SENTINEL

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

D5.7 - Best practices for maintaining and operating the system in the long term - TRL 7

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 5
Deliverable Title	D5.7 - Best practices for maintaining and operating the system in the long-term - TRL 7
Version	1.4
Date of Submission	27/05/2024
Main Author(s)/ Editor(s)	Ruben Costa (UNINOVA)
Contributor(s)	Siranush Akarmazyan (ITML), Yannis Skourtis (IDIR), Marinos Tsantekidis (AEGIS), Dimitra Malandraki (CECL)
Reviewer(s)	Mihalis Roukounakis (CG), Stavros Rafail Fostiropoulos (ITML)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	14/03/2024	Table of Contents	Confidential
1.1	26/04/2024	1st round of contributions	Confidential
1.2	10/05/2024	2nd round of contributions	Confidential
1.3	24/05/2024	Integration of comments from reviewers	Confidential
1.4	27/05/2024	Final version ready	Public

Table of Contents

List of Figures

Abbreviations

Abbreviation	Explanation
ARIA	Accessible Rich Internet Application
BRMS	Business Rules Management System
CSRA	Cybersecurity Risk Assessment
DoA	Description of Action
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
FFV	Full-Featured Version
GDPR	General Data Protection Regulation
MISP	Malware Information Sharing Platform
OTM	Organisational and Technical Measure
PDP	Personal Data Protection
SME	Small and Medium-sized Enterprise
UI	User Interface
UX	User Experience
WCAG	Web Content Accessibility Guidelines

Executive Summary

This deliverable, D5.7 “Best practices for maintaining and operating the system in the long-term - TRL 7”, outlines the best practices for maintaining a smooth operation of the SENTINEL system after the end of the project, detailing the comprehensive internal testing procedures, scalability assessments, and the legal, ethical, operational, and accessibility considerations implemented throughout the project lifecycle.

Throughout the project, an internal testing procedure was developed and executed, ensuring that the SENTINEL platform performs optimally across various technical and user-experience metrics. This procedure was instrumental in identifying and rectifying several distinct issues, categorized into functional/performance bugs, user interface bugs, and content errors. These efforts have significantly enhanced the platform's reliability and user-friendliness.

Additionally, this deliverable discusses the scalability of the SENTINEL platform, showcasing its ability to handle increased loads of user demands effectively. The accessibility aspect of the platform is also discussed and analysed through this deliverable. The platform was tested against international web accessibility standards to ensure that it is inclusive and accessible to all users.

From a legal and ethical standpoint, SENTINEL has maintained strict adherence to GDPR and other relevant data protection regulations, establishing a solid framework for data handling and security. The legal and ethical dimensions of the platform are discussed here as well, ensuring ongoing compliance and responsiveness to regulatory changes.

1 Introduction

1.1 Purpose of the document

1.1.1 Scope

The purpose of this deliverable is to describe the scope, design rationale, technical details, and integration activities for SENTINEL's final version.

In terms of design rationale, technical details and integration activities, this document explains how the SENTINEL consortium selected a representative set of use cases and defined a series of end-to-end scenarios that connect all layers of the SENTINEL architecture, providing meaningful functionalities to the end-user. In technical terms, we have defined the role of each module, designed and implemented the interfaces and integrated the pieces into a solution that realises the purpose of the interim version.

1.1.2 Contribution to WP5 and project objectives

This deliverable has been composed within the context of WP5 "SENTINEL continuous integration and system validation". It constitutes the second major output of Task 5.3 "From the prototype to the final solution". Based on the Description of Action (DoA), WP5 is responsible for:

- Ensuring the seamless integration of SENTINEL components into a unified toolkit, usable by SMEs/MEs.
- Continuously optimising the SENTINEL platform through an iterative process (testing-improvement-testing).
- Supporting the project's sustainability and commercial exploitation.

This is the last concrete step towards achieving the objectives of this work package and it builds upon SENTINEL final product (D5.6), which is the final integrated SENTINEL framework showcasing the full functionality of SENTINEL components alongside improvements at the user interface.

The provisions made to ensure the feasibility and the extensibility of an integrated SENTINEL solution, as well as the processes established, clearly contribute to the following project-wide objectives:

- **Project Objective 1.** Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS) that enables Speed, Flexibility, Quality, Efficiency and Security for SMEs/MEs. Validate, demonstrate, and carry out experimental evaluation of the proposed framework in real-world SMEs/MEs operation scenarios.
- **Project Objective 4.** Facilitate an efficient exploration of cost-efficient, intelligent, and automated PDP compliance and Identity Management full potential in SMEs/MEs environments and realise societal and economic opportunities by validating SENTINEL framework in real-world settings via use cases driven by complementary industries.

1.1.3 Relation to other WPs and Deliverables

Following the quality tests performed under T5.2 “Continuous integration towards the realisation of a complete system” and the T6.3 “Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs”, this deliverable aims to describe the activities that will ensure the project’s viability in the years to come. As this deliverable aims to describe the best practices for maintaining and operating the SENTINEL platform in the long term, it is very closely related to the technical developments of the platform assets addressed in WP2, WP3, WP4 and WP5.

1.2 Structure of the document

The rest of this document is structured as follows:

- Section 2 presents the internal testing procedure used to guide testers through a structured process of identifying bugs, typos, usability issues, and other irregularities.
- Section 3 highlights the technical aspects of SENTINEL which need to be addressed in the face of potential market adoption and scaling up of the system.
- Section 4 presents the process to ensure the legal and ethical standards governing the operation of the SENTINEL platform.
- Section 5 demonstrates the SENTINEL Wiki which provides guidelines to navigate through the platform and the same time serves as a knowledge source for potential users.
- Finally, section 6, concludes the document and points out future steps.

1.3 Intended readership

This document is intended for both consortium members and external stakeholders. Consortium members involved in the implementation of the SENTINEL technologies have provided descriptions of the assets they provide. This document will be used as their reference and provide scope, whilst they continue with development work. This includes any fine-tuning and adjustments to cater for the pilot activities until the end of the project. Moreover, the SENTINEL pilot partners (CG, TIG and other third-parties brought through DIH) will also benefit from this document, since it provides a clearer overview of the capabilities and benefits of SENTINEL, thus facilitating their involvement in WP6.

External stakeholders will be informed on the technological offerings provided and how they are being integrated into a platform that will meet the overarching objectives of the project, as well as the expectations and needs of its intended users. It will also facilitate future exploitation actions and build a solid ecosystem of stakeholders around the SENTINEL framework, as part of WP7 activities.

2 Internal Testing Procedure

To ensure a thorough and effective internal testing procedure for the SENTINEL platform, it's crucial to establish a sound methodology that guides testers through a structured process of identifying bugs, typos, usability issues, and other irregularities. Here's a comprehensive description of a methodology tailored for the SENTINEL project:

Figure 1. Internal testing procedure

2.1 Preparation Phase

Within the preparation phase, we had to ensure that all testers were equipped with the necessary access credentials and permissions to fully explore the platform. To highlight that, testers were mainly the SENTINEL partners not involved in the technical development of the platform. Next, we established a stable testing environment that include a variety of devices and browsers to ensure compatibility across different platforms. Additionally, we provided testers with comprehensive documentation that details the platform's intended functionality and a user workflow, highlighting the specific areas of focus to be tested.

1. Register into the SENTINEL platform here: https://platform.sentinel-project.eu/
2. Create a complete profile for your organisation
3. Create and populate one or more personal data processing activities (PAs)
4. Commit at least one PA to the permanent record of processing activities (ROPA)
5. Execute one or more self-assessments:
    a. GDPR Compliance Self-Assessment (GDPRCSA)
    b. Data Protection Impact Assessment (DPIA)
    c. Cybersecurity Risk Assessment (CSRA)
6. SENTINEL leverages data gathered during the previous steps, to calculate recommendations of measures, software and training material, tailored to your organisation. These may be browsed under "Policy"
7. SENTINEL also keeps track of which recommended measures are implemented and which are still pending.
8. Use SENTINEL's cybersecurity tools: the CyberRange, and the Simulation Environment. Explore the CyberRange interface, to recreate the cyber setup of your organisation and learn how to do cyber defence. Play around in Airbus' new CyberRange Gaming interface to enact cyber best practices and scenarios in a gamified manner.
9. Browse the Observatory for up-to-date information on the latest threats and vulnerabilities data from open threat intelligence platforms (for expert and technical cybersecurity staff), as well as for handling incidents and reporting/sharing them to the appropriate communities.
10. Finally, if you have installed and integrated a SENTINEL-integrated cybersecurity infrastructure monitoring plugin, such as Security Infusion, you will be able to receive security notifications.

Figure 2. Internal Testing User Workflow

We initiated the internal testing procedure, with an orientation session to familiarize testers with the platform's features and the expected behaviours. We also presented the communication tools and channels that testers could use to report issues and pose questions.

Within the testing and validation exercise please take into account the following important aspects:

1. Check for any features that do not work as intended. This includes buttons that don't respond, broken links, or features that behave unpredictably.
2. Look for elements that may be confusing or difficult to navigate. Assess the intuitiveness of the layout and whether the user journey through the platform feels logical and seamless.
3. Be attentive to any instances of the platform being slow to respond, crashing, or having long loading times. Also, note any situations where the platform consumes excessive resources on your device.
4. Look for typos, grammatical errors, and any incorrect or outdated information within the platform's content.
5. Test the features that allow users to provide feedback or seek support. This includes the SENTINEL Wiki and tooltips which dynamically appear within the platform.

Please, provide your overall experience and impression of the platform and any suggestions for improvement, whether they be additional features, design changes, or other enhancements, using the template file here: https://nextcloud.sentinel-project.eu/f/35465 (make a new copy with your organization name)

Figure 3. Internal Testing recommendations and Reporting Channels

2.2 Execution Phase

The execution phase, dealt with guiding the testers through each feature and function of the platform. This approach ensured that no critical aspects were overlooked. We encouraged testers to carry out the previously identified workflows and recommendations, by taking note of any deviations from the expected outcomes. One important aspect to highlight, was to allocate sufficient time for testers to engage in creative exploration of the platform beyond the structured tests. This period of exploratory testing is crucial for identifying issues that may not emerge during more controlled testing phases.

2.3 Reporting Phase

The reporting phase was responsible for collecting feedback from testers in a standardised form. We used Excel spreadsheet (see Appendix-I: SENTINEL internal testing questionnaire), to capture essential details such as the nature of the bug, severity level, and any accompanying screenshots or suggested fixes. Additionally, we established a routine, where testers were expected to submit their findings and engage in brief discussions to clarify any ambiguities. At the end of the reporting phase, we organized a review meeting with the objective to go over the findings, in order to prioritise issues based on their severity and impact and discuss the next steps.

2.4 Conclusion Phase

All findings were consolidated into a comprehensive report that details the bugs discovered, usability concerns, performance issues, and overall impressions from testers. Additionally,

actionable recommendations were included that were derived from testers' feedback to refine and enhance the platform.

The report illustrates that 111 issues were identified, during the internal testing. We classified the issues into 3 different categories:

- Functional/Performance Bugs:
  - Logic Errors: Incorrect calculations or flawed business logic leading to unexpected results.
  - Input/Output Errors: Issues with input acceptance or incorrect outputs generated by the system.
  - Integration Failures: Problems when different components or systems interact or communicate.
  - Load Issues: Slow response times or system crashes under heavy load conditions.
  - Memory Leaks: Unintended memory consumption that degrades performance over time.
  - Resource Exhaustion: Excessive use of system resources like CPU or disk space.
- User Interface bugs:
  - Layout Issues: Misalignments, inconsistent spacing, or overlapping elements in the UI.
  - Navigation Problems: Broken links, non-responsive buttons, or confusing navigation paths.
  - User Experience Flaws: Elements that confuse the user or complicate the user experience.
  - Accessibility Issues: Problems faced by users with disabilities, impacting their ability to use the platform.
  - Help and Documentation Gaps: Inadequate or misleading user help and documentation.
- Content Errors: Typos, grammatical errors, incorrect content, or outdated information.

From the 111 identified issues, 57 were related to UI bugs, 47 to Functional/Performance bugs and 10 content errors. All the identified issues were carefully reviewed and solved.

3 Scalability, Accessibility and Evolving User Requirements

This section is dedicated to technical aspects of SENTINEL which need to be addressed in the face of potential market adoption and scaling up of the system. These aspects primarily address scalability, accessibility and evolving business requirements.

3.1 Scalability

In a scaling scenario, the SENTINEL platform will need to support a significantly higher number of concurrent users, compared to the period of development and testing.

The final SME-centric workshop (Feb 2024) provided a fertile testing ground to formulate assumptions and execute tests. The initial assumptions are that one thousand (1000) active/named users on the platform would roughly translate to about twenty (~20) concurrent or ~2/3 simultaneous users. The 20 SMEs, with roughly one user assigned to each SME during the final workshop, were in the same physical location and the tests involved their concurrent access and usage of the platform. SENTINEL demonstrated **resilience, robustness and good response times** to all of these tests. This initial assumption of ~1k active users/licenses is deemed sufficient for the mid-term to support a successful stage of SENTINEL's go-to-market. After this, the infrastructure should be tested again leveraging the appropriate Cloud simulation toolkits and a decision needs to be made on how to scale further if required, considering deploying additional computing, networking and storage resources, performance optimisations, caching, load balancing, etc.

3.2 Accessibility

The SENTINEL platform is heavily based on the user interface (UI) and on the user experience (UX). Thus, during the development of the web interface of the platform, mock-ups were designed and assessed/improved by both the technical team and the business logic team of the project, while a continuous internal evaluation of the UI and UX was performed during each development cycle, leading to mature, robust, and user-friendly dashboard. This evaluation effort had 2 critical angles: to find the best possible way to present complex concepts, while also presenting the platform accessibility. To evaluate the bridging of the SENTINEL offerings with the demands of a modern web application in terms of accessibility, apart from the external (to the project) presentations and validations, we performed a series of evaluations through accessibility tests.

To evaluate the SENTINEL's web interface against a set of accessibility standards we used multiple automated tests that were offered as browser extensions. Since we wanted the platform to be evaluated against official guidelines, we used tools that comply with the Web Content Accessibility Guidelines (WCAG). WCAG are part of a series of web accessibility guidelines published by the Web Accessibility Initiative (WAI), which is the main international standards organisation for the Internet. The main tools that we used for our evaluation are:

1. Lighthouse, open source, developed by Google.
2. Axe DevTools, developed by Deque Systems and WCAG 2.1 AA compliant.
3. WAVE evaluation toolkit, developed by WebAIM.

When the SENTINEL web interface was mature enough, we conducted a series of evaluations to identify and tackle any kinds of accessibility issues. Following are some notable issues that have

been identified with the use of the above tools and have been addressed to comply with the WCAG:

- The ‘Skip to content’ feature has been enabled for users who navigate the SENTINEL platform using screen readers or keyboard-only navigation.
- For all the buttons, especially for the action buttons like “Back”, “Home”, “Profile”, “Notification”, that do not contain text but rely only on the identification of their icons, we have embedded text in a way that screen readers will be able to read them.
- Elements on each dashboard have been updated to meet minimum colour contrast ratio thresholds.
- We have updated the text on each link, to be discernible and unique for the screen reader users.
- In general, special attention was given to all the elements that contain Accessible Rich Internet Application (ARIA) roles, so that all their child elements contain specific roles that comply with WCAG.

Most of those tools do not provide a numerical score, since their focus is to offer insights into the accessibility status of a web page, helping developers ensure that their content is accessible to all users. But the Lighthouse browser extension offers a kind of accessibility score that each dashboard offers. It is noteworthy to mention that the combined feedback from those tools managed to upgrade the overall score on the SENTINEL web interface from 22/28 to 26/28, and in many dashboards to 27/28.

3.3 Evolving User Requirements

SENTINEL has been engineered, from the ground up, with a versatile, modular and decoupled architecture precisely to accommodate any evolving business requirements in a manner that will not require major efforts or reengineering of the SENTINEL core. Some examples of such requirements and how they are currently addressed by the system are:

- The need to “plug” into the system additional functionalities, diverging critically from the current SENTINEL V2 feature set, such as new types of self-assessment modules (e.g. plug-ins), interfaces and integrations with third-party tools (e.g. cybersecurity or infrastructure monitoring tools). This is addressed through the system’s generic and decoupled architecture which allows for the easy addition of functionality through the integration of third-party software as plug-ins through the adapter pattern.
- The need for the system to recommend (and enforce/monitor the implementation of) new/dynamic measures, not currently included in the common OTM taxonomy. This is addressed through the dynamic nature of both the Common Repo, the Recommendation Engine and the Policy Drafting / Enforcement components, all of which support a dynamic structure of OTMs which may be edited and repopulated to reflect updated cybersecurity, privacy and data protection requirements or measures as, for example, is the case with “custom” measures recommended by local authorities (DPAs) to DPOs and data protection officers for organisations / SMEs to observe. The users, in this case, would have to input the new OTM(s) in one of the existing categories in the system, and this measure would be recommended and monitored and applied to their own organisation only, not globally.

- The need to introduce new custom OTM selection rules, considering the estimated risk level or other custom factors, without writing code. This is addressed through SENTINEL's dynamic rule engine and BRMS (Business Rules Management System) which supports unlimited custom rules based on the different SENTINEL SME profiling data model, combined with the assessment of risk and the results of the three self-assessments (GDPRCSA, DPIA, CSRA).
- The need to connect to additional open-source third-party sources for cybersecurity data and threat intelligence. This is addressed in the SENTINEL Observatory through the MISP platform which offers the addition of extra feeds and sources to our deployed MISP instance. Apart from the addition of multiple pilot specific feeds on SENTINEL's dedicated instance, we also integrated an additional MISP instance from the CONCORDIA project that was funded from the European Union's Horizon 2020 Research and Innovation program.

4 Legal, Ethical, Operational

A comprehensive process to update the legal and ethical standards governing the operation of the SENTINEL platform has been established to ensure compliance and transparency. This process includes aligning all data collection, processing, and storage practices with the General Data Protection Regulation (GDPR) and other relevant data protection laws. A Data Protection Officer (DPO) for SENTINEL was appointed to monitor continuously the evolving legal and regulatory framework related to GDPR, including national laws, decisions from regulatory authorities, European Data Protection Board (EDPB) opinions, and case law. This officer is responsible for notifying the Platform Owners of any significant changes that could impact SENTINEL's offering.

Moreover, it is ensured that SENTINEL users have a clear understanding of how the platform operates and utilises their data, supported by the provision of GDPR-compliant template texts for information notices, privacy policies, data processing agreements, and the exercise of data subject rights. The platform's risk analysis and information security plans, including measures to maintain user anonymity, are regularly and emergently reviewed and updated. Additionally, the SENTINEL Ethics Manual is annually reviewed and updated.

The platform meticulously avoids infringing on the intellectual property rights of others, encompassing software licenses, content, and third-party integrations. Clear lines of accountability have been implemented to address data breaches or operational failures effectively. Moreover, the platform adheres to international guidelines for web content accessibility, ensuring inclusivity and accessibility for all users. Our commitment to accessibility is evidenced through compliance with the Web Content Accessibility Guidelines (WCAG). SENTINEL's platform has been independently evaluated to meet WCAG 2.1 AA standards, ensuring that all users, regardless of disability, can navigate and benefit from our services.

Regarding impact assessments, SENTINEL will regularly conduct Data Protection Impact Assessments (DPIAs), especially when new data processing technologies or techniques are introduced. These assessments are crucial in identifying and mitigating any potential risks to data subjects, emphasising our proactive stance on privacy and security.

Through these comprehensive measures, SENTINEL not only upholds legal and ethical standards but also sets a precedent in operational excellence, ensuring that the platform remains trustworthy, secure, and inclusive.

5 SENTINEL User Manual

This section presents the SENTINEL Wiki[1], which aims to be a comprehensive guide to navigating and to maximising the capabilities of the SENTINEL platform. Designed with a focus on practicality and user engagement, SENTINEL Wiki serves as both an educational tool and a technical resource, enhancing end-users' understanding of key cybersecurity and personal data protection concepts within the SENTINEL ecosystem.

The SENTINEL wiki is designed to be a practical, user-centric tool that in the first place aims to help users navigate through the different features of the SENTINEL platform. Besides that, it provides educational information aimed at enhancing user understanding when it comes to the context of cybersecurity and personal data protection. SENTINEL wiki is a standalone open-source tool where each user can enrich it with content or update the already existing information, based on the user permissions. It also interfaces with the SENTINEL platform through an API allowing the user to browse through the wiki content directly from the help button of the platform. The SENTINEL wiki consists of a number of pages and has the following structure.

5.1 Introduction page

This is the introductory page that the users see as soon as they log in. It serves as a brief welcoming note and outlines the purpose of the pages, aiming to provide simple guidance to help newcomers understand the functions and benefits of SENTINEL. It shows SENTINEL "in a nutshell", mentions potential users and finally provides a linear pipeline of action through the different functions.

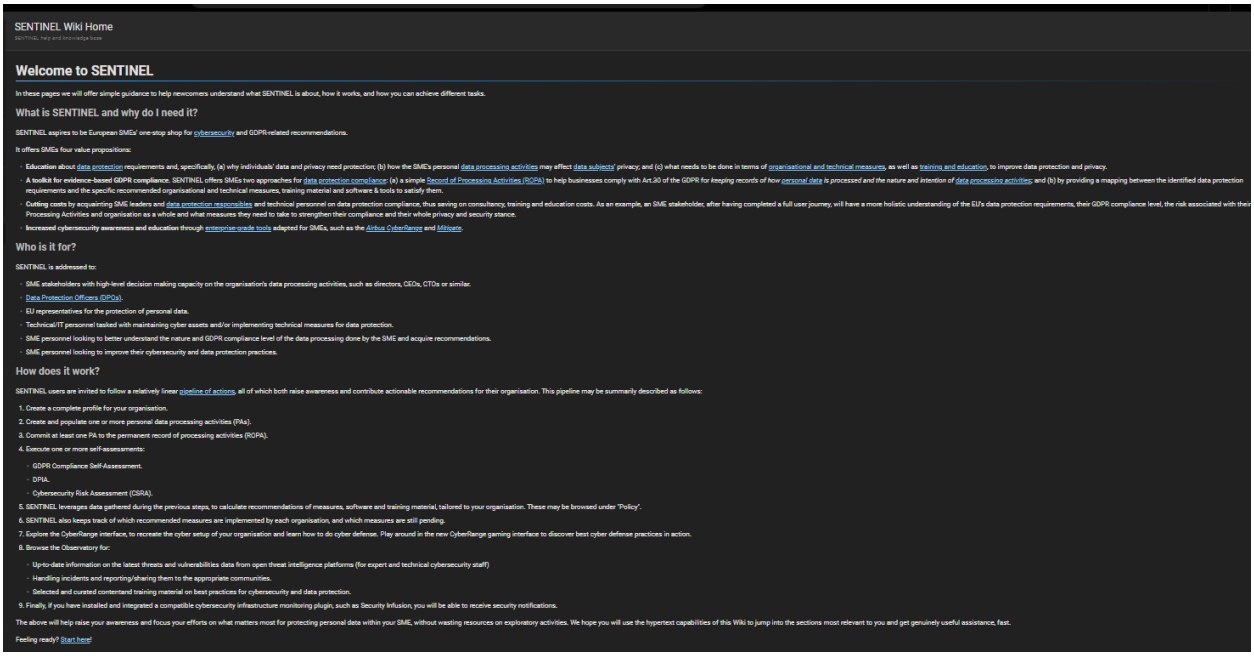

Figure 4. Introduction page

[1] https://wiki.sentinel-project.eu/

5.2 Glossary page

A wiki page is dedicated to the glossary relevant to the SENTINEL context. Here, the user can find out how SENTINEL perceives and uses some of the most common terms and abbreviations found in the context of cybersecurity and personal data protection, using short descriptions. Most of the terms are hyperlinked to other sections of the wiki and the help pages to add interactivity and a quicker reference for the reader.

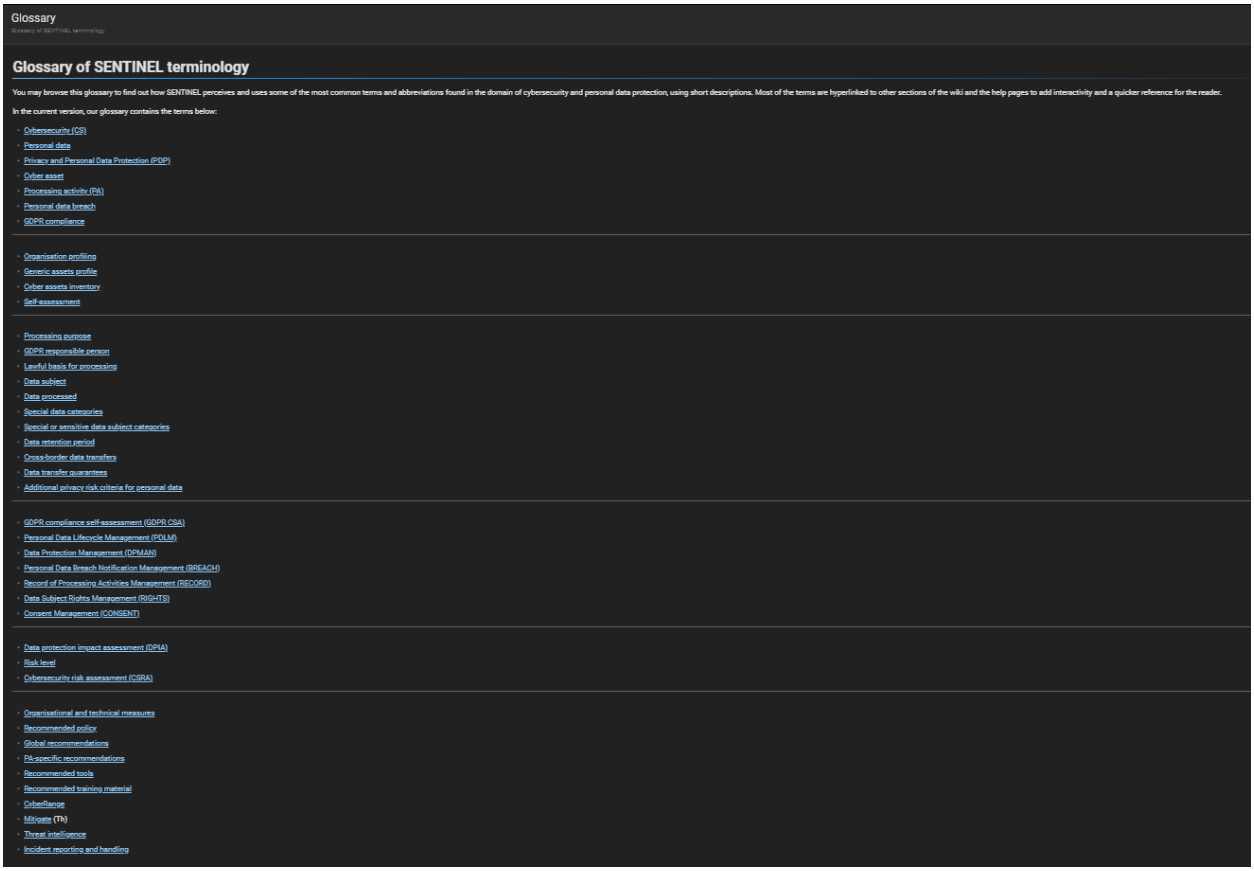

Figure 5. Glossary page

5.3 Getting Started

In the main page of the SENTINEL wiki, the user can find a “Getting Started” guide which provides guidance and helps user to navigate SENTINEL's most important functions, page by page. The help pages are linked in hyperlinks in a hierarchical manner. Within each help page, we provide the relevant topic, context (a short description), procedure (how to use the page), prerequisites (if applicable and, possibly, a list with references to related topics. Annotated screenshot(s), with highlighted focus areas are also provided where applicable. Finally, we provide navigation links to the previous and the next topic, on each page. An indicative help page is the Basic Organisation Data which is dedicated to helping the users create their organisation profile in the respective tab of the SENTINEL platform.

6 Conclusion and future steps

With the conclusion of the SENTINEL project, we can claim that the comprehensive testing and validation phases have highlighted the robustness and adaptability of the platform. Through meticulous internal testing, including functional, performance, and user interface evaluations, the testing and validation phases enabled to identify and correct a wide range of issues, enhancing the overall usability and effectiveness of the platform. This process has not only proven the platform's capabilities in real-world scenarios but also highlighted areas for future enhancement.

As future steps, the SENTINEL platform is set to continue towards full-scale implementation and broader market integration. The next steps involve further refining the platform based on the large-scale feedback received from upcoming testing phases and ongoing user engagement. This includes continuous updates to the legal, ethical, and operational frameworks to ensure compliance with evolving regulations and standards. Additionally, the exploitation of the SENTINEL platform will also focus on expanding features and functionalities to accommodate new cybersecurity threats and challenges.

In conclusion, the SENTINEL project, with its innovative approach to enhancing cybersecurity for SMEs, can make a significant impact on the digital security landscape in Europe. The project's future initiatives will build on its current achievements, driving forward the development of more secure, efficient, and user-friendly digital solutions.

Appendices

Appendix-I: SENTINEL internal testing questionnaire

	No	Page	URL	Comment
EXAMPLE	*0*	*My Organisation*	*https://platform.sentinel-project.eu/profile*	*Profile completeness colour remains orange even if I have completed my profile.* *It would be nice if it changes to green to signal completion, or even changing the colour to green throughout with a percentage indicator to confirm progress.* *It would also be prudent to consider [visual] access for people - for example, the light/mid grey font colour could be a barrier to access for some groups (i.e., dyslexia, VI, etc.)*
	1			
	2			
	3			
	..			