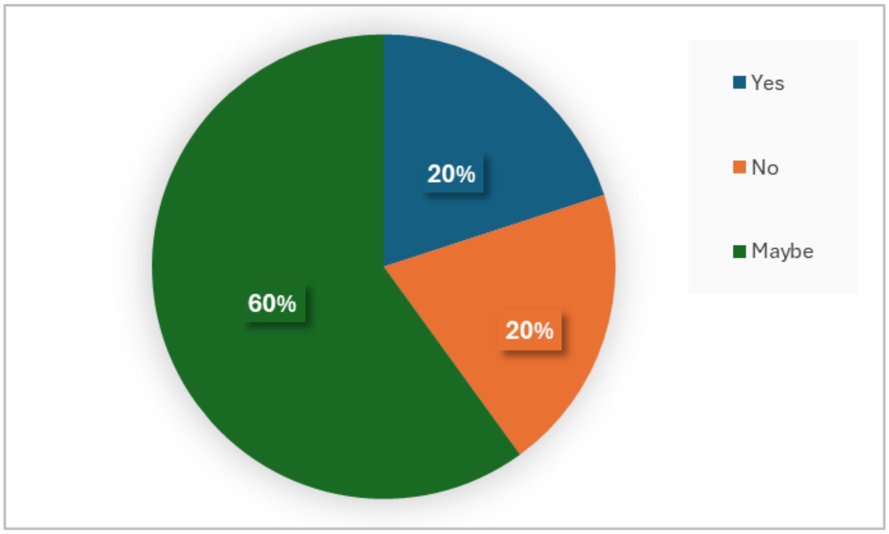

Figure 9. 4th questionnaire: Did you find SENTINEL a potential solution to be implemented within your company?

Looking ahead, 29% indicated plans to invest in similar platforms within 2 years, with another 14% eyeing a longer timeframe. Only, 19% answered negatively to this question, while 38% remained neutral.

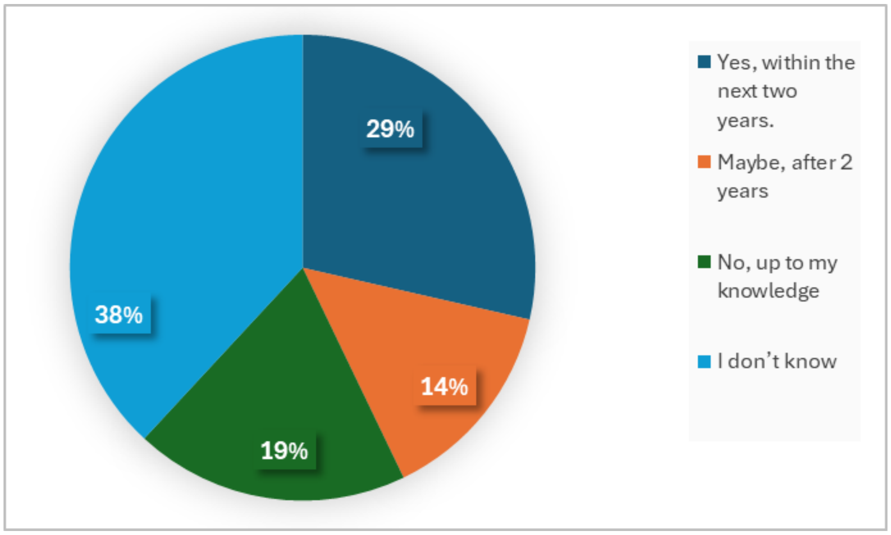

Figure 10. 4th questionnaire: Does your company plan to invest in tools/services like SENTINEL in the future?

The final question (Figure 11) had the objective of getting feedback about what is considered the most useful SENTINEL offering for their business. The "A toolkit for evidence-based GDPR compliance" offering was found to be the most valuable toolkit for our respondents (55%), while the "SME Training and Education", "Automated policy recommendation and real time monitoring" as well as "Cybersecurity awareness and CyberRange training" got almost equal interest from the participants.

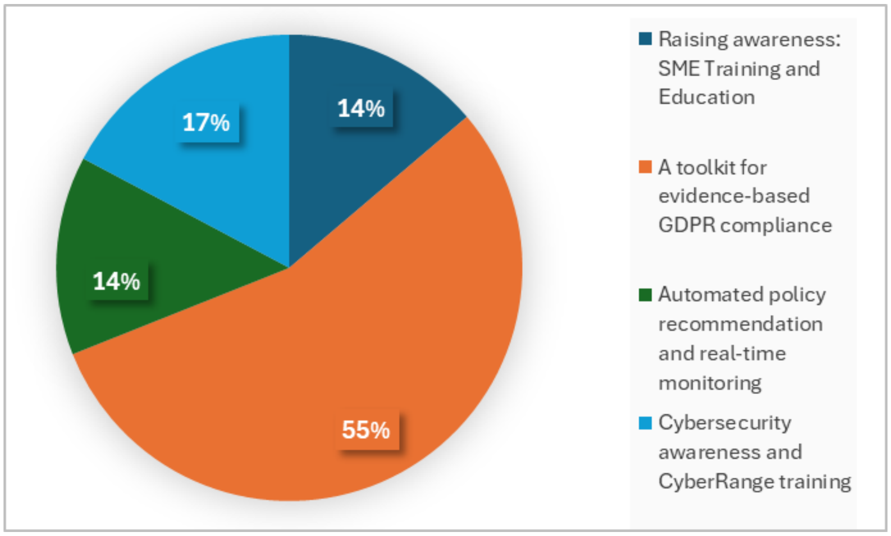

Figure 11. 4th questionnaire: Which of the following SENTINEL offerings would be more useful for your business needs?

In summary, the insights gathered from the workshop survey provide a clear roadmap for enhancing the SENTINEL platform's efficacy in addressing the pressing challenges of data protection and GDPR compliance. By leveraging the identified areas for improvement, such as targeted awareness campaigns, streamlined user experiences, and tailored support services, Sentinel can support companies to achieve GDPR compliance and improve their data protection.

4.2 Analysis of the 5th SMEs Engagement Questionnaire

As described in Section 3.2, the final SME-centric workshop was organized by ITML, supported by the consortium and occurred during the 2nd day of the 7th SENTINEL plenary meeting. This workshop covered both evaluation aspects of Task 6.4 “Evaluation and impact analysis” and the stakeholder engagement activities of Task 7.4 “SENTINEL ecosystem building: Continuous engagement of technology providers, SMEs/MEs”.

The event was moderated by ITML, and the questionnaire sections were moderated by UNINOVA which conducted the participants to all questions promoting interaction and collecting data. As described in, Section 3.2, the SME-centric workshop had a twofold perspective: i) to engage more SMEs to communicate the project’s findings and enhance the SENTINEL ecosystem (Task 7.4) and ii) to allow additional SMEs to test and validate the SENTINEL solution (Task 6.4). Thus, the interactive questionnaire was divided into two main parts to address these objectives. The 1st part refers to profiling end-users and identifying further personas to build a community ecosystem around the project’s results, analysed in the current deliverable. The 2nd part reflects questions concerning the testing and validation of the SENTINEL solution, presented and analysed in D6.3 “Assessment report and impact analysis”.

The workshop gathered 11 new SME representatives in addition to SENTINEL internal end users coming from CG and TIG companies (including Sportif, Dimension Care), EAB members and the SENTINEL project partners. For more information about the organisation process of the 5th SME-centric workshop, list of the participant companies and evaluation results please refer to D6.3 “Assessment report and impact analysis”.

A detailed overview of the SME’s answers on the 1st part of the questionnaire can be found in the next sub-sections.

4.2.1 Profiling

In the first round of questions, the objective was to profile the audience present at the event. This information is of paramount importance for tailoring the technical vocabulary and enhancing the user experience during the presentation. As shown in Figure 12, 78% of the audience present specializes in Technology, Information Security, Data Protection, and Engineering. The reflection of this sample enables a more technical assessment of the SENTINEL platform's features. An audience with more technical knowledge can more easily grasp concepts present in the tool and thus provide feedback based on technical grounds.

In the sample of this survey, it was also identified that the majority had intermediate to advanced knowledge of the General Data Protection Regulation (GDPR) (Figure 13). Once again, this means that participant feedback may contain an evaluation regarding the topic with a more technical approach.

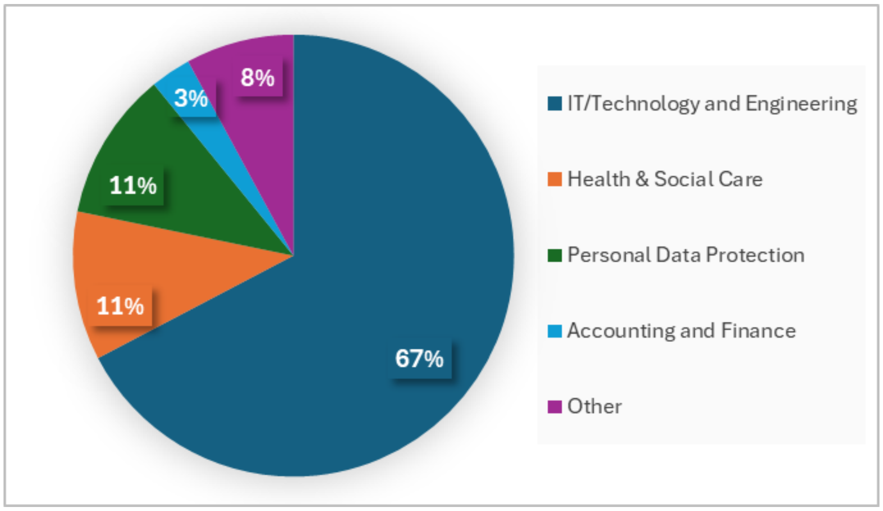

Figure 12. 5th questionnaire: What is your area of expertise?

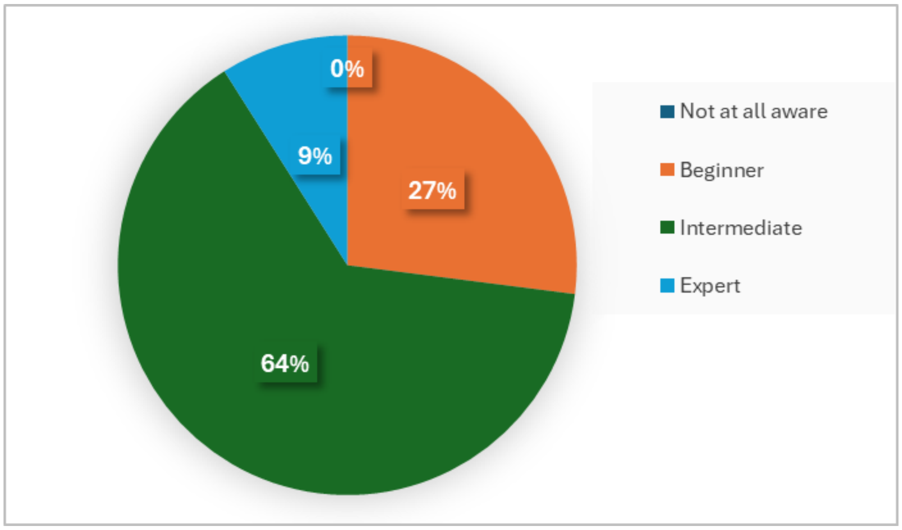

Figure 13. 5th questionnaire: Please identify your level of knowledge regarding personal data protection and EU GDPR

4.2.2 Existing solutions and resources

During the second phase of the questionnaire, topics were highlighted to demonstrate market characteristics and levels of investment in tools of this nature. This analysis is very relevant for the Exploitation phase, as it addresses indicators of investment in personal data protection platforms. In the first question, we observed that 75% of the participants indicate that their organisation does not use software for data protection compliance (Figure 14).

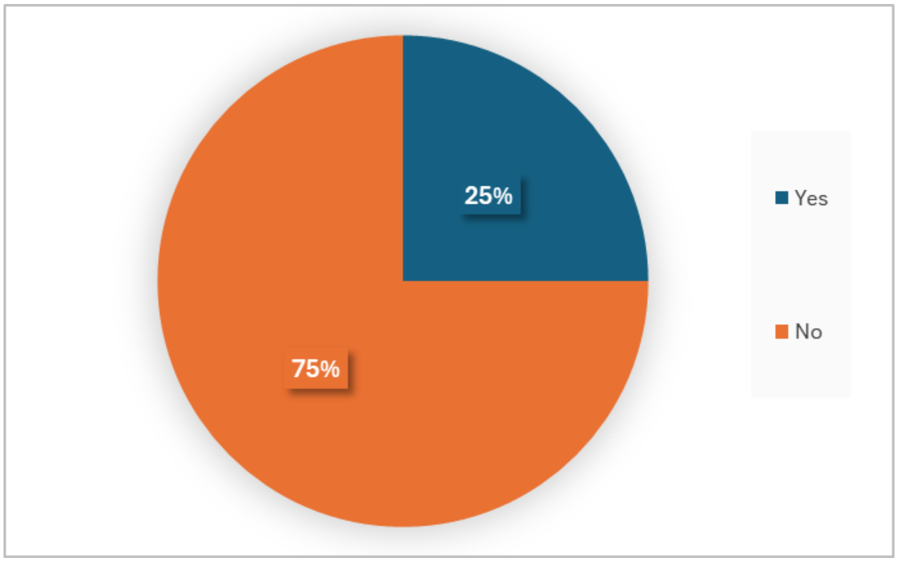

Figure 14. 5th questionnaire: Does your organisation employ any tools or services for privacy assessment to estimate and/or support its GDPR compliance?

More than 50% of organisations that use software/external services for data protection, that costs from €1,000 and €9,999 annually, while 21% of companies use tools/services that cost up to € 1,000. With these results, we can measure and project the market value that the SENTINEL platform can achieve. Additionally, the numbers indicate a large market that is still relatively unexplored.

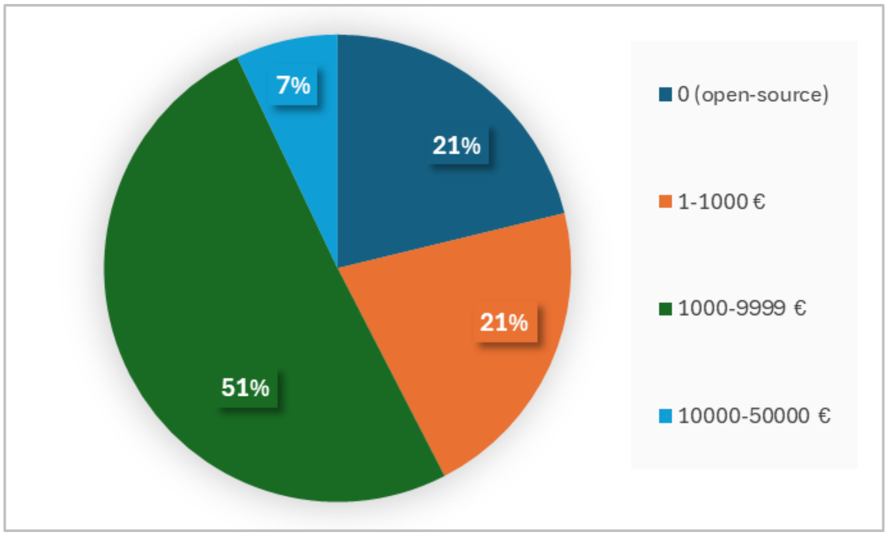

Figure 15. 5th questionnaire: If you employ services for privacy assessment, what are your annual expenses, approximately?

4.2.3 Needs and expectation

In Part 3, questions were posed regarding some of our indicators, reflecting the level of satisfaction of the sample after the SENTINEL platform presentation. From these inquiries, it was evident that there was no outright rejection of the technology presented. As shown in Figure 16

67% of the participants defined the platform as "useful for their company," while the remaining 33% indicated "maybe," showing uncertainty. This segment of uncertainty may be related to the sample's profile, which still lacks high levels of awareness regarding data protection, or to the variety of company profiles present, some of which may not have seen a practical application for their organization during the presentation.

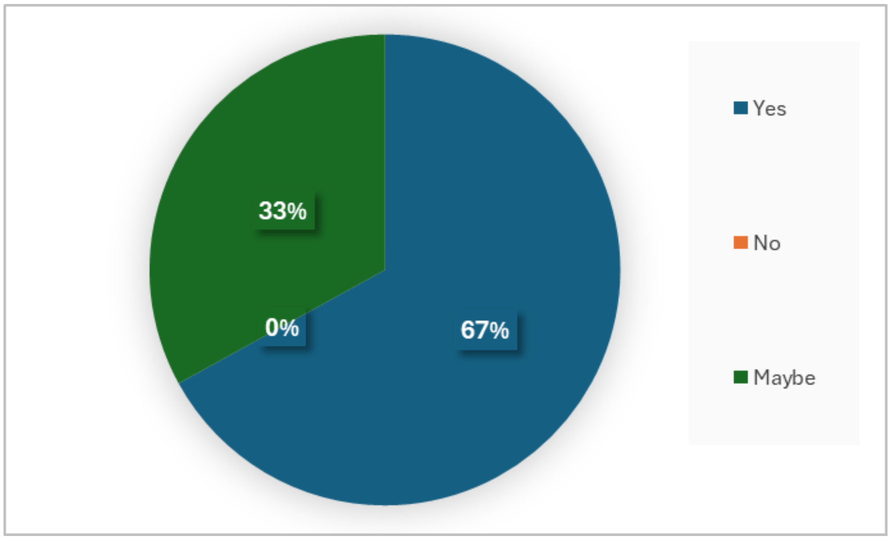

Figure 16. 5th questionnaire: Did you find SENTINEL a potential solution to be implemented within your company?

In the subsequent question, respondents were asked about their investment plans in tools similar to SENTINEL. This inquiry aimed to assess organizations' intentions regarding services and tools available in the market. Half of the companies in the sample indicated their intention to invest in data protection tools over the next two years. Meanwhile, 37% of companies opted for a "maybe" regarding investment after two years (Figure 17). This indicates the level of awareness among companies regarding GDPR and that they are already incorporating investment in tools and solutions to ensure the protection of personal data into their plans.

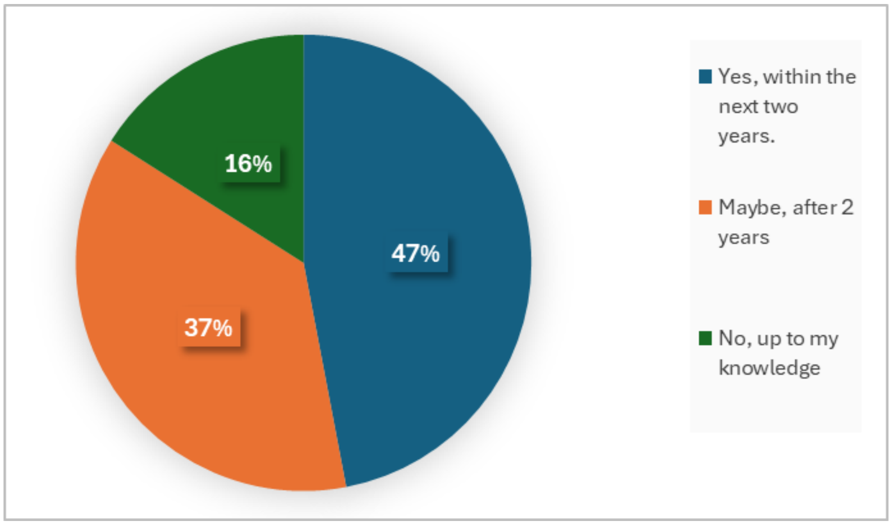

Figure 17. 5th questionnaire: Does your company plan to invest in tools/services like SENTINEL in the future?

Finally, the respondents where equality selected the “A toolkit for evidence-based GDPR compliance” and “SME training and Education” offerings to be the most useful solutions to cover their current business needs. “Automated policy recommendation and real time monitoring” as well as “Cybersecurity awareness and CyberRange training” got almost equal interest from the participants.

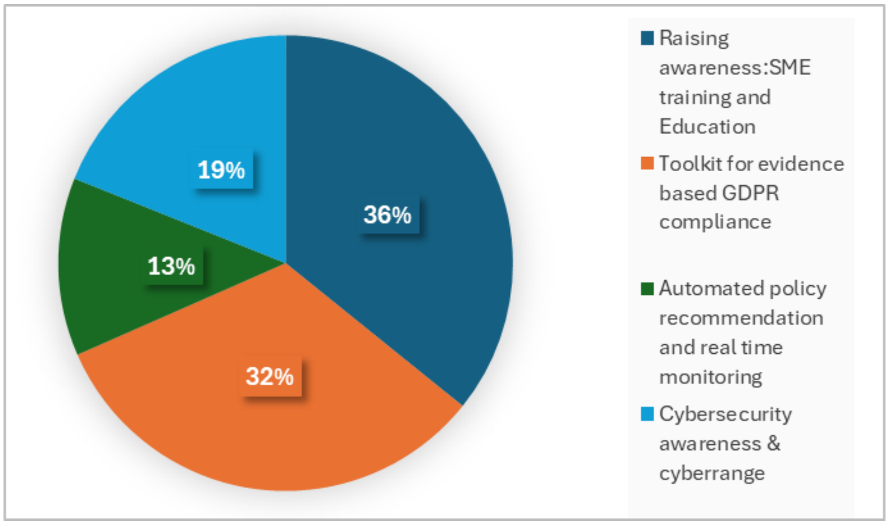

Figure 18. 5th questionnaire: Which of the following SENTINEL offerings would be more useful for your business needs?

Overall, in this latest survey, we've noticed that organizations are starting to pay more attention to the subject. The efforts invested in raising awareness are beginning to yield their first results, which, combined with the developed platform, have great potential for adoption by organizations.

The SENTINEL platform is generally perceived positively by the end users and the benefit of the solution is more evident when hands-on demonstrations are provided during the SENTINEL testing phase. End users also indicate that the solution provides more control over their business operation and increases the level of GDPR knowledge and experience.

5. Insights from the SENTINEL's SME Engagement Activities

5.1 Overall Analysis of SMEs engagement questionnaires

This section conducts a comprehensive analysis of all our end-user engagement activities. In this respect, it includes supplementary information based on the analyses from the 1st, 2nd, and 3rd workshops, previously reported in the earlier version of this report (D7.5), in addition to the 4th and 5th workshop results. The scope is to take into account the recommendation received during our last review meeting, by consolidating and encapsulating the end-users' feedback received from all five workshops.

The five SME-centric workshops conducted during the SENTINEL project offered comprehensive insights into the attitudes and practices of SMEs concerning GDPR compliance, cybersecurity, and data protection. In this respect, the 1st workshop was held in **M4** in person and gathered 12 companies discussing GDPR-related issues. The 2nd workshop was conducted in **M12** in virtual mode gathering 25 companies mainly from the IT and technology area. The 3rd workshop was held in person in **M17** attracting more than 70 participants' attention. This workshop also served as a stage where the MVP of the SENTINEL platform was demonstrated among external stakeholders. Starting from this event, we began to focus specifically on profiling SMEs, understanding their level of knowledge in data protection, and gathering feedback on SENTINEL offerings. In **M28**, the 4th workshop took place as part of the SENTINEL pilot 3 activities gathering 48 additional SME representatives that were invited not only to participate in the workshop but also test and validate the entire platform. Finally, the 5th workshop took place in **M33** in person gathering more than 40 people and inviting the workshop participants to test, validate and provide feedback about the final version of the SENTINEL platform. It should be mentioned that the organisation of these five (5) workshops evolved in parallel to SENTINEL technical developments. At the early project stage (**M1-M12**), where we had only the theoretical concepts of the SENTINEL project, we focused more on investigating the SMEs GDPR awareness and implementation of data protection measures within their organisation and revealing their existing challenges in this respect. During these initial workshops, we aimed to raise awareness among SMEs rather than gather concrete feedback about the SENTINEL offerings. Our focus was on understanding whether SMEs were aware of intelligent one-stop-shop solutions for compliance services and if they were willing to invest in such tools. It was only during the 3rd workshop and onwards that we were able to obtain specific reactions to the SENTINEL offerings. This shift occurred because participants could see live demonstrations of the platform, even though it was still an MVP. These live demonstrations created a significant impact, allowing SMEs to better understand the practical applications and benefits of the SENTINEL platform. This demanded altering the workshop organisation tactic as well as modifying the questionnaire by trying to create our SMEs' profiles, their data processing activities and whether they use tools like SENTINEL. As a result, the workshops became interactive, and the survey questions accompanied by stepwise demonstration of the SENTINEL platform so the user can be able to easily and intuitively understand what SENTINEL does. This approach helped not only evaluate/test the SENTINEL platform but also obtain useful information about the attendees' interest/acceptance on the SENTINEL offerings during the workshops.

A brief information about the workshops' occurrence date, type, number of attendees as well as the number of questionnaire respondents are presented in the table below while key insights achieved from all 5 workshops classified under "**Profiling", "Existing solutions and resources" and "Needs and expectation" categories** are illustrated in the next sub-sections.

Table 1. SENTINEL SME-centric workshops

	Date	Workshop nature	Number of workshop attendees	Number of questionnaire respondents
1st workshop	**M4**	**Hybrid**	**12**	**12**
2nd workshop	**M12**	**Online**	**25**	**4**
3rd workshop	**M17**	**Physical**	**70**	**50**
4th workshop	**M28**	**Online**	**48**	**26**
5th workshop	**M33**	**Physical**	**40**	**20**

5.1.1 Profiling

Figure 19 highlights the areas of expertise of respondents from the SME-centric workshops. The distribution shows that 64% of respondents are primarily involved in IT, Technology, and Engineering. This high percentage indicates a strong technical background among the participants, which can be beneficial for understanding and implementing advanced data protection and cybersecurity measures. Only 4% of respondents belong to the production sector, suggesting that data protection and cybersecurity might not be the primary focus for these participants, potentially requiring more targeted awareness and training initiatives. 3% of respondents are from sales and marketing, a sector that often handles significant amounts of personal data, indicating a need for improved data protection practices and GDPR compliance. 4% of respondents work in accounting and finance, and given the sensitivity of financial data, this sector's involvement underscores the importance of robust data protection measures. 5% of respondents come from health and social care, a sector with stringent data protection requirements due to the handling of sensitive health data. Additionally, 5% of respondents specialize in personal data protection, indicating a dedicated focus on data privacy and compliance within some of the participating SMEs. The analysis of Figure 19 suggests that while there is a strong technical presence among the respondents, there are also significant contributions from sectors that handle sensitive data. This diverse expertise highlights the importance of tailoring data protection and GDPR compliance strategies to meet the specific needs of various industries. Enhancing awareness and providing specialized training can help bridge the knowledge gap, particularly for sectors like production and sales and marketing, which may not traditionally prioritize data protection.

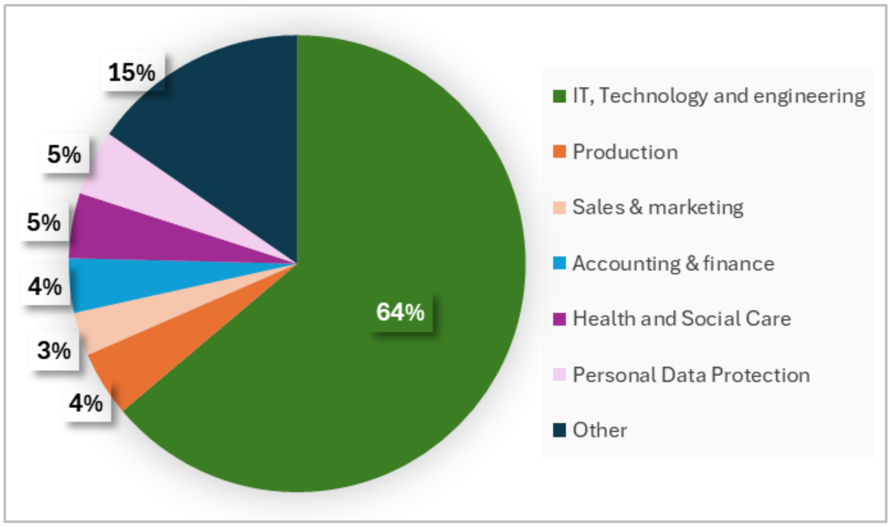

Figure 19. What is your area of expertise?

Figure 20 focuses on the types of data processing activities conducted by the respondents' organizations. The data reveals that a significant portion of SMEs process customer-related data, accounting for 34% of the responses. This highlights the importance of customer data protection as a critical aspect for many SMEs, given the potential risks and regulatory requirements associated with handling personal data. Employee-related data processing is the next most common activity, reported by 30% of respondents. This suggests that many SMEs also focus on internal data protection measures to safeguard employee information, which is essential for compliance with data protection regulations and maintaining employee trust. Industrial data processing activities were noted by 22% of respondents, indicating that a smaller but notable segment of SMEs handles data related to industrial processes. This type of data processing often involves operational information, which, while not personal data, still requires robust protection measures to prevent industrial espionage and ensure operational integrity. The emphasis on customer and employee data processing stresses the dual focus on external and internal data protection requirements within SMEs. The relatively lower percentage of industrial data processing suggests that while it is important, it may not be the primary focus for most SMEs in the context of data protection and GDPR compliance.

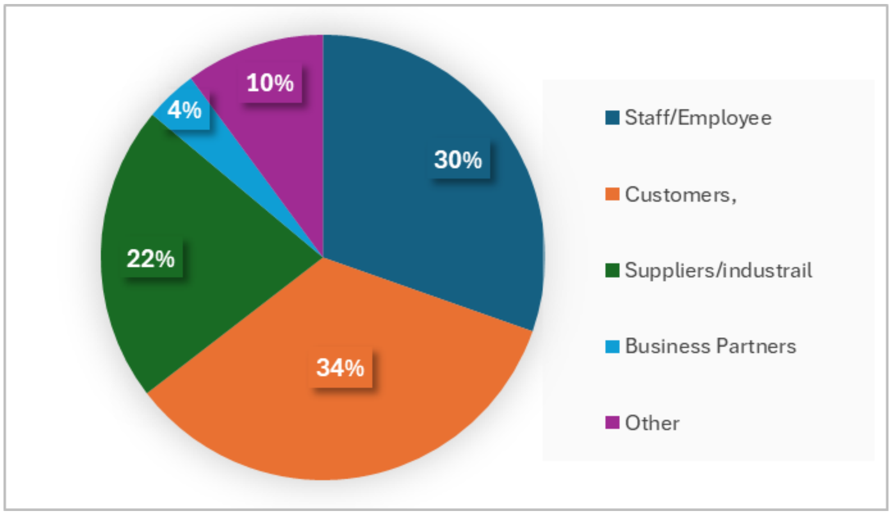

Figure 20. What type of data does your organisation process?

Figure 21 presents the level of GDPR knowledge and awareness among the respondents from the SME-centric workshops. The figure indicates that a majority of participants possess either basic or intermediate knowledge of GDPR and data protection regulations. Despite their technological backgrounds, many respondents are still in the early stages of understanding GDPR requirements. This suggests that while there is some foundational awareness, there is a significant need for further education and training to enhance their comprehension and application of GDPR principles. The data reveals that almost half of the SME representatives are considered beginners in terms of knowledge about personal data protection and EU GDPR. This beginner status highlights a critical gap in understanding that could impact their ability to effectively implement necessary data protection measures and comply with regulatory requirements. The presence of beginners, even among technically proficient professionals, emphasizes the complexity of GDPR and the continuous need for targeted educational initiatives.

Intermediate knowledge levels are also prevalent among the respondents, indicating that while these individuals have a better grasp of GDPR concepts, there is still room for improvement. Intermediate knowledge suggests that these participants are aware of the basic principles and some practical aspects of GDPR but may lack a deeper understanding required for full compliance and advanced data protection strategies.

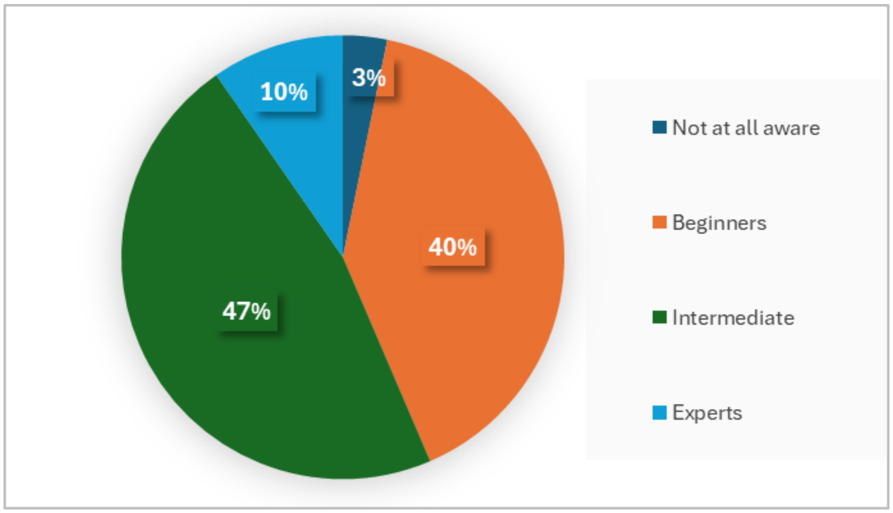

Figure 21. Please identify your level of knowledge regarding personal data protection and EU GDPR

5.1.2 Existing solutions and resources

Figure 22 examines the usage of internal security and privacy policies, as well as tools and services for assessing and supporting GDPR compliance among the respondents' organisations. The data reveals that there is a notable variation in the adoption and implementation of these measures within SMEs.

A significant portion of respondents reported not using any dedicated software or external services for GDPR compliance. On a similar level of magnitude, other respondents reported not being aware of any dedicated software or external services for GDPR compliance. This indicates a substantial gap in the adoption of formal tools and policies that are critical for ensuring data protection and regulatory compliance. The absence of such tools could be attributed to factors such as limited resources, lack of awareness, or the complexity involved in integrating these solutions into their existing workflows. Around 1/3 of the respondents reported using software solutions or services, indicating a more comprehensive approach to GDPR compliance. These organisations are likely investing more significantly in their data protection frameworks, combining the benefits of automated tools with expert guidance to ensure robust compliance measures.

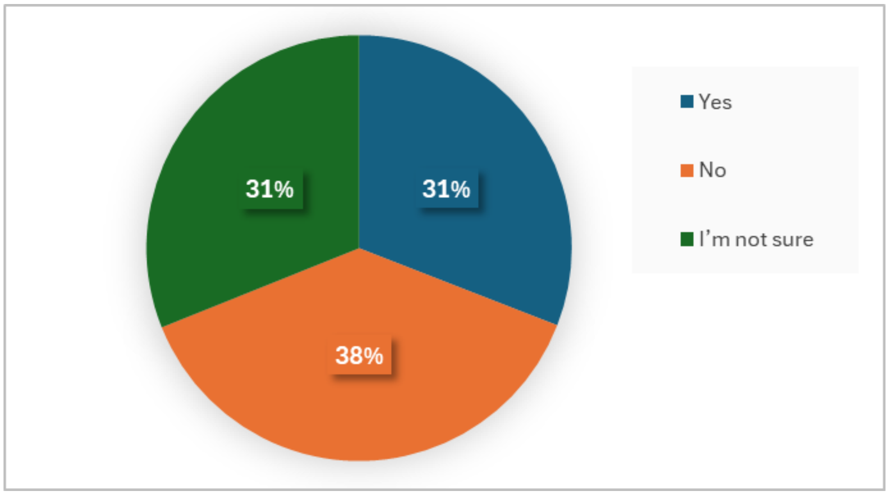

Figure 22. Does your organisation employ any tools or services for privacy assessment to estimate and/or support its GDPR compliance?

Figure 23 provides insights into the approximate annual costs and expenses that SMEs incur on GDPR-related tools, services, and consultations. The analysis reveals significant variability in spending patterns, reflecting the diverse financial capacities and priorities of different SMEs regarding data protection and compliance. A notable 37% of respondents were unable to specify their annual expenditures on GDPR-related tools and services. This high percentage of uncertainty suggests a lack of tracking or awareness of the costs associated with GDPR compliance within many SMEs. This could indicate that for many SMEs, GDPR compliance expenses are not separately accounted for, or that they are integrated into broader IT or operational budgets without distinct categorization.

Among the respondents who did specify their expenditures, 30% reported spending between €1,000 and €9,999 annually. This mid-range expenditure indicates a moderate level of investment in GDPR compliance, reflecting an awareness of the importance of data protection but possibly constrained by budget limitations. These SMEs are likely investing in essential tools and services that provide baseline compliance and protection measures. Another 16% of respondents reported annual expenses up to €999, which represents minimal investment in GDPR compliance. This low expenditure could be due to budgetary constraints, smaller data protection needs, or a lack of perceived risk. SMEs in this spending category may be relying on basic, often manual, compliance measures and free or low-cost tools.

Only 7% of respondents indicated spending between €10,000 and €50,000 annually on GDPR compliance. This higher level of investment likely corresponds to larger organisations or those with more complex data protection needs. These organisations are likely using comprehensive GDPR compliance solutions, including advanced software tools, external consultancy services, and possibly even dedicated compliance teams.

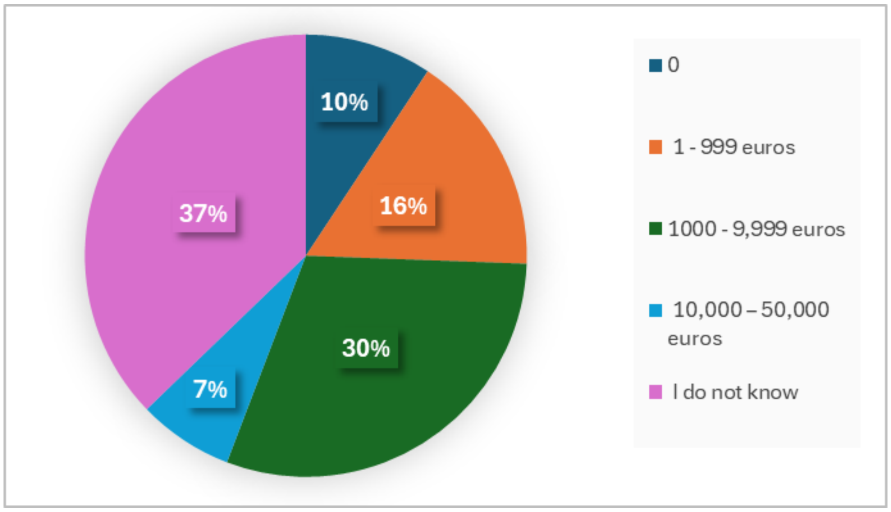

Figure 23. If you employ services for privacy assessment, what are your annual expenses, approximately?

5.1.3 Needs and expectation

Figure 24 examines user acceptance of intelligent one-stop-shop solutions for compliance services among the SMEs participating in the workshops. The analysis of user acceptance is crucial for understanding how willing and ready these SMEs are to adopt new technologies and practices to enhance their data protection and GDPR compliance. To note that, we were able to demonstrate the SENTINEL offerings starting from the 3rd workshop, as previously mentioned.

The data shows that 43% of the participants found the SENTINEL platform to be useful for their companies. This majority indicates a strong positive reception to the platform, suggesting that many SMEs recognize the value and benefits of adopting comprehensive GDPR compliance tools. The perceived usefulness likely stems from the platform's ability to streamline compliance processes, offer real-time monitoring, and provide automated policy recommendations, which can significantly reduce the complexity and burden of GDPR compliance for SMEs. Furthermore, 50% of respondents expressed uncertainty about the platform's usefulness, indicating a segment of users who are either unsure about its applicability to their specific needs or require more information and hands-on experience before making a decision. This uncertainty could be due to several factors, including a lack of familiarity with the platform's features, concerns about integration with existing systems, or skepticism about the return on investment.

The absence of significative rejection of such solutions, suggests that even those who are uncertain are open to exploring its potential benefits further. This openness presents an opportunity for targeted demonstrations, trials, and detailed explanations of the platform's capabilities to address any concerns and showcase its practical applications.

The analysis of user acceptance highlights the importance of continued engagement and education efforts to increase confidence and trust in new GDPR compliance solutions like the SENTINEL platform. Providing additional resources, such as case studies, user testimonials, and hands-on workshops, can help bridge the gap for those who are uncertain and facilitate a smoother adoption process.

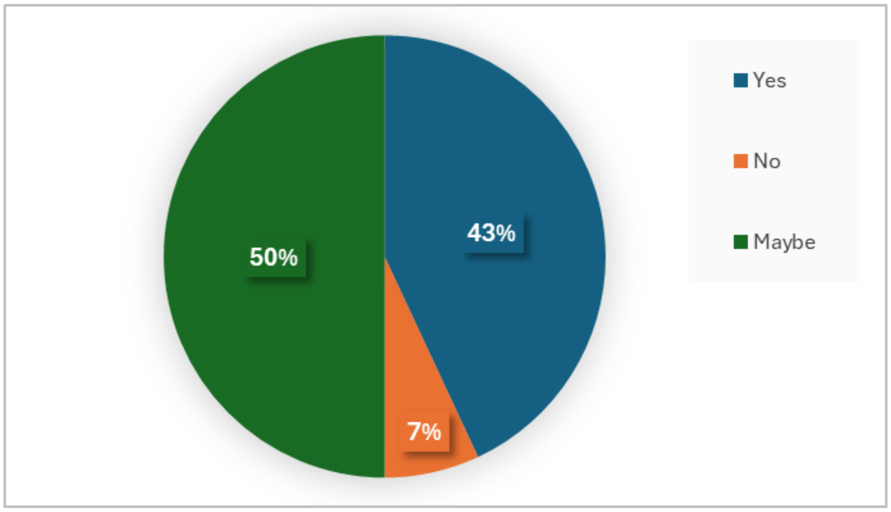

Figure 24. Did you find SENTINEL a potential solution to be implemented within your company?

Figure 25 examines the user investment plans of SMEs concerning GDPR-related tools and services, including the SENTINEL platform. This analysis provides insights into the future intentions of SMEs regarding their spending on data protection and compliance solutions.

The data reveals that 33% of the participants indicated their intention to invest in data protection tools over the next two years. This significant proportion suggests a strong recognition among SMEs of the importance of enhancing their GDPR compliance frameworks. The willingness to invest within this timeframe indicates a proactive approach to data protection, driven by the increasing awareness of regulatory requirements and the potential risks associated with non-compliance.

In the meanwhile, 28% of the respondents opted for a "maybe" regarding their investment plans after two years. This group represents a more cautious segment of SMEs that may be influenced by factors such as budget constraints, ongoing evaluation of current compliance efforts, or awaiting further developments in data protection technologies. Their tentative stance suggests that while they are aware of the need for investment, they may require more convincing evidence of the return on investment or the practical benefits of new tools and services.

Only a smaller portion of respondents, 15%, expressed no immediate plans to invest in GDPR-related tools. This could be due to several reasons, such as existing satisfaction with their current compliance measures, perceived low risk, or financial limitations. For these SMEs, demonstrating the specific advantages and cost-effectiveness of advanced compliance solutions could be crucial in shifting their perspective.

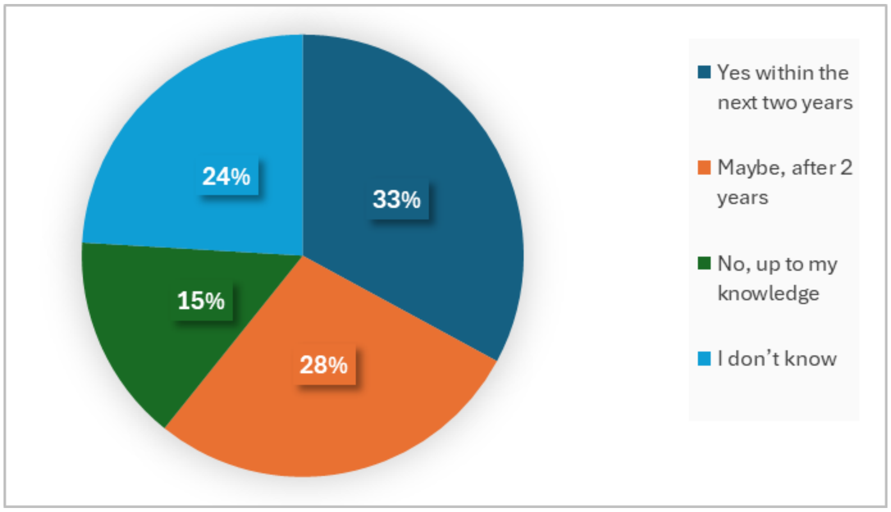

Figure 25. Does your company plan to invest in tools/services like SENTINEL in the future?

Figure 26 provides insights into users’ interest in the various offerings of the SENTINEL platform. This analysis helps to understand which features and services are most valued by SMEs and can guide the development and marketing strategies for the platform.

The data shows that the most valued offering is the "Toolkit for Evidence-Based GDPR Compliance," which garnered interest from 32% of the participants. This high level of interest indicates that SMEs are particularly concerned with achieving and demonstrating compliance with GDPR regulations. The toolkit’s ability to provide clear, actionable steps and documentation to meet compliance requirements is likely a key factor driving this interest. It underscores the need for practical, user-friendly tools that simplify the complexities of GDPR compliance and provide concrete evidence of adherence to regulatory standards.

The "SME Training and Education" offering also received significant interest. SMEs recognize the importance of educating their staff about data protection principles and GDPR compliance. Training and education can enhance overall awareness and ensure that employees at all levels understand their roles and responsibilities in protecting personal data. This offering helps build a culture of compliance within organizations, making it an essential component for many SMEs.

Interest in "Automated Policy Recommendation and Real-Time Monitoring" reflects SMEs' desire for dynamic, responsive tools that can adapt to changing data protection needs and provide continuous oversight. This offering is valued for its ability to proactively manage data protection policies and quickly respond to potential compliance issues, reducing the risk of data breaches and ensuring ongoing adherence to GDPR requirements.

The "Cybersecurity Awareness and CyberRange Training" offering also attracted interest, highlighting the importance of cybersecurity in the broader context of data protection. This interest suggests that SMEs are looking for comprehensive solutions that not only address GDPR compliance but also enhance their overall cybersecurity posture. CyberRange training, which offers hands-on experience in simulated environments, is particularly appealing for its practical approach to improving cybersecurity skills and preparedness.

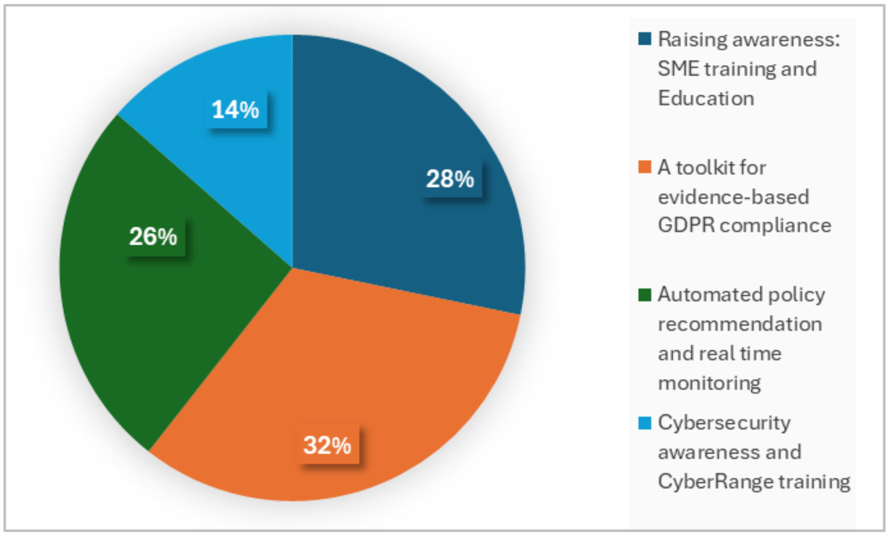

Figure 26. Which of the following SENTINEL offerings would be more useful for your business needs?

6. Conclusion

The objective of this deliverable is to report and analyze the results of ecosystem building activities that were undertaken in the last 18 months (M19-M36) of the project's lifetime. Furthermore, it presents and summarises important takeaway as a result of our stakeholder engagement activities conducted over the entire duration of the project.

During the first 12 months of the project, physical engagement with SME was relatively difficult, due to the COVID-19 pandemic, but during the last phase of SENTINEL, more SMEs were engaged. The evidence of this obstacle is also visible from the number of responses gained for the 1st and 2nd questionnaires, when compared with the last ones.

Within the last 18 months of project duration, SENTINEL triggered engagement activities with two additional EDIHs and one industrial association of SMEs. Such synergies have contributed to the organization of two additional SME-centric workshops (4th and 5th workshops). The objective was to consolidate SENTINEL's mission and main objectives across the European SMEs.

This report provides insights into user acceptance by describing the activities and research performed to understand and improve user acceptance/interests. Key experiences and feedback were gathered through questionnaires allowing us to evaluate the SENTINEL platform's usefulness and its' potential to be adopted by SMEs/MEs. In this regard, the feedback on SENTINEL's offerings gathered during the 4th and 5th workshop was notably positive, highlighting a growing readiness among SMEs/MEs to adopt the SENTINEL solution. It is worth mentioning that during the last workshop, an encouraging 67% of attendees found the SENTINEL platform to be beneficial for their companies. This strong affirmation of the platform's utility emphasizes its relevance and potential impact on their operations. Furthermore, the majority of surveyed companies expressed a clear intention to invest in data protection tools like those offered by SENTINEL within or after the next two years. This reflects a proactive approach to compliance with regulations like GDPR and a commitment to safeguarding personal data. This data strongly suggests that SMEs are not only aware of the importance of data protection but are also increasingly prepared to adopt advanced solutions like SENTINEL to enhance their capabilities.

From the first to the fifth SME-centric workshop in the SENTINEL project, there was a noticeable evolution in the engagement and sophistication of the SMEs' approach to GDPR compliance and data protection. Initially, SMEs showed some awareness and implementation of data protection measures, with substantial gaps in compliance and proactive data protection strategies. Also, SENTINEL offerings were presented on a very conceptual stage. The positive outcome of these workshops was highly supported by the SENTINEL technical developments, with a clear shift towards better understanding, higher adoption of security measures, and greater openness to investing in data protection technologies. There was a significative contribution, with the SENTINEL platform being presented with real use-case examples, starting from the 3rd SME-centric workshop. By the fifth workshop, there was an increased readiness among potential end-users to integrate and invest in new technologies like the SENTINEL platform, reflecting a significant growth in both awareness and the practical application of GDPR knowledge within these enterprises. This progression indicates a successful impact of the workshops in enhancing SMEs' data protection capabilities and compliance frameworks.

References

[1] European Parliament and Council of the European Union. Regulation (EU) 2016/679 (GDPR) Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EL

[2] Deliverable D6.2 (2023), “SENTINEL Demonstration - final execution project.”, SENTINEL EU H2020 Project.

[3] Deliverable D6.3 (2024), “Assessment report and impact analysis”, SENTINEL EU H2020 Project.

Appendices

Appendix-I: SENTINEL Interactive Questionnaire

Part I: Participants Introduction

Question: 1.1 - What is your area of expertise?

Options

IT/Information Security

Personal Data Protection

Technology and Engineering

Human Resource Management

Production

Sales & Marketing

Accounting and Finance

Health & Social Care

Other

Question: 1.2 - What type of data does your organization process? (one or more options)

Options

Customer

Staff/Employee

Suppliers/Industrial

Business Partners

Other

Question: 1.3 - Please identify your level of knowledge regarding GDPR (General Data Protection Regulation).

Options

Not at all aware

Beginner

Intermediate

Expert

Question: 1.4 - Does your organisation use security/privacy policies software/services for data protection compliance?

Options

Yes

No

I’m not sure

Question: 1.5 If yes, what are your annual approximate costs?

Options

0 €

1-999 €

1,000-9,999 €

10,000-50,000 €

>50,000 €
I don't know

Question: 1.6 - Did you find SENTINEL a potential solution to be implemented within your company?

Options

Yes
No
Maybe

Question: 1.7 Does your company plan to invest on such tools/services in the future?

Options

Yes, within the next two years
Maybe, after 2 years
No, up to my knowledge
I don't know

Question: 1.8 - Which of the following SENTINEL services would be more useful for your business needs?

Options

Raising awareness: SME Training and Education

A toolkit for evidence-based GDPR compliance

Automated policy recommendation and real time monitoring

Cybersecurity awareness and CyberRange training