



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

D6.3 - Assessment report and impact analysis



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	1 st 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 6
Deliverable Title	D6.3 - Assessment report and impact analysis
Version	2.0
Date of Submission	31/05/2024
Main Editor(s)	Kostantinos Poullos (STS), Eleni-Maria Kalogeraki (FP)
Contributor(s)	Siranush Akarmazyan (ITML), Stavros Rafail Fostiropoulos (ITML), Nick Papaoikonomou (STS), Nikos Kardoulakis (STS), Thanos Karantjias (FP), Philippe Valoggia (LIST), Manolis Falelakis (INTRA), Yannis Skourtis (IDIR), Evangelia Kavakli (IDIR), George Hatzivasilis (TUC), George Tsirantokanis (TUC), Apostolos Dollas (TUC), Alexander Shevtsov (TUC), Maria Mastoraki (TUC), Ioannis Charalampos Mitropoulos (TUC), Costa Drakonakis (TUC), Dimitrios Tirovolas (TUC), Ioannis Arkalakis (TUC), Anthi Barbaki (TUC), Andreas Mprokalakis (TUC), Costas Spiridakis (TUC), Evaggelia Papadogiannaki (TUC), Thomas Oudin (ACS), Dimitra Malandraki (CECL), Mihalis Roukounakis (CG), Ruben Costa (UNINOVA), Daryl Holkham (TIG), Marinos Tsantekidis (AEGIS)
Reviewer(s)	Philippe Valoggia (LIST), George Hatzivasilis (TUC)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
1.0	24/02/2024	ToC	Confidential
1.1	22/03/2024	Updated ToC	Confidential

1.2	02/04/2024	Partners input collected	Confidential
1.3	05/04/2024	Consolidated version	Confidential
1.4	19/04/2024	Partners input collected	Confidential
1.5	26/04/2024	Consolidated version	Confidential
1.6	10/05/2024	Partners input collected	Confidential
1.7	16/05/2024	Draft released for review	Confidential
1.8	24/05/2024	Review conducted by LIST, TUC	Confidential
1.9	29/05/2024	Reviewers' comments addressed	Confidential
2.0	31/05/2024	Final version ready	Public

Table of Contents

List of Figures	6
List of Tables	6
Abbreviations	8
Executive Summary	10
1. Introduction	11
1.1 Purpose of the document	11
1.1.1 Scope	11
1.1.2 Contribution to WP6 and project objectives.....	11
1.1.3 Relation to other WPs tasks and deliverables	12
1.2 Structure of the document.....	12
1.3 Intended readership	13
2. SENTINEL Evaluation Aspects	14
2.1 SENTINEL user-centric evaluation.....	14
2.1.1 Overview of the SENTINEL experimentation process	14
2.1.2 Overview of the SENTINEL evaluation process	15
2.2 The persona-based approach	17
2.3 Updates and enhancements on SENTINEL User Evaluation Questionnaire	18
3. SME-centric Workshop for Demonstrating SENTINEL solution	21
3.1 Workshop objective.....	21
3.2 Workshop overview: preparations, setup, and demonstration	21
3.2.1 Enterprises recruitment.....	21
3.2.2 Communication.....	22
3.2.3 The SME-centric Workshop	23
3.3 The SENTINEL experiment of the SME-centric Workshop.....	25
3.3.1 Purpose of the SENTINEL experiment.....	25
3.3.2 SENTINEL use cases and experiment workflow	25
3.4 SME workshop evaluation results	33
3.4.1 Participants Introduction	34
3.4.2 User Satisfaction.....	35
3.4.3 SENTINEL Overall evaluation.....	39
3.4.4 Express end-user opinion and additional comments	43
4. Overall SENTINEL Assessment.....	46

4.1	SENTINEL Validation and Verification	46
4.1.1	SENTINEL Validation.....	46
4.1.2	SENTINEL Verification.....	55
4.2	SENTINEL functional completeness assessment towards SMEs requirements	63
4.2.1	SENTINEL platform assessment towards Business Requirements	63
4.2.2	SENTINEL platform towards Application Requirements.....	77
4.3	Impact Assessment.....	93
4.3.1	SENTINEL evaluation outcomes.....	93
4.3.2	KPIs/KRs assessment	97
5.	Conclusion	101
	References	103
	Appendices	105
	Appendix-I: SENTINEL Interactive Questionnaire.....	105
	Part II: SENTINEL hands-on training	105
	Appendix-II: Templates for assessing the SENTINEL platform towards Business and Application Requirements.....	111
	Template of assessing the SENTINEL platform towards Business Requirements (BRs)..	111
	Template of assessing the SENTINEL platform towards Application Requirements (ARs)	112

List of Figures

Figure 1. Overview of SENTINEL testing and evaluation activities towards project’s technical achievements.....	17
Figure 2. SENTINEL final SME-centric Workshop poster and social media post.....	22
Figure 3. Registration form.....	23
Figure 4. SENTINEL registration environment	26
Figure 5. SENTINEL My Organisation.....	27
Figure 6. Create/edit a Processing Activity.....	28
Figure 7. SENTINEL ROPA	29
Figure 8. Perform GDPR Compliance Self-Assessment.....	30
Figure 9. Review GDPR Compliance Self-Assessment results of organisation’s PAs	30
Figure 10. Acquire Policy Recommendations.....	31
Figure 11. Track Recommendations’ implementation status within the organisation.	32
Figure 12. Software tools and training materials suggested for OTMs.....	32
Figure 13. It was easy creating account and organisation in the SENTINEL platform	35
Figure 14. It was easy completing the organisation profile in the SENTINEL platform.....	35
Figure 15. Did you use a Processing Activity template?	36
Figure 16. It was easy to complete my first Processing Activity.....	36
Figure 17. I was able to commit my PA to the ROPA	37
Figure 18. It was easy to execute the GDPR Compliance Self-Assessment.....	37
Figure 19. Executing a GDPR Compliance Self-Assessment was fast and efficient	38
Figure 20. I am satisfied with the quality of the GDPR Compliance Self-Assessment result.....	38
Figure 21. It was easy to acquire Recommendations	39
Figure 22. Acquiring Recommendations was fast and efficient.....	39
Figure 23. SMEs/MEs end-users’ opinion of UI/UX capabilities.....	40
Figure 24. I did not face any interruptions while using the platform	41
Figure 25. SENTINEL provides all the functionalities I expect to have for assessing GDPR compliance.....	41
Figure 26. SENTINEL provides all the functionalities I expect to have for assessing GDPR compliance.....	42

List of Tables

Table 1. User personas of the SME centric Workshop and their requirements	18
Table 2. Mapping of personas characteristics with questions of the user evaluation interactive questionnaire	20
Table 3. SENTINEL final SME-centric Workshop agenda	24
Table 4. The list of SMEs participated in the final SME-centric workshop.....	24
Table 5. Validation outcomes of Clingenics Pilot.....	46
Table 6. Validation outcomes of TIG Pilot	49
Table 7. Validation outcomes of DIH pilot and SMEs user-centric workshop.....	53
Table 8. Verification outcome of SENTINEL components	55
Table 9. Verification outcome of SENTINEL plugins	58

Table 10. SENTINEL addressing SME’s Confidentiality, Integrity, Availability, and non-Repudiation requirements	64
Table 11. SENTINEL platform towards non-functional/quality requirements.....	65
Table 12. SENTINEL platform towards generic cybersecurity requirements.....	67
Table 13. SENTINEL platform towards generic PDP requirements	70
Table 14. SENTINEL platform towards privacy enhancing requirements	73
Table 15. SENTINEL platform towards cybersecurity technical capabilities	74
Table 16. SENTINEL platform towards business continuity.....	77
Table 17. SENTINEL platform towards encryption	78
Table 18. SENTINEL platform towards data anonymisation, pseudonymisation, obfuscation....	78
Table 19. SENTINEL platform towards logging	79
Table 20. SENTINEL platform towards analytics and visualisation.....	79
Table 21. SENTINEL platform towards flexibility of capabilities.....	80
Table 22. SENTINEL platform towards flexibility of policies	81
Table 23. SENTINEL platform towards secure data exchange.....	82
Table 24. SENTINEL platform towards SME onboarding	82
Table 25. SENTINEL platform towards RASE scoring.....	83
Table 26. SENTINEL platform towards plugin Recommendations and Policy Drafting	83
Table 27. SENTINEL platform towards Policy Monitoring.....	84
Table 28. SENTINEL platform towards Incident Response	85
Table 29. SENTINEL platform towards Policy Orchestration	85
Table 30. SENTINEL platform towards Training Recommendations	86
Table 31. SENTINEL platform towards Knowledge sharing.....	86
Table 32. SENTINEL platform towards Compliance Monitoring	87
Table 33. SENTINEL platform towards Confidentiality, Integrity, Availability and non-Repudiation	88
Table 34. SENTINEL platform towards Usability	89
Table 35. SENTINEL platform towards Cost-effectiveness	90
Table 36. SENTINEL platform towards Scalability.....	90
Table 37. SENTINEL platform towards Authentication, Authorisation and Accounting	92
Table 38. SENTINEL platform towards use of Common Language	92
Table 39. SENTINEL evaluation outcomes	94
Table 40. KPIs/KRs final assessment	97

Abbreviations

Abbreviation	Explanation
AAA	Authentication, Authorisation, Accounting
AR	Application Requirement
BCP	Business Continuity Plan
BR	Business Requirement
CAPEC	Common Attack Pattern Enumeration and Classification
CG	Clingenics
CIA	Confidentiality, Integrity, and Availability
CPE	Common Platform Enumeration
CS	Cybersecurity
CSA	Compliance Self-Assessment
CSRA	Cybersecurity Risk Assessment
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DC	Dimensions Care
D6.3	Deliverable 6.3
DIH	Digital Innovation Hub
DLP	Data Leak Protection
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPP	Data Protection Policy
DRP	Disaster Recovery Plan
EAB	Executive Advisory Board
FFV	Full-Featured Version
FVT	Forensics Visualisation Toolkit
GA	Grant Agreement
GDPR	General Data Protection Regulation
IIoT	Industrial Internet of things
KB	Knowledge Base
KER	Key Exploitable Result
KR	Key Result
KPI	Key Performance Indicator
ME	Micro Enterprise
MS	Milestone
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
NDA	Non-Disclosure Agreement
NF	Non-Functional
NVD	National (NIST) Vulnerability Database
OTM	Organisational and Technical Measure
PA	Processing Activity
PDLM	Personal Data Lifecycle Management
PDP	Personal data protection
PET	Privacy Enhancing Technologies
RBAC	Role Base Access Control
RE	Requirements Engineering

ROPA	Registry of Processing Activities
SDLC	Software Development LifeCycle
SME	Small-Medium sized Enterprise
SUS	System Usability Scale
T	Task
TIG	Tristone Investment Group
UI / UX	User Interface / User Experience
WP	WorkPackage
XSS	Cross-Site Scripting

Executive Summary

The SENTINEL D6.3 deliverable provides a comprehensive assessment and impact analysis of the SENTINEL platform, focusing on real-life experiment evaluations conducted as part of task 6.4 (T6.4) activities of WP6. This document outlines the final stages of the evaluation process in line with the technical progress of the SENTINEL platform. It describes how the user-centric evaluation methodology and the experimentation protocol were applied to assess the SENTINEL platform. Furthermore, it presents the user personas profiling of the SENTINEL functionalities following a persona-based approach, identified under T6.4 activities. In addition, the current deliverable presents the final pilot event conducted in the physical SME-centric Workshop in M33, which engaged a group of SMEs/MEs aiming to: i) test and evaluate the SENTINEL Final Product (released in M30) as part of the works of T6.3 and ii) demonstrate the main project's achievements to liaise with various enterprises of different industry/technical domains as a continuous engagement in building the SENTINEL ecosystem, addressing the objectives of Task 7.4 (T7.4). The feedback received was considered where possible in the platform technical refinements carried out until M36 under the activities of Task 5.3 (T5.3). In addition, the input gained could be considered beyond the project lifespan for maintaining and operating the platform in the long term and raising its exploitation capacity.

Furthermore, validation and verification outcomes of the platform assessment are reported, according to the three pilot results, the final SME-centric Workshop results, and the verification internal testing performed by the project technical partners in a laboratory environment across the technical development lifecycle. In addition, to enhance the SENTINEL evaluation aspects, we assessed the SENTINEL platform capabilities, performance, and functional completeness against covering the Business and Application Requirements identified under the tasks T1.1 and T1.2. The evaluation outcomes are presented in the current deliverable. Eventually, after conducting an impact assessment, we calculated the project's KPIs/KRs associated with the SENTINEL platform evaluation. The results are reported in the current document.

The ultimate purpose of the SENTINEL evaluation process was to ensure that the platform meets end-user requirements, offering robust and user-centric solutions for security, privacy, and data protection. This deliverable combines feedback and results obtained from various stakeholders (mostly SMEs, including MEs, larger enterprises and members of the project's Executive Advisory Board as well), providing insights into the platform's effectiveness and areas for improvement.

1. Introduction

1.1 Purpose of the document

Section 1.1.1 provides the scope of the current deliverable, whereas Section 1.1.2 describes the report's contribution to WP6 and project objectives. Finally, Section 1.1.3 describes the deliverable's relation to other WPs, tasks, and deliverables.

1.1.1 Scope

This document aims to present the comprehensive assessment of the SENTINEL platform and the impact analysis performed considering the results retrieved from real-life experiments conducted in the context of the SENTINEL project. It aims to highlight the testing, demonstration, and validation of the final version of the SENTINEL platform (SENTINEL Final Product), focusing on its offerings to SMEs across various fields, and providing insights into the project's final results and future implications.

1.1.2 Contribution to WP6 and project objectives

The work conducted in this report is highly related to the WP6 following objectives:

Objective 1: Finalization of the experimentation protocol based on end-users' requirements.

D6.3 presents the iterative refinement and application of the experimentation protocol, incorporating end-user feedback to ensure the SENTINEL platform meets their specific needs. This process ensures the final protocol is robust, user-centric, and effectively addresses real-world requirements.

Objective 2: Realization of real-life demonstrators based on both consortium members and external entities engaged via DIHs.

This report details the deployment and execution of real-life demonstrators with consortium members and external entities engaged under the works of T6.2 and T6.3, crucial for testing and validating the SENTINEL Final Product. Moreover, it aimed at assessing the platform's functionality and adaptability in real-world scenarios.

Objective 3: Provide detailed validation and evaluation of the SENTINEL platform from a usability and end-user point of view.

The document provides a comprehensive evaluation of the SENTINEL platform, focusing on validation aspects of usability, satisfaction, acceptance, etc, to elicit end-user feedback. Specifically, it analyses the user experience and satisfaction levels, ensuring that the platform is not only technically sound but also user-friendly and effective in meeting the needs of its target audience. In addition, verification aspects were considered by technology providers to assess the platform's performance and technical capabilities.

The current report describes the pilot validation and verification results retrieved from the three SENTINEL pilots, the final pilot event, and the verification internal tests. Moreover, a thorough analysis was conducted to assess the platform towards meeting a set of Business and Application Requirements identified in tasks T1.1 and T1.2. Eventually, considering the overall impact, the SENTINEL KPIs/KRs related to the SENTINEL platform evaluation were assessed to measure

the project's success (some KPIs/KRs were already successfully achieved in M30 and thus analysed in D6.2 [1]).

1.1.3 Relation to other WPs tasks and deliverables

The current deliverable presents the final pilot event carried out with the physical “SME-centric Workshop” in M33 to test and validate the SENTINEL Final Product, released in M30. The workshop engaged various internal and external SMEs, including pilot owners (i.e., Clingenics (GG), Tristone Investment Group (TIG) and sister-engaged companies, UNINOVA and external SMEs recruited by Digital Innovation Hubs (DIHs) and project partners, including the Executive Advisory Board members. In this vein, D6.3 reports activities of Task 6.2 “Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care” (T6.2), and Task 6.3 “Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs” (T6.3). In addition, the SME-centric Workshop is related to the activities of Task 7.4 “SENTINEL ecosystem building: Continuous engagement of technology providers, SMEs/MEs” (T7.4) in communicating the project results to a variety of enterprises and expanding the SENTINEL ecosystem. The workshop analysis from this perspective is reported in the deliverable D7.6 “Ecosystem building & SMEs engagement report - final version” [2].

Nevertheless, the current report aims to analyse the overall SENTINEL platform's assessment and impact, providing validation and verification outcomes and the final assessment of the respective KPIs/KRs related to SENTINEL evaluation to measure the project's success. Thus, D6.3 is highly associated with the outcomes of Task 6.4 “Evaluation and Impact Analysis” activities (T6.4). Concerning the verification processes, the current deliverable is closely associated with the activities of Task 5.3 “From the prototype to the final solution” (T5.3), as the latter provides feedback on the verification results concerning the internal testing procedures conducted in M33 by the project's technical partners and reported in the deliverable D5.7 “Best practices for maintaining and operating system in long term - TRL 7” [3]. Conversely, the evaluation outcomes of the current deliverable, provided by the workshop end-users, give input to the works of Task 5.3, considered in the platform's final technical refinements and maintenance/operational activities where possible. In addition, the feedback received from the SME end-users could be considered in the SENTINEL platform technical enhancements and improvements beyond the project's termination to raise its exploitation aspects defined in Task 7.3 “Exploitation and standardisation activities and best practices towards a holistic privacy-by-design European” (T7.3). Moreover, the current deliverable indicates how the SENTINEL user-centric approach and the experimentation protocol of Task 6.1 “SENTINEL experimentation protocol alignment and pilots' setup” (T6.1) is applied to the project's evaluation processes.

1.2 Structure of the document

The current deliverable is structured as follows:

- Section 1 gives an overall presentation of the current document.
- Section 2 presents an overview of the SENTINEL experimentation and evaluation processes conducted to test and evaluate the SENTINEL platform within the scope of WP6 activities.
- Section 3 provides details on the preparations and execution of the SENTINEL project's final SME-centric Workshop, covering enterprise recruitment, communication strategies,

event setup, and the structure of the workshop, including registration, demonstrations, and participants' feedback.

- Section 4 analyses the validation and verification processes for the SENTINEL platform, assessing its functionalities and performance metrics to ensure alignment with SMEs' requirements and regulatory standards, and provides insights into its effectiveness and areas for improvement.
- Section 5 summarises the overall success and challenges faced during the implementation and evaluation phases, highlighting the effectiveness of the SENTINEL platform in meeting its objectives.

1.3 Intended readership

The deliverable is intended for the consortium members and stakeholders external to the project, primarily addressed to SMEs and MEs since the dissemination level of D6.3 is public. This document is a guide to both consortium members and external readers to understand the SENTINEL overall evaluation and impact analysis.

2. SENTINEL Evaluation Aspects

The current chapter incorporates all SENTINEL evaluation aspects identified to assess the SENTINEL platform. Section 2.1 briefly describes the SENTINEL experimentation protocol and the application of the user-centric evaluation methodology to test and evaluate the SENTINEL platform. Section 2.2 presents the design of personas considered in the platform's technical works, whereas Section 2.3 describes the updates on the SENTINEL User Evaluation Questionnaire to capture the needs of the final SME-centric Workshop evaluation (M33).

2.1 SENTINEL user-centric evaluation

This section presents an overview of the experimentation processes undertaken for testing and evaluating the SENTINEL platform in the context of WP6 activities.

2.1.1 Overview of the SENTINEL experimentation process

The experimentation process followed the SENTINEL experimentation protocol selected under T1.3 and refined under T6.1 (reported in deliverables D1.3 [4] and D6.1 [5], respectively). The SENTINEL experimentation protocol prescribes the entire experimentation process followed by the project, which relies on a twofold purpose of verification and validation to test and evaluate the SENTINEL platform both from technical and business/socio-economic perspectives. Moreover:

- the *verification process* aimed at testing and evaluating the SENTINEL platform, its components (SENTINEL core components, SENTINEL plugins), functionalities and system performance, engaging technology providers as evaluators via conducting verification tests in a security laboratory environment (technical evaluation);
- the *validation process* aimed at aligning the SENTINEL platform with the specific SMEs/MEs requirements addressing evaluation in real-life conditions by SMEs/MEs users (non-technical evaluation).

The experimentation process was built on the collaboration of both technical partners and SME/ME stakeholders, conducted as an iterative and incremental procedure of the SENTINEL experiments aiming to:

- i) reflect revisions of the pilot cases, due to the refinement of pilot requirements, goals, and expectations;
- ii) be aligned with the technical updates and development progress of the SENTINEL platform.

The SENTINEL experimentation protocol contained two main phases:

- the Definition phase (consisting of the *scoping* and *planning* phases) sets the boundaries of the experiments and defines goals, tasks, participants, quality metrics, and benchmarks to be measured where applicable (identified in D1.3, analysed in D6.1).
- the Operational phase (including the *execution* and *analysis* phases) concerns the performance of verification tests by technical partners and implementation of real-life experiments in the SENTINEL platform by SME/ME end-users (SMEs/MEs' trials execution via pilot experiments) along with the conduction of the SENTINEL platform

assessment through evaluation means. In addition, during this phase, the evidence gained was interpreted either in a quantitative or qualitative approach, producing analytics and specifying the evaluation outcomes (cf. MVP evaluation in D6.1, pilot evaluation in D6.2 [1], final pilot evaluation and overall results of the current deliverable).

2.1.2 Overview of the SENTINEL evaluation process

The SENTINEL evaluation process followed the User-Centric Evaluation Methodology, defined under the works of T6.1, presented in D6.1 [5]. The methodology complements the SENTINEL experimentation protocol (cf. 2.1.1) in defining in detail the exact evaluation process undertaken by the project to assess the SENTINEL platform throughout its development lifecycle, generate evidence, and produce results.

The SENTINEL evaluation process comprised the experimentation protocol phases, described in Section 2.1.1, applying all the identification, planning, execution, and analysis procedures as thoroughly prescribed in the User-Centric Evaluation Methodology of D6.1.

Concerning the *identification* and *planning* procedures (see pre-pilot phase in Figure 1), to define the use cases and types of experiments for testing and evaluating the SENTINEL platform, we considered the feedback elicited from SMEs/MEs after implementing the SCORE Requirements Engineering (RE) approach (cf. D1.1 [6]) in relation with the SENTINEL offerings (under the works of tasks T1.1 and T1.2 during M1-M6), ending up with two focused pilot cases engaging experiments of sectorial Processing Activities (PAs) related to genomics and childrencare, and SMEs generic type of experiments (cf. SENTINEL Pilots in D6.2 [1] and Section 3.3 of the final SME-centric Workshop description of the current document). The pilot cases and the respective PA experiments were refined before the Pilots' execution considering the SENTINEL technical progress towards the project's objectives and stakeholders' needs (cf. D6.1). To evaluate the SENTINEL platform, an online User Evaluation Questionnaire was prepared and provided to the SMEs/MEs end-users after conducting the trials, which was updated whenever needed to reflect the pilot requirements and the SENTINEL platform technical updates. An additional evaluation form was prepared to receive further feedback from the end-users towards UI/UX perspectives (cf. MVP evaluation in D6.1, CG Pilot evaluation in D6.2). Specific timeplans set out and followed by the SENTINEL Pilots (see Figure 1). Moreover, quality metrics and benchmarks were identified to measure the validation and verification results, which outcomes are reported in the current deliverable (cf. Section 4.1.1 and 4.1.2). In addition, the project Key Performance Indicators (KPIs)/ Key Results (KRs) related to the SENTINEL evaluation process were identified and monitored following the SENTINEL KPIs/KRs approach, presented in D6.1, from the beginning of the project until its completion (cf. Section 4.3.2).

The *pilot execution* and *validation* procedures (business and socio-economic evaluation) supported some preparatory pilot activities. Such activities included a recruitment process monitored by UNINOVA and Digital Innovation Hubs (DIHs), which engaged several external SMEs to participate in the Minimum Viable Product (MVP) evaluation (cf. D6.1), DIH Pilot evaluation (cf. D6.2) and final pilot event, i.e., the SME-centric workshop (cf. Section 3.2 of the current deliverable). Other preparatory activities contained logistics procedures and the creation of SENTINEL User instructions given to end-users before committing to the trials. The SENTINEL platform was tested and evaluated at distinct periods of technical achievements (cf. Figure 1): after the MVP release (M12), an initial execution was performed (pre-pilot phase); after the

SENTINEL Full-Featured version (FFV) release (1st prototype) three Pilots were conducted (i.e., the CG Pilot, TIG Pilot, DIH Pilot – pilot phase); after the Final Product release (2nd prototype) a final pilot event occurred (i.e., the final testing and validation) engaging both internal and external SMEs/MEs and members of the Executive Advisory Board (EAB). Before the end-user trials execution, a demonstration workshop was carried out for each Pilot (i.e., the CG Demonstration Workshop in M22, the TIG Demonstration Workshop in M24, the DIH Demonstration Workshop in M28 and the SME-centric Workshop in M33, depicted in Figure 1). The demonstration workshops aimed at illustrating the SENTINEL project idea, the GDPR compliance and cybersecurity concepts and SMEs key-challenges along with the platform's capabilities and test cases. The three digital demonstration workshops were recorded with participants' consent and disseminated to pilot end-users to utilise them as additional training material. Overall, 29 end-users from 2 internal and 25 external SMEs/MEs and 3 EAB members conducted trials and evaluated the SENTINEL platform (via online questionnaire and UI/UX evaluation forms as described previously), ranging from the MVP evaluation until the final pilot event. During the trials' execution, 12 different PAs were utilised in the experiments. The end-users feedback was a continuous effort in the SENTINEL platform technical progress until the project termination to address SME user needs. Specifically, the input received from the MVP evaluation was considered in the FFV (1st prototype) development, the three Pilots evaluation feedback was considered in the Final Product (2nd prototype) development, whereas the input gathered from the SME-centric Workshop of M33 was considered, where possible, in the final refinements for maintenance and operational procedures of the final product, carried out until M36.

The verification procedures included verification tests of the platform conducted in a security laboratory environment by technical partners throughout the SENTINEL platform's development lifecycle. Moreover, under the activities of T5.3. the project partners were requested in M33 to self-assess the SENTINEL platform (see internal SENTINEL platform testing in D5.7 [3]). The outcomes of this internal testing were considered in the platform technical refinements before conducting the final pilot event (SME-centric Workshop of M33).

To analyse the evidence gained from the overall evaluation, we adopted a hybrid approach encompassing quantitative and qualitative results. Specifically, the pilot evaluation results (business and socio-economic evaluation) were presented in analytics (e.g. statistic pie and column charts). To assess the SENTINEL platform towards the identified validation metrics and benchmarks (cf. Section 4.1.1), the pilot evaluation results were considered. To assess the SENTINEL platform towards the specified verification quality metrics and benchmarks (cf. Section 4.1.2), the technical partners' verification tests were considered. The analysis continued assessing whether the SENTINEL platform capabilities covered the business (SMEs) and application (technical) requirements identified under tasks T1.1 and T1.2 (cf. Section 4.2), considering the evaluation outcomes derived from different perspectives (e.g., the questionnaire results, the SENTINEL platform evaluation towards specific validation/verification variables, the outcomes from the technical tests conducted, etc.). The KPIs/KRs related to SENTINEL evaluation were assessed as a continuous monitoring process reflecting all relevant evaluation aspects and presented in a quantitative approach along with textual justification. The final KPIs/KRs assessment is reported in Section 4.3.2.

The following Figure 1 displays a timeline of the SENTINEL platform technical development progress towards the pilot operations, the project's phases (i.e., Baseline M1-M6, Innovation M7-

M18, Demonstration M19-M30, Consolidation M31-M36) and Milestones (MS1-MS6), clarified in the project’s Grant Agreement (GA). The platform’s technical progress and testing verification activities are illustrated on the upper side of the image, whereas WP6 pilot validation activities are highlighted at the bottom side of the image.

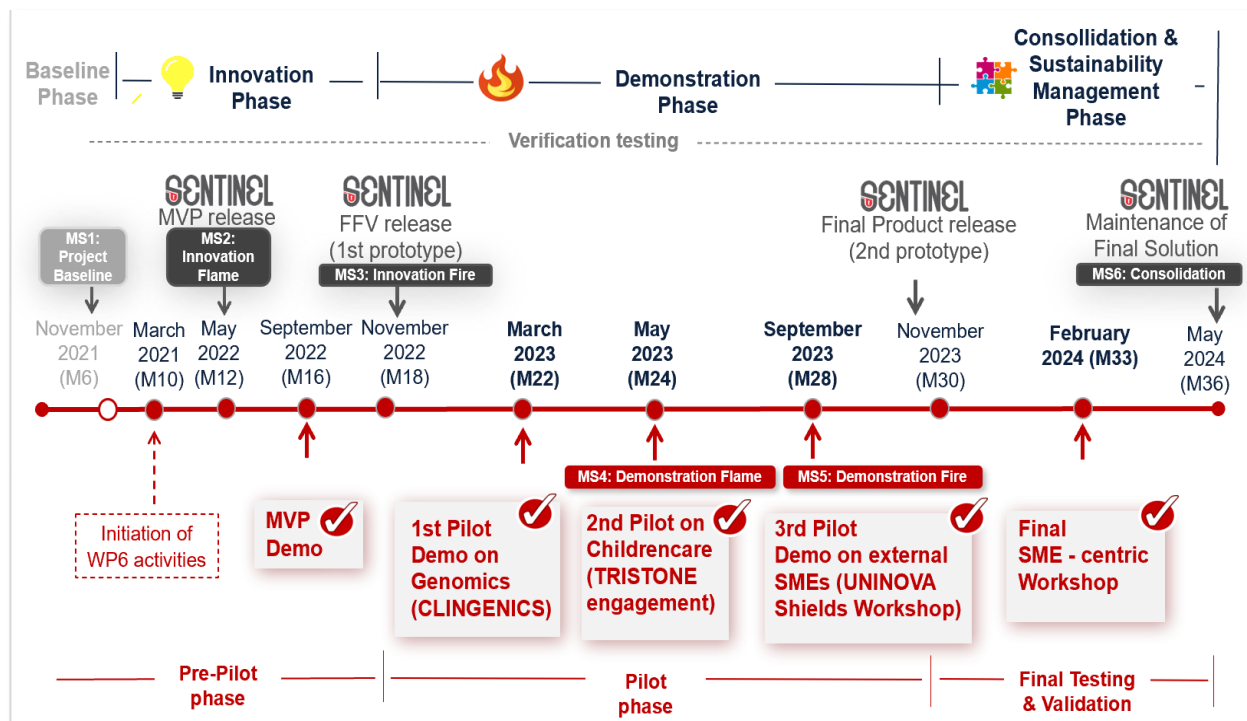


Figure 1. Overview of SENTINEL testing and evaluation activities towards project’s technical achievements

2.2 The persona-based approach

To achieve a better alignment between the user needs, expectations and experience towards the SENTINEL platform, a persona-based approach has been used. Personas are abstract representations that describe the goals, skills, and interests of the targeted users of the SENTINEL platform.

This approach was used during the SENTINEL testing and validation phases, for assisting the design of user experiments (user flows) and for defining appropriate user help that best suits the requirements of the diverse groups represented by the personas.

To facilitate the data collection and identification of user personas, we have utilised a template based on the PATHY technique [7] consisting of six fields (Who, Context, Technology experiences, Problems, Needs, and Existing solution) that describe the persona’s characteristics, the environment they engaged in, their technical proficiency, the problems they are facing and how they want to solve them, and current problem-solving options.

The main instrument for collecting information from end-users was the user evaluation questionnaire, filled by SMEs/MEs end-users participating in the three (3) Pilots (i.e., the TIG, CG, and DIH Pilots), during the testing and validation of the SENTINEL FFV version (cf. D6.2).

Analysis of the data collected has revealed several commonalities between user attributes based on their technology expertise and needs, grouped into 5 user personas engaging specific SENTINEL functionalities addressing the respective user requirements (cf. D6.2).

This association of user personas to required SENTINEL functionalities has guided the refinement of the user interface (Dashboard) and help wizard (SENTINEL Wiki) for the final version of the SENTINEL integrated solution (2nd prototype – Final Product). In addition, it assisted in the design of the experiments workflow and evaluation questionnaire utilised in the final SME-centric Workshop of M33 (cf. Section 3).

In particular, the experimental workflow focused on the requirements of the two user personas mainly represented among the workshop participants: (a) SME administrative staff discovering GDPR compliance and (b) SME IT personnel responsible for achieving GDPR compliance (see Table 1).

Table 1. User personas of the SME centric Workshop and their requirements

Persona description	Percentage of Participants (100%)	Required SENTINEL functionalities
SME administrative staff discovering GDPR compliance	66,5%	Creation of PAs ¹ , Use of ROPA ² , Acquire policy recommendations (Data protection recommendations)
SME IT personnel responsible for achieving GDPR compliance	29,5%	Creation of PAs, Use of ROPA, GDPR Compliance Self-Assessment (CSA), Data Protection Impact Assessment. Acquire policy recommendations (All recommendations)

2.3 Updates and enhancements on SENTINEL User Evaluation Questionnaire

To develop the questionnaire of the SME-centric Workshop, we relied on the continuous iterative experimentation process (defined in D6.1 and summarised in Section 2.1 of the current report) of updating the evaluation instruments to address the ad hoc SMEs needs as the project technical developments became more mature. In this vein, enhancements to the SENTINEL User Evaluation questionnaire were provided to ensure the alignment of end-users requirements with the SENTINEL technical achievements and the project’s objectives. To meet this goal, we scrutinised the evaluation objectives of the final workshop.

¹ Processing Activities

² Registry Of Processing Activities

The questionnaire aimed at gathering feedback from usability, satisfaction, learnability, UI/UX, user acceptance, time efficiency, and business performance perspectives among various SMEs/MEs deriving from different sectors. An additional objective was to retrieve input from end-users after communicating the project results and examine whether the platform meets the SMEs needs. The feedback received could assist in the final technical refinements of the platform until the project termination.

To revise and update the questionnaire, we also studied the user personas identified already from the previous pilot evaluation (cf. D6.2) depending on the level of the users' expertise on GDPR compliance and cybersecurity, and their organisation-specific needs for compliance, according to their status. Considering the identified personas, we selected four (4) SENTINEL representative use cases that could better respond to the generic type of PA experiments undertaken by the different SMEs/MEs, as depicted below:

- Platform registration – Organisation Profile
- Develop a Processing Activity (PA) – Commit to ROPA
- Execute GDPR CSA
- Acquire Recommendations

These use cases were mapped to the SENTINEL User Evaluation Questionnaire, focusing on questions that better address the specific quality metrics presented above to meet the workshop evaluation objectives. Considering that the workshop intended to be physical with a specific duration allocated to evaluate the SENTINEL offerings, we selected the most critical questions from the previous version of the SENTINEL User Evaluation Questionnaire and updated where needed to address the current evaluation requirements. In addition, as described in Section 1 of this report, the workshop evaluation aimed at profiling end-users and identifying further personas to build a community ecosystem around the project's results as part of T7.4 activities. Therefore, updates of the questionnaire included the addition of questions to cover T7.4 objectives and understand the end-users' level of maturity with regards to the adoption and investment in Personal Data Protection (PDP) and GDPR compliance assessment tools (reported in D7.6 [1]). Eventually, we came up with the following high-level structure, which supported the creation of an online User Interactive Questionnaire that was given to the attendees to be filled gradually in an interactive manner after completing the demonstration and testing of its specific use case, as stated above:

Part I: Participants Introduction (comprising 8 questions)

- Profiling (3 questions)
- Existing solutions and resources (2 questions)
- Needs and expectation (3 questions)

Part II: SENTINEL hands-on training (comprising 25 questions)

- **User Satisfaction** (12 questions) with respect to:
 - Platform registration-Organisation Profile (2 questions)
 - Develop a Processing Activity (PA) (2 questions)
 - Commit to ROPA (2 questions)
 - Execute GDPR CSA (3 questions)

- Acquire Recommendations (3 questions)
- **Overall evaluation** (11 questions)
 - User Interface/User Experience (UI/UX) (3 questions)
 - Business Performance (8 questions)
- **Express end-user opinion and additional comments** (2 questions)

The questionnaire was divided into two main parts to follow the workshop’s flow. In addition, the 1st part, which indicates informative content of the organisation and the respective end-user, is connected with the activities of T7.4 on profiling the end-users and identifying further personas to build a community-an ecosystem around the project’s results. Thereby, the 1st part of the questionnaire is described in detail in D7.6 [1], whereas an extensive analysis of the 2nd part of the questionnaire results is presented in this report (cf. Section 3.4) as it reflects questions aimed at gathering end-users feedback after experiencing the hands-on training and testing the SENTINEL platform under the scope of real-life scenarios.

The following Table 2 illustrates the mapping of the personas’ characteristics, identified in D6.2 [1], with the questions of the revised SENTINEL User Evaluation (interactive) Questionnaire.

Table 2. Mapping of personas characteristics with questions of the user evaluation interactive questionnaire

Template field	Relevant question(s)
<i>How</i>	Please identify your level of knowledge regarding GDPR (General Data Protection Regulation).
<i>Technology Expertise</i>	What is your area of expertise?
<i>Existing Solution and resources:</i>	Does your organisation use security/privacy policies software/services for data protection compliance? If yes, what is the approximate annual cost?
<i>Needs/Expectations</i>	Did you find SENTINEL a potential solution to be implemented within your company? Does your company plan to invest on such tools/services in the future? Which of the following SENTINEL services would be more useful to your business needs? Do you anticipate that exploiting SENTINEL could potentially increase your market share in the coming years? If so, to what extent?

3. SME-centric Workshop for Demonstrating SENTINEL solution

This section outlines the objectives, preparatory activities, and the actual demonstration of the SME-centric Workshop. Furthermore, it provides detailed information on the experiment objectives, the SENTINEL use cases supporting the experiment, and its workflow.

3.1 Workshop objective

The SENTINEL Final Product (2nd prototype) was released in M30 considering in its technical development the valuable feedback gathered by internal and external SME end-users from the three digital Pilots, which occurred during the project's Demonstration Phase (M19-M30). To utilise the project's final product in real-world scenarios and raise its credibility and acceptability, a final pilot event was organised in Greece (M33). It aimed at communicating face-to-face the main achievements of SENTINEL and its innovation capacities to different types of SMEs/MEs representing various business sectors and elaborating with this physical interaction how the SENTINEL offerings can add value to the SMEs' core business activities related to personal data protection and cybersecurity.

In the frame of T6.3, additional external SMEs/MEs have been engaged and invited to test the SENTINEL offerings through a generic experiment, addressing all use cases of the SENTINEL platform. The workshop's objective is directly linked with iKPI-11.1 "At least 20 third-party entities (SMEs/MEs) directly using SENTINEL's tools/services", iKPI-12.1 "At least four (4) start-ups and spin-offs boosted exploiting SENTINEL security services", and KR-6.3 "At least six (6) third-party collaborations to be established for further applicability verification". Apart from testing the SENTINEL functionalities the aim was to assess the platform under specific evaluation criteria, such as usability, performance efficiency, user satisfaction, UI/UX, and time efficiency via an interactive questionnaire. The feedback collected from the workshop participants intended to facilitate the final technical refinements of the SENTINEL platform operated until the project's termination in M36 (T5.3).

3.2 Workshop overview: preparations, setup, and demonstration

This section presents the concluding pilot event to test and evaluate the SENTINEL Final Product (2nd prototype). The following sections incorporate the workshop's preparatory activities, enterprise recruitment process, logistics, and workshop demonstration.

3.2.1 Enterprises recruitment

The engagement of additional companies not only aided in demonstrating the scalability, reliability, and maintainability of the SENTINEL platform but also helped to be aligned with SENTINEL's goal of democratising access to high-end digital security tools for all businesses, regardless of their size, scope, and financial capabilities. Moreover, expanding into additional business sectors could provide strategic advantages in terms of credibility and acceptability of the SENTINEL platform. In this context, the final SENTINEL SME-centric Workshop was realised. The recruiting process of workshop participants was performed by leveraging the SENTINEL partners' channels and networks. The recruitment process involved the creation of informative and compelling materials that explain the value proposition of the SENTINEL platform for SMEs.

This encompassed clear information on security, privacy, and data protection feature, which are the core concept of the SENTINEL project.

3.2.2 Communication

The communication and dissemination strategy for the event aimed at attracting SMEs using SENTINEL's digital channels. An official event poster was created, including information, the agenda, and a QR code for the printed version. The poster (Figure 2) was distributed on the project's social media platforms, via email to the project partners' network of contacts, and on the SENTINEL website³.



Figure 2. SENTINEL final SME-centric Workshop poster and social media post

The registration process⁴ was conducted online through a form (Figure 3) to gather basic initial data. We collected email addresses, names, company names, and obtained authorization for data.

³ SME-centric Workshop announcement on the SENTINEL project's website: <https://sentinel-project.eu/news-events/SENTINELFinalSME-centric-Workshop/>

⁴ SENTINEL SME-centric workshop Registration link: https://docs.google.com/forms/d/e/1FAIpQLScHVpcoV8mCFZhgJb-4YDfVXM7bZ6Sm0JiMGjlcEtQ_UdEGUQ/viewform



The image shows a registration form for the SENTINEL SME-centric workshop. At the top, the word "SENTINEL" is written in a large, bold, grey font. The letter "S" is stylized with a red shield containing a white keyhole icon. Below the title, the text reads: "The SENTINEL project invites you to participate in a workshop on GDPR compliance, cybersecurity, privacy and personal data protection for SMEs. The workshop will be held at the Golden Age Hotel of Athens on the 27th of February, from 09:30 - 14:30 EET." Further down, it specifies the event location: "Event location: 57 Michalakopoulou Street, 115 28 Athens Greece". At the bottom, it says: "Please, register your attendance in the form below."

Figure 3. Registration form

The final SENTINEL SME-centric workshop concluded the testing and validation phase of SENTINEL the platform with the participation of external SMEs. The testing and validation of the platform was a crucial step for both SENTINEL, and the SMEs, to ensure that they are effectively safeguard their data and comply with GDPR [8].

3.2.3 The SME-centric Workshop

The SME-centric Workshop welcomed companies from the private sector, mostly Small and Medium-sized Enterprises (SMEs), including spin-offs, startups, and large enterprises, without any domain restrictions. Almost forty (40) people in total participated comprising external entities, the consortium partners and EAB members. It was an interactive workshop with a friendly environment for all the participants.

As delineated in the workshop's agenda in Table 3, the entire duration of the event was five (5) hours, including multiple sections, such as a brief introduction to the SENTINEL project, general overview of the workshop scope and its purpose, SENTINEL key concepts, and hands-on demonstration on key functionalities of the platform. To streamline the testing process, the hands-on demonstration was divided into four (4) core parts giving the workshop attendees enough time to test the SENTINEL platform functionality-by-functionality (for further details see Section 3.3.2). After each testing stage, the attendees were invited to express their impressions. The workshop gathered eleven (11) new companies' representatives in addition to SENTINEL internal end-users. The latter were participants from CG and TIG companies (including Sportif and Dimensions

Care). Furthermore, EAB members and project partners of SENTINEL participated in the workshop. Table 4 presents the list of external companies.

Table 3. SENTINEL final SME-centric Workshop agenda

27 Feb 2024 SME-centric workshop Moderator: ITML		
09:30 - 10:00	Registration and coffee	
10:00 - 10:05	Opening & Welcome	ITML
10:05 - 10:20	The SENTINEL project: Overview	ITML
10:20 – 10:30	Participants introduction <ul style="list-style-type: none"> ○ Interactive Questionnaire (PART I) 	UNINOVA – Attendees
10:30 - 10:50	SENTINEL key concepts (20 min.)	LIST
10:50 – 11:20	SENTINEL Platform registration - Organisation Profile <ul style="list-style-type: none"> ○ Illustrate functionalities. ○ End-users testing ○ Interactive Questionnaire (PART II) 	INTRA, UNINOVA, Attendees - technical partners' support
11.20 – 12.10	Develop a PA - Commit to ROPA (50min.) <ul style="list-style-type: none"> ○ Illustrate functionalities. ○ End-users testing ○ Interactive Questionnaire (PART II) 	IDIR, UNINOVA, Attendees - technical partners' support
12.10 – 12.20	Coffee Break	
12.20 - 12:40	GDPR CSA – Acquire Recommendations <ul style="list-style-type: none"> ○ Illustrate functionalities. ○ End-users testing ○ Interactive Questionnaire (PART II) 	ITML, UNINOVA, Attendees - technical partners' support
12.40 - 13:00	SENTINEL Cybersecurity tools End-users testing	Attendees - technical partners' support
13:00 - 13:30	Overall evaluation – wrap up <ul style="list-style-type: none"> ○ Interactive Questionnaire (PART II) ○ Q&As 	UNINOVA, Attendees ALL
13:30 - 14:30	Lunch	

Table 4. The list of SMEs participated in the final SME-centric workshop

SME name	Sector
TREDIT	Consultants for Transport, Development, and Information Technology
Zelus	IT company
DRAXIS	Environmental IT
DNA Creative	Web, mobile and software application
Dienekes	IT, spin-off
Cyberalytics	Cyber Security
PRAXI Network	Consulting / Technology Transfer
Watergate	Web Development, Bespoke IT Systems
Security Labs Consulting (SLC)	Cybersecurity, Maritime Transport
OCEANIC MARINE SERVICES	Shipping Services
Aktor (Intrakat Group)	Construction

3.3 The SENTINEL experiment of the SME-centric Workshop

The current section highlights the purpose of the SENTINEL experiment, the experiment's workflow, and the actual SENTINEL use cases implemented by the workshop's end-users to test and evaluate the SENTINEL platform.

3.3.1 Purpose of the SENTINEL experiment

The purpose of the SENTINEL experiment was to determine the usability of the SENTINEL platform by SMEs. Usability is a measure of how easy and effective it is for an actor to use a system to achieve their desired goals. Usually, usability testing focuses on the user's experience when interacting with a system.

The aspects of usability assessed during the experiment are the following:

- Ease of use: To what extent the platform is intuitive to use.
- Performance Efficiency: How the platform allows the user to complete tasks quickly and efficiently.
- Learnability: Is the platform easy to learn, even for users with no prior experience with the platform?
- User satisfaction: Does the platform satisfy its users?

In addition, the SENTINEL experiment aimed to scrutinise the user acceptance of SENTINEL towards leveraging the enterprises' processes related to personal data protection handling, storage and retention, and cybersecurity management. It also targeted at evaluating the SENTINEL platform upon business performance characteristics, such as cost/effort reduction and resource utilization with respect to enterprises' needs.

The workshop end-users aimed at conducting generic experiments of Processing Activities (PAs)⁵ pre-defined in the SENTINEL platform. Nevertheless, the end-users had the opportunity to create their organisation PAs.

3.3.2 SENTINEL use cases and experiment workflow

The last SENTINEL experiment aimed at testing a set of SENTINEL functionalities tailored to different user personas identified from the three Pilots, following the SENTINEL persona-based approach (cf. D6.2 [1]). These personas have been developed based on the users' needs, type, and level of knowledge and technology expertise in GDPR compliance and cybersecurity. In this light, the SENTINEL experiment was divided into four (4) main use cases:

- SENTINEL Platform registration – Organisation Profile.
- Develop a Processing Activity (PA) – Commit to ROPA⁶.
- GDPR CSA – Acquire Policy Recommendations.
- SENTINEL Cybersecurity tools.

⁵ According to GDPR [8], Processing Activity is considered a wide range of operations performed on personal data by manual or automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction of personal data.

⁶ The SENTINEL Registry Of Processing Activities (ROPA) addresses the Record Of Processing Activities requirement of GDPR [8] (cf. Art. 30)

The first three use cases reflect users either seeking for awareness of or being involved in GDPR compliance processes whereas the latter use case refers to users either willing to gain a further education on privacy and cybersecurity or dealing with information security and personal data protection issues. The SENTINEL four (4) high level use cases encompass a set of actions undertaken to accomplish each use case. Depending on the user's expertise on GDPR compliance and cybersecurity, as stated above, the Workshop's end-users were requested to implement these actions and fulfil each use case. A low-level brief description of the SENTINEL uses cases, and their workflow are depicted hereafter. Further analysis of this set of actions to accomplish the SENTINEL user journey can be found online in the SENTINEL Wiki⁷, representing a comprehensive guide for navigating and maximizing the capabilities of the SENTINEL platform. Further details are available in D5.7 [3].

- **SENTINEL Platform registration – Organisation Profile.**
 - **SENTINEL Platform registration.** The user visits the SENTINEL platform through the link <https://platform.sentinel-project.eu> and registers/signs in to his/her account in the SENTINEL platform as indicated.
 - **Organisation Profile.** It engages basic information about user's business (e.g., the trading name, business sector, the business country origin and size), information on responsible persons of the organisation for personal data protection, for populating organisation's generic cyber assets profile and creating an asset inventory (ascribed to IT/cybersecurity professionals or experts), for reporting information on organisation's-wide measures implemented for GDPR compliance and managing personal data and potential data breaches.

Figure 4 illustrates the SENTINEL registration/login environment.

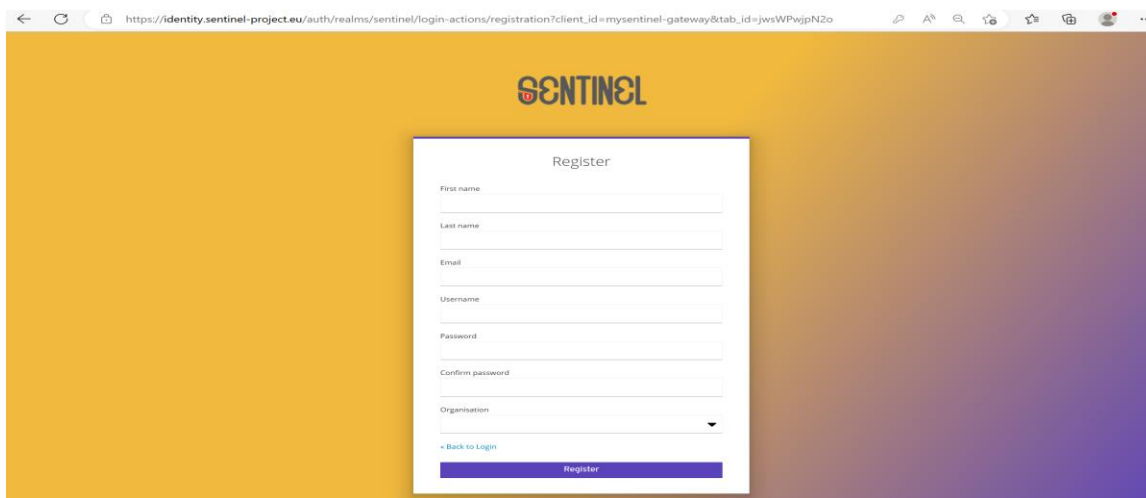
The image shows a web browser window displaying the SENTINEL registration page. The page has a yellow and purple gradient background. At the top center, the 'SENTINEL' logo is visible. Below the logo is a white 'Register' form. The form contains the following fields: 'First name', 'Last name', 'Email', 'Username', 'Password', 'Confirm password', and 'Organisation' (a dropdown menu). At the bottom of the form, there is a link for '< Back to Login' and a blue 'Register' button. The browser's address bar shows the URL: 'https://identity.sentinel-project.eu/auth/realms/sentinel/login-actions/registration?client_id=mysentinel-gateway&tab_id=jwsWPwjpn2o'.

Figure 4. SENTINEL registration environment

Figure 5 shows the Organisation Profile environment.

⁷ SENTINEL Wiki pages: <https://wiki.sentinel-project.eu/>.

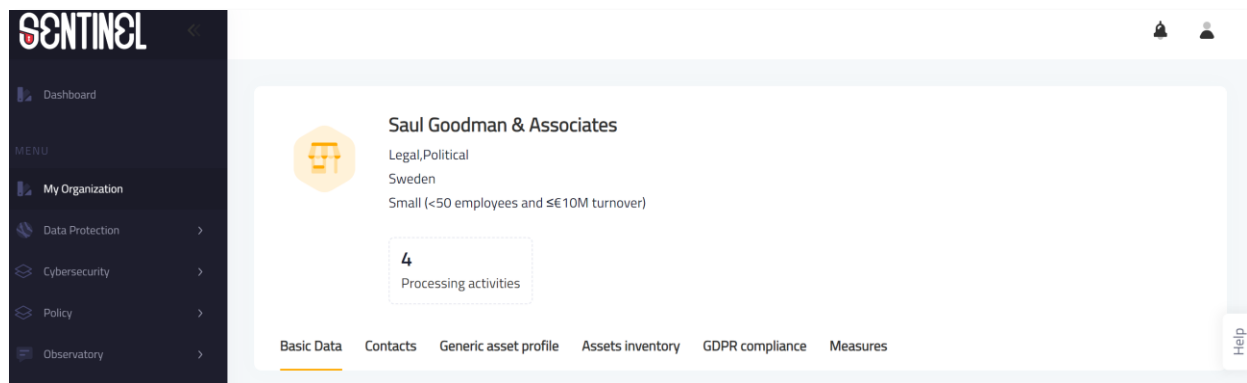


Figure 5. SENTINEL My Organisation

- **Develop a Processing Activity (PA) – Commit to ROPA.**
 - Develop a PA. A part of profiling the organisation refers to adding/editing/viewing information on its personal data processing activities distinguished into nine (9) discreet data groups related to
 - PA identity and basic data
 - PA purpose
 - Data subjects
 - Data types handled and sensitive data reporting
 - data Recipients
 - Risks
 - GDPR compliance (i.e., consent, rights and personal data lifecycle management)
 - cyber assets associated with the PA
 - Organisational and Technical Measures (OTMs) pertaining to the specific PA.

The following Figure 6 illustrates a set of actions to accomplish this use case (further explained in SENTINEL Wiki).

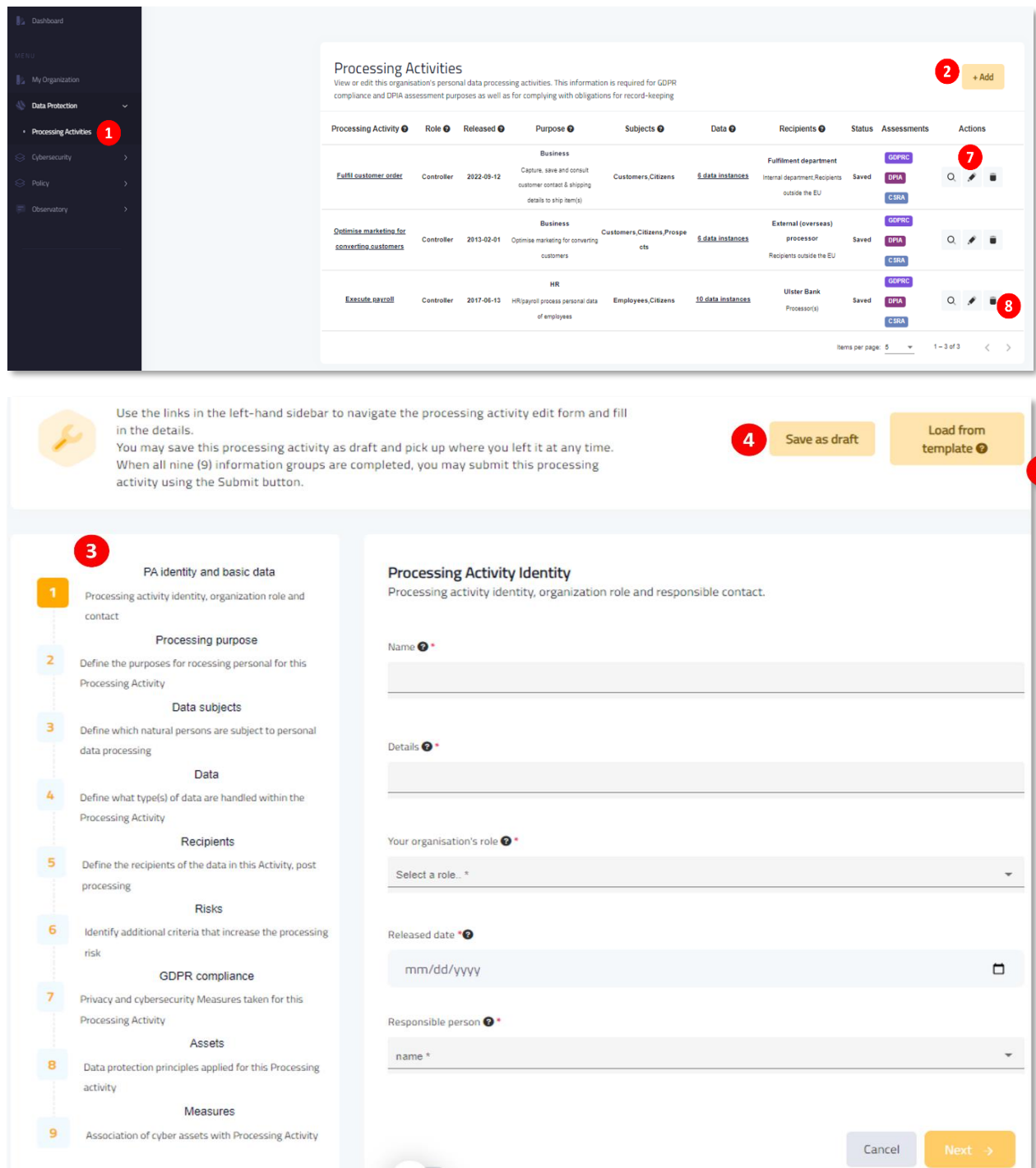


Figure 6. Create/edit a Processing Activity

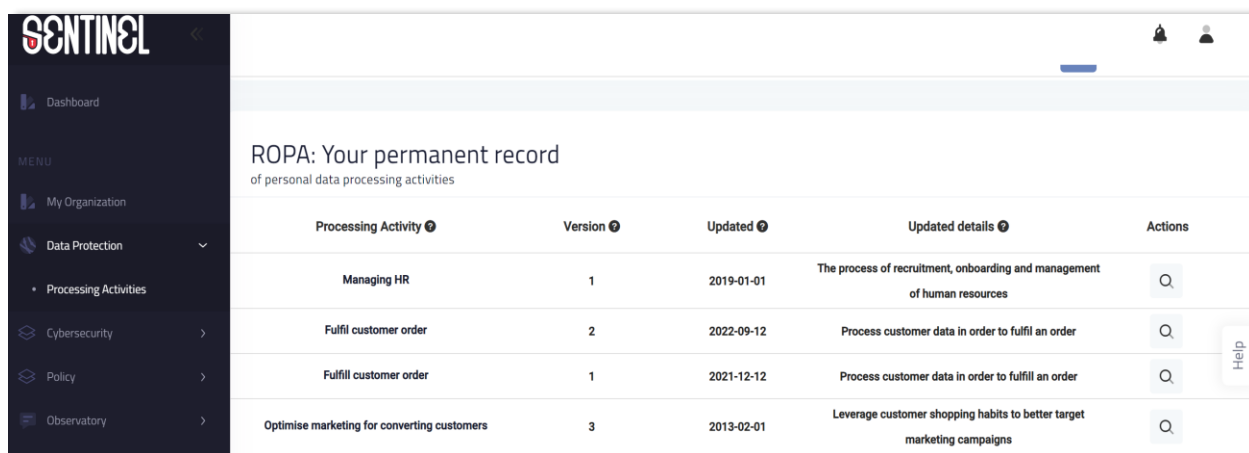
- Commit to ROPA. It refers to creating permanent records of the registered PAs in the Registry of Processing Activities (ROPA)⁸. Maintaining a ROPA helps

⁸ ROPA: a detailed, permanent, immutable and auditable record which outlines the data processing activities carried out by an organisation.

organisations demonstrate compliance with the GDPR's accountability principle (cf. Art. 30 of the GDPR), which requires organisations to be able to demonstrate how they comply with data protection principles. In addition, it serves as a tool for organisations to have an overview of their data processing activities and ensure transparency and accountability in the handling of personal data. The current use case embraces the following set of actions:

- Creating a ROPA entry / committing a PA to the ROPA
- Viewing a ROPA entry
- Exporting a ROPA entry
- Marking a PA in the ROPA as inactive

Figure 7 below illustrates indicative examples of ROPA permanent records.



The screenshot shows the SENTINEL interface with a sidebar menu on the left containing 'Dashboard', 'My Organization', 'Data Protection', 'Processing Activities', 'Cybersecurity', 'Policy', and 'Observatory'. The main content area is titled 'ROPA: Your permanent record of personal data processing activities'. It displays a table with the following data:

Processing Activity	Version	Updated	Updated details	Actions
Managing HR	1	2019-01-01	The process of recruitment, onboarding and management of human resources	Q
Fulfill customer order	2	2022-09-12	Process customer data in order to fulfill an order	Q
Fulfill customer order	1	2021-12-12	Process customer data in order to fulfill an order	Q
Optimise marketing for converting customers	3	2013-02-01	Leverage customer shopping habits to better target marketing campaigns	Q

Figure 7. SENTINEL ROPA

The first two use cases constitute the data entry phase intending to capture all the data necessary for self-assessment and for producing tailored policy recommendations, as well as for raising users' cyber awareness and GDPR requirements and compliance standing.

- **GDPR CSA – Acquire Policy Recommendations.**
 - **GDPR CSA.** The GDPR Compliance Self-assessment (CSA) allows the user to determine whether OTMs implemented to meet data protection requirements are complete, appropriate, effective, and demonstrable. It engages a set of actions. Depending on the information provided by the user in the PA (GDPR Compliance group), SENTINEL will determine and assign a “compliance rating” (i.e., Record Management (RECORD)/ Personal Data Lifecycle Management (PDLM)/ Management of individuals rights (RIGHTS)/ Management of individuals consent (CONSENT)) of the under-examination PA.

Figure 8 delineates the ‘GDPRCSA’ tab found in each PA allowing the user to perform a GDPR Compliance Self-assessment whereas depicts the assessment results of organisation’s under-examination PAs. In addition, the SENTINEL platform provides Data Protection Impact Assessment (DPIA) which should be conducted in case a PA is ranked with high risk (cf. art. 35 of GDPR). Since most

of the end-users had limited expertise on topics of GDPR and personal data protection, this service was available to be explored by the end-users optionally and it is not considered as a SENTINEL use case of the current workshop.

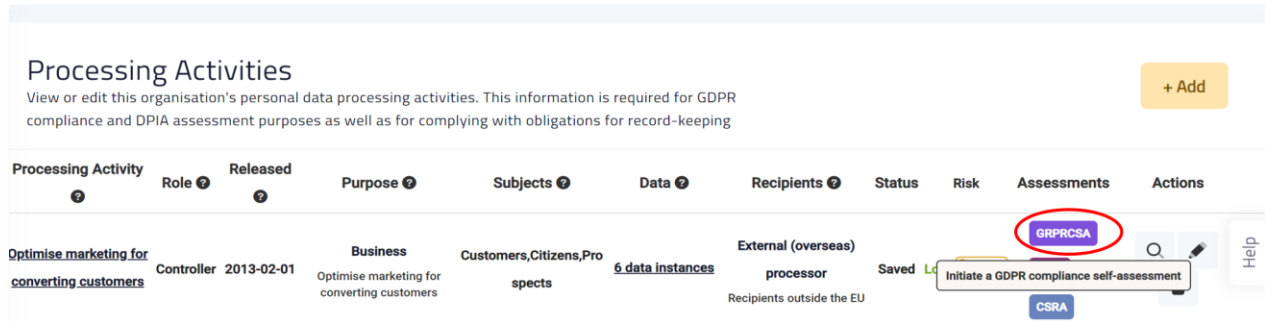


Figure 8. Perform GDPR Compliance Self-Assessment.

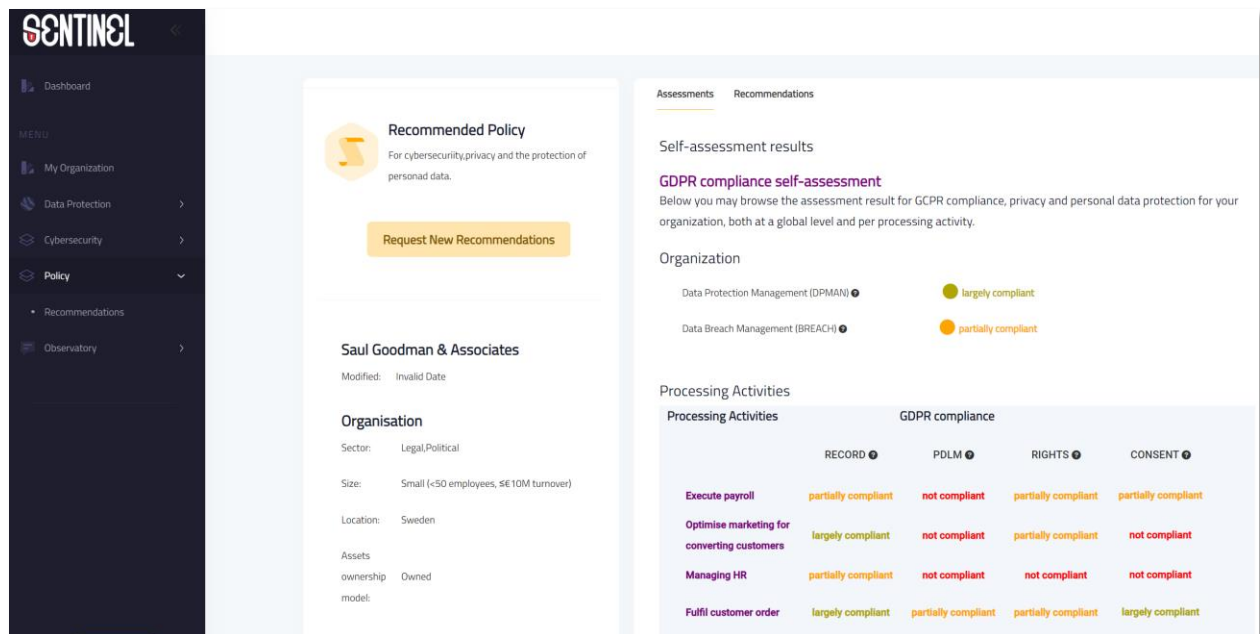


Figure 9. Review GDPR Compliance Self-Assessment results of organisation's PAs

- **Acquire Recommendations.** It allows the user to generate and review a SENTINEL policy and acquire a set of tailor-mades, human-readable, enforceable and actionable recommendations (namely a set of OTMs) at organisational level and PA level (Figure 10). The received policy draft relies on the information registered by the user in the Organisation Profile and each completed PA providing a full list of proposed recommendations containing procedures, technologies, tools, and educational material. Proposed recommendations are grouped into global (organisation-wide) recommendations and PA-specific recommendations. As clarified above, the delivered recommendations engage a set of organisational and technical measures related to GDPR compliance, privacy, and security. The user may navigate into each Organisational or Technical measure and track its implementation status (Figure 11), i.e., either “Pending” or “Implemented” (cf.

Table 27 in Section 4.2.2). Moreover, the user may get advised through each OTM on suggested software and tools that could be utilised to address the respective recommendation fully or cover specific aspects (see “Software & Tools” in Figure 12). Furthermore, for each OTM training materials are provided to facilitate the user to better understand, and determine actions pertain to the proposed recommendation in his/her organisation (see “Training Materials” in Figure 12). The current use case is accomplished by the following set of actions (further analysed in SENTINEL Wiki):

- Generate a Policy
- Review Recommendations
- Policy Monitoring

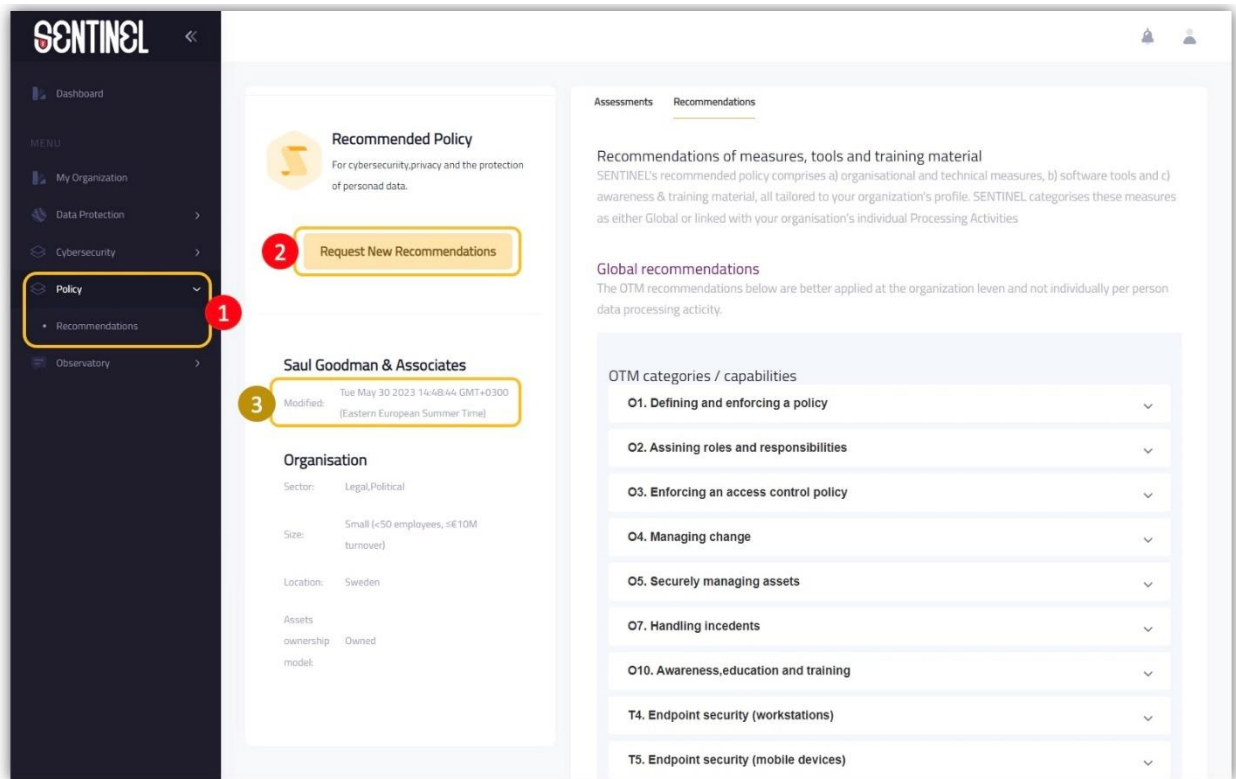


Figure 10. Acquire Policy Recommendations

MEASURES

T1.L.1: User Access Provisioning

A formal user access protocol shall be implemented to assign or revoke access rights for all user types to all systems and services. A strict access control system shall be implemented and maintained for all users accessing the organisation's IT assets. The protocol should provide for creating, approving, reviewing and deleting user accounts, their roles and their permissions.

Processing Activities where this measure is applicable:

- Execute payroll Implementation Status: **Pending**
- Managing HR Implementation Status: **Pending**
- Fulfil customer order Implementation Status: **Implemented**
- Optimise marketing for converting customers Implementation Status: **Implemented**

T1.L.2: Personal User Accounts

This measure is recommended because this processing activity's risk is HIGH

Figure 11. Track Recommendations' implementation status within the organisation.

06.H.7: [Managing Data Subjects' Consent] Quality assessment of mechanism to provide and withdraw consent

An assessment shall be regularly made to evaluate the quality and efficiency of data subjects' consent management mechanism.

Processing Activities where this measure is applicable:

- Managing HR Implementation Status: **Pending**
- Optimise marketing for converting customers Implementation Status: **Pending**

SOFTWARE & TOOLS:

- CNIL's Privacy Impact Assessment tool
- DPIA. <https://www.cnil.fr/en/privacy-impact-assessment-pla>
- Data Protection Impact Assessment (DPIA)

Analysis of both Processing Activities (PAs) and SME Profile to determine GDPR Compliance Level.

- GDPR Compliance Self assessment

Analysis of both Processing Activities (PAs) and SME Profile to determine GDPR Compliance Level.

TRAINING MATERIAL:

Recommended material:

- [Data Privacy Week: 6 Best Practices for Your End Users](#)
- [Wiretaps to Big Data: Privacy and Surveillance in the Age of Interconnection](#)
- [The Essential Guide to Online Privacy & Security in 2022](#)
- [Data Privacy Fundamentals](#)
- [GDPR Compliance: "Explain Like I'm Five" with Data Privacy Expert](#)
- [GDPR data controllers and data processors](#)
- [Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#)

Figure 12. Software tools and training materials suggested for OTMs

- **SENTINEL Cybersecurity tools.** A set of cybersecurity tools and functionalities are available in the SENTINEL platform to allow users to raise awareness on topics of

cybersecurity, to assess and manage risks on cyber assets, to avoid/handle data breaches and security incidents and leverage enterprises' personal data protection. Indicatively:

- Executing Cybersecurity Risk Assessment (CSRA). Performing risk assessment on a specific PA to estimate risks, threats, and vulnerabilities on cyber assets involved in the PA. A complementary simulation environment allows the users to further experiment on cyber-attack scenarios.
- CyberRange Gaming. An external simulation service for hands-on cybersecurity training.
- Exploring the Observatory. An interface to open vulnerability and threat repositories (Knowledge Base) supporting also a Threat Intelligence content that monitors a number of open security data sharing platforms.
- Reporting incidents. It supports a capability of sharing incident or breaches and propagating the data to the appropriate third parties or communities.

The current use case is optional suggested for users with IT or cybersecurity background.

3.4 SME workshop evaluation results

As mentioned previously in Section 3.2.3, in the final SME-centric Workshop representatives from eleven (11) additional external enterprises participated. In addition, in the current Workshop four (4) SMEs performed the CG Pilot and TIG Pilot during the Demonstration Phase (i.e., Clingenics (CG) and Tristone Investment Group (TIG) internal project companies and Sportif and Dimensions Care SMEs (engaged by TIG)) were also involved. Moreover, in this last pilot event three (3) EAB members participated.

In total, twenty (20) end-users deriving from all these enterprises, including the EAB members conducted trials to test and evaluate the SENTINEL platform. With this respect, seventeen (17) end-users utilised two (2) Processing Activities (PAs) experiments pre-defined in the SENTINEL platform (i.e., the "Marketing activities & Communication" PA and the "Recruitment Process" PA), whereas three (3) new PAs were developed by three (3) SME end-users on handling personal data, according to their daily operations.

During the event, all end-users executing the trials utilised the following SENTINEL functionalities (cf. SENTINEL use cases in Section 3.3.2): platform registration, creating a PA and committing it to ROPA, executing GDPR CSA and acquiring recommendations. Each testing was followed by filling out an online interactive questionnaire (cf. Appendix-I). This questionnaire was broken down into different subsections to assist the end-user to leave feedback after completing each testing session. The questionnaire incorporates a group of questions supporting the following sections, as described in Section 2.3:

Part I: Participants Introduction (comprising 8 questions)

- Profiling
- Existing solutions and resources
- Needs and expectation

Part II: SENTINEL hands-on training (comprising 25 questions)

- User Satisfaction (12 questions) with respect to:
 - Platform registration
 - Develop a PA
 - Commit to ROPA
 - Execute GDPR CSA
 - Acquire Recommendations
- Overall evaluation (11 questions)
 - User Interface/User Experience (UI/UX)
 - Business Performance
- Express end-user opinion and additional comments (2 questions)

As mentioned in Section 2.3, Part I of the questionnaire covers the evaluation objectives of T7.4. Therefore, questions of Part I are analysed in Section 4.2 of D7.6 [2] and they are briefly presented in the following section, 3.4.1. The current report presents an extensive analysis of Part II of the questionnaire results (cf. sections 3.4.2, 3.4.3, 3.4.4), as it reflects questions for gathering end-users feedback after experiencing the hands-on training and testing the SENTINEL platform in the scope of real-life scenarios.

3.4.1 Participants Introduction

“Participants Introduction” refers to Part I of the interactive questionnaire which contains information for profiling the end-users and their organisations and identifying further personas to build the SENTINEL community ecosystem around the project’s results (cf. D7.6).

The SME-centric Workshop of M33 encompassed end-users with primary areas of expertise mostly related to IT/Information Security, Technology and Engineering and Personal Data Protection and Health & Social Care, whereas very few end—users were experts in Accounting and Finance. The respondents appertain to different organisation departments, i.e., R&D, Management, Human Resources, Quality, Cybersecurity, GDPR Compliance and Auditing, and hold either managerial positions (i.e., Co-Founder, Director, Officer, Auditor, Head, Administrative or Project/Technical Manager) or research-related or technical development-related positions. From the interaction gained between the SENTINEL partners and the enterprises attendees during the workshop’s hands-on training and trial execution, it is concluded that most end-users’ had low expertise in cybersecurity, data protection and GDPR, (considered as beginners), whereas few end-users had an intermediate level of expertise and very few end-users were considered experts in these topics.

Most end-users do not utilise software tools/ external consulting services for data protection compliance and in case they do they allocate budget that does not exceed 10,000 € annually. In addition, most end-users considered SENTINEL as a potential solution to be utilised by their company. Most end-users illustrated their intention to invest on such tools in the near future reflecting SMEs raised interest in adopting evidence-based GDPR compliance solutions. Detailed questionnaire results are presented in Section 4.2 of D7.6.

3.4.2 User Satisfaction

In this section, the User Satisfaction related to i) Platform registration, ii) Develop a PA, iii) Committing the PA to ROPA, iv) Executing GDPR CSA and v) Acquiring Recommendations are presented and further discussed to elicit information considering their satisfaction level after testing the SENTINEL platform's core functionalities.

i) Platform registration: Almost all respondents either strongly agreed or agreed that it was easy to create an account and organisation in the SENTINEL platform (cf. Figure 13 and Q2.1 of Appendix-I). Similarly, most of the respondents found easy completing their Organisation Profile (cf. Figure 14 and Q2.2 of Appendix-I).

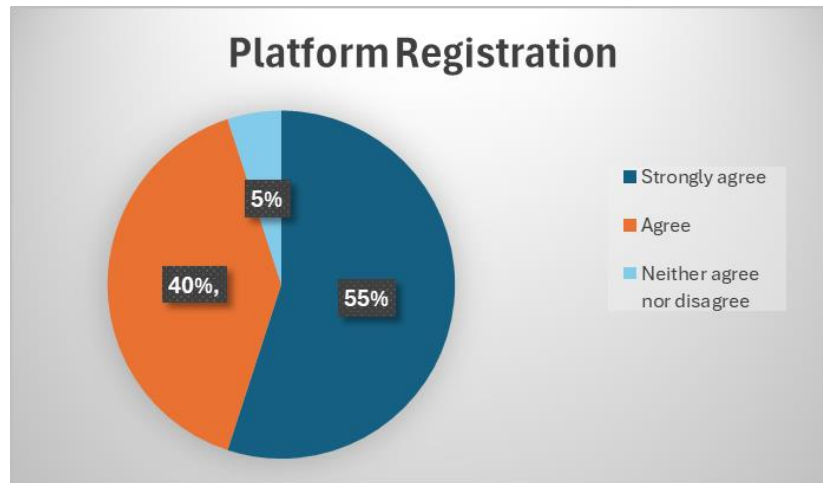


Figure 13. It was easy creating account and organisation in the SENTINEL platform

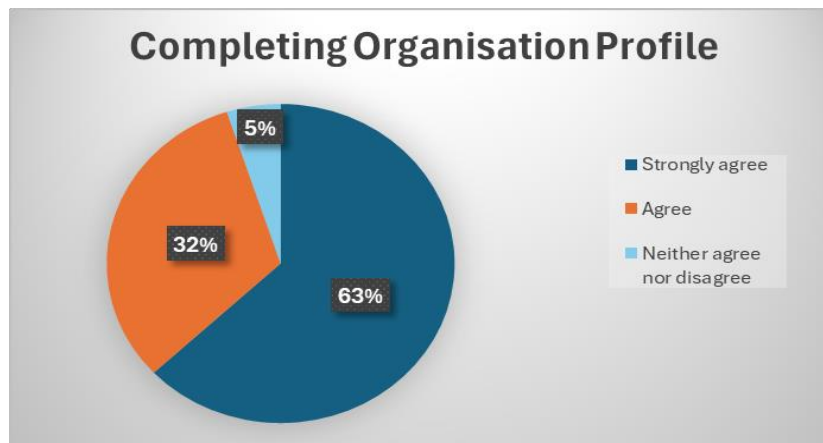


Figure 14. It was easy completing the organisation profile in the SENTINEL platform

ii) Develop a PA - 85% of respondents used pre-filled templates to create their first Processing Activities (Figure 15). Furthermore, 15% of them created their own processing activities while testing the platform (Figure 15). Among all respondents, 11% strongly agreed and 32% agreed that it was easy to create their first Processing Activity in the SENTINEL platform, whereas 41% of end-users were not sure about the statement. Furthermore, 16% of respondents did not find it

an easy task (Figure 16). The current analysis corresponds to questions Q2.3 and Q2.4 of the SENTINEL Interactive Questionnaire (cf. Appendix-I).

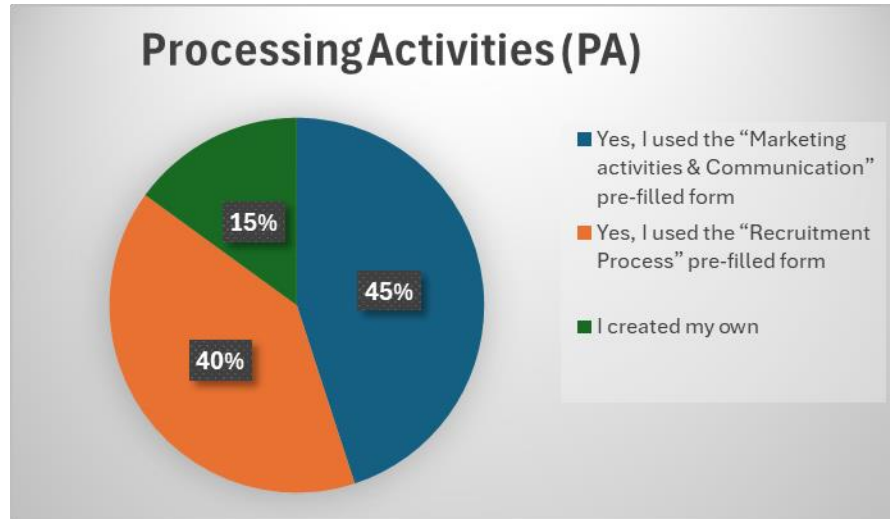


Figure 15. Did you use a Processing Activity template?

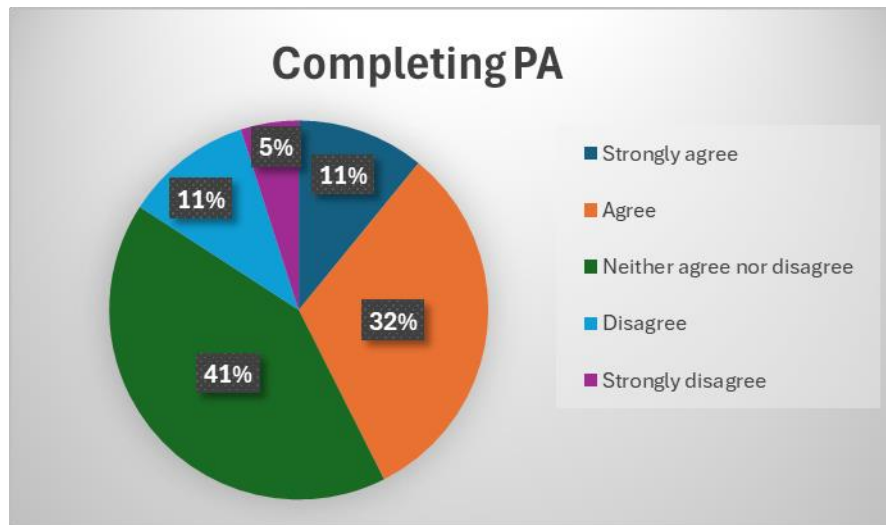


Figure 16. It was easy to complete my first Processing Activity

iii) Commit to ROPA - After successfully developing Processing Activities the end-users were asked to commit it to ROPA and provide their feedback on this task. As shown in Figure 17, around 37% respondents strongly agreed and 26% respondents agreed that they were able to successfully complete this task. Moreover, 21% respondents neither agreed nor disagreed with the statement. A small number of respondents (16%) found this task difficult.

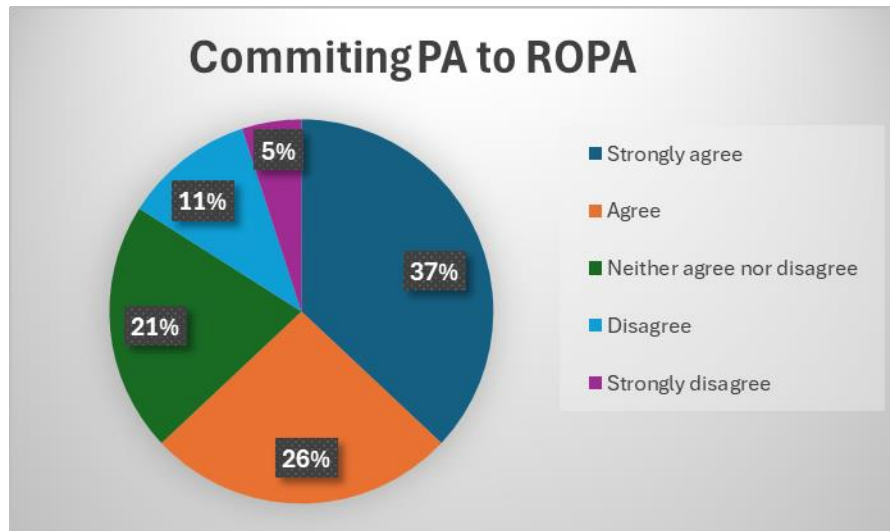


Figure 17. I was able to commit my PA to the ROPA

Moreover, 5% of the respondents strongly agreed and 37% agreed that completing and committing PAs was fast and efficient whereas 32% neither agreed nor disagreed and the rest respondents did not agree with the statement. The current analysis relies on questions Q2.5 and Q2.6 of the SENTINEL Interactive Questionnaire respectively (cf. Appendix-I).

iv) Executing GDPR Compliance Self-Assessment (GDPR CSA) – Executing the GDPR CSA functionally found to be easy for most end-users. As shown in Figure 18, around 16% respondents strongly agreed and 73% agreed that they were able to successfully complete this task. Only few respondents (11%) either disagreed or strongly disagreed with the statement. Similarly, 24% respondents strongly agreed, and 58% respondents agreed that the execution of GDPR CSA was fast and efficient, whereas the rest of respondents (18%) neither agreed nor disagreed (Figure 19). In addition, 25% respondents strongly agreed, and 56% respondents agreed that they were satisfied with the quality of the GDPR Compliance Self-Assessment result whereas the rest of respondents (19%) neither agreed nor disagreed (Figure 20). This analysis refers to questions Q2.7-Q2.9 of the SENTINEL Interactive Questionnaire respectively (cf. Appendix-I).



Figure 18. It was easy to execute the GDPR Compliance Self-Assessment



Figure 19. Executing a GDPR Compliance Self-Assessment was fast and efficient



Figure 20. I am satisfied with the quality of the GDPR Compliance Self-Assessment result

v) Acquiring Recommendations - A set of questions was focused on revealing the respondents' opinion on SENTINEL Recommendations. As shown in Figure 21, most of the respondents either strongly agreed or agreed (28% and 61% respectively) that it was easy to acquire policy recommendations in the SENTINEL platform. Based on Figure 22, most of the respondents either strongly agreed or agreed (22% and 61% respectively) that acquiring policy recommendations was fast and efficient. In addition, 18% of the end-users positively responded that SENTINEL organisational and technical measures are described accurately and clearly. The analysis described, relies on questions Q2.10-Q2.12 of the SENTINEL Interactive Questionnaire respectively (cf. Appendix-I).

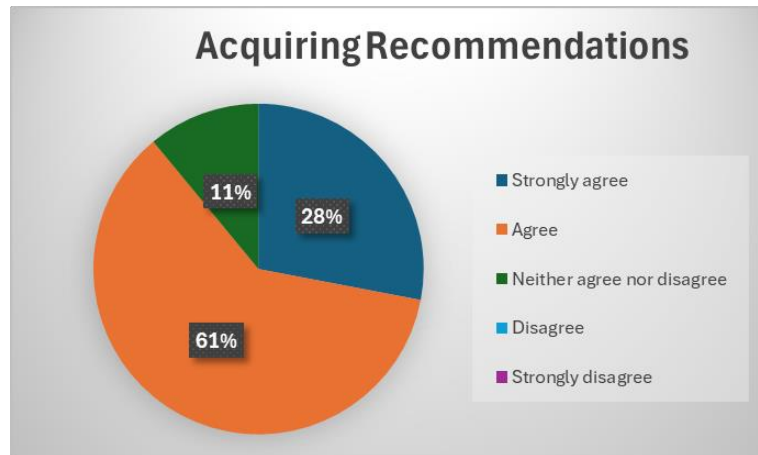


Figure 21. It was easy to acquire Recommendations



Figure 22. Acquiring Recommendations was fast and efficient

3.4.3 SENTINEL Overall evaluation

The current section comprises workshop' questionnaire's results referring to generic evaluation of the SENTINEL platform addressing UI/UX and business performance aspects. In this overall evaluation, the Cybersecurity Tools were also engaged in the questions to have the chance to retrieve feedback by end-users who might optionally utilised the opportunity to test them.

i) SENTINEL UI/UX capabilities - To assess the overall performance of the SENTINEL platform, the respondents were asked to answer several questions regarding the UI/UX capabilities. With respect to the SENTINEL platform visualisation capabilities

- On the bright side, 80% respondents strongly agreed and 10% agreed that the help menu was useful and valuable. Only 10% of respondents neither agreed nor disagreed with the statement.
- Around 50% respondents either strongly agreed or agreed that “the use of terms throughout SENTINEL is consistent”, whereas 32% respondents neither agreed nor

disagreed with the statement. Finally, around 25% of attendees did not support the statement.

- Regarding the description of organisational and technical measures, around 45% of respondents supported that the description was accurate and clear, whereas 35% respondents neither agreed nor disagreed and 20% did not agree with the statement.
- Finally, 30% respondents supported that the SENTINEL platform provides user friendly environment, 21% respondents voted that on-screen messages are properly positioned within the SENTINEL platform, 19% voted that it offers a set of different screens which are cohesive in look-and-feel, 15% supported that the characters on the screen that are easy-to-read, while based on 13% of respondents the organisation of information within the platform is accurate and clear (Figure 23).

The analysis above refers to questions Q2.13-Q2.15 of the SENTINEL Interactive Questionnaire (cf. Appendix-I).

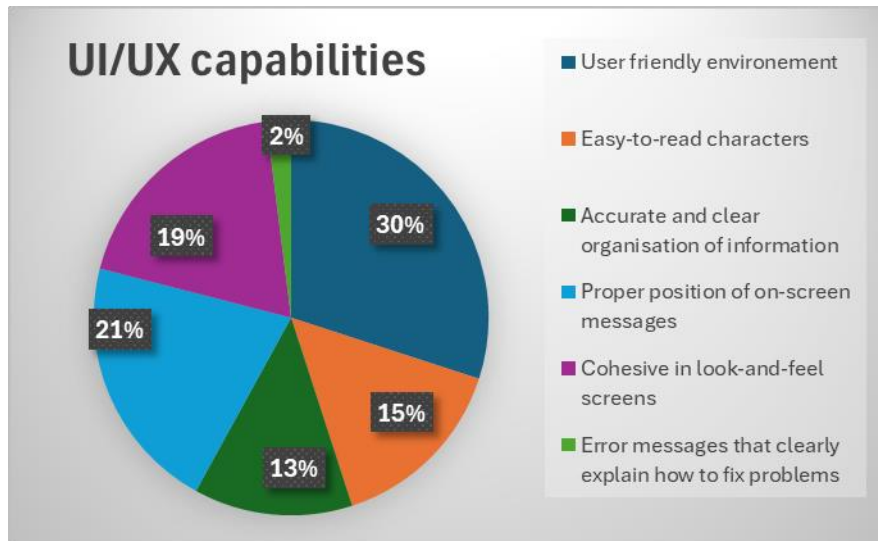


Figure 23. SMEs/MEs end-users' opinion of UI/UX capabilities

ii) Business Performance - 61% of respondents did not face any interruptions while using the SENTINEL platform. Nevertheless, 11% of end-users seem not having strong opinion on this, while very few respondents (i.e., 28%) supported that they faced some interruptions while using the SENTINEL platform.

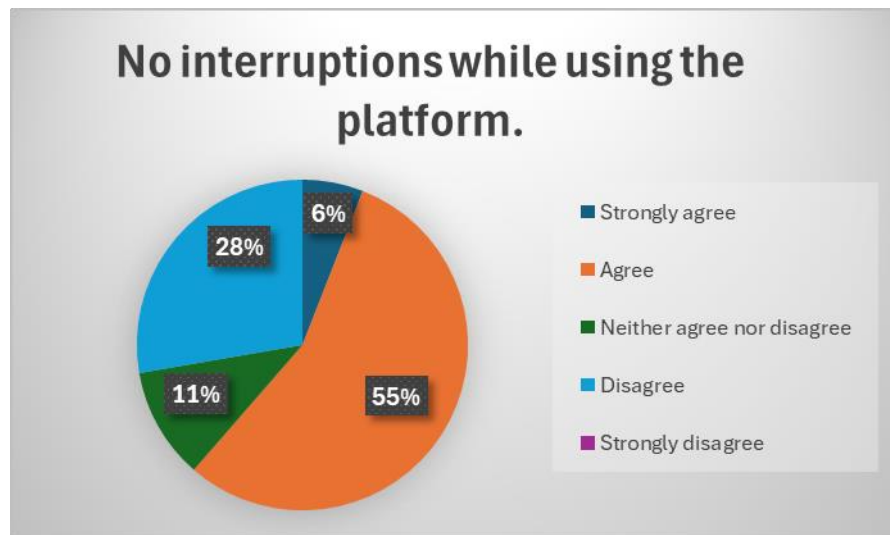


Figure 24. I did not face any interruptions while using the platform

Regarding the question on where SENTINEL can be helpful, 19% of end-users answered that the platform can identify and record their organisations' processing activities, 25% of respondents answered that SENTINEL can help them to "understand their organisations' GDPR compliance requirements" whereas 22% respondents think that it can acquire good practices to better protect their data. Furthermore, 12% respondents believe that SENTINEL can help forming their organisations' cybersecurity and personal data protection strategy. In addition, 7% end-users, believe that SENTINEL can be helpful either to identify how to address privacy and cybersecurity challenges, whereas 7% respondents voted that it can facilitated them in detecting possible attack scenarios that could lead to data breach and 7% respondents voted that it could help them identify different types of threats/attacks (e.g. data storage, accessibility).

Regarding the SENTINEL functionalities, 55% of respondents either strongly agreed or agreed that SENTINEL provides all the functionalities they expect to have for assessing GDPR compliance. However, around 35% neither agreed nor disagreed with this statement while around 10% disagreed on this (Figure 25).

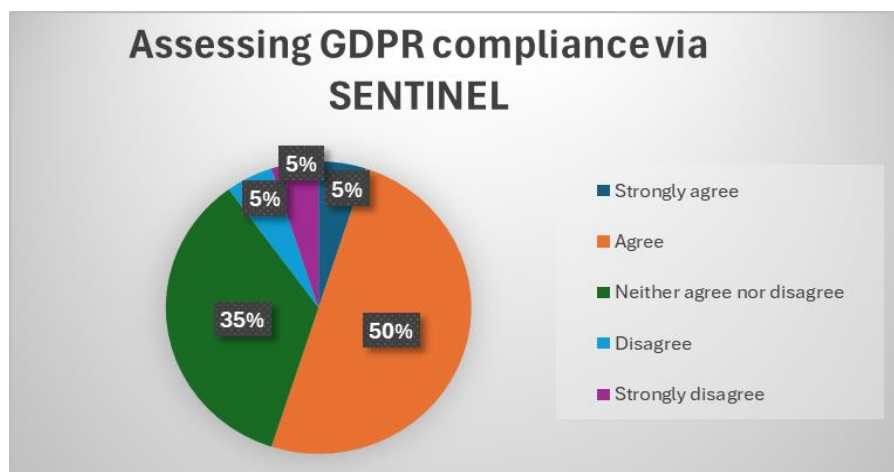


Figure 25. SENTINEL provides all the functionalities I expect to have for assessing GDPR compliance

Furthermore, concerning the respondents' replies towards SENTINEL measures/recommendations:

- 38% of the end-users voted that they could improve the effectiveness of cybersecurity and personal data of my organization.
- 29% of the end-users found them helpful in achieving GDPR compliance.
- 14% of the end-users voted that they helped them to implement controls that limit any types of unauthorized data access.
- 10% of the end-users think they can improve security of information/data exchange.
- 5% of the end-users voted that they could mitigate risks/threats identified on cyber assets.
- 5% of the end-users think they can ensure maintenance and retention of data.

Interestingly, based on the opinion of 68% end-users, SENTINEL can simplify their GDPR compliance, whereas only 32% respondents do not support this statement (Figure 26).

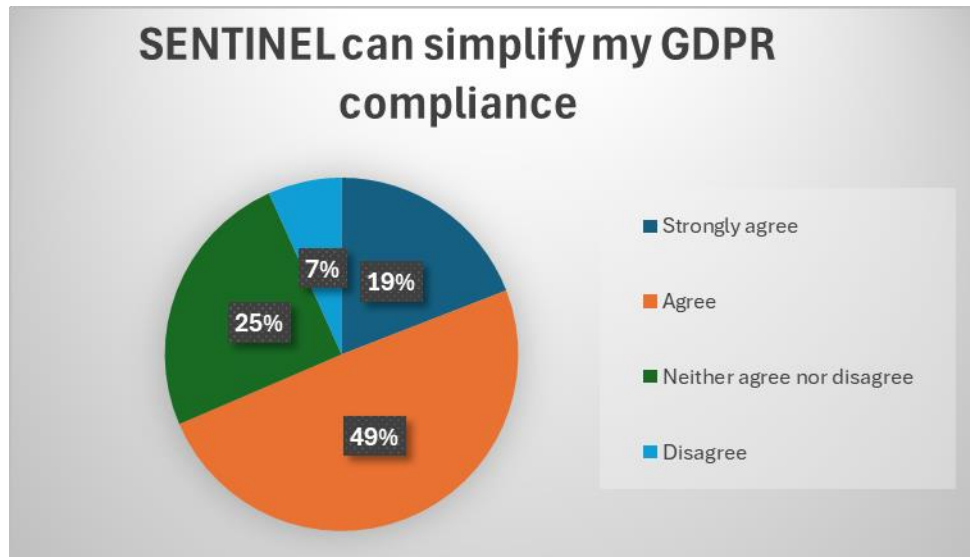


Figure 26. SENTINEL provides all the functionalities I expect to have for assessing GDPR compliance

When questioned on whether the use of SENTINEL will not necessitate additional human and/or financial resources (e.g. hiring external cybersecurity analysts and privacy experts) from their organisation only 28% of respondents either strongly agreed or agreed that additional resources will not be required to invest, while 17% neither agreed nor disagreed. Moreover, 22% of respondents strongly disagreed and 33% of them disagreed with this statement.

Furthermore, regarding the SENTINEL services that could be more useful to their business needs:

- 20% of the respondents voted for the GDPR Compliance Self-Assessment service.
- 14% of the respondents voted for the ROPA service.
- 13% of the respondents voted for the Processing Activity service.
- 13% of respondents voted for the Data Protection Impact Assessment service.
- 13% of respondents voted for the Policy Recommendations service.
- 9% of the respondents voted for the Cybersecurity Risk Assessment service.
- 6% of the respondents voted for the Organisation Profile service.

- 5% of the respondents voted for the Reporting Incidents service.
- 4% of the respondents voted for the CyberRange Gaming.
- 3% of the respondents voted for the Observatory services.

Eventually, concerning the question whether they anticipate that exploiting SENTINEL could potentially increase their organisation's market share in the coming years and if so, to what extent:

- 58% of the respondents answered that they do not know.
- 21% of the respondents answered positively and believe that it could potentially increase their organisation's market share at least by 5%.
- 16% of the respondents answered positively and believe that it could potentially increase their organisation's market share at least by 15%.
- 5% of the respondents answered positively and believe that it could potentially increase their organisation's market share at least by 10%.

The above analysis related to business performance evaluation results corresponds to questions Q2.16-Q2.23 of the Interactive Questionnaire (cf. Appendix-I).

3.4.4 Express end-user opinion and additional comments

The SENTINEL Interactive Questionnaire engaged two questions which encouraged the end-users to answer in free text without any pre-defined options to allow them to express their own opinion gained after experiencing the SENTINEL platform.

Regarding their overall impression gained after testing the SENTINEL platform and their thoughts on SENTINEL most competitive advantages:

- 4 respondents characterised the SENTINEL platform as *"useful"*.
- 3 respondents replied that its completion requires a GDPR expert.
- 3 respondents found as most competitive advantages the *"GDPR compliance assessment"* and the *"training"* ability to SME.
- 1 respondent commented that SENTINEL most competitive advantage is that it provides *"all in one place for GDPR"*.
- 1 respondent mostly liked in SENTINEL its *"adaptation"* capacity to *"company's needs"*.
- 1 respondent commented that SENTINEL is a *"productive tool"*.
- 1 respondent found as the most competitive advantage its *"completeness"*, *"format"* and that raises the user *"awareness"*. An additional respondent supported the latter.
- 1 respondent commented that *"it has highlighted a need for a greater focus on GDPR compliance in our organisation"*.
- 1 respondent commented that *"As long as it is open access it will be interesting"*.
- 1 respondent commented that *"basic GDPR knowledge"* is needed to use SENTINEL.
- 1 respondent commented that there is a lot of information to be completed and time is needed.

Additional specific comments or suggestions for improvements were provided as follows:

- 1 respondent commented to *"shorten"* it.
- 1 respondent suggested that *"filtering input"* could be *"useful"*.
- 1 respondent suggested to enhance its learnability.

- 5 respondents commented that it *“needs to be more user-friendly”*. Moreover, 1 of them added that it is especially needed for those lacking extensive GDPR knowledge.
- 1 respondent replied that the *“Terminology needs to be more SME-friendly”*.
- 1 respondent commented that *“user onboarding could help”*.
- 1 respondent suggested to add *“more PA templates”* (i.e. PAs pre-defined by SENTINEL), improve risk assessment and GDPR trainings.
- 1 respondent commented that *“Questions in the GDPR compliance section maybe simpler or with less options”*.
- 1 respondent suggested to leverage *“sentence conciseness”*.
- Another respondent suggested to *“simplify questions”*.
- A respondent suggested to *“add classification”* indicators to track organisations compliance status over time.
- A respondent replied that titles of *“SENTINEL measures”* could be *“clearer”*.
- A respondent commented that *“GDPR compliance is an ongoing process”*.
- 1 respondent suggested to represent the level of compliance in a quantitative approach (*“percentage”*).

The current analysis is elicited from responses provided for questions Q2.24-Q2.25 of the SENTINEL Interactive Questionnaire (cf. Appendix-I).

After the completion of the SME-centric Workshop, a round table discussion was initiated between the SENTINEL consortium and its EAB members who participated in the Workshop. The EAB members gave valuable feedback after experiencing the SENTINEL platform.

Remarks/suggestions provided by the EAB members are presented in the following:

- GDPR awareness and information should be provided to SMEs before using SENTINEL, to ensure that information is understood and completed correctly.
- The creation of templates per sector and typical processing operations is recommended to better guide the SMEs through SENTINEL.
- The role of ROPA (cf. article 30 of GDPR obligation [8]) should be detailed and clarified.
- The risk assessment should consider data protection risks and non-technical risks, such as people.
- Data protection-by-design and by-default, personal data minimization aspects should be included in the platform.
- Data subjects' rights and transparency obligations should be included.
- Processors' role and their obligations, in terms of data protection, in contractual agreements.
- ePrivacy legislation obligations (e.g. cookies, tracking, marketing communications) should be included.
- SENTINEL organisations ranking level regarding the risk level of each organisation.
- SENTINEL 'alarm system' for future vulnerabilities.
- Spread a word regarding 'CyberRange' gamification.
- Enhance SENTINEL with different types of feedback and notifications to end-users (e.g., *“In this section you may need technical help”*).
- Consider invitation mechanisms for organisations to join SENTINEL.

- Share responsibility context (e.g., illustrate Art.24 aspects of GDPR [8] which can be reported by the DPO of the organisation).
- Enhance the visibility of 'help' button.
- Receive focused alerts from the SENTINEL platform usage (branch classification and nature/origin).

Valuable points commented additionally include:

- “Nice” visual environment.
- SENTINEL Recommendations of measures are “*satisfactory*”.
- The existence of Cyber Range gamification is “*valuable*”.

Some feedback collected from the SME-centric Workshop was considered in the technical refinements of the SENTINEL platform during M34-M36 (as part of T5.3 activities cf. D5.7 [3]). Feedback that was not possible to be considered in the platform’s technical enhancements conducted until M36 could be considered beyond the project’s lifespan to maintain, leverage its operations and raise its exploitation capacity (T7.3) in the long-term.

4. Overall SENTINEL Assessment

In this section, the overall SENTINEL platform assessment from both business/socio-economic and technical aspects gathered as a continuous process from the MVP evaluation until the SME-centric Workshop final pilot event is analysed towards specific validation and verification metrics, benchmarks, baselines and targeted values defined in D6.1 [5]. In addition, the SENTINEL platform capabilities and functional completeness were assessed towards covering the Business and Application Requirements identified in tasks T1.1 and T1.2. Eventually, considering all obtained evidence and its interpretation, an impact assessment of the overall evaluation outcomes is carried out, and the KPIs/KRs that did not reach their targets in M30 were finally assessed and reported.

4.1 SENTINEL Validation and Verification

This section provides an in-depth analysis of the validation and verification processes for the SENTINEL platform. It examines how the platform's functionalities and performance metrics have been assessed to ensure alignment with SMEs' requirements and regulatory standards. The results from these validation activities offer insights into the platform's effectiveness and areas for improvement.

4.1.1 SENTINEL Validation

This section illustrates the SENTINEL platform assessment upon specific validation metrics based on prominent quality models and standards, such as the SQuaRE model of ISO/IEC 25010:2011, and the System Usability Scale (SUS) model [9], [10], [11]. The achieved results were estimated for the FFV validation activities conducted in the context of the three (3) Pilots, i.e., the CG Pilot, the TIG Pilot and the DIH Pilot, including the SENTINEL Final Product validation realised in the final pilot event (the SME-centric Workshop of M33).

4.1.1.1 SENTINEL validation outcomes of Clingenics Pilot

The SENTINEL validation outcomes retrieved from the Clingenics (CG) Pilot (SENTINEL FFV testing) and the achieved results are depicted hereunder in Table 5.

Table 5. Validation outcomes of Clingenics Pilot

Validation variable		Metric	Baseline value	Expected result	Achieved Results
Business	Service/product quality	Number of SENTINEL services/components corresponding to CG's needs and requirements.	MVP version	At least 5 SENTINEL services/components leveraged	All SENTINEL services included as test cases in the CG experiments leveraged by CG (cf. sections 3.5.2 and 3.6 of D6.2 [1]). SENTINEL services are thoroughly described in KR-3.2 justification reported in D6.2 and D8.3 [12])

	Reliability	<u>Availability:</u> Counting the overall availability of the SENTINEL platform.	100% available during the MVP testing	100% availability	Each time CG used the SENTINEL platform it was completely 100% available at the corresponding stage
	Maintainability	<u>Reusability:</u> Testing the reusability of the SENTINEL platform.	N/A	Dichotomous score: True	True: Using the SENTINEL platform more than once helped CG to be more concern about CS and PDP
	Satisfaction	<u>Learnability:</u> The level of satisfaction while using the SENTINEL platform.	Learnability at MVP evaluation stage 3/5 (60%)	SUS score: ≥4 out of 5	SUS score 4/5: After the first use of the SENTINEL platform the level of knowledge were increased more than 80%
	Usability	The level of usefulness of the SENTINEL platform.	Usability at MVP stage 3/5 (60%)		SUS score 5/5, achieved at 100%
	Performance Efficiency	<u>Time efficiency:</u> Accept that the platform maintains time efficiency with respect to cybersecurity (CS) and personal data protection (PDP) processes completion.	Time efficiency at MVP evaluation stage 2/5 (40%)	SUS score: ≥4 out of 5	SUS score 4/5 (80%): The use of SENTINEL platform saves time compared to traditional ways (e.g. the SENTINEL ROPA services)
		<u>Resource utilization:</u> Accept that the platform brings resource effectiveness regarding CS and PDP processes completion.	Current resource utilized for CS and PDP management processes are based only company's human knowledge and expertise.		Improvement of resource acquisition to any kind of CS and PDP processes completion and/or processes thanks to SENTINEL.
CS & PDP	Compliance	<u>Conformance:</u> SENTINEL's consistency in providing GDPR compliant measures/rec ommendation	No OTMs are associated with GDPR's requirements.	For each GDPR requirement, there is at least one corresponding OTM.	All recommendations proposed by ENISA [13],[14],[15] were mapped to the GDPR requirements [8]. Nevertheless, some requirements were not covered by these

		according to the risk level of PA.			recommendations and thus specific GDPR measures were added at the SENTINEL Final Product (M30). Moreover, Category 6 of SENTINEL Organisational measures was enhanced with countermeasures for managing GDPR compliance as presented in Table 10 of D3.3 [16].
		Number of anonymisation and pseudonymisation techniques recommended	1 end-user password encryption technique already used	At least 2 new anonymisation and/or pseudonymisation techniques recommended by SENTINEL.	CG used at least 2 anonymized techniques recommended by SENTINEL to convert the file names provided by the user to anonymized files
Threat containment		Number of security risks detected	0 security risks identified only attack scenarios available at MVP stage	Detection of at least 2 types of risks for corresponding pilot assets of declared Processing Activities (PAs) (e.g. by conducting cs risk assessment using SENTINEL cs component).	More than 10 risks were tested and reported during the CG PA experiments after successfully conducting Cybersecurity Risk Assessment on PAs cyber assets. Different types of attacks identified for these risks from CAPEC [17] and CWE [18] of MITRE repositories (e.g. code injection, Cross-Site Scripting (XSS), etc)
		Number of security risks mitigated	0 security risks mitigated as no risks identified at MVP stage.	Mitigation of at least 2 types of risks related to data storage and accessibility via SENTINEL OTMs recommendations	All risks identified were taken under consideration and observation. Respective OTMs recommended to address the reported risks.
Data breach prevention		Number of possible attack scenarios that could lead to data breach	0 attack scenarios leading to data breach at MVP stage.	Detection of at least 2 attack scenarios of under examination pilot assets that could initiate a breach of data confidentiality, integrity or availability (e.g. using SENTINEL simulation environment to	CG worked with more than 6 attack scenarios during tests and all cases were passed successfully. CG also received suggestions, such as backup policies, Network Security, Server and database security, etc.

				discover respective possible cyber-attacks / threats paths and patterns on the pilot assets).	
		Number of incidents prevented	0 incidents prevented at MVP stage.	SENTINEL recommendations should provide measures (OTMs) that prevent at least 2 types of privacy incidents (e.g. ransomware attacks, DDoS attacks and other types of data breaches).	Since there was no incident, we took under consideration the OTM recommendations received and got more compatible with GDPR and PDP during our processing activities (e.g. SENTINEL organisational measures for handling incidents – Category 7, cf. Table 11 of D3.3 [16]).

4.1.1.2 SENTINEL validation outcomes of Tristone Investment Group Pilot

The SENTINEL validation outcomes derived from the Dimensions Care (DC), Sportfit and Beyond Limits evaluation conducted in the context of the TIG Pilot activities and during the final pilot event are presented in Table 6.

Table 6. Validation outcomes of TIG Pilot

Validation variable		Metric	Baseline value	Expected result	Achieved Results
Business	Satisfaction	<u>Learnability:</u> The level of satisfaction while using the SENTINEL platform.	MVP evaluation stage	SUS score: ≥4 out of 5	SUS Score 4/5: Improved satisfaction following initial DC and Sportfit pilot activity.
	Usability	The level of usefulness of the SENTINEL platform.		SUS score: ≥4 out of 5	SUS Score 4/5: TIG consider SENTINEL to be invaluable in securing GDPR compliance.
	Performance efficiency	<u>Resource utilisation:</u> Accept that the platform does not slow systems down or implement any unnecessary barrier to access. Ensure that the system		Satisfied with system performance	There is no indication that the platform would slow ICT/software systems utilised in the TIG pilots (SUS Score 5/5 (100%)).

	works seamlessly with third party MIS software.				
	<u>Cost/effort reduction:</u> Cost effectiveness compared to other cybersecurity and privacy management solutions.	Cost of technologies related to CS and privacy already utilized by the pilot owner (where applicable)		Reduction of resources/cost related to any kind of GDPR compliance activities and /or processes thanks to SENTINEL.	This is associated with KR-1.3 reduction of compliance costs justification (cf. Section 4.3.2, D8.3 [12]. To estimate the cost/effort reduction, the project's consortium developed a business model and crafted a pricing strategy for SENTINEL (cf. Section 6 of D7.9 [20]), providing low and affordable costs for SMEs, substantially cutting compliance expenses against high compliance consultants fees impacting SMEs. To draw such conclusions, we explored pricing strategies of competitors (cf. Section 6 of D7.9 [20]), and evaluated the perceived value of SENTINEL Key Exploitable Results (KERs) (cf. Go-to-Market Use Model in D7.8 [21]). In that sense, SENTINEL can potentially reduce such costs of TIG Pilot enterprises.
	<u>Time efficiency:</u> Accept that the platform maintains time efficiency with respect to CS and PDP processes completion.	MVP evaluation stage		SUS score: ≥4 out of 5	SUS Score 4/5: The information/data input requirements are time consuming (as such requirements of any other platform requirements). Nonetheless, efficiencies will be gained once the core processes have been captured. Increased familiarity by using SENTINEL and thereby increased time efficiency.
Service/product quality	Number of SENTINEL services/components corresponding to TIG's needs and requirements.	MVP evaluation stage		At least 5 SENTINEL services/components leveraged	At least 5 SENTINEL services/components can improve existing measures/compliance systems: <ul style="list-style-type: none"> • Commit PA to ROPA • DPIA • Training modules • Policy recommendations • Asset management

CS & PDP	Compliance	Number of comprehensive and updated Data Protection Policies (DPPs) and processes obtained that meet the requirements of Health and Social Care SMEs.	Already have in place 2 (1 related to TIG's internal administration processes and 1 related to more generic/business specific DPP)	At least 2 Data Protection Policies (DPPs) and processes related to Health and Social Care SMEs recommended by SENTINEL.	Several SENTINEL measures related to PDP received. For instance, nine (9) SENTINEL organisational measures were delivered for defining and enforcing a Policy – Category 1 (cf. D3.3 [16]).
		Number of consent procedures obtained (incl. information notices, consent forms, procedures on data subject's rights).	Already have in place: -Subject access request form - Consent/ confidentiality form -Non Disclosure Agreement (NDA)	At least 3 consent procedures related to Health and Social Care SMEs recommended by SENTINEL.	Consent procedures were recommended by SENTINEL. For instance, 4 SENTINEL organisational measures related to Managing Data Subjects' Consent for GDPR (Category 6) received (cf. D3.3): <ul style="list-style-type: none"> • Request for consent; • Consent withdrawal; • Preference implementation; • Record of consent and withdrawal.
		Number of new organizational measures enacted equivalent to the ISO/IEC 27001 information security standard.	Number of organizational measures already in place	At least 3 new organizational measures recommended by SENTINEL	SENTINEL provided several technical measures following ISO/IEC 27001 international standard on information security [22], addressing CIA ⁹ aspects (cf. BR-CIAs in Table 10 of Section 4.2.1 in the current deliverable)
	Threat containment	Number of security risks detected	0 security risks detected at MVP stage	Detection of at least 2 of risks for corresponding pilot assets of declared Processing Activities (PAs) (e.g. by conducting cs risk assessment using SENTINEL cs component).	>/ 2 risks identified during the TIG Pilot PA experiments after conducting Cybersecurity Risk Assessment (CSRA) on cyber assets of the registered PAs (accomplished at the final pilot event).

⁹ Confidentiality, Integrity and Availability.

		Number of security risks mitigated	0 security risks mitigated as no risks identified at MVP stage	Mitigation of at least 2 types of risks related to data storage and accessibility via SENTINEL OTMs recommendations	For all risks identified related OTMs were recommended by the SENTINEL platform, such as: i) SENTINEL technical measures for “Secure Storage of Redundant Backups” and “Strong Encryption of Backups at Storage” which reside in backup policy related measures of Category 7 cf. Table 21 of D3.3) addressing data storage issues, and ii) SENTINEL organisational measures for managing GDPR compliance (category 6 cf. Table 10 of D3.3) addressing accessibility issue (accomplished at the final pilot event in M33).
	Data breach prevention	Number of possible attack scenarios that could lead to data breach	0 attack scenarios leading to data breach at MVP stage.	Detection of at least 2 attack scenarios of under examination pilot assets that could initiate a breach of data confidentiality, integrity or availability (e.g. using SENTINEL simulation environment to discover respective possible cyber-attacks / threats paths and patterns on the pilot assets).	At least 2 attack scenarios that could lead to loss of CIA were developed concerning cyber assets of registered PAs using the SENTINEL simulation environment at the final pilot event in M33.
		Number of incidents prevented	0 incidents prevented at MVP stage.	SENTINEL recommendations should provide measures (OTMs) that prevent different types of privacy incidents (e.g. ransomware attacks or DDoS attacks or other types of data breaches).	SENTINEL OTM recommendations received related to organisational measures for handling incidents (Handling incidents – Category 7) or related to technical measures, such as network traffic monitoring and network access control (Network Security – Category 6 cf. D3.3 [16]). Their implementation could potentially prevent such incidents (accomplished at the final pilot event).

4.1.1.3 SENTINEL validation outcomes of external SMEs/MEs

The SENTINEL validation outcomes elicited from the DIH Pilot generic experiment, Sportfit and Beyond Limits evaluation conducted in the context of the TIG Pilot are presented in Table 7.

Table 7. Validation outcomes of DIH pilot and SMEs user-centric workshop

Validation variable		Metric	Baseline value	Expected result	Achieved Results	
Business	Satisfaction	<u>Learnability</u> : The level of satisfaction while using the SENTINEL platform.	MPV evaluation stage	SUS score: ≥4 out of 5	DIH Pilot: SUS score 3/5. Approximately 60% of participants agreed at the FFV stage that the most of features are easy to understand and use (My Organisation, PA, ROPA, GDPR CSA, DPIA, CSRA, Recommendations, Observatory and Reporting Incidents) At the final pilot event the SUS score of DIH respondents to the previous statement was raised to 4/5 (80%).	
	Usability	The level of usefulness of the SENTINEL platform.		SUS score: ≥4 out of 5	SUS score 3/5. At the final pilot event approximately 67% of participants agreed that SENTINEL can be useful within their company	
	Performance efficiency	<u>Resource utilization</u> : Accept that the platform does not slow systems down or implement any unnecessary barrier to access.			Satisfied with system performance	The platform services are offered online, which does not impact the speed of system while processing.
		<u>Cost/effort reduction</u> : Cost effectiveness compared to other cybersecurity and privacy management solutions.	N/A		Reduction of resources/cost related to any kind of GDPR compliance activities and /or processes thanks to SENTINEL	This is addressed by the SENTINEL pricing model and strategy compared to other competitors analysed in D7.8 [21], D7.9 [20] and associated with KR-1.3 justification (cf. Section 4.3.2, D8.3 [12])
		<u>Time efficiency</u> : Accept that the platform maintains time efficiency with respect to CS and PDP processes completion.	MVP evaluation stage		SUS score: ≥4 out of 5	SUS score 4/5: More than 80% of external SMEs end-users found that executing a GDPR CSA and acquiring policy recommendations were fast and efficient processes (reported at the final pilot event).
	Service/product quality	Number of SENTINEL services/components	MVP evaluation stage		At least 5 SENTINEL services/components leveraged	All SENTINEL services/components (addressed in KR-3.2 cf. D8.3 [12], D6.2

		corresponding to pilot case needs and requirements.			[1]) leveraged in PA experiments executed during the DIH Pilot cf. Section 5.5.2 of D6.2 [1]
CS & PDP	Compliance	Number of consent procedures/mechanisms obtained (incl. information notices, consent forms, procedures for the exercise of data subject's rights).	MPV evaluation stage	At least 2 consent procedures related to the needs of the engaged SMEs/MEs recommended by SENTINEL	5 SENTINEL organisational measures identified related to managing data subjects consent (managing GDPR compliance, Category 6 in Table 10 of D3.3), e.g.: i) Quality assessment of mechanism to provide and withdraw consent, ii) Record of consent and withdrawal.
		New OTM measures enacted equivalent via SENTINEL.	MVP evaluation stage	At least 2 OTM measures (organisational and/or technical) recommended by SENTINEL	Several OTMs were recommended by SENTINEL (96 organisational measures related to ENISA recommendations and GDPR requirements and 79 technical measures addressing ISO/IEC 27001 [22] information security requirements related to CIA and PDP requirements.
	Threat containment	Security risks identified via SENTINEL	0 security risks identified at MVP stage	Detection of at least 2 types of risks for corresponding pilot assets of declared Processing Activities (PAs) (e.g. by conducting cs risk assessment using SENTINEL cs component).	More than 2 risks identified on cyber assets of PA experiments when conducting CSRA associated with corresponding threats and weaknesses of MITRE open repositories [17],[18]. In addition, 70% of the respondents replied positively that the simulation environment helped them to identify risks and threats on registered assets. Specifically, a respondent commented that it "provides a vulnerability list depending on the device in place".
	Data breach prevention	Incidents/attacks prevented via SENTINEL	0 incidents prevented at MVP stage.	SENTINEL recommendations should provide measures (OTMs) that prevent different types of privacy incidents (e.g. ransomware attacks, DDoS attacks	70% of the respondents replied positively that SENTINEL provides recommendations to address/manage the issues/risks, stated above, to the registered assets.

				and other types of data breaches).	In addition, 60% of the respondents commented that it helped them to identify possible attack scenarios (Malware, virus attack, phishing and smishing cyber-attacks concerns). The respondent expressed as well that SENTINEL could help to alleviate such concerns.
--	--	--	--	------------------------------------	--

4.1.2 SENTINEL Verification


The current section presents the verification outcomes reported against the baseline values and the expected results after testing the SENTINEL platform and its components and plugins either by the technical partners in a security laboratory environment or by pilot end-users when executing trials (i.e., concerning UI/UX related variables). To verify the obtained values, a set of benchmark standards and approaches were adopted, such as the System Usability Scale (SUS) model [11], ISO/IEC 27001 [22], Google Analytics, GDPR Regulation [8], threat and vulnerability catalogues of MITRE, i.e., CAPEC [17], CWE [18], CVE [19], the vulnerability severity framework CVSS of FIRST [23], etc.

4.1.2.1 Verification of SENTINEL components

This section depicts the verification outcomes concerning the SENTINEL components, i.e, MySentinel, the Profile Service, the Self-Assessment Engine, the Recommendation Engine, the Policy Drafting, the Incident Handling, the Observatory and SENTINEL as integrated platform.

Table 8. Verification outcome of SENTINEL components

Asset	Verification variable	Metric	Baseline value (MVP stage)	Benchmark	Expected result	Achieved Results
MySentinel (AEGIS)	Usability	Use of colors	3/5	User questionnaires (SUS rating 0-5)	5/5	4/5
		System feedback				5/5
		System response to errors				5/5
		System clutter				5/5
		User's subjective satisfaction				4/5
	Performance	Page load time/Response time	10 seconds	Google Analytics	5 seconds	0.9
Profile Service	Functional suitability	Use cases supported	Use cases / data	a) organisation; b)	a) organisation; b) PAs;	<ul style="list-style-type: none"> • Organisation: basic info; assets; global OTMs; org risk level • PAs: basic data, purpose,

			representations supported at the MVP stage	PAs; c) GDPRCSA results; d) DPIA results; e) recommendations; f) policy draft	c) GDPRCSA results; d) DPIA results; e) recommendations; f) policy draft; g) asset inventory; h) policy enforcement status; i) ROPA; j) SCORE elements	subjects, data, recipients, risks; GDPRCSA inputs; DPIA inputs; relationships to assets; PA-specific OTMs; <ul style="list-style-type: none"> • ROPA • GDPRCSA results • DPIA results • CSRA results • Recommendations+Policy Draft received
	Performance	Latency	Response time of the microservice	N/A	5s	~4.4s
	Availability	% of requests satisfied	no. of requests	% of requests satisfied	>99% <1% error rate	100%
Self-assessment Engine (IDIR)	Functional suitability	Number of plugins supported for assessment eligibility check	2	additional SA tools supported	>=3	3 (GDPR CSA, DPIA, CSRA)
	Performance	Latency	Response time of the microservice	N/A	5s	4454.2ms 
	Availability	% of requests satisfied	no. of requests	% of requests satisfied	>99% <1% error rate	100%
Recommendation	Availability	uptime	N/A	N/A	0,99	0,99999
		% of requests	no. of requests	% of requests	>99%	99,999%

		satisfied		satisfied		
	Performance	Latency (responsiveness)	Response time of the module	N/A	5s	50ms
Policy Drafting (FP)	Performance	Latency	Response time of the module	N/A	5s	50ms
	Availability	% of requests satisfied	no. of requests	% of requests satisfied error rate	>99% <1%	99,999%
Incident Handling (ITML)	Availability	uptime	N/A	N/A	0,99	0,99999
		% of requests satisfied	no. of requests	% of requests satisfied	>99%	99,999%
	Performance	Latency (responsiveness)	Response time of the module	N/A	5s	50ms
Observatory (ITML)	Interoperability	no. of data exchange interfaces implemented	2	additional interfaces added	4	4
	Availability	percentage of requests satisfied	no. of requests	% of requests satisfied	>99%	99,999%
	Performance	latency	response time	N/A	5s	50ms
Integrated platform (INTRA)	Functional suitability	end-to-end tests for all usage scenarios (pass/fail)	Partial test cases at MVP stage	N/A	pass end-to-end tests for all usage scenarios (100%)	100%
	Confidentiality (data encryption at rest and in transit)	Encryption verification tests (success / failure) - Data encryption and other confidentiality mechanisms utilised)	N/A	N/A	Encryption enabled both at rest and in transit	Encryption enabled both at rest (AES-256) and in transit (SSL)
	Usability	user's subjective	4/5 (80%) at FFV	User questionn	>4 out of 5	5/5 (100%) at SME-centric Workshop final evaluation

		satisfaction	evaluation stage from the three Pilots	users (SUS rating 0-5)		
	Availability	percentage of automated requests satisfied	N/A	% of requests satisfied	>95%	100%

4.1.2.2 Verification of SENTINEL plugins

This section displays the verification outcomes concerning the SENTINEL plugins, i.e., Security Infusion, IdMS as-a-service, GDPR compliance Self-Assessment, MITIGATE Risk Management, Data Protection Impact Assessment, CyberRange, Forensics Visualisation Toolkit, Open source and external plugins.

Table 9. Verification outcome of SENTINEL plugins

Plugins	Verification variable	Metric	Baseline Value	Benchmark	Expected result	Achieved Results
Security Infusion (ITML)	Security	Detection Time	<4000ms	testing on a single agent on failed login attempts (20attempts/min)	<800ms	700ms
		no. of security related incidents detected	N/A	N/A	99%	99.9%
	Performance	Latency	response time	N/A	5s	4s
IdMS as-a-service (ITML)	Functional suitability / Verify implementation of GDPR user rights (access, information, rectification, erasure, portability, etc.)	role base access control (RBAC) in place and verified	Compliance with all rules and regulations	N/A	MyData architecture for IdMS as a service natively embedded	The design of My Account page as part of the effort for the IdMS to make one step towards MyData paradigm.
	Confidentiality (data encryption at rest and in	security measures applied to ensure	>3	N/A	5	Security measures applied in IdMS include >5 measures to ensure confidentiality: user

	transit)	confidentiality				registration, account recovery, profile management, credentials management, and consent management.
	Authentication and authorization (verify implementation of SSO mechanism)	concurrent user sessions and user logins	10000 1/sec		20000 3/sec	IdMS provides authentication, authorization and Single Sign-On capabilities with 20000 3/sec concurrent sessions and user logins
GDPR compliance Self-Assessment (LIST)	Identify OTMs implemented to meet data protection requirements	% completeness of PA description	0%	GDPR	75%	A significant amount of information is needed to complete the description of PAs. It is possible to reach 100% of information provided in multiple steps.
	Determine Compliance Level of Processing activity	% of compliance assessment performed in comparison with nb of PAs recorded in ROPA	0%	GDPR	75%	100%. Once PA is recorded, it is very easy to launch an automated assessment of compliance level.
	Identify and understand how to improve GDPR compliance level	% of User satisfaction	0%	GDPR	75%	100%. Satisfaction of the users are related to their awareness level regarding their obligations under GDPR
MITIGATE - Risk Management (FP)	Security	Threat probability calculation per asset	number of Threat Probability calculations conducted for specific assets	Deviations from the expected result (CWE [18], CAPEC of MITRE [17])	Threat Probability calculation of all threats detected on assets participating in the Processing Activity/ies (PA(s)) under assessment	100% achieved. Tested: i) during the three pilots and the final SME user-centric workshop by a number of end-users, ii) in a lab environment by technical partners. Moreover, the CSRA was performed on the users' companies cyber assets engaged in the PAs as declared in the SENTINEL platform. In all cases, for each cyber asset respective threat results received per PA presenting information, such as, CAPEC MITRE [17] threat ID along with attack

						patterns description and CWE MITRE [18] per asset. For each type of threat, the respective threat probability was successfully calculated in a qualitative approach per asset. The threat results were shown per threat level and per asset risk level. For instance, during the testing by a technical partner for 2 cyber assets out of 4 participating in the PA (i.e., a workstation and an Office software) we received 82 CAPEC threats in total for both assets (i.e., 3 threats for the 1 st asset and 79 threats for the 2 nd) specifying for each threat all information described above.
Security	Vulnerability level calculation per asset	number of Vulnerability Level calculations conducted for specific assets	Deviations from the expected result (NVD [24],NIST CSRC [25])	Vulnerability Level calculation of all vulnerabilities identified on assets participating in the PA(s) under assessment	100% achieved. Same as previously. Tested via the pilots and partners technical checks and in all cases the Vulnerability Level was estimated for each identified vulnerability per asset participating in the under-assessment PA. In addition, each identified vulnerability was juxtaposed to the related threat illustrating to the user potential attack scenarios on the assets. For instance, according to the previous indicative testing we received several related vulnerabilities for each threat following the MITRE, NIST predefined benchmarks [19], [24] .	
Security	Impact level calculation per asset	number of Impact Level calculations conducted for specific assets	Deviations from the expected result (CVSS 3.1 [23])	Impact Level calculation of all assets participating in the PA(s) under	100% achieved. Same as previously. Tested via the pilots and partners technical checks and in all cases the Impact Level was successfully provided	

					assessment	(in qualitative approach) for each identified vulnerability per asset participating in the under-assessment PA based on the CVSS 3.1 [23] specification, including vulnerability details and the vulnerability severity score. No deviations identified in all experiments.
Security	Risk level calculation per asset	number of Individual Risk Level calculations conducted for specific assets	Deviations or not from the expected result (ISO/IEC 27001 [22])	Individual Risk Level calculation of all assets participating in the PA(s) under assessment		100% achieved. Same as previously. Tested via the pilots and partners technical checks and in all cases the dominant Individual Risk Level was successfully provided and depicted as previously following qualitative measured scale (from Very Low to Very High) per asset participating in the under-assessment PA. For instance, in the previous example, the Individual Risk Level both for the workstation and the Office software was “Medium”. No deviations reported.
Security	number of attack scenarios per vendor's product request (attack scenarios are defined with relations of vendors' products to corresponding threats and vulnerabilities wherever exist)	Number of attack scenarios produced	Deviations or not from the expected result	all possible attack scenarios for all vendors' products requested		100% achieved. Test during the pilots and via technical partners in a lab environment. All possible attack scenarios received. No deviations reported. For instance, as described in Section 4.1.1.1 in the context of the CG Pilot validation, more than 6 attack scenarios scrutinised and developed successful results illustrating relation triplets of assets with vulnerabilities and threats per asset MITRE CPE [26] characteristic.

Data Protection Impact Assessment (STS)	Functional suitability	Risk score calculation per processing activity	N/A	N/A	response with a scoring result	Response with a scoring result with a breakdown of the overall score derived from the average score of 8 categories
	Performance	page load time, response time	response time of <2000ms	N/A	<1000ms	<700ms
	Availability	Uptime	no. of requests	% of requests satisfied	99%	99.9%
CyberRange (ACS)	Security	no. of infrastructure assets supported	N/A	N/A	5/5	5/5: mail server, Active Directory, database, web server, client workstation
	Security	no. of vulnerabilities analysed	N/A	N/A	5/5	5/5: phishing, low encryption, Local File Inclusion, weak credential, social engineering.
Forensics Visualisation Toolkit (AEGIS)	Usability	Use of colors	3/5	User questionnaires (SUS rating 0-5)	5/5	5/5
		System feedback				5/5
		System response to errors				5/5
		System clutter				5/5
		User's subjective satisfaction				4/5
	Performance	Page load time/Response time	10 seconds	Google Analytics	5 seconds	1.2
Effectiveness	Perceived relevance of data	5/5	User questionnaires (SUS rating 0-5)	5/5	5/5	
Open source and external plugins (TUC)	Functional suitability	no. of requirements achieved	N/A	N/A	100% coverage of the considered OTM capabilities (10 operational and 10 technical)	-Several tools have been recorded for each OTM, covering also different operating systems and level of required expertise from the user. -Several training materials have been recorded for each OTM, covering also different level of user expertise. Also, several of

						these elements have been mapped within the SENTINEL Wiki as additional reading material for the various terms and concepts that are explained there.
	Ease of integration	setup overhead	Adequate APIs to add, retrieve, update, and delete tools and training material in a SENTINEL repository.	N/A	A fine-grain mechanism to ingest the data in a local database	A model has been defined (describing each tool's details) and parsed by the recommendation engine. APIs have been created and the data are stored in a database, internally within the SENTINEL Platform.
	Maintainability	support community size	Each of the recommended plugins that a user has to installed it in his/her system, should be supported by an active community that maintains it and takes care of its security.	Methodologies that evaluate open source projects ^{10, 11, 12}	All plugins that need installation in the user's environment are evaluated and found secure for use.	Around 50 tools were included along with 100 accompanying training materials. A methodology was followed to verify that the tools are safe to use and are supported by an active community.

4.2 SENTINEL functional completeness assessment towards SMEs requirements

This section presents whether the SENTINEL platform functionalities and capabilities cover the Business and Application Requirements identified in D1.2 [27] using the assessment templates identified in D6.1 [5].

4.2.1 SENTINEL platform assessment towards Business Requirements

Within this Section, Business Requirements (BR) (cf. D1.2) are grouped into six (6) high-level families (i.e., BR-CIA¹³, BR-NFR¹⁴, BR-GEN¹⁵, BR-PDP¹⁶, BR-PET¹⁷, BR-CS¹⁸) and assessed per

¹⁰ Opensource Security Index: <https://opensourcesecurityindex.io/>
¹¹ OpenSSF Best Practices: <https://www.bestpractices.dev/en/projects>
¹² Opensource Insights: <https://deps.dev/>
¹³ Confidentiality, Integrity, Availability, Non-Repudiation
¹⁴ Non-Functional Quality
¹⁵ Generic Cybersecurity
¹⁶ Personal Data Protection
¹⁷ Privacy Enhancing Technologies
¹⁸ Cybersecurity Technical

distinct high-level family to facilitate the reader and avoid providing exhaustive redundant information.

Table 10. SENTINEL addressing SME’s Confidentiality, Integrity, Availability, and non-Repudiation requirements

Business Requirements ID/Name related	<ul style="list-style-type: none"> BR-CIA001/ Confidentiality BR-CIA002/ Integrity BR-CIA003/ Availability BR-CIA004/ Non-repudiation 	Business Requirements Family (Type)	CIA-high level (BR-CIA)
Description	<ul style="list-style-type: none"> Protect assets from being exposed to unauthorized parties, for example in the case of a data breach Only allow modification of assets by authorized individuals Ensure the continuous availability of the SME services and data to authorised internal and external entities Provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed 		
Rationale in SENTINEL	<p><u>Confidentiality/Integrity/ Availability</u>: core requirements belonging to the CIA triad, which permeate every technical implementation of both contributed and SENTINEL components, for CS and PDP.</p> <p><u>Non-repudiation</u>: considered as an addition to the core CIA triad. This requirement should be satisfied by technical SENTINEL implementations which enforce authenticating identities.</p>		
Means of technical implementation	<p><u>Confidentiality</u>: i) Identity management, authorisation, authentication and access control technologies (against data breaches); ii) Unobservability; iii) Encryption; iv) Anonymisation; iv) Pseudonymisation; v) Data obfuscation; v) Disclosure control; vi) Network security (secure network configurations, firewalls, WAFs, IDS etc); vii) Best CS workplace practices; viii) Endpoint protection software; ix) Email & mobile security</p> <p><u>Integrity</u>: i) Identity management, authorisation, authentication and access control technologies (against unauthorized data modification); ii) Unobservability; iii) Encryption and cryptographic integrity controls; iv) Endpoint protection software; v) Best CS workplace practices.</p> <p><u>Availability</u>: Endpoint protection software; ii) Identity management, authorisation, authentication and access control technologies (against service disruptions); iii) Network security (secure network configurations, firewalls, WAFs, IDS etc against DoS and similar disruptions); iv) Backup software and business continuity planning and services; v) Secure, redundant and available infrastructure, including Cloud, configurations</p> <p><u>Non-repudiation</u>: i) Cryptographic non-repudiation controls (PKI, digital signatures etc); ii) Email security; iii) IAM; iv) Logging, record keeping and audit management</p>		
Evaluation Methodology	<p>Tested i) in a Lab environment, and ii) via trials execution during the CG Pilot and validated through replying to specific corresponding questions in the online SENTINEL User Evaluation Questionnaire and towards validation metrics related to CS and PDP.</p>		
Evaluation outcomes	<p>Pass</p> <p>Since SENTINEL Technical Measures are based on ISO/IEC 27001:2013 [22] which addresses CIA, there are several SENTINEL measures addressing such SMEs requirements. A few examples are presented in the following.</p> <p><u>BR-CIA001, BR-CIA002, BR-CIA003</u>: indicative examples of OTMs addressing CIA requirements can be identified in the Organisational Measures for assigning roles and</p>		

	responsibilities – Category 2, Organisational Measures for enforcing an access control policy – Category 3, Organisational Measures for managing data processors for the GDPR – Category 6, Technical Measures for server and database security – Category 3, Technical Measures for endpoint security (workstations) – Category 4, Technical Measures for endpoint security (mobile devices) – Category 5 Validation towards respective quality metrics, such as compliance (e.g. conformance and anonymisation techniques), data breach prevention and threat containment. It reached the expected results (cf. section 4.1.1.1)
Evaluator	Technical partners, CG end-users
Evaluation phase	During the FFV development and the CG Pilot
Comments	All above presented OTMs are described in D3.3.

Table 11. SENTINEL platform towards non-functional/quality requirements

Business Requirements ID/Name related	Business Requirements Family (Type)	Non-functional / quality (BR-NFR)
<ul style="list-style-type: none"> • BR-NFR001/ Usability • BR-NFR002/ Cost-effectiveness • BR-NFR003/ Scalability 		
Description	<ul style="list-style-type: none"> • Provide cybersecurity, privacy and personal data protection solutions: <ul style="list-style-type: none"> ○ easy and intuitive to use; ○ at a cost-effective level for the participant SMEs. • Deploy scalable cybersecurity, privacy and personal data protection solutions which can effectively support the SME as its business and requirements grow 	
Rationale in SENTINEL	<p><u>Usability:</u> SENTINEL, as an integrated digital framework, should be intuitively presented to participant SMEs as a compliance-as-a-service offering and not add additional admin burden to their everyday process.</p> <p><u>Cost-effectiveness:</u> One of the main purposes of SENTINEL is to provide cybersecurity, privacy, and personal data protection services in a cost-effective manner. The implementation of its proposed OTMs should not consume more human and financial resources compared to hiring external CS experts and implementing their recommendations.</p> <p><u>Scalability:</u> We interpret scalability as the SENTINEL platform’s capability to offer a continuous service which adapts to the SME needs as the company evolves – not as a service users would only visit once, to get a set of policy recommendations.</p>	
Means of technical implementation	<p><u>Usability:</u> The user journey across the SENTINEL components and services should be easily navigable and the value to be gained understandable and attainable for end-users (UX). Finally, the individual web implementations and front-end components should be realised with best UI practices in mind.</p> <p><u>Cost-effectiveness:</u> The SENTINEL recommendation engine should consider various cost factors which are weighted highly against the budget restrictions provided by the SME.</p> <p><u>Scalability:</u> It is attained by a) emphasising the usability and perceived value of components such as the observatory, the compliance centre, the enforcement centre and the incident response centre, which boost the total lifetime value which end SME users get from leveraging SENTINEL in a continuous manner; and b) enabling the core self-assessment and recommendation components to reassess the SME CS and</p>	

	<p>PDP stance often and update the existing recommendations to reflect the new company scale and requirements and they grow.</p>
<p>Evaluation Methodology</p>	<p><u>BR-NFR001/Usability</u>: The testing and validation of SENTINEL platform upon UI/UX perspectives was a continuous effort of pilot end-users starting from the MVP release until the SENTINEL final product. Specifically, we organized 3 pilot executions (i.e., CG Pilot, TIG Pilot, DIH Pilot) and a last pilot event (i.e. the SME user-centric workshop in M33) with a set of trials performed by 29 pilot end-users deriving from 2 internal and 25 external SMEs who validated the SENTINEL platform via the online SENTINEL User Evaluation Questionnaire (cf. D6.2; D6.1). Specifically, for assessing the SENTINEL user journey, we identified a set of questions based on the System Usability Scale (SUS) evaluation [11] addressing UI/UX and user satisfaction quality metrics and respective sub-metrics (e.g. learnability) following quality models, such as the ISO/IEC 25010:2011 [9]. All these questions were consolidated in respective sections of the questionnaire. Moreover, additional end-users textual feedback towards SENTINEL UI/UX perspectives was collected from internal pilot owners (i.e. CG and TIG end-users) via completing an excel evaluation for SENTINEL MVP (cf. D6.1) and FFV (cf. D6.2) versions. The overall end-user feedback was processed, presented in analytics (cf. D6.1, D6.2, D6.3) and measured in a quantitative approach using the System Usability Scale (SUS), as depicted in the validation variables tables (cf. 4.1.1).</p> <p><u>BR-NFR002/ Cost-effectiveness</u>: concerning this requirement, we identified a specific question in the SENTINEL User Evaluation Questionnaire asking the end-users whether they believe that the use of SENTINEL will not necessitate additional human and/or financial resources (e.g. hiring external cybersecurity analysts and privacy experts) for implementing the OTMs recommended by SENTINEL. Furthermore, we gathered information on how much they spend on data protection compliance software/services on an annual basis. In addition, we gathered validation results concerning a specific cost/effort reduction validation variable metric. All this information together with desk research conducted to gather information and insights on commercial tools/services like SENTINEL have helped us to illustrate the cost-effectiveness aspect of the SENTINEL platform.</p> <p><u>BR-NFR003/ Scalability</u>: to test whether this requirement was satisfied by SENTINEL, we encouraged pilot owners (e.g. CG end-users) to use the SENTINEL platform as a continuous process at different time periods, e.g. CG end-users during the CG Pilot execution (M23-M27) and in the final pilot event (M33). Specifically, the maintainability validation metric was identified to measure the satisfaction of this requirement with the dichotomous score “true/false”.</p>
<p>Evaluation outcomes</p>	<p>Pass</p> <p><u>BR-NFR001/ Usability</u>: Concerning the questions related to usability and user satisfaction metrics, we reached positive responses¹⁹ in all pilots on average, including the final SME user-centric workshop (cf. pilot results in sections 3.6, 4.6, 4.7.3.3, 5.6 of D6.2 and final SME user-centric workshop results in section 3.4). In addition, this is documented in the pilot validation tables by reaching the expected result (cf. section 4.1.1), i.e. SUS score: ≥4 out of 5 (score 4 corresponds to “agree” responses whereas score 5 refers to “strongly agree” responses)</p> <p><u>BR-NFR002/ Cost-effectiveness</u>: Based on feedback from questionnaires during SME workshops, and as noted in a report by GDPR.EU [28], small businesses spend between €1,000 and €50,000 on GDPR compliance, covering consultant fees and technology costs. Furthermore, according to the final SENTINEL business model and initial pricing strategy, the price of the SENTINEL platform under standard plan is estimated at 348 €/year, and under premium plan at 708 €/year. This pricing strategy is</p>

¹⁹ A positive response is defined as a situation where the percentage of "Agree" or "Strongly agree" responses surpasses the percentage of "Neither Agree nor Disagree", "Disagree" or "Strongly disagree" responses (N/A answers not counted).

	<p>aimed at keeping costs low and affordable for most SMEs, substantially cutting compliance expenses, especially where SMEs would typically incur high fees from compliance consultants.</p> <p><u>BR-NFR003/ Scalability:</u> With respect to scalability as interpreted above, the SENTINEL platform was used as a continuous process by CG end-users and Dimensions Care and Sportfit end-users on behalf of TIG (during the respective pilots and the last SME user-centric workshop, presented in the current deliverable). The related validation result reached the expected outcome (cf. 4.1.1.1) and additionally CG pilot end-users reported that using the SENTINEL platform more than once helped them to raise their concern about cybersecurity (CS) and personal data protection (PDP). Nevertheless, improvements in scalability undertaken during the final technical refinements of the platform until M36 considering the feedback received from the final pilot event of M33. These improvements are reported in D5.7.</p>
Evaluator	Pilot end-users
Evaluation phase	<ul style="list-style-type: none"> • SENTINEL MVP testing and validation (M16-M17) • SENTINEL FFV (1st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, DIH Pilot) during the Demonstration phase (M19-M30) • SENTINEL Final Product (2nd prototype) in the final SME user-centric workshop (M33)
Comments	All above findings have been documented in deliverables D6.2, D6.3, D7.8, D7.9, D8.3

Table 12. SENTINEL platform towards generic cybersecurity requirements

Business Requirements ID/Name related	<ul style="list-style-type: none"> • BR-GEN001/Policy Drafting • BR-GEN002/Policy Enforcing • BR-GEN003/ AAA • BR-GEN004/ Incident reporting and handling • BR-GEN005/ Awareness, education, training • BR-GEN006/ Unlinkability • BR-GEN007/ Undetectability/unobservability • BR-GEN008//Self-assessment • BR-GEN009 "Business continuity" 	Business Requirements Family (Type)	Generic Cybersecurity (BR-GEN)
Description	<ul style="list-style-type: none"> • Draft an internal policy for the SME, recommending specific organisational and technical measures to be implemented, in accordance with the risk level associated with specific data processing operations. • Monitor the implementation of specific policy points and track their progress. • Authentication, Authorisation and Accounting (AAA): to provide the technical means for a) identifying users; b) granting access to resources based on their explicitly defined privileges and c) all related logging, record keeping and supporting auditing. • Establish planning, procedures and technical means for ensuring and orderly and effective response to cybersecurity incidents and data breaches. • Take measurable actions towards more and better knowledge towards cybersecurity, privacy and personal data protection for participant SMEs. • Prevent potential attackers from linking information to natural persons or other sensitive or personally identifiable information. • Prevent potential attackers from detecting information of interest or observing related operations. • Provide the means for participant SMEs to self-assess their current standing in terms of cybersecurity and personal data protection, including w.r.t. OTMs for GDPR compliance. 		

	<ul style="list-style-type: none"> Implement organizational measures for business continuity as well as SME-wide data backup, restore and other technical procedures (e.g., disaster sites).
<p>Rationale in SENTINEL</p>	<p><u>Policy Drafting</u>: Take into account a) the risk level associated with specific identified SME personal data processing operations and b) the intelligent recommendations proposed by the digital core to draft a policy that is readable and trackable by both machine and human.</p> <p><u>Policy Enforcing</u>: SENTINEL proposes a hybrid policy enforcement approach where organisational and other measures which have to be human-tracked are supported by digitalised checklists and progress indicators, similar to project management tool. Specific components which enable the digital tracking of the implementation of technical measures (e.g., via agent-based security monitoring) will be taken into account for a fully automated tracking and reporting.</p> <p><u>AAA</u>²⁰: an integral part of every CS and PDP policy. SENTINEL will tackle this requirement by recommending internal and external components for both on-premises and Cloud SME infrastructures and services.</p> <p><u>Incident reporting and handling</u>: incident response in SENTINEL should be tackled during the 'lifecycle support' phase of SME participation, in the incident response centre, along with the compliance and enforcement centres.</p> <p><u>Awareness, education, training</u>: Cyber awareness and training is a requirement that should be present in every SENTINEL implementation that is user-facing. SENTINEL tackles this through a) simple and attainable CS recommendations and checklists to improve the workplace cyber culture; b) targeted recommendations of CS and PDP training and educational courses tailored to individual company requirements.</p> <p><u>Unlinkability (data minimisation), undetectability and unobservability</u>: important techniques for enhancing privacy, pursuant to art.32 of GDPR.</p> <p><u>Self-assessment</u>: playing a pivotal role in SENTINEL, it provides both an entry point for SME participants and a process which they revisit as their requirements change. Self-assessment provides the basis for a) evaluating the current CS and PDP status; b) calculating RASE scoring; c) sharing critical input data to the Recommendation Engine and d) recommending targeted trainings.</p> <p><u>Business continuity</u>: SENTINEL should a) recommend robust organisational measures for business continuity as part of the drafted policy and b) provide the technical means by which these can be enforced.</p>
<p>Means of technical implementation</p>	<p><u>Policy Drafting/Enforcing</u>: Implementation of the policy drafting and enforcement module (T3.4).</p> <p><u>AAA</u>: SENTINEL will provide robust AAA capabilities through a) the IdMS component, taking over managing customers' personal data for GDPR compliance and b) through provisioning external (open source and commercial) IAM and identity management & auth proxy services as a technical measure, where recommended.</p> <p><u>Incident reporting and handling</u>: Implementation SENTINEL's trustworthy incident reporting and sharing module (T3.2) which interfaces with the recommendation engine, policy enforcement module, the MySentinel dashboard and the SENTINEL Observatory.</p> <p><u>Awareness, education, training</u>: a) providing external training content (e.g., educational courses) with the appropriate metadata for effective recommendations (T2.4); b) performing recommendations tailored to individual participants following self-assessment (T4.3).</p>

²⁰ approached as IAM when emphasising identity management.

	<p><u>Unlinkability, Undetectability and Unobservability:</u> a) Obfuscation, Pseudonymization, AI-assisted PETs for unlinkability. (T2.4), b) Robust IAM; Data minimisation, encryption, data obfuscation; Disclosure control for Undetectability and Unobservability_(T2.4).</p> <p><u>Self-assessment:</u> Implementation of SENTINEL’s self-assessment centre, including tailor-made requirement analysis, RASE scoring and training courses recommendations (T4.3).</p> <p><u>Business continuity:</u> i) Implementation of the policy drafting and enforcement module (T3.4) and ii) selection and recommendation of appropriate external OS or commercial technical solutions (e.g., Cloud or local backup services etc).</p>
<p>Evaluation Methodology</p>	<p>The SENTINEL platform was assessed upon addressing these requirements via a set of pilot experiments involving 12 different types of PAs, conducted by 29 end-users and through several trials during the three Pilots (i.e., the CG Pilot, TIG Pilot, DIH Pilot) and the SME-centric Workshop (additional 3 EAB members participating in the latter) under the activities of T6.2 and T6.3, considering also the internal testing procedure performed by project partners, occurred under the activities of T5.3 (cf. D5.7).</p> <p>Each of the PA experiments performance, required from end-users to implement a set of test cases in the SENTINEL platform, including: i) the conduction of self-assessments, e.g. CGPR Compliance Self-Assessment (CSA), Cybersecurity Risk Assessment (CSRA), ii) Acquiring and tracking Policy Recommendations engaging a group of Organisational and Technical Measures (OTMs) and receiving a list of respective training material, and iii) utilising additional SENTINEL cybersecurity services via the CyberRange gaming and the observatory repositories to identify cyber-attacks and security incidents. The pilot end-users provided feedback from the experience gained via online questionnaire responses (either using the SUS scale model or by responding in a textual format) and validating the SENTINEL platform towards specific corresponding variables and quality metrics, such as compliance, threat containment and data breach prevention for which baseline values and benchmarks were identified where applicable (cf. validation variables template in Appendices).</p>
<p>Evaluation outcomes</p>	<p>Pass.</p> <p><u>BR-GEN001, BR-GEN002, BR-GEN005, BR-GEN008, BR-GEN009:</u> The SENTINEL platform provides 20 categories of OTMs based on ISO/IEC 27001:2013 [22] and the ENISA’s risk-based approach [13],[14],[15], including 96 Organisational and 79 Technical measures grouped and categorized by an associate risk level. In addition, for education and training purposes, it provides 54 open-source tools and 114 training elements related to CS and PDP covering all SENTINEL OTMs which enhance the long-term maintainability and they are ease to integrate or applied in the SMEs’ information systems.</p> <p>For each PA experiment, a CSA self-assessment was performed, the PA risk level was successfully calculated and respective OTMs were received. Most end-users responded positively that Policy Recommendations are described accurately and clearly (cf. results of CG Pilot, DIH Pilot in D6.2 Sections 3.6.2, 5.6.2 and final SME user-centric workshop results in D6.3 Section 3.4.2). In addition, the achieved results towards compliance metrics reached the targeted values (cf. validation variable tables in Section 4.1.1). For instance, regarding CG Pilot validation results, SENTINEL OTMs improved the company’s compliance efficiency at 40% (cf. 4.1.1.1).</p> <p><u>BR-GEN003:</u> For each PA experiment conducted by an end-user a set of OTMs recommended policies was received. The SENTINEL platform defines OTMs based on assets ownership and locality declared by the SME user in the Organisation Profile.</p> <p>Furthermore, we provide different recommendation (in terms of policy-text) for the same OTM depending on whether the assets are owned by the SME or not owned and if</p>

	<p>owned depending on whether the assets are hosted on-premises or in the cloud by a vendor following a hybrid approach in case there are assets hosted on-premises and assets hosted in the cloud.</p> <p><u>BR-GEN004</u>: The SENTINEL incident reporting and sharing module capability was successfully tested by technical partners in a laboratory environment. It was optionally provided to end-users for exploration. Nevertheless, during the DIH Pilot, 60% of end-users responded positively that it was easy to understand the use of SENTINEL incident reporting and sharing environment (cf. D6.2 Section 5.6.2). Moreover, Privacy incidents can be prevented by implementing SENTINEL recommendations.</p> <p><u>BR-GEN006, BR-GEN007</u>: This corresponds to the validation results towards: i) the data breach prevention metrics which reached the expected outcome (cf. D6.2 Section 4.1.1). For instance, concerning the CG Pilot, focused pilot experiments were conducted related to genomics topic of healthcare and more than 6 attack scenarios were investigated on cyber assets participating in the identified PAs using the SENTINEL simulation environment. In addition, the received OTMs recommendations raised end-users awareness on PDP and GDPR compliance of their PAs, and ii) anonymized techniques derived from SENTINEL OTMs were considered as measures to prevent adversaries from identifying information of interest (cf. D6.2 Section 4.1.1.1)</p>
Evaluator	Pilot end-users (both from internal and external SMEs)
Evaluation phase	<ul style="list-style-type: none"> • SENTINEL FFV (1st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, DIH Pilot) during the Demonstration phase (M19-M30) • SENTINEL Final Product (2nd prototype) in the final SME user-centric workshop (M33)
Comments	All above modules have been implemented in the SENTINEL platform and documented in the following technical deliverables D3.1, D3.2, D3.3, D2.1, D2.2, D2.3, D4.1, D4.2, and D4.3.

Table 13. SENTINEL platform towards generic PDP requirements

Business Requirements ID/Name related	<ul style="list-style-type: none"> • BR-PDP001/ Data collection & flow mapping • BR-PDP002/ Record keeping and audit management • BR-PDP003/ Data sovereignty & portability • BR-PDP004/ DPIA • BR-PDP005/ Data transfers, vendor & 3rd party management • BR-PDP006/ DPO management • BR-PDP007/ Notices & consent management • BR-PDP008/ Compliance & accountability 	Business Requirements Family (Type)	Generic PDP (BR-PDP)
Description	<ul style="list-style-type: none"> • Perform a detailed map of the SME's data flows in order to evaluate associated privacy risk. • Enforce companywide OTMs for documenting non-repudiable records, processes, and accountability for the data stored by the SME. • Provide the technical means by which a) end-users are made the sovereign owners of their own personal data, with portability, updating, deletion, disclosure (e.g., to SMEs) and b) data remain physically within their legally bound sovereign geographical area(s). • Data protection impact assessment: To identify and evaluate risk associated with the SME's data processing activities. 		

	<ul style="list-style-type: none"> • Provide a complete and integrated third-party risk management solution for GDPR compliance, including managing risk related to processors and sub-processors. • Provide the company’s assigned DPO with the technical means to organise and monitor work. • Provide the SME with the technical means to be able to demonstrate that personal data of third parties (data subjects) are processed in a transparent manner (right to be informed), and the means for data subjects to provide their voluntary and explicit consent to this processing. • Provide the SME with the appropriate technical means to be able to demonstrate the implemented OTMs and their effectiveness when requested, as well as monitor overall GDPR compliance.
<p>Rationale in SENTINEL</p>	<p><u>Data collection & flow mapping</u>: In SENTINEL, a lightweight (due to its automated nature) approach for mapping data processing operations for GDPR compliance takes part during self-assessment, when the overall data processing environment and its different procedures are evaluated. Where a more rigorous is indicated, the appropriate external components shall be recommended.</p> <p><u>Record keeping and audit management</u>: partly satisfied by the generic CS technical requirement for AAA (Accounting). Record keeping is observed by several SENTINEL components such as the IdMS (T2.2), the GDPR compliance framework (T2.1), MITIGATE (T2.3) and the DPIA suite (T4.2).</p> <p><u>Data sovereignty & portability</u>: as a locale-specific requirement, it is one that SENTINEL should address in every related PDP component.</p> <p><u>DPIA</u>: traditionally human-centric assessment where assessors evaluate risk by deeply understanding the environment wherein data processing operations take place within a company. SENTINEL, by automating parts of the process, cuts costs, and offers benefits to SMEs which can describe their processing in a way that enables automated risk assessment.</p> <p><u>Data transfers, vendor & 3rd party management</u>: SENTINEL should address data processor management requirements in every related PDP component.</p> <p><u>DPO management</u>: SENTINEL should address DPO needs and requirements in every related PDP component.</p> <p><u>Notices & consent management</u>: SENTINEL should simplify the needs for implementing transparency and consent mechanisms by integrating it into PDP policy in clear terms and providing the technical means to enforce it.</p> <p><u>Compliance & accountability</u>: One of the overarching benefits of SENTINEL is that it promises a 360o view of the participant SME’s GDPR standing w.r.t. compliance. This view is made attainable through the integration of a number of interrelated components.</p>
<p>Means of technical implementation</p>	<p><u>Data collection & flow mapping</u>: i) SME self-assessment for PDP; and ii) selection and recommendation of appropriate external OS or commercial solutions (as part of a data governance policy).</p> <p><u>Record keeping and audit management</u>: parts related to GDPR compliance are satisfied, in conjunction with Data collection & flow mapping requirement by recommending technical solutions for data inventory, mapping, logging and data processing recording for each DP operation.</p> <p><u>Data sovereignty & portability</u>: a) SENTINEL IdMS (T2.2); b) GDPR compliance framework (T2.1); c) external components for complex implementations as required</p> <p><u>DPIA</u>: a) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3); b) DPIA within the Security and Privacy assurance Suite (T4.2); and c) External components or human intervention when unavoidable (T2.4).</p>

	<p><u>Data transfers, vendor & 3rd party management</u>: a) GDPR compliance framework (T2.1) – in part ; b) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3) – in part; and c) External components as recommended (T2.4).</p> <p><u>DPO management</u>: Compliance centre. Enforcement centre. Observatory. Incident response centre. Integrated PDP related SENTINEL components.</p> <p><u>Notices & consent management</u>: a) as a drafted policy item; b) as guidance for SMEs to self-implement (e.g., via CMS-website modules or 3rd party technical integrations, e.g., in GDPR email campaigns) or c) external components as recommended (T2.4) when a more holistic approach is called for.</p> <p><u>Compliance & accountability</u>: i) All contributed and external PDP components (T2.3; T2.4); ii) Compliance centre (T5.2, T5.1); iii) Enforcement centre (T5.2, T5.1); iv) Observatory (T4.4); and v) PDP and data privacy compliance framework (T2.1)</p>
<p>Evaluation Methodology</p>	<p>Tested i) in a Lab environment; and ii) via trials execution during the CG Pilot and validated through replying to specific corresponding questions in the online SENTINEL User Evaluation Questionnaire and towards validation metrics related to GDPR compliance.</p>
<p>Evaluation outcomes</p>	<p>Outcomes of the evaluation (i.e., pass/ fail/ untested and summary of outcome):</p> <p><u>Data collection & flow mapping</u> [Pass]: 85% of users used generic PAs to create their own PAs. Only 15%, create their own PAs. Identification of PAs remains a key challenge for SMEs. Generic PAs ease this identification.</p> <p><u>Record keeping and audit management</u> [Pass]: In SENTINEL, access to SENTINEL’s functionalities as GDPR Self-assessment, DPIA, Cybersecurity Risks Assessment requires first to record the PA. By mandating the record of PAs, the use of SENTINEL promotes auditability and accountability of SMEs.</p> <p><u>Data sovereignty & portability</u> [Data sovereignty: Pass / portability: untested]: Compliance with GDPR has been successfully tested, _GDPR CSA provides an assessment of measures implemented to ensure compliance with GDPR. It also provides SMEs with a list of OTMs to implement to increase accountability level. Data portability functionality has not been tested since it has decided to implement it.</p> <p><u>DPIA</u> [untested]: Because such functionality was not implemented for testing sessions, it has not been tested.</p> <p><u>Data transfers, vendor & 3rd party management</u> [Pass]: GDPR CSA includes a set of questions related to the management of transfer of data.</p> <p><u>DPO management</u> [Pass]: SENTINEL provides assigned DPO with a compliance dashboard allowing them to have an overview of PAs ’status according to GDPR.</p> <p><u>Notices & consent management</u> [Pass]: All requirements related to transparency and consent management are included in assessment provided by GDPR CSA.</p> <p><u>Compliance & accountability</u> [Pass]: The different modules provided by SENTINEL allows SMEs to verify whether appropriate organisational and technical measures are implemented to ensure the protection of personal data. By recording this measure, SENTINEL make the obligation for SMEs to demonstrate their compliance easier.</p>
<p>Evaluator</p>	<p>Pilot end-users</p>
<p>Evaluation phase</p>	<ul style="list-style-type: none"> • SENTINEL FFV (1st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, DIH Pilot) during the Demonstration phase (M19-M30). • SENTINEL Final Product (2nd prototype) in the final SME user-centric workshop (M33).

Comments	-
-----------------	---

Table 14. SENTINEL platform towards privacy enhancing requirements

Business Requirements ID/Name related	<ul style="list-style-type: none"> • BR-PET001/ Encryption • BR-PET002/ Data minimisation • BR-PET003/ Data anonymisation, pseudonymisation, obfuscation • BR-PET004/ Advanced PETs 	Business Requirements Family (Type)	Privacy enhancing (BR-PET)
Description	<ul style="list-style-type: none"> • Ensure the confidentiality of data at rest or in transit via cryptography. • Provide the OTMs for the SME to limit that personal data processed to what is necessary and not hold more than is absolutely needed for the processing operation. • Provide the technical means for the SME to de-identify personal data, rendering them anonymous or unreadable to potential threats, ensuring privacy by design. • Provide state-of-the-art privacy enhancing techniques such as differential privacy, secure multiparty computation, homomorphic encryption and zero-knowledge proofs. 		
Rationale in SENTINEL	<p><u>Encryption</u>: SENTINEL will recommend technologies which apply encryption at various layers of the data stack to offer better privacy by design in the transformed data processing operations.</p> <p><u>Data minimisation</u>: SENTINEL will recommend technologies that make data minimisation feasible at various layers of the data stack to offer better privacy by design in the transformed data processing operations.</p> <p><u>Data anonymisation, pseudonymisation, obfuscation</u>: SENTINEL will recommend technologies that improve privacy by design in the transformed data processing operations.</p> <p><u>Advanced PETs</u>: SENTINEL will recommend technologies that improve privacy by design through state-of-the-art PETs in the transformed data processing operations only in specific scenarios where such advanced techniques are suitable and attainable for the SME.</p>		
Means of technical implementation	All PET requirements are satisfied by Policy Recommendations and external components (T3.3, T3.4, T2.4).		
Evaluation Methodology	Tested i) in a Lab environment, ii) via trials execution during the CG Pilot and validated through specific corresponding questions responses via the SENTINEL User Evaluation Questionnaire and towards validation metrics related to PDP compliance.		
Evaluation outcomes	<p>Pass</p> <p><u>BR-PET001, BR-PET002, BR-PET003, BR-PET004</u>: As reported in D3.3, SENTINEL Organisational Measures of Category 6 “Managing GDPR Compliance” address the GDPR specific requirements. In addition, there are several SENTINEL Technical Measures recommending the application of PETs and corresponding educational material and tools. Such Technical Measures are indicatively presented below along with the category they belong:</p> <ul style="list-style-type: none"> • Technical Measures for network security – Category 6 <ul style="list-style-type: none"> ○ Strong Encryption and WiFi Security on Wireless Access • Technical Measures of Authentication and Access Control – Category 1: <ul style="list-style-type: none"> ○ Hash and/or Encryption Techniques on Passwords (for owned assets) • Technical Measures for server and database security – Category 3: 		

	<ul style="list-style-type: none"> ○ Encryption for Data at-Rest (for owned assets) ○ Drives with Built-In Encryption (for owned assets) ○ Pseudonymization Techniques ○ Privacy-by-Design Techniques at the Database Layer • Technical Measures for endpoint security (workstations) – Category 4 <ul style="list-style-type: none"> ○ Policy on the use of cryptographic controls on Drives • Technical Measures for endpoint security (mobile devices) – Category 5 <ul style="list-style-type: none"> ○ Policy on the use of cryptographic controls on the Data Stored at Mobile Devices • Technical Measures for backup policy – Category 7 <ul style="list-style-type: none"> ○ Strong Encryption of Backups before Transmission ○ Strong Encryption of Backups at Storage • Technical Measures for application lifecycle security – Category 8 <ul style="list-style-type: none"> ○ Privacy Techniques for Addressing Security Requirements <p>50% of end-users of the CG Pilot on genomics (healthcare) positively responded on exploring SENTINEL recommendations/suggested tools/techniques related to anonymisation and pseudonymisation (cf. D6.2 [1] Section 3.6.5). They utilised anonymized techniques recommended by SENTINEL OTMs to convert the file names provided by the user to anonymised files (cf. Section 4.1.1.1).</p>
Evaluator	Technical partners, CG end-users
Evaluation phase	During the CG Pilot of testing and validation activities towards SENTINEL FFV (1 st prototype) M23-M27 (cf. D6.2)
Comments	All above OTMs are thoroughly described in D3.3.

Table 15. SENTINEL platform towards cybersecurity technical capabilities

Business Requirements ID/Name related	<ul style="list-style-type: none"> • BR-CS001/ Endpoint security • BR-CS002/ Vulnerability assessment, penetration testing • BR-CS003/ Email security • BR-CS004/ Network security • BR-CS005/ IAM (identity/access mgmt.) • BR-CS006/ Cloud security • BR-CS007/ Software lifecycle security • BR-CS008/ Monitoring and alerting • BR-CS009/ Logging 	Business Requirements Family (Type)	Cybersecurity Technical (BR-CS)
Description	<ul style="list-style-type: none"> • Provide the technical means (software) for securing SME end-user devices such as desktops, laptops, and mobile devices from being maliciously exploited by CS threats. • Provide the technical capabilities for identifying risks and vulnerabilities in the SME's computer and network infrastructure, hardware, applications, and other IT assets, including by means of safely exploiting these vulnerabilities. • Provide the technical means for protecting the SME's email accounts, email content, and related communications against unauthorized access, loss or compromise, including retention for legal and forensic purposes as per statutory requirements. • Recommend and implement OTMs to protect the usability, availability and integrity of the SME's network and data from all CS threats and data breaches. • This refers to the technical implementation of generic cybersecurity requirement BR-GEN003. The recommended technical means should be able to define and manage the roles and access privileges of individual entities (users and devices) to the SME's 		

	<p>Cloud and on-premises apps, endpoint devices and network resources at both the low (e.g., network resource, infrastructure) and high (app, SSO, etc) layers of the IT stack.</p> <ul style="list-style-type: none"> • Provide third-party (Cloud)-delivered and monitored CS services. • Provide the technical means to recommend and monitor cybersecurity requirements during software development lifecycles (SDLC) • Provide the technical capabilities to continuously monitor the SME’s IT assets for vulnerabilities and enforcement of policy, and send alerts to the associated event management system and personnel, in the case of incidents.
<p>Rationale in SENTINEL</p>	<p><u>Endpoint security</u>: SENTINEL should go beyond mere antivirus software recommendation and incorporate more holistic endpoint protection OTMs, such as threat detection, investigation, and response, endpoint device management, data leak protection (DLP), among others, to face today’s evolving threat landscape.</p> <p><u>Vulnerability assessment, penetration testing</u>: SENTINEL provides several components as part of its core framework which assess and evaluate an organisation’s CS vulnerabilities. Their individual capabilities will be defined in details and the resulting metadata used for smart recommendations, configuration, and policy drafting.</p> <p><u>Email security</u>: SENTINEL will recommend technologies that improve email cybersecurity both at the email server level where required (e.g., email proxies and secure gateways) and at the endpoints (e.g., MFA, encryption, etc).</p> <p><u>Network security</u>: Creating a secure network infrastructure for SMEs can be a complex task that includes many policy and technical implementation points. SENTINEL will provide the means to audit the SME’s current infrastructure configuration, the balance of on-premises vs Cloud resources and their individual configurations and recommend the proper policy and OTMs to secure it.</p> <p><u>Identity Access Management (IAM)</u>: SENTINEL will recommend IAM policy and OTMs which are fit for the company’s size and asset configurations, taking into account potential Cloud implementations.</p> <p><u>Cloud security</u>: SENTINEL will recommend third-party cybersecurity-as-a-service solutions when these can fill identified gaps in the drafted policy, as far as the requirements for usability, scalability and cost-effectiveness are satisfied.</p> <p><u>Software lifecycle security</u>: SENTINEL will prescribe secure SDLC practices and policies for SMEs who have in-house software development as a core process.</p> <p><u>Monitoring and alerting</u>: SENTINEL provides a number of components as part of its core framework which provide robust monitoring and altering functionality.</p> <p><u>Logging</u>: SENTINEL provides a dedicated component for advanced forensic visualisations and analytics.</p>
<p>Means of technical implementation</p>	<p><u>Endpoint security</u>: Policy recommendations and external components (T3.3, T3.4, T2.4)</p> <p><u>Vulnerability assessment, penetration testing</u>: Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Airbus CyberRange (T4.1), and Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.</p> <p><u>Email security</u>: Policy recommendations and external components (T3.3, T3.4, T2.4)</p> <p><u>Network security</u>: Airbus CyberRange (T4.1), MITIGATE (T2.3), Security Infusion (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) as necessary.</p> <p><u>IAM/ Cloud/ Software lifecycle security</u>: Policy recommendations and external components (T3.3, T3.4, T2.4) as required.</p>

	<p><u>Monitoring and alerting</u>: Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.</p> <p><u>Logging</u>: Forensics Visualisation Toolkit (T5.1), (T5.2). Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.</p>
<p>Evaluation Methodology</p>	<p>SENTINEL cybersecurity capabilities were tested i) in a lab environment, ii) via trials execution during the three Pilots and validated through specific corresponding questions of the SENTINEL User Evaluation Questionnaire and towards validation metrics related to threat containment and data breach prevention.</p>
<p>Evaluation outcomes</p>	<p>The above categories of requirements are covered either by SENTINEL OTMs corresponding categories or specific recommendations are provided depending on the assets' ownership and locality. Indicative examples of relevant OTMs are documented in the following.</p> <p><u>BR-CS001</u>: SENTINEL OTMs addressing this requirement are:</p> <ul style="list-style-type: none"> • All Technical Measures for endpoint security (workstations) – Category 4 (9 in total) • All Technical Measures for endpoint security (mobile devices) – Category 5 (9 in total) <p><u>BR-CS002</u>: Indicative SENTINEL OTMs addressing this requirement are:</p> <ul style="list-style-type: none"> • Technical Measures for application lifecycle security – Category 8 <ul style="list-style-type: none"> ○ Management of technical vulnerabilities ○ Regular Penetration Testing ○ Assets' Security Vulnerabilities Identification <p><u>BR-CS003, BR-CS004</u>: Indicative SENTINEL OTMs addressing these requirements reside in Technical Measures for network security – Category 6</p> <p><u>BR-CS005</u>: Indicative SENTINEL OTMs addressing this requirement reside in Organisational Measures for Enforcing an access control policy – Category 3 and Technical Measures for Authentication and access control – Category 1</p> <p><u>BR-CS006</u>: Indicative SENTINEL OTMs related to third-part (Cloud)-delivered and monitored CS Services can be considered in:</p> <ul style="list-style-type: none"> • Organisational Measures for securely managing assets – Category 4 (e.g. Asset Management) • Technical Measures for backup policy – Category 7 (e.g. Strong Encryption of Backups before Transmission) <p><u>BR-CS007</u>: Indicative SENTINEL OTMs addressing this requirement reside in Technical Measures for server and database security – Category 3 and Technical Measures for application lifecycle security – Category 8</p> <p><u>BR-CS008, BR-CS009</u>: Indicative SENTINEL OTMs addressing these requirements are:</p> <ul style="list-style-type: none"> • Organisational Measures for handling incidents – Category 7 (e.g. Enforcement of Detailed Tracking and Event Logging Mechanisms for Recording Incidents and Data Breaches) • Technical Measures for logging and monitoring – Category 2 <ul style="list-style-type: none"> ○ Event Logging ○ Logging of all types of Data Processing. ○ Timestamp and Protection of log information. ○ Clock synchronisation. ○ Administrator and Operator Logs. ○ Modification and Deletion of Log Files. ○ Log File Health Monitoring.

	<ul style="list-style-type: none"> ○ Reporting information security weaknesses. ○ Logging of all types of Data Processing. ○ Timestamp and Protection of log information. ○ Administrator and Operator Logs. ○ Modification and Deletion of Log Files. ○ Log File Health Monitoring. <p>Validated towards metrics, such as threat containment and data breach prevention during the three Pilots (cf. Section 4.1.1) and reached the achieved results. For instance, CG end-users explored more than 6 attack scenarios on their cyber assets using SENTINEL simulation environment and they raised their awareness on backup policies, Network Security, Server and database security from the SENTINEL OTM recommendations received. In addition, during the three pilots most end-users positively responded that SENTINEL OTMs can raise the cybersecurity of their cyber assets (cf. D6.2 Section 6.1).</p>
Evaluator	Technical partners, pilot end-users
Evaluation phase	During the CG Pilot of testing and validation activities towards SENTINEL FFV (1 st prototype) M23-M27 (cf. D6.2)
Comments	All above described OTMs are presented in D3.3.

4.2.2 SENTINEL platform towards Application Requirements

This section presents the assessment of SENTINEL platform capabilities and functionalities towards covering the functional and non-functional Application Requirements (AR).

4.2.2.1 Assessment of Functional Requirements

The current section illustrates the assessment of SENTINEL platform capabilities and functionalities towards covering the Functional Application Requirements (AR-FR). They are grouped into high-level families wherever needed to facilitate the reader and avoid duplication of information.

Table 16. SENTINEL platform towards business continuity

ID/Name	AR-FR001/ Business continuity	Type	Functional	Importance	Low
Description	To implement measures for business continuity as well as data backup. Robust backup and restore processes as well as virtual resources redundancy etc should be ensured by the SENTINEL architecture for continuity and contingency while delivering the SENTINEL services to participants.				
Context / Module	Core Context, Recommendation Engine				
Evaluation Methodology	This requirement was fulfilled via the implementation of organizational measures for business continuity as well as data backup, restore and other technical procedures.				
Evaluation outcomes	Pass. Policies recommended for addressing business continuity, restore processes and backup policy can be identified under Organisation measures for managing Business Continuity - Category 8 and Technical Measures for Backup Policy - Category 7. Furthermore, three (3) external tools and fifteen (15) external online courses and training				

	material are offered for Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) reputation management concepts to mitigate damages, recover business operations, and avoid critical business interruption.
Evaluator	All technical partners
Evaluation phase	Throughout the platform development lifecycle
Comments	The above OTMs and external tools and training are presented and described in D3.3 and D2.3.

Table 17. SENTINEL platform towards encryption

ID/Name	AR-FR002/ Encryption	Type	Functional	Importance	Medium
Description	To ensure the confidentiality of data at rest or in transit via cryptography. SENTINEL should encrypt a) participants' data and b) data in transit (SSL/HTTPS, etc) where appropriate, for additionally enhancing participants' privacy.				
Context / Module	MySentinel / IdMS				
Evaluation Methodology	Verified by several trials throughout the platform development				
Evaluation outcomes	100% pass				
Evaluator	ITML				
Evaluation phase	During the MVP, Full-Featured Version release and Final product				
Comments	-				

Table 18. SENTINEL platform towards data anonymisation, pseudonymisation, obfuscation

ID/Name	AR-FR003/ Data anonymisation, pseudonymisation, obfuscation	Type	Functional	Importance	Medium
Description	To provide the technical means for the SME to de-identify personal data, rendering them anonymous or unreadable to potential threats, ensuring privacy by design. SENTINEL should adopt data minimisations, purpose limitation and storage limitation principles in practice where participants' data are concerned, including measures for privacy enhancements (anonymisation, pseudonymisation, data obfuscation etc).				
Context / Module	N/A				
Evaluation Methodology	N/A				

Evaluation outcomes	N/A
Evaluator	INTRA
Evaluation phase	During the SENTINEL FFV (1 st prototype) development phase (M13-M18)
Comments	This requirement was dropped. As the project progressed it became clear that the data shared would by no means be sensitive. Moreover, given that requirement AR-FR002/Encryption was satisfied we decided not to implement this during the lifetime of the project.

Table 19. SENTINEL platform towards logging

ID/Name	AR-FR004/ Logging	Type	Functional	Importance	Medium
Description	SENTINEL should provide non-repudiable logging and auditing-supporting capabilities within its participant data-handling core contexts.				
Context / Module	N/A				
Evaluation Methodology	N/A				
Evaluation outcomes	N/A				
Evaluator	INTRA				
Evaluation phase	During the SENTINEL FFV (1 st prototype) development phase (M13-M18)				
Comments	After careful assessment we reckoned that the effort to implement a comprehensive cross-service logger would be quite high. On the other hand, the benefits would be negligible, especially in the context of the project lifetime.				

Table 20. SENTINEL platform towards analytics and visualisation

ID/Name	AR-FR005/ Analytics and visualisation	Type	Functional	Importance	Medium
Description	To provide the technical means, strategies, processes, and tools to diagnose, predict, and prevent cybersecurity incidents, along with the visualisations that can make data analysis understandable and actionable to analysts. The SENTINEL dashboard should provide dynamic real-time visualisations of participants data in the form of tables, smart charts and dashboard widgets (e.g., policy overview based on risk levels, progress towards policy implementation, incidents and status reporting and visualisations based on feedback from relevant plugins (FVT, MITIGATE, DPIA, and SI etc).				

Context / Module	MySentinel
Evaluation Methodology	For the evaluation of the platform analytics and visualisations, we pro-actively created mock-ups for the User Interface which were evaluated by the technical partners and the Project's consortium in terms of user friendliness. During the project's implementations and all the components integration, for each new dashboard, the same approach was followed. After the development of each use case and the interface, feedback was gathered through evaluation questionnaires that were circulated to the pilots but also representatives of SMEs.
Evaluation outcomes	The overall score of the relevant questionnaires' responses where 90% fully positive with users responding with the highest scores in a SUS scale rating of 0-5.
Evaluator	The evaluation was initially performed by all the technical partners of the consortium, later from the Project's pilots, and finally by external end-users.
Evaluation phase	The evaluation of the user friendliness and how intuitive the visualisations of the Sentinel platform are, was constant throughout the entire duration of the Project.
Comments	It is worth mentioning that a lot of effort has been given to the User Interface of the Sentinel Platform, since it is a solution that contains a lot of difficult terminology for non-experts. Thus, multiple additions and changes have been applied on the dashboards. Special tables have been created, intuitive tooltips and pop-up notification, wiki content and instructions on each dashboard, etc.

Table 21. SENTINEL platform towards flexibility of capabilities

ID/Name	AR-FR006/ Flexibility of capabilities	Type	Functional	Importance	High
Description	Be able to incorporate and/or remove capabilities provided by external software in a reasonably easy manner, without affecting the operation of the rest of the system. The CS and PDP offerings of the SENTINEL platform are provided by the incorporation of specialised software, developed, and maintained by external parties, independently of the system. Hence, SENTINEL should not depend on a stiff set of such components, but rather make provisions for their easy incorporation and removal.				
Context / Module	Core-Plugins repo				
Evaluation Methodology	<p>The requirement for SENTINEL to incorporate and remove capabilities from external software seamlessly was fully met through a strategic implementation approach.</p> <p>Firstly, our architecture was built upon microservices, ensuring modularity and flexibility. Each assessment module, including GDPR CSA, DPIA, CSRA, and CyberRange, was deployed as separate, standalone services. This design choice allowed for easy integration with SENTINEL without affecting the core system's operation.</p> <p>Furthermore, our services were stateless, meaning they could be scaled independently and replaced without disrupting the system's functionality. This enabled us to incorporate specialized software for CS and PDP offerings effortlessly.</p> <p>Adopting the orchestrator pattern further enhanced our ability to integrate external</p>				

	<p>capabilities smoothly. The orchestrator managed the communication and coordination between various microservices, ensuring seamless operation and easy incorporation or removal of components.</p> <p>By implementing adapters for each external service, we ensured compatibility with SENTINEL while maintaining independence from any specific set of components. Consequently, SENTINEL can adapt to evolving requirements and incorporate new capabilities with minimal effort, fulfilling the requirement for easy integration and removal of external software without impacting system operation.</p>
Evaluation outcomes	Pass (100% satisfied by design)
Evaluator	INTRA, all technical partners
Evaluation phase	Continuous starting from the platform design (D1.2 in M6) and until the end of the project (M36)
Comments	-

Table 22. SENTINEL platform towards flexibility of policies

ID/Name	AR-FR007/ Flexibility of policies	Type	Functional	Importance	High
Description	Be able to incorporate and/or remove security policy descriptions in a reasonably easy manner, without affecting the operation of the rest of the system. SENTINEL's recommendations and prescriptions in terms of Organisational and Technical Measures (OTMs), practices and policies for SMEs need to be updated and extended. The flexibility should consider interdependencies and the potential locking of existing OTMs in recommended policies.				
Context / Module	Core-Policies repo				
Evaluation Methodology	Review of the functionality by technical partners, during the weekly technical meetings.				
Evaluation outcomes	Pass, with comments.				
Evaluator	IDIR / FP				
Evaluation phase	M24-M36				
Comments	SENTINEL is founded on a flexible and modular architecture which affords a high degree of flexibility, not just for adding features or capabilities, but also for enriching existing repositories of data, information and knowledge. One example of this is the dependency between Core's "Common Repo" and "Recommendation Engine" components and the pluggable "Policy Drafting" component. Their collaboration allows SENTINEL to serve users with up-to-date recommendations of OTMs, tools and trainings as part of the drafted Policy. Although amending the core classification to accommodate OTM updates				

	or additions, currently requires some manual effort (due to the existence of more than one authoritative OTM source without a syncing mechanism between them) we can still support that policies can be relatively flexibly updated to in track with real-life data protection and cybersecurity developments and requirements.
--	---

Table 23. SENTINEL platform towards secure data exchange

ID/Name	AR-FR008/ Secure data exchange	Type	Functional	Importance	High
Description	SENTINEL should be able to exchange data with (sent to or receive from) third-party apps and platforms over secure APIs.				
Context / Module	Observatory (primary), Incident response (secondary)				
Evaluation Methodology	Tests on the interconnection between external platforms and SENTINEL Observatory to ensure seamless data transfer				
Evaluation outcomes	Pass				
Evaluator	ITML, AEGIS, and INTRA				
Evaluation phase	Throughout the project				
Comments	SSL encryption used throughout				

Table 24. SENTINEL platform towards SME onboarding

ID/Name	AR-FR009/ SME onboarding	Type	Functional	Importance	High
Description	SENTINEL should allow new participants to enrol in SENTINEL by creating an account and performing an initial profiling (requirements elicitation).				
Context / Module	MySentinel (primary), Self-Assessment (secondary)				
Evaluation Methodology	Functionality of registration mechanism tested by creating new accounts form an early phase of the project. Scalability and performance were also tested during the SMEs workshop where multiple accounts needed to be created in parallel.				
Evaluation outcomes	Pass				
Evaluator	All technical partners				
Evaluation phase	Throughout the platform development lifecycle				
Comments	-				

Table 25. SENTINEL platform towards RASE scoring

ID/Name	AR-FR010/ RASE scoring	Type	Functional	Importance	High
Description	SENTINEL should be able to assess and persistently store each SME participant's current status regarding their identified CS and PDP gaps in the form of "RASE", a multifactorial storage object which will be created following the participant's initial profiling (requirements elicitation) and updated after participating at each additional self-assessment pipeline or module. RASE forms the input of the recommendation engine from the SME's side.				
Context / Module	Self-assessment (primary), MySentinel, and Core (secondary)				
Evaluation Methodology	a) Evaluation by technical partners, during the weekly technical meetings. b) Evaluation in trials and the SME workshops.				
Evaluation outcomes	Pass				
Evaluator	IDIR				
Evaluation phase	M24-M36				
Comments	In SENTINEL's final version, the RASE score comprises: a) assessed risk level of each PA (SA engine); b) assessed risk level of the organisation as a whole (SA engine); c) OTMs implanted at the org level; d) OTMs implemented at the PA level; e) PA details – some of which may trigger custom OTM selection rules; f) ORG details – some of which may trigger custom OTM selection rules; g) the results of the GDPRCSA assessment; h) the results of the DPIA assessment, if any; and i) the results of the CSRA assessment(s).				

Table 26. SENTINEL platform towards plugin Recommendations and Policy Drafting

ID/Name	Recommendations and Policy Drafting: AR-FR011/ Plugin Recommendations AR-FR012/ Policy Drafting	Type	Functional	Importance	High
Description	<ul style="list-style-type: none"> SENTINEL should be able to make recommendations for a) OTMs and b) specific plugins, by considering the elements of a participant's RASE score, the attributes of the objects in the plugins repository and other data as necessary. SENTINEL should be able to draft a human- and machine-readable CS and PDP policy for the participant SME, by considering a) the output of the recommendation engine and b) the available objects in the policy repository. 				
Context / Module	Core-Recommendation engine, (primary), Core-Plugins repo (secondary)				
Evaluation Methodology	Evaluation by technical partners, during the weekly technical meetings. Evaluation in trials and the SME workshops.				

Evaluation outcomes	Pass, with remarks.
Evaluator	IDIR, and FP
Evaluation phase	M24-M36
Comments	SENTINEL's final version produces a human-readable policy, in the form of OTMs, tools and trainings, grouped by OTM category (20 categories total: 10 organisational and 10 technical). A <i>machine-readable output is not yet supported</i> , although there is functionality for exporting the recommendations / policy in PDF format.

Table 27. SENTINEL platform towards Policy Monitoring

ID/Name	AR-FR013/ Policy Monitoring	Type	Functional	Importance	Medium
Description	SENTINEL should be able to help participants track progress of their policy enforcement and implementation of specific OTMs.				
Context / Module	Core-Policy Enforcement Monitoring (primary), MySentinel, Core (secondary)				
Evaluation Methodology	<p>The statuses supported by SENTINEL concerning OTM implementation are the following:</p> <ul style="list-style-type: none"> • <i>Pending</i> (for OTMs which are recommended but not implemented as manually declared by the user). • <i>Implemented</i> (OTMs implemented as manually declared by the user). <p>The implementation status is provided at recommended OTM level for global recommendations and at PA level for individual (partial) recommendations. Towards this, the generation process of a SENTINEL policy properly considers the declared OTMs at the completed profile of all organization PAs. It should be noted that the monitoring process is available and recorded within the lifecycle of a specific generated policy.</p> <p>When a new policy draft is created, SENTINEL will intelligently update the implementation status of all OTMs (both global and PA-specific ones) of <i>“pending”</i>, depending on whether they are now recommended or not. <i>Implemented</i> OTMs are left unchanged in all scenarios.</p>				
Evaluation outcomes	Pass. For each OTM recommendation received upon PA experiments its implementation status (as indicated above) successfully depicted. The evaluation of SENTINEL towards this requirement conducted through PA experiments performed either by technical partners internal testing or by pilot end-users through trials execution. Specifically, 32 end-users in total (including 3 EAB members) conducted PA experiments and successfully received Recommendations along with their implementation status.				
Evaluator	Technical Partners, pilot end-users				
Evaluation phase	<ul style="list-style-type: none"> • Throughout the platform development lifecycle • SENTINEL FFV (1st prototype) pilot testing and validation during the Demonstration phase (M19-M30) 				

	<ul style="list-style-type: none"> SENTINEL Final Product (2nd prototype) in the final SME-centric workshop (M33)
Comments	-

Table 28. SENTINEL platform towards Incident Response

ID/Name	AR-FR014/ Incident Response	Type	Functional	Importance	Medium
Description	SENTINEL should provide a complete digital framework for responding to, handling, managing, and reporting CS incidents and data breaches.				
Context / Module	Incident response (primary), Observatory (secondary)				
Evaluation Methodology	Systematic review of the functionality of Incident response and Observatory throughout weekly Scientific & Technical meetings.				
Evaluation outcomes	Pass				
Evaluator	Technical partners				
Evaluation phase	<ul style="list-style-type: none"> Throughout the platform development lifecycle SENTINEL FFV (1st prototype) pilot testing and validation during the Demonstration phase (M19-M30) SENTINEL final product (2nd prototype) in the final SME-centric workshop (M33). 				
Comments	-				

Table 29. SENTINEL platform towards Policy Orchestration

ID/Name	AR-FR015/ Policy Orchestration	Type	Functional	Importance	Medium
Description	SENTINEL should help participants implement the recommended/drafted policy by (a) providing clear guidelines for each OTM and (b) providing installation and configuration guidelines for the suggested internal or external plugins, which may or may not be attached to an OTM.				
Context / Module	Core-Policy Drafting (primary), and Core-Policy Enforcement Monitoring (secondary)				
Evaluation Methodology	For each recommended OTM the SENTINEL platform proposes (i) available training material available to allow the SME to train their members and staff for better understand, manage, and satisfy the specific need, and (ii) available tools and solutions that can be utilised from the SME to properly enforce technical mechanisms that will help the organization to satisfy the specific Recommendation.				
Evaluation outcomes	Pass. Around 50 tools were included along with 100 accompanying training materials. Further information is presented in the verification variables table (cf. SENTINEL Open-source and external plugins in Section 4.1.2).				
Evaluator	Technical Partners, pilot end-users				

Evaluation phase	<ul style="list-style-type: none"> • SENTINEL FFV (1st prototype) pilot testing and validation during the Demonstration phase (M19-M30) • throughout the platform development lifecycle
Comments	Further information is presented in Table 30 for AR-FR016 requirement.

Table 30. SENTINEL platform towards Training Recommendations

ID/Name	AR-FR016/ Training Recommendations	Type	Functional	Importance	Medium
Description	SENTINEL should be able to make recommendations for external trainings in the form of links to courses and educational material (e.g., for technical IT staff or other staff) by considering the elements of a participant's RASE score, the attributes of the objects in the training content repository and other data as necessary.				
Context / Module	Core-Recommendation engine (primary), and Core-Trainings Repo (secondary)				
Evaluation Methodology	<p>Information concerning the external training material (e.g., description, related user expertise level, link to the source, etc.) is stored internally within the SENTINEL Platform in a local database. The data model includes features that permit the mapping of these elements with OTMs. Based on the overall evaluation of the SENTINEL methodology, recommendations of training material can be made when an OTM is not covered adequately by an examined organization.</p> <p>Throughout the development of the SENTINEL solution, it was verified that the incorporated list of training material covers all OTMs, and the Recommendation Engine can successfully retrieve the required elements.</p>				
Evaluation outcomes	Pass				
Evaluator	All technical partners				
Evaluation phase	Throughout the platform development lifecycle				
Comments	-				

Table 31. SENTINEL platform towards Knowledge sharing

ID/Name	AR-FR017/ Knowledge sharing	Type	Functional	Importance	Medium
Description	SENTINEL should provide access to an open Knowledge Base (KB) accompanied with collaboration tools (FAQ, forum) to boost the openness in sharing CS and PDP-related knowledge among participants.				
Context / Module	Observatory Information Exchange, and Observatory UI				
Evaluation	<ul style="list-style-type: none"> • Ensure access to external open security platforms. 				

Methodology	<ul style="list-style-type: none"> Reporting of data and privacy breaches identified to incident response platforms. Continuous two-way communication between Observatory KB and open security platforms.
Evaluation outcomes	Pass
Evaluator	All technical partners
Evaluation phase	Throughout platform development
Comments	-

Table 32. SENTINEL platform towards Compliance Monitoring

ID/Name	AR-FR018/ Compliance Monitoring	Type	Functional	Importance	Medium
Description	SENTINEL should help participants monitor their progress towards GDPR compliance through monitoring the implementation of OTMs for PDP.				
Context / Module	<p>MySentinel – Dashboard: Monitoring of GDPR compliance is ensured by a dashboard providing information about compliance with GDPR. Information displayed are results of SENTINEL’s modules as GDPR CSA, DPIA, Recommendations, and Cybersecurity assessment. The following aspects of monitoring are addressed:</p> <ul style="list-style-type: none"> - <u>Observation</u>: dashboard allows to gain a comprehensive view of the compliance level of PAs and to identify what measures to implement to improve it. - <u>Measurement</u>: What is being observed is measuring according a four-level measurement scale. - <u>Alerting</u>: Visualisation of information is enhanced by using colour codes (red, orange, and green). Red colour allows to easily identify which points require attention and action from SMEs. <p>SENTINEL’s dashboard does not allow tracking of progress in compliance effort.</p>				
Evaluation Methodology	At the end of the trials, participants are surveyed about the relevance and quality of the dashboard to determine the company’s compliance status and identify priority action points. The relevance of the evaluation is contingent upon the existence of a certain number of PAs recorded in the SENTINEL ROPA. Indeed, if there are only less than 5 PAs recorded, it does not make sense to consider monitoring as important. During trials, such number has not been reached.				
Evaluation outcomes	<p><u>Observation</u>: untested <u>Measurement</u>: untested <u>Alerting</u>: untested</p> <p>These aspects of monitoring have not been tested as there were not enough PAs recorded to make monitoring key for the SMEs.</p>				
Evaluator	Pilot and workshop participants.				
Evaluation phase	SENTINEL FFV (1 st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, and DIH Pilot) during the Demonstration phase (M19-M30)				

Comments	-
-----------------	---

4.2.2.2 Assessment of Non-Functional Requirements

This Section presents the assessment of SENTINEL platform capabilities towards covering the Non-Functional Application Requirements. Again, the non-functional Requirements are grouped into high-level families wherever needed to simplify the assessment process and omit unnecessary, redundant information.

Table 33. SENTINEL platform towards Confidentiality, Integrity, Availability and non-Repudiation

ID/Name	CIA triad and non-repudiation: AR-NFR001/ Confidentiality AR-NFR002/ Integrity AR-NFR003/ Availability AR-NFR004/ Non-Repudiation	Type	Non-Functional	Importance	Medium
Description	<ul style="list-style-type: none"> To protect assets from being exposed to unauthorized parties, for example in the case of a data breach, SENTINEL must treat participant's data with confidentiality. The implementation of the technical components of the SENTINEL architecture (modules etc) considering the Confidentiality, Integrity and Availability (CIA) triad Non-Functional (NF) requirements. To only allow modification of assets by authorised individuals, SENTINEL should preserve the integrity of participant's data within the platform. The implementation of the technical components of the SENTINEL architecture (modules etc) will address the CIA triad NF requirements To ensure the continuous availability of the SME services and data to authorised internal and external entities. The implementation of the technical components of the SENTINEL architecture (modules etc) should consider the CIA triad NF requirements. To provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed. SENTINEL should provide non-repudiable logging and auditing-supporting capabilities within its participant data-handling core contexts. We consider non-repudiation as an addition to the core CIA triad. This requirement should be satisfied by the technical SENTINEL implementations, which enforce authenticating identities. 				
Context / Module	N/A				
Evaluation Methodology	Evaluation by technical partners, during the weekly technical meetings. Evaluation in trials and the SME workshops				
Evaluation outcomes	Pass, with remarks.				
Evaluator	FP, ITML, IDIR, AEGIS, and INTRA				
Evaluation phase	M12-M36				

Comments	<p>There has been an effort, after M12, to design and implement a cybersecurity concept for SENTINEL as a platform, thus satisfying AR-NFR001, AR-NFR002, AR-NFR003 and AR-NFR004. This requirement was also highlighted during the project’s initial technical review around M12. The premise behind this thinking is that, although SENTINEL does not store, handle or process sensitive <i>personal data</i>, it still stores some organisational details which, if exposed, could pose a threat to participant SMEs by revealing high-level details about their cybersecurity posture, data protection practices, etc. An example of this is the asset inventory coupled with the results of CSRA assessments which expose tangible vulnerabilities of specific organisational and/or PA-related assets. Such vulnerabilities are potentially directly exploitable by bad actors in the case of a SENTINEL data breach.</p> <p>Leading up to the final version of SENTINEL, the steps we have taken to harden the platform have been:</p> <ul style="list-style-type: none"> • Confidentiality <ul style="list-style-type: none"> ○ Security of data in-transit: SSL encryption used throughout (also see AR-FR008), API security (authentication, etc) ○ Security of data at-rest: data minimisation (Profile Service) ○ Access management: Adoption of robust and community-tested IAM framework (Keycloak) for authentication, authorisation and access control • Integrity <ul style="list-style-type: none"> ○ Identity and access management best practices ○ Business continuity policy, backups and data replication • Availability <ul style="list-style-type: none"> ○ Business continuity policy, backups and data replication ○ Best SDLC management and CI/CD practices towards availability ○ A decoupled architecture, providing availability by-design by not propagating a potential failure of a component over to the rest of the system <p>Non-repudiation: not applicable in SENTINEL.</p>
-----------------	---

Table 34. SENTINEL platform towards Usability

ID/Name	AR-NFR005/ Usability	Type	Non-Functional	Importance	High
Description	To provide cybersecurity, privacy and personal data protection that are easy and intuitive to use. SENTINEL, as an integrated digital framework, should be intuitively presented to participant SMEs as a compliance-as-a-service offering and not add additional admin burden to their everyday process. The user journey across the SENTINEL components and building blocks should be easily navigable and the value to be gained understandable and attainable for end-users (UX). Finally, the individual web implementations and front-end components should be realised with best UI practices in mind.				
Context / Module	MySentinel				
Evaluation Methodology	Please refer to Table 11: BR-NFR001/Usability				

Evaluation outcomes	Pass. Please refer to Table 11: BR-NFR001/Usability
Evaluator	Pilot end-users
Evaluation phase	<ul style="list-style-type: none"> • SENTINEL MVP testing and validation (M16-M17) • SENTINEL FFV (1st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, DIH Pilot) during the Demonstration phase (M18-M30) • SENTINEL Final Product (2nd prototype) in the final SME user-centric workshop (M33)
Comments	-

Table 35. SENTINEL platform towards Cost-effectiveness

ID/Name	AR-NFR006/ Cost-effectiveness	Type	Non-Functional	Importance	High
Description	To provide cybersecurity, privacy and personal data protection solutions at a cost-effective level for the participant SMEs. The use of SENTINEL must be cost-effective for participant SMEs. The implementation of its proposed OTMs should not consume more human and financial resources compared to hiring external CS experts and implementing their recommendations. SENTINEL should consider various cost factors which are weighted highly against the budget restrictions provided by the SME.				
Context / Module	Core-recommendation engine				
Evaluation Methodology	Please refer to Table 11: BR-NFR002/ Cost-effectiveness				
Evaluation outcomes	Pass. Please refer to Table 11: BR-NFR002/ Cost-effectiveness				
Evaluator	Pilot end-users, exploitation manager of SENTINEL				
Evaluation phase	<ul style="list-style-type: none"> • SENTINEL FFV (1st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, DIH Pilot) during the Demonstration phase (M18-M30). <p>Desk analysis on cost-effectiveness of SENTINEL after the release of the 2nd prototype (M30).</p>				
Comments	All above activities are reported in D7.8, D7.9, D8.3				

Table 36. SENTINEL platform towards Scalability

ID/Name	AR-NFR007/ Scalability	Type	Non-Functional	Importance	Low
Description	To deploy scalable cybersecurity, privacy and personal data protection solutions, which can effectively support the SME as its business and requirements grow. We interpret scalability as the SENTINEL platform's capability to offer a continuous service, which adapts to the SME's needs as the company evolves – not as a service that users would only visit once to get a set of policy recommendations. Scalability is attained by a)				

	emphasising the usability and perceived value of components such as the observatory, the compliance centre, the enforcement centre and the incident response centre, which all boost the total lifetime value that end SME users get from leveraging SENTINEL in a continuous manner; and by b) enabling the core self-assessment and recommendation components to reassess the SME CS and PDP stance often and update the existing recommendations to reflect the new company scale and requirements as they grow.
Context / Module	Core (primary), Plugins (secondary)
Evaluation Methodology	Evaluation by technical partners, during the weekly technical meetings. Evaluation in trials and the SME workshops
Evaluation outcomes	Pass, with remarks.
Evaluator	IDIR
Evaluation phase	M24-M36
Comments	<p>A) Technical scalability {In sync with the approach mentioned in D5.7} In a scaling scenario, the SENTINEL platform will need to be able to serve a higher demand by supporting a significantly higher number of concurrent users, compared to the period of development and testing. The recent 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 February’s 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, should technical scaling needs escalate, the infrastructure will have to be tested again leveraging the appropriate Cloud simulation toolkits and a decision made on how to scale further if required, considering deploying additional computing, networking and storage resources, performance optimizations, caching, load balancing, etc.</p> <p>B) Functional scalability SENTIEL accommodates several evolving business SME requirements in a scalable manner:</p> <ul style="list-style-type: none"> • An always-up-to date, albeit immutable, <i>record of processing activities (ROPA)</i>, which can always be updated with newer and up-to-date version of the SME’s personal data processing activities, to remain compliant with GDPR Art. 30. • Offering instant and unlimited generations of and updated <i>recommended policy</i>. • The <i>Observatory</i> is always up to date with the latest OSINT and other 3rd party and openly available information, with no effort on the part of the user. <p>Instant and unlimited <i>self-assessments (GDPRCSA, DPIA, CSRA)</i>, applicable to organisations’ personal data processing activities, able to accommodate changing and evolving requirements, practices or new capabilities.</p>

Table 37. SENTINEL platform towards Authentication, Authorisation and Accounting

ID/Name	AR-NFR008/ AAA	Type	Non-Functional	Importance	Medium
Description	To provide the technical means for a) identifying users; b) granting access to resources based on their explicitly defined privileges and c) all related logging, record keeping and supporting auditing. AAA (which may be approached as Identity and Access Management (IAM) when emphasising identity management) is an integral part of every CS and PDP policy. SENTINEL will tackle this requirement by recommending internal and external components for both on-premises and Cloud SME infrastructures and services.				
Context / Module	N/A				
Evaluation Methodology	Tests on the IdMS services to ensure authentication, authorisation and accounting.				
Evaluation outcomes	Through its IdMS service SENTINEL provides authentication, authorization and Single Sign-On capabilities with 200003/sec concurrent sessions and user logins.				
Evaluator	ITML and end-users				
Evaluation phase	Throughout the platform development testing lifecycle Final SME workshop where multiple users created SENTINEL accounts				
Comments	All above technical developments are reported in D2.1-D2.3				

Table 38. SENTINEL platform towards use of Common Language

ID/Name	AR-NFR009/ Common language	Type	Non-Functional	Importance	High
Description	To use a standardised terminology for representing CS and PDP concepts. To ensure compatibility across internal and external components, SENTINEL needs an explicit formal specification of the concept related to the CS and PDP domains.				
Context / Module	Vulnerabilities & Compliance Knowledge Base				
Evaluation Methodology	<p>Following standardised approaches, such as CPE MITRE [26] for asset management, CVE MITRE [19], CVSS [23] specification for vulnerabilities management, CWE MITRE [17], CAPEC MITRE [17], for Common Weakness and Threat Management, MITRE ATT&CK framework [35] for attack techniques and tactics management, MITRE D3FEND framework [36] for defend controls management. In addition, OTMs related to CS and PDP were structured based on ISO/IEC 27001:2013 104[22] information security international standard and ENISA risk assessment approach [13],[14],[15] respectively. Furthermore, MISP Threat Intelligence open-source repository [37] is utilised in the Knowledge Base</p> <p>PDP concepts within the SENTINEL platform (e.g. in PA, ROPA, CSA, DPIA components) were identified based on GDPR Regulation [8] and ISO/IEC 33k series [38], i.e., ISO/IEC 33004 for Assessment model, ISO/IEC 33003 for Measurement scale</p>				

	<p>and ISO/IEC 33002 for Assessment method.</p> <p>To evaluate the standardised terminology followed to represent CS and PDP concepts, we identified 3 related questions which were communicated via the online questionnaire during the 3 Pilots (i.e., CG Pilot, TIG Pilot, and DIH Pilot)</p>
Evaluation outcomes	<p>Pass.</p> <p>The proper utilization of the ISO27001 and the ENISA framework for specifying the 10 Organizational and 10 Technical categories, as well as the 96 specific Organizational measures and 79 Technical Measures is a proof that the glossary and the terms are not generated in the SENTINEL project on the contrary we used world-wide accepted terminologies. The fact that all assessment types are based at world-wide accepted and well-known methodologies is a proof as well. For instance, the CSRA provides results and security findings which are globally recognized, since these are published in open repositories such as the NIST Vulnerability Database [24], the CAPEC MITRE threat repository [17], etc.</p> <p>Towards this continuous effort of utilising world-wide terms and well-known practices, pilot end-users responded to questions concerning whether:</p> <ul style="list-style-type: none"> i) the language used in SENTINEL is comprehensive (achieved 80% positive responses in during the DIH Pilot – cf. D6.2 Section 5.6.3). ii) the use of terms throughout SENTINEL is consistent (most end-users responded positively in the three pilots (i.e., CG Pilot 100%, TIG Pilot 100%, DIH Pilot 60% - cf. D6.2 Section 3.6.3, 4.6.3, 4.7.3.3.3, 5.6.3).
Evaluator	Pilot end-users
Evaluation phase	Technical Verification within the platform’s technical development lifecycle, SENTINEL FFV (1 st prototype) pilot testing and validation (i.e., CG Pilot, TIG Pilot, and DIH Pilot) during the Demonstration phase (M19-M30)
Comments	All above standardised approaches are reported in D2.3, D3.3, D4.3 and D6.2

4.3 Impact Assessment

This section details the evaluation outcomes of the SENTINEL platform, examining its performance in real-world scenarios. It outlines the results, offering a comprehensive understanding of the platform’s strengths and areas for improvement, and highlights the practical benefits and challenges encountered during testing. Additionally, the section assesses Key Performance Indicators (KPIs) and Key Results (KRs) where needed to measure the project’s success and identify areas for further enhancement.

4.3.1 SENTINEL evaluation outcomes

Table 39 summarises the positive feedback and areas needing improvement based on the three pilot results (cf. D6.2) and the final pilot event (cf. Section 3.4 of the current deliverable). Feedback derived from multiple-choice questions is identified as positive when the percentage of "Agree" or "Strongly Agree" responses exceeds the combined percentage of "Neither Agree nor Disagree", "Disagree", and "Strongly Disagree" responses. Responses marked as N/A or "Neither Agree nor Disagree" are not included in this calculation Input related to UI/UX aspects, help menu enhancements, terminology clarification and platform scalability, accessibility aspects were

considered in the last technical refinements conducted until M36. Further suggestions for improvements analysed in Table 39 could be considered beyond the project’s lifespan to raise its exploitation and sustainability aspects.

Table 39. SENTINEL evaluation outcomes

Part A - User Satisfaction		
Category Name	Positive Feedback	Suggestions/ Room for improvements
Usability, Time Efficiency, Functional Suitability and System Performance	<ul style="list-style-type: none"> • In terms of usability and learnability: <ul style="list-style-type: none"> ○ Create My Organisation Details ○ Develop a Processing Activity ○ Commit a Processing Activity to ROPA ○ Execute GDPR CSA ○ Execute CSRA ○ Acquiring Policy Recommendations ○ Observatory ○ Reporting Incidents • The experiment workflow was streamlined and easy to follow. • SENTINEL Recommendations to Organisational and Technical Measures (OTMs) are described accurately and clearly. • It was easy to understand the structure and logic of the SENTINEL Dashboard Menu and easy to use. • Satisfied with system performance without facing any interruptions while using the platform. • Satisfied with the performance of the SENTINEL platform in terms of speed when executing: <ul style="list-style-type: none"> ○ A GDPR Compliance Self-Assessment. ○ Acquire Policy Recommendations 	<ul style="list-style-type: none"> • Improve content and terminology. • Elements that are missing and must be fulfilled to complete an analysis are not always clearly indicated. • Domain specific vocabulary used, which is hard for a basic user to understand. • OTM's do not appear to be specific. • Observatory looks aimed at IT professionals rather than beginner or intermediate. • Not satisfied with the performance of the SENTINEL system in terms of speed when executing: <ul style="list-style-type: none"> ○ A Data Protection Impact Assessment. ○ Exploring the Observatory
User Interface/User Experience (UI/UX)	<ul style="list-style-type: none"> • The help menu was useful. • User-friendly environment. • The position of messages on the screens is proper. • The different screens of SENTINEL are cohesive in look-and-feel. • The characters on the screens are easy to read. • Accurate and clear organization of information • The language used in SENTINEL is comprehensive and the use of terms consistent. 	<ul style="list-style-type: none"> • Improve presentation of progress/error messages in some cases. • Can be a bit overwhelming for someone who reviews these topics annually.

	<ul style="list-style-type: none"> • SENTINEL has clearly marked way-finding buttons (exit, back, next page, etc.) • The interface of SENTINEL is pleasant 	
<p>CyberRange Gaming</p>	<ul style="list-style-type: none"> • Helps exploring different types of threats and attacks related to data storage and accessibility. • The CyberRange Gaming helps detecting, analysing and better understanding vulnerabilities on ICT assets. • The CyberRange external simulation training service provided a realistic environment in emulating real-world cyber threats and incidents. • A good test of knowledge • Covering a big range in many issues of daily office /web procedures 	<ul style="list-style-type: none"> • Does not work well in all browsers. • Sometime freezes. • Too much information/text and graphics and the access to real practices and instructions is not clear. • CyberRange Gaming needs improvement, it is not a gaming experience more like a test feeling. • Needs a homogenisation in the interface in terms of vocabulary. • The test was not easy for a normal web/office user.
<p>Results, Security, Quality, Personal Data Protection and Compliance</p>	<ul style="list-style-type: none"> • SENTINEL measures/recommendations can help to achieve GDPR compliance • SENTINEL measures/recommendations can assure privacy of related data. • identify and record my organisation's processing activities • SENTINEL Cybersecurity simulation environment has helped to identify risks/threats to registered assets. • SENTINEL measures/recommendations can mitigate risks/threats identified. • SENTINEL Cybersecurity simulation environment has helped to identify possible attack scenarios. • Privacy incidents can be prevented by implementing SENTINEL recommendations. 	<ul style="list-style-type: none"> • SENTINEL platform is not easy to learn for people with low expertise in GDPR and cybersecurity. • Time needed to complete the PA and DPIA
<p>Business Performance</p>	<ul style="list-style-type: none"> • SENTINEL can help understand my organisation's GDPR compliance requirements • SENTINEL can simplify GDPR compliance. • SENTINEL provides all the functionalities expected to have for assessing GDPR compliance. • The measures recommended by SENTINEL can improve: <ul style="list-style-type: none"> ○ Implementation of controls that limit any type of unauthorized access to the data 	<ul style="list-style-type: none"> • The use of SENTINEL will necessitate additional human and/or financial resources

	<ul style="list-style-type: none"> ○ Security of information/data exchange ○ Maintenance and retention of data ● The measures recommended by SENTINEL address challenges/ improve the effectiveness of an organisation regarding CS and PDP. ● SENTINEL helps to form an organisations' cybersecurity and personal data protection strategy. ● Satisfied with the quality of the GDPR Compliance Self-Assessment result. ● SENTINEL can be used for all processing activities and assets used for data storage and accessibility in my organisation. ● SENTINEL simplifies cybersecurity risk analysis compared to tools/services currently used. 	
Part B – User opinions		
Category Name	Positive Feedback	Suggestions/ Room for improvements
Express end-users' opinion and additional comments	<ul style="list-style-type: none"> ● Useful in terms of learning, training, and testing knowledge concerning GDPR compliance. ● All in one place for GDPR. ● The quality of SENTINEL privacy assessments (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) results in general can be described in general: <ul style="list-style-type: none"> ○ Helpful, very promising, appealing. ○ A productive tool to protect the organisation requirements. ● Insight into GDPR and its necessity. ● Recommendations found most positive functionality. ● Awareness of cybersecurity and risks ● As long as it is open access this will be interesting. ● SENTINEL most competitive advantage its “<i>completeness</i>”, “<i>format</i>” and that raises the user “<i>awareness</i>”. 	<ul style="list-style-type: none"> ● Useful tool, but more relevant for GDPR experts and IT professionals ● More user-friendly, e.g. : clearer terminology, shorten its content, simplify measures titles-more focused recommendations), leverage sentence conciseness, simplify questions and compliance section, enrich help menu with further notifications, especially for people lacking GDPR knowledge. ● Could be useful to add filtering options ● Enhance learnability, add more PA templates focused on sectorial aspects, add typical processing operations to better guide the SMEs ● Enhance cybersecurity risk analysis (e.g. add non-technical risks, set alarm system for future vulnerabilities) and GDPR trainings ● Spread CyberRange gamification ● Add classification indicators to track organisations compliance status over time. ● Represent the level of compliance in a quantitative approach (“percentage”) ● Further analyse the role of ROPA ● separate modules of security and GDPR.

		<ul style="list-style-type: none"> • Enhance with Data protection-by-design and by-default, personal data minimization aspects, data subjects' rights and transparency obligations • Enhance description of processors' role and their obligations, in terms of data protection, in contractual agreements. • Include ePrivacy legislation obligations (e.g. cookies, tracking, marketing communications) • Set ranking regarding risk at organisation level • Industrial Internet of things (IIoT) security and cloud security coverage. • Initiate invitation mechanisms for companies to join SENTINEL • A customisable dashboard could be desirable
--	--	--

4.3.2 KPIs/KRs assessment

The current section provides the assessment of the fifteen (15) KPIs/KRs related to the evaluation process of SENTINEL, specified in D6.1 [5]. To assess the KPIs/KRs, a continuous monitoring process carried out to review their progress and performance at distinct time periods towards the project's objectives, as presented in D6.1. In this vein, most of KPIs/KRs (11/15) were already achieved by M30 and thoroughly reported in D6.2 (i.e., KR-1.1, KR-1.5, KR-2.2, KR-2.3, KR-2.4, KR-2.5, KR-3.1, KR-3.2, KR-3.3, KR-4.2, and KR-4.5). The following table illustrates the progress report on the achievement of the KRs that were not fully accomplished by M30, i.e. KR-1.2, KR-1.3, KR-1.4, and KR-3.4. The KPIs/KRs assessment aims to measure the progress and effectiveness of various project objectives, e.g. considering for each demonstrator both operational aspects (cost, service levels, etc.) and technical aspects (performance of solution).

Table 40. KPIs/KRs final assessment

<p>KR-1.1: Successful integration and orchestration of SENTINEL technology offerings. Owner: INTRA</p>
<p>Already achieved and reported in D6.2.</p>
<p>KR-1.2: 40% improved compliance efficiency for SMEs/MEs. Owner: LIST</p>
<p>Efficiency indicates how consistently things are done right. Applied to SENTINEL, measuring efficiency requires calculating the rate at which an SME can complete the assessment of all their personal data processing activities (PAs), which, in turn requires comparing the number of PAs for which compliance with GDPR has been established/assessed to the total of PAs the company is accountable for. This is calculated as follows:</p>
$\text{Compliance efficiency} = \frac{\text{PAs assessed}}{\text{Total PAs}} * 100$
<p>Practically speaking, improving compliance efficiency implies then to increase the number of PAs that have been described, recorded in SENTINEL's ROPA, and assessed through either GDPR CSA or DPIA. To establish this KR, it is first necessary to compare for each user of SENTINEL evolution of their compliance efficiency rate. To do so, compliance efficiency was measured twice: before using</p>

SENTINEL (T_0), and after a period of use (T_1). KR-1.2 resulted in the average of the variation of compliance efficiency rate of SENTINEL users (n).

$$KR1.2 = \frac{\sum_1^n Compliance\ efficiency(T_1) - Compliance\ efficiency(T_0)}{n}$$

After the release of FFV of the SENTINEL platform, the SENTINEL compliance services testing has been intensified in Y3 by selecting four (4) PAs to be tested and experimented by the SENTINEL pilot partners (Dimensions Care and Clingenics company). In particular, for the scope of the SENTINEL platform testing and validation during the M19-M33 phase (defining as a period use –“T1”), DC proposes two (2) ((i) Dimensions Care Children’s Case Records and ii) Safe Recruitment and Criminal Record Checks) and CG two (2) ((i) Security of user/client data and i) Proactive Security of genomic data) PAs to test and measure the compliance efficiency by utilising the compliance efficiency indicators presented above. These PAs are thoroughly analysed and reported in D6.2. By the end of project CG has recorded one additional PA by testing 3 PAs in total. As a results, five (5) PAs have been selected and successfully recorded within the SENTINEL platform. It should be mentioned that prior to SENTINEL (T_0), both pilot owners had challenges and issues in keeping records of their PAs. Specifically, CG did not record their PAs and thanks to SENTINEL CG maintains records of three of these processing activities now. CG has a better understanding of the subject now and look forward to expanding and covering the full range of their PAs. In addition, DC required improvement in terms of centralising the records and completeness. Prior SENTINEL, DC although maintained records of PAs however in an isolation without having a single central record/point of reference such as would be provided through SENTINEL. As illustrated in the following table, we have increased the compliance efficiency beyond the initially defined expectations.

	Total PAs examined	T₀ - PAs Assessed / (Compliance efficiency)	T₁ (M19-M33) – PA Assessed / (Compliance efficiency)
SENTINEL pilot partners (Clingenics and Dimensions Care)	5	0 (0)	5 (100%)

KR is considered ~100% achieved.

KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives. Owner: STS

Drawing on data from market research²¹ and the feedback received as part of the SENTINEL stakeholder engagement activities (cf. D7.6 “Ecosystem building and SMEs engagement report - final version”) as well as based on the report by GDPR.EU [28], small businesses spend between €1,000 and €50,000 on GDPR compliance, covering consultant fees and technology costs. Using this information as a baseline, in the third year, the consortium benefited from the Horizon Results Booster Initiative²², finalised the SENTINEL business model by also drafting a pricing strategy. According to this strategy, the price of the SENTINEL platform under standard plan is estimated at 348 €/year, and under premium plan at 708 €/year. This pricing strategy is aimed at keeping costs low and affordable for most SMEs, substantially cutting compliance expenses. If we assume that in average SMEs spent €1,000 (minimum GDPR compliance costs based on the literature data), then SENTINEL has a potential to reduce compliance related costs by i) ~65% when the SENTINEL platform is offered under standard pricing model and ii) ~30% when the SENTINEL platform is offered under premium pricing model. Given the fact that the SENTINEL platform offered via standard pricing plan would probably be the most attractive option for the vast majority of SMEs (due to its appealing cost) we can consider this KR successfully achieved. Generally speaking, it is encouraging to discover that SENTINEL can potentially lead to substantial reduction of the GDPR compliance costs especially for those SMEs who typically incur high fees from compliance consultants. More information on the SENTINEL financial analysis, pricing model as well as

²¹ <https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/> [Accessed 31 May 2024]

²² <https://www.horizonresultsbooster.eu/ServicePacks/Details/6>

other comparison analysis with competing tools can be found in D7.9 “Final business model, market analysis and long-term sustainability report”. KR is considered ~100% achieved.

KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU. Owner: **UNINOVA**

SENTINEL has organized five (5) SME-centric workshops (September 2021, May 2022, October 2022, September 2023, and February 2024), with the objective of raising awareness in SMEs/MEs all over the EU about GDPR compliance and PDP, to showcase the SENTINEL offerings and to assess their acceptance and willingness to adopt GDPR compliance services like SENTINEL. In this respect, the SENTINEL consortium has prepared a questionnaire to record the increase of user acceptance of the SENTINEL platform during its different development stages: SENTINEL MVP, and final version. In this regard, during the 3rd workshop where the SENTINEL MVP demonstration took place 29% of participants accepted that SENTINEL can be a potential solution to be implemented in their companies, 42% have answered that they could consider investing in tools/services similar to SENTINEL within the next 2 years. During the last workshop, where the final version of the SENTINEL platform’s demonstration took place 67% of participants accepted that SENTINEL can be a useful solution to be implemented in their companies. Furthermore, more than 80% of participants have answered that they could consider investing in tools/services similar to SENTINEL within the next 2 years or after 2 years. The results achieved indicate that there is a more than 30% increase in the users’ acceptance as well as willingness to adopt GDPR compliance services like SENTINEL.

SENTINEL versions	User acceptance (%)	User willingness to invest (%)	Increase (%)
SENTINEL MVP (M12)	29%	42%	>30%
SENTINEL Final (M30)	67%	80%	

More in-depth analysis of the responses can be found in D7.5 “Ecosystem building and SMEs engagement report - interim version” and D7.6 “Ecosystem building and SMEs engagement report - final version”.KR is considered 100% achieved.

KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility Owner: **ACS**

Already achieved and reported in D6.2

KR-2.2: Implement a dynamic rule insertion mechanism for the Recommendation Engine, providing predicates, variables and actions for forming rule expressions, addressing at least 135 organisational and technical measures (OTMs). Owner: **ITML**

Already achieved and reported in D6.2

KR-2.3: Test GDPR compliance and digitalised DPIA self-assessment framework Owner: **STS**

Already achieved and reported in D6.2

KR-2.4: Offer robust and easy to adopt data access management, authentication, authorisation and record keeping technologies to SMEs/MEs for GDPR compliance. Owner: **ITML**

Already achieved and reported in D6.2

KR-2.5: Ensuring the delivery, adoption, and utilization of a unified Identity Management System.

Already achieved and reported in D6.2

KR-3.1: More than (20) novel services and tools utilised and integrated from diverse multi-domain technological areas and applied in SMEs/MEs environments. Owner: **FP**

Already achieved and reported in D6.2

KR-3.2: At least (10) tools and services related to data protection, data privacy management, security assurance and compliance. Owner: **IDIR**

Already achieved and reported in D6.2

KR-3.3: Update and enrich the SENTINEL OTMs classification and their mappings to adapt to the dynamic properties of the SENTINEL Recommendation Engine. Owner: **ITML**

Already achieved and reported in D6.2
KR-3.4: A dynamic Recommendation Engine which is both i) performant, with responsiveness (latency) lower than 3 sec and ii) highly available, with over 99% requests satisfied on average. Owner: ITML
The current version of the RE, as included in the Final Product has been measured to i) responsiveness of about 50ms and ii) 100% availability. Although a new mechanism has been introduced enabling more complex rules the system is still highly performant and responsive. KR is considered 100% achieved.
KR-4.2: Delivery of three (3) integrated versions of the SENTINEL framework. Owner: INTRA
Already achieved and reported in D6.2
KR-4.5: Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs. Owner: AEGIS
Already achieved and reported in D6.2

5. Conclusion

The current deliverable marks the final assessment of the SENTINEL platform and the impact analysis. It describes the extensive work conducted in real-life experiment evaluations under WP6 activities. This report analysed the iterative process of applying the experimentation protocol to SENTINEL platform testing and evaluation processes (T6.1), summarizes the pilot cases, and the engagement of SMEs through DIHs, all aimed at ensuring that the SENTINEL platform meets end-user requirements effectively.

The SENTINEL platform has been successfully implemented and validated across various real-life scenarios of 12 different Processing Activities (PAs) experiments. Among these, two (2) experiments focused on sectorial PAs related to genomics and socialcare (T6.2) demonstrated the platform's capability to utilise SENTINEL in different operational environments, providing robust security, privacy, and data protection solutions.

Furthermore, D6.3 presents the final SME-centric Workshop occurred in M33 which relied on the participation of various enterprises of different sectors, aiming to address testing and validation objectives of the SENTINEL Final Product and communicate the project's findings. Engaging enterprises of different sizes, such as Small and Medium-sized Enterprises/ Micro-Enterprises (SMEs/MEs), and different types, such as spin-offs and startups, via Digital Innovation Hubs (DIHs) (T6.3) proved effective in gathering diverse feedback and validating the platform in practical settings. This collaboration not only facilitated widespread testing but also enhanced the platform's credibility and acceptance among potential users and leveraged the SENTINEL ecosystem (T7.4).

The detailed validation and verification processes, focusing on functionality, usability, and performance metrics, provided a clear understanding of the platform's strengths and areas for improvement. These metrics are essential for continuous development and ensuring the platform's alignment with regulatory standards and user expectations. The assessment of SENTINEL platform capabilities towards specified business and application requirements illustrated the platform's functional completeness and efficiency in meeting the end-user needs. The verification aspects addressed by project partners through technical tests in the platform within its development lifecycle (e.g. internal platform testing of T5.3). The feedback gained from the SME-centric Workshop of M33 was considered in the final technical refinements of the platform to improve its scalability and accessibility aspects (T5.3). The evidence obtained from the overall SENTINEL platform evaluation (delving into business/socio-economic and technical perspectives) was considered to calculate the project's KR/KPIs and assess the project's success (T6.4).

WP6 testing, validation, evidence interpretation and monitoring activities were fully aligned with the project's technical work allowing end-users to assess the SENTINEL platform as a continuous process at distinct periods of technical achievements (i.e., testing and evaluating the three subsequent versions of the platform; MVP, FFV and Final Product). WP6 activities were directly associated with the accomplishment of MS4 "Demonstration Flame" (M24), MS5 "Demonstration Fire" (M30) and MS6 "Consolidation" (M36). Moreover, until M24, CG and TIG Demonstration workshops were realised, until M30 three major pilot executions conducted (i.e., CG Pilot, TIG Pilot engaging a set of sister companies, and DIH Pilot encompassing various external SMEs. Eventually, up to M36 the additional workshop conducted engaging both internal and external

SMEs and the results retrieved from the overall SENTINEL platform evaluation across the project's lifespan were analysed and the impact was assessed.

The findings and insights from this deliverable highlight the potential for further research and development in the field of cybersecurity, privacy, and data protection for SMEs. Future projects should build on the success of SENTINEL, exploring new technologies and methodologies to enhance security and compliance in SMEs/MEs enterprises.

The SENTINEL project has made significant steps in bridging the security, privacy, and data protection gap for SMEs in Europe. The comprehensive validation and impact analysis presented in this deliverable confirm the platform's effectiveness and provide a solid foundation for future improvements and innovations. The continued collaboration with SMEs and DIHs will be crucial in maintaining the relevance and efficacy of the SENTINEL platform in an ever-evolving digital landscape.

References

- [1] Deliverable D6.2 (2023), “SENTINEL Demonstration - final execution”, SENTINEL EU H2020 Project.
- [2] Deliverable D7.6 (2024), “Ecosystem building and SMEs engagement report – final version”, SENTINEL EU H2020 Project.
- [3] Deliverable D5.7 (2024), “Best practices for maintaining and operating the system in the long-term - TRL 7”, SENTINEL EU H2020 Project.
- [4] Deliverable D1.3 (2021), “The SENTINEL Experimentation Protocol”, SENTINEL EU H2020 Project.
- [5] Deliverable D6.1 (2022), “SENTINEL Demonstration - initial execution and evaluation”, SENTINEL EU H2020 Project.
- [6] Deliverable D1.1 (2021), “The SENTINEL Baseline”, SENTINEL EU H2020 Project.
- [7] Ferreira, B., Williamson, S. et al. (2018), Technique for representing requirements using personas: a controlled experiment, IET Software, 12(3), June 2018, pp. 280 – 290
- [8] 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>
- [9] ISO/IEC 25010: 2011 “Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models”. Online available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en> (Last accessed: 10-11-2022)
- [10] Miguel, J. P.; Mauricio, D.; Rodriguez, Glen. (2014) “A review of software quality models for the evaluation of software products”. arXiv preprint arXiv:1412.2977
- [11] Brooke, J. (2013). “SUS: a retrospective”. Journal of usability studies, 8(2), 29-40.
- [12] Deliverable D8.3 (2024), “Yearly project management report - third version”, SENTINEL EU H2020 Project.
- [13] ENISA (2015a). Cloud Security Guide for SMEs: Cloud computing security risks and opportunities for SMEs. European Union Agency for Network and Information Security.
- [14] ENISA (2015b). Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. European Union Agency for Network and Information Security.
- [15] ENISA (2016). Guidelines for SMEs on the security of personal data processing. European Union Agency for Network and Information Security.
- [16] Deliverable D3.3 (2023), “The SENTINEL digital core: Final product”, SENTINEL EU H2020 Project.
- [17] Common Attack Pattern Enumeration and Classification MITRE. Online available: <https://capec.mitre.org/>
- [18] Common Weakness Enumeration MITRE. Online available: <https://cwe.mitre.org/>
- [19] Common Vulnerabilities and Exposures. MITRE. Online available: <https://cve.mitre.org/>
- [20] Deliverable D7.9 (2024), “Final business model, market analysis and long-term sustainability report”, SENTINEL EU H2020 Project.
- [21] Deliverable D7.8 (2024), “Exploitation strategy, standardisation activities and best practices - final version”, SENTINEL EU H2020 Project.

- [22] International Standards Organisation. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Online available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>
- [23] Common Vulnerability Scoring System. FIRST. Online available: <https://www.first.org/cvss/>
- [24] National Vulnerability Database (NVD). Online available: <https://nvd.nist.gov/>
- [25] Security Content Automation Protocol. Online available: <https://csrc.nist.gov/projects/security-content-automation-protocol>
- [26] Common Platform Enumeration. MITRE. Online available: <https://nvd.nist.gov/products/cpe>
- [27] Deliverable D1.2 (2021), “The SENTINEL Technical Architecture”, SENTINEL EU H2020 Project.
- [28] GDPR.EU report (2019). “GDPR Small Business Survey – Insights from European small business leaders one year into the General Data Protection Regulation”. Online Available: <https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf>
- [29] Deliverable D2.1 (2021), “The SENTINEL privacy & data protection suite for SMEs/MEs: MVP”, SENTINEL EU H2020 Project.
- [30] Deliverable D2.2 (2021), “The SENTINEL privacy & data protection suite for SMEs/MEs: Fullfeatured version”, SENTINEL EU H2020 Project.
- [31] Deliverable D2.3 (2021), “The SENTINEL privacy & data protection suite for SMEs/MEs: Final product”, SENTINEL EU H2020 Project.
- [32] Deliverable D4.1 (2021), “The SENTINEL services: MVP”, SENTINEL EU H2020 Project.
- [33] Deliverable D4.2 (2022), “The SENTINEL services: Full-featured version”, SENTINEL EU H2020 Project.
- [34] Deliverable D4.3 (2023), “The SENTINEL services: Final product”, SENTINEL EU H2020 Project.
- [35] ATT&CK. MITRE. Online available: <https://attack.mitre.org/techniques/enterprise>
- [36] D3FEND. MITRE. Online available: <https://d3fend.mitre.org/>
- [37] MISP Open Source Threat Intelligence Platform. Online available: <https://www.misp-project.org/>
- [38] ISO/IEC 33000 family on Process Assessment. Online available: <https://committee.iso.org/sites/jtc1sc7/home/projects/flagship-standards/isoiec-33000-family.html>

Appendices

Appendix-I: SENTINEL Interactive Questionnaire

Part II: SENTINEL hands-on training

User Satisfaction

SENTINEL Platform registration – Organisation Profile

Question: 2.1 It was easy to create my account and organisation.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.2 It was easy to complete my Organisation Profile details.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Develop a Processing Activity

Question: 2.3 Did you use a PA template?

Options
Yes, I used the “Marketing activities & Communication” pre-filled form
Yes, I used the “Recruitment Process” pre-filled form
No, I created my own.

Question: 2.4 It was easy to complete my first Processing Activity.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Commit the Processing Activity to ROPA

Question: 2.5 I was able to commit my PA to the ROPA.

Options

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Not Applicable

Question: 2.6 Completing and committing my PA was fast and efficient.

Options

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Not Applicable

Execute GDPR CSA

Question: 2.7 It was easy to execute the GDPR Compliance Self-Assessment.

Options

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Not Applicable

Question: 2.8 Executing a GDPR Compliance Self-Assessment was fast and efficient.

Options

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Not Applicable

Question: 2.9 I am satisfied with the quality of the GDPR Compliance Self-Assessment result.

Options

Strongly agree Agree Neither agree nor disagree Disagree Strongly disagree Not Applicable
--

Acquire Recommendations

Question: 2.10 It was easy to acquire Recommendations.

Options

Strongly agree Agree Neither agree nor disagree Disagree Strongly disagree Not Applicable
--

Question: 2.11 Acquiring Recommendations was fast and efficient.

Options

Strongly agree Agree Neither agree nor disagree Disagree Strongly disagree Not Applicable
--

Question: 2.12 SENTINEL organisational and technical measures are described accurately and clearly.

Options

Strongly agree Agree Neither agree nor disagree Disagree Strongly disagree Not Applicable
--

Overall Evaluation

User Interface/ User Experience

Question: 2.13 The help menu was useful.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.14 SENTINEL provides...

Options
a user-friendly environment
characters on the screen that are easy-to-read
accurate and clear organization of information
proper position of on-screen messages
a set of different screens which are cohesive in look-and-feel.
error messages that clearly explain how to fix problems

Question: 2.15 The use of terms is consistent and the language is comprehensive.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Business Performance

Question: 2.16 I did not face any interruptions while using the platform.

Options
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.17 SENTINEL can help me...

Options

identify and record my organisation's processing activities
understand my organisation's GDPR compliance requirements
form my organisation's cybersecurity and personal data protection strategy
identify how to address privacy and cybersecurity challenges
identify possible attack scenarios that could lead to data breach
identify different types of threats/attacks (e.g. data storage, accessibility)
acquire good practices to better protect my data.

Question: 2.18 SENTINEL provides all the functionalities I expect to have for assessing GDPR compliance.

Options

Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.19 SENTINEL measures/recommendations can...

Options

help me to achieve GDPR compliance
improve the effectiveness of cybersecurity and personal data of my organization
prevent/minimise privacy incidents
mitigate risks/threats identified on cyber assets
improve security of information/data exchange
ensure maintenance and retention of data
help me to implement controls that limit any types of unauthorized data access

Question: 2.20 SENTINEL can simplify my GDPR compliance.

Options

Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.21 – The use of SENTINEL will not necessitate additional human and/or financial resources.

Options

Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Not Applicable

Question: 2.22 - Which of the following SENTINEL services would be more useful to your business needs?

Options

Filling in My Organisation Profile
Creating a Processing Activity
Using the ROPA
Executing GDPR Compliance Self-Assessment
Executing Data Protection Impact Assessment
Executing Cybersecurity Risk Assessment
Acquiring policy recommendations
Exploring the Observatory
Reporting incidents
CyberRange Gaming

Question: 2.23 Do you anticipate that exploiting SENTINEL could potentially increase your market share in the coming years? If so, to what extent?

Options

I do not know.
Yes, by at least 5%
Yes, by at least 10%
Yes, by at least 15%
Yes, by at least 20%

Express end-user opinion and additional comments

Question: 2.24 What is your overall impression after testing SENTINEL. Which are the most competitive advantages?

[free text answer]

Question: 2.25 Do you have any specific comments or suggestions for improvement?

[free text answer]

Appendix-II: Templates for assessing the SENTINEL platform towards Business and Application Requirements

Template of assessing the SENTINEL platform towards Business Requirements (BRs)

ID/Name of related Requirements	<i>Identifier/Name of the user requirement, e.g. CIA001 Triad/Confidentiality</i>	Requirements Type	<i>Requirements category level, functional/non functional</i>
Description	<i>Description of the Requirement</i>		
Rationale in SENTINEL	<i>SENTINEL approach to cover the current requirement</i>		
Means of technical implementation	<i>Describe the corresponding SENTINEL components/plugins</i>		
Evaluation Methodology	<i>Brief description of the performed evaluation (e.g. types of testing such as pilot experiment, system trials, other types of tests, and any literature or documentation or method used for the evaluation, etc.)</i>		
Evaluation outcomes	<i>Outcomes of the evaluation (i.e., pass/fail/untested and summary of outcome)</i>		
Evaluator	<i>Specify the entity/type of user that conducted the evaluation</i>		
Evaluation phase	<i>Identify the specific period where the evaluation took place (e.g. during the preparation phase right before each pilot, in pilot demonstration, prototype releases)</i>		
Comments	<i>Additional information worth mentioning, e.g. respective pilot case/experiment, user actions, exclusions, suggestions, etc.</i>		

Template of assessing the SENTINEL platform towards Application Requirements (ARs)

ID/Name	<i>Unique ID/name of the requirement, e.g. AR-FR001 encryption</i>	Type	<i>Functional/ Non-functional</i>	Importance	<i>High/ Medium/ Low</i>
Description	<i>Description of the requirement</i>				
Context / Module	<i>Primary and secondary context (and/or specific module, tool, plugin) of SENTINEL that primarily catered or assisted for the specific requirement respectively (where applicable).</i>				
Evaluation Methodology	<i>Brief description of the performed evaluation (e.g. types of testing, such as experiments, trials, verification tests in lab environment, etc. and any literature or documentation or method used for the evaluation, etc.)</i>				
Evaluation outcomes	<i>Outcomes of the evaluation (i.e., pass/fail/untested and summary of outcome)</i>				
Evaluator	<i>Specify the entity/user that conducted the evaluation (e.g. internal technical user, technical provider, etc.)</i>				
Evaluation phase	<i>Identify the distinct period where the evaluation took place (e.g. during the preparation phase right before each pilot, in pilot demonstration, prototype releases)</i>				
Comments	<i>Additional information worth mentioning, e.g. respective pilot case/experiment or test case, user actions, exclusions, suggestions, etc (if any).</i>				