SENTINEL

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

D8.3 - Yearly project management report – third version

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

Project Information

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

Document Information

Work Package	Work Package 8
Deliverable Title	D8.3 - Yearly project management report - third version
Version	1.5
Date of Submission	31/05/2024
Main Editor(s)	Siranush Akarmazyan (ITML)
Contributor(s)	Stavros Rafail Fostiropoulos (ITML), Anna Maria Anaxagorou (ITML), Philippe Valoggia (LIST), Yannis Skourtis (IDIR), Konstantinos Poulios (STS), Manolis Falelakis (INTRA), Marinos Tsantekidis (AEGIS), George Hatzivasilis, Papadogiannaki Evangelia, Kontogiorgakis Ioannis, Shevtsov Alexander (TUC), Thomas Oudin (ACS), Ruben Costa (UNINOVA), Mihalis Roukounakis (CG), Daryl Holkham (TIG), Dimitra Malandraki (CECL), Eleni-Maria Kalogeraki, Thanos Karantjias, Natalia Christofi (FP)
Reviewer(s)	Konstantinos Poulios, Emmanouil Christodoulakis (STS), Peri Loucopoulos (IDIR)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	26/02/2024	ToC	Confidential
1.1	06/03/2024	Draft shared for input collection	Confidential
1.2	22/04/2024	Draft shared for review	Confidential
1.3	16/05/2024	Review conducted by IDIR, STS	Confidential
1.4	23/05/2024	Reviewers’ comments addressed	Confidential
1.5	31/05/2024	Final version ready	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
CERTs	Computer Emergency Response Teams
CSA	Compliance Self-Assessment
CS	Cyber-Security
CSIRTs	Computer Security Incident Response Teams
CSRA	Cybersecurity risk assessments
D#	Deliverable #
DFB	Data Fusion Bus
DIH	Digital Innovation Hub
DoA	Description of Action
DMP	Data Management Plan
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EAB	External Advisory Board
EDAC	Ethical and Data privacy Advisory Committee
EDPB	European Data Protection Board
FFV	Full Featured Version
GA	Grant Agreement
GDPR	General Data Protection Regulation
IdMS	Identity Management System
ISMS	Information Security Management System
KPIs	Key Performance Indicators
KRs	Key Results
ME	Micro Enterprise
MISP	Malware Information Sharing Platform
MS	Milestone
MVP	Minimum Viable Product
OTMs	Organization and Technical Measure
PAs	Processing Activities
PC	Project Coordinator
PDP	Personal Data Protection
PPP	Public-Private Partnership
RE	Recommendation Engine
REA	Research Executive Agency
ROPAs	Records of processing activities
SCORE	Security Capability-Oriented Requirements Engineering
SME	Small – Medium Enterprise
T#.#	Task #.#
ToC	Table of Contents
TRL	Technology Readiness Level
UI	User Interface
WP #	Work Package #
Y#	Year #

Executive Summary

This document presents the project's main activities and achievements in relation to the project objectives, expected impact, innovations, communication, dissemination, and exploitation activities conducted during the third year (Y3) of the SENTINEL project (M25-M36). Furthermore, it provides a detailed description of the scientific and technical progress in all work packages towards the successful completion of the respective Work Package (WP) objectives. The report illustrates the work carried out per task and per partner for each work package, overviews the submitted deliverables, the achieved milestones, potential deviations.

Within the third year of the project, the Demonstration Phase (M19-M30) was accomplished demonstrating the operation of the SENTINEL platform in real-life SME environments and successfully completing MS5 "Demonstration Fire". In this respect, the SENTINEL project has delivered its full-featured platform together with its tools and services such as GDPR Compliance Self-Assessment (GDPR CSA) module, Identity Management System (IdMS), Data Protection Impact Assessment (DPIA) toolkit, GDPR compliant recording of PAs (ROPA), Cybersecurity risk assessment (CSRRA/MITIGATE), Cyber Range simulations, Policy recommendation and enforcement, Cyber incident reporting and handling, Observatory. During this period, the tools and services targeted above successfully demonstrated through seven (7) use cases that were initially defined in the SENTINEL project.

In the last project year, SENTINEL has triggered engagement activities with two additional DIHs and one industrial association of SMEs. Such synergies have contributed to the organization of two additional SME-centric workshops (4th and 5th workshops). The objective was to consolidate SENTINEL's mission and main objectives across the European SMEs. In this regard, the feedback on SENTINEL's offerings gathered during the 4th and 5th workshop was notably positive, highlighting a growing readiness among SMEs/MEs to adopt the SENTINEL solution.

SENTINEL progressed also with respect to the finalising of the project's main offerings by shaping the exploitation landscape mapped with SENTINEL's tools and services. Another important milestone was an update of the SENTINEL business model and value proposition elaborating on the project's four main offerings that have been developed extensively as a result of technical development conducted.

Presently, SENTINEL is in the Consolidation & Sustainability Management Phase (M31-M36) and very close its closure. This stage focused on fine tuning the SENTINEL platform, on completing its set of features and fixing any defects identified through the pilots' execution to come up with an almost ready-for-market offering. In this context a sound business plan is being formulated to ensure the platform's sustainability at the end of the project. The phase can be considered accomplished when all the above-mentioned activities are reported in ten (10) deliverables and successfully submitted to the REA (M36).

1. Introduction

1.1 Purpose of the document

The purpose of D8.3 "Yearly Project Management Report - third version" is to report on all the project activities executed during the third project year [from M25 (June 2023) to M36 (May 2024)] It illustrates the key activities and achievements regarding the project objective, expected impact, innovations, communication, dissemination, and exploitation activities. In addition, it covers the advancements in relation to the project objectives through the specific measures (KRs/KPIs) initially defined in the Grant Agreement (GA).

During the reference period, the SENTINEL consortium has continued to keep the initially defined time plan for all activities, in accordance with the proposal specified in Annex 1 of the GA. Following the same approach applied in the previous Yearly Project Management Reports (D8.1 and D8.2), this document presents the key insights of SENTINEL by providing updates on the general status of the project, enabling visibility of the overall work accomplished by the whole team. In such a manner, the reader of this report can get a complete image of the work carried out for all the work packages including the activities carried out per task and per beneficiary during the last project year. Furthermore, it provides an overview of all submitted deliverables, achieved milestones, core achievements with respect to project objectives, expected impact, innovations, communication, dissemination, and exploitation activities. Although the report is focused mainly on the Y3 project activities, the goal is to provide an overall overview of the project and help follow-up the different activities ongoing in the framework of the SENTINEL project.

1.2 Structure of the document

The document is presented via six (6) sections which are explained as follows:

- **Section 1** outlines the purpose of this report, its relation to other tasks and deliverables, and a brief description of the methodology followed.
- **Section 2** presents the main scientific and technical achievements in Y3 towards the project objectives.
- **Section 3** provides detailed description of the technical progress in all the WPs including work carried out per task and per partner, submitted deliverables, achieved milestones.
- **Section 4** and **Section 5** cover the project's main activities and achievements with respect to the expected impact, innovations, and communication, dissemination, and exploitation activities.
- **Section 6** summarizes the document with concluding remarks.

1.3 Intended readership

The report is part of WP8 "Project management" and is directly linked to all activities conducted in the SENTINEL WPs and tasks. It reports the progress and the consortium's main achievements focusing on the third project year by illustrating the successful completion of all the project objectives, deliverables and milestones. This document serves as a final report produced as part of Task 8.1 and Task 8.2 by providing a complete overview of the SENTINEL activities and main achievements. It is primarily addressed to the members of the project consortium while it may serve as an informative report for any external party interested as it is a public report.

2. Project objectives: Explanation of the work carried out by the beneficiaries during the 3rd Year

2.1 Objective 1 - Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS)

Objective 1 is achieved through work mainly undertaken in WP2, while the integration and interoperability of the respective components into a unified platform was performed in WP5.

In Y3, a major contribution towards Objective 1, is the delivery of the final product version of the three modules developed within WP2: the GDPR Compliance Self-Assessment module (GDPR CSA) and the Identity Management System (IdMS).

The final product version of GDPR CSA introduces two major improvements. Specifically, the model and assessment scale have been modified to highlight the conditions of SMEs' responsibility for data protection. Accordingly, instead of emphasizing compliance, the assessment highlights the SME's situation regarding its accountability. The second improvement is related to the integration of SENTINEL's OTMs taxonomy in GDPR CSA. The final product version takes into account OTMs implemented and it provides now the list of OTMs to implement in order to increase the accountability level.

A new registration process has been designed for the final product version of IdMS. In addition, the user interface has been updated to allow users to monitor their activities and be aware of their data. Those advancements are essential for making IdMS more consistent with the principles of MyData model.

More information on the design, architecture and operation of the IdMS system and the GDPR CSA can be found in D2.3 "The SENTINEL privacy and data protection suite for SMEs/MEs: Final product".

The table below provides a summary of the KRs related to Objective 1, including their status update, the activities conducted in Y3 towards their successful completion.

Table 1. KRs status update - Objective 1

KR-1.1	**Successful integration and orchestration of SENTINEL technology offerings**	**Achieved**
The refined architecture, as presented in D1.2, was designed to accommodate all SENTINEL offerings and provide the means for incorporating external ones in the form of plugins. Due to an integration-first approach that has been followed throughout the project development, interfaces and messaging formats as well as sequence diagrams have been defined and documented. As a result, we are confident that all project technologies are going to be integrated successfully and on time. This was reflected on the MVP, presented in D5.4, the Full-Featured Version (FFV), described in D5.5 as well as the final version, specified in D5.6. All SENTINEL components and technology offerings were successfully integrated and demonstrated. **Linked WP: 5; Owner: INTRA**		
KR-1.2	**40% improved compliance efficiency for SMEs/MEs**	**Achieved**
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:

$$Compliance\ efficiency = \frac{PAs\ assessed}{Total\ PAs} * 100$$

By providing innovative and user-centric data protection services such as the ROPA, GDPR CSA and DPIA, SENTINEL is expected to boost compliance efficiency by at least 40 percentage points. 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 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-M30 phase (defining as a period use –"T_1"), Dimensions Care proposes two (2) ((i) Dimensions Care Children's Case Records and ii) Safe Recruitment and Criminal Record Checks) and Dimensions Care 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. In particular, 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	T_0 - PAs Assessed / (Compliance efficiency)	T_1 - PA Assessed / (Compliance efficiency)
SENTINEL pilot partners (Clingenics and Dimensions Care)	5	0 (0)	5 (100%)

Linked WP: 2; Owner: LIST, FP

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

Drawing on data from market research[1], GDPR.EU[2] as well as based on the feedback received as part of the SENTINEL stakeholder engagement activities (cf. D7.6 "Ecosystem building and SMEs engagement report - final version"), 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 Initiative[3], finalised the

[1] https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/ [Accessed 31 May 2024]
[2] https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf [Accessed 31 May 2024]
[3] https://www.horizonresultsbooster.eu/ServicePacks/Details/6

SENTINEL business model by also drafting a pricing strategy. According to this strategy, the price of the SENTINEL platform under standard pricing plan is estimated at 348 €/year, and under premium pricing 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 other comparison analysis with competing tools can be found in D7.9 "Final business model, market analysis and long-term sustainability report". **Linked WP: 6; 7 Owner: STS**		
KR-1.4	**30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.**	**Achieved**
Regarding KR-1.4, 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. Within this context, in Y2, the SENTINEL offerings have been identified, so as to start motivating attendees and grasping their attention towards the project's tools and compliance services. Based on the established list of offerings, the SENTINEL consortium has prepared a questionnaire to record user acceptance of SENTINEL offerings. It is worth to mention, that 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, while 54% choose that the "GDPR compliance, recommendation and real-time monitoring" are the most useful services among the SENTINEL tools to be used in their own business. More in-depth analysis of the responses can be found in D7.5 "Ecosystem building and SMEs engagement report - interim version". Following the same approach, in Y3, two more workshops have organised where the SENTINEL FFV demonstration took place and SMEs that opted in for trialling the SENTINEL offerings together with additional external SMEs were contacted and invited to test the SENTINEL services integrated within the SENTINEL platform and fill in the questionnaire. It is worth mentioning, that during the 5th workshop, where the Final SENTINEL platform 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. More in-depth analysis of the responses can be found in D7.6 "Ecosystem building and SMEs engagement report - final version". **Linked WP: 7; Owner: UNINOVA**		
KR-1.5	**Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility**	**Achieved**
This KR is directly connected with the expectations and goals of plugins, such as ACS's CyberRange and ITML's Security Infusion and thus is addressed in that context. The goal is to provide a quantitative measurement of the final results of this task with regard to data integrity and confidentiality. On that note, we first deployed our solution as part of a real use case and then performed the evaluation with respect to the objective of KR-1.5. During Y1, ACS has conducted several meetings with the project's end users to get information such as identify a list of threats that could potentially occur and respectively be avoided, their infrastructure with regard to OTMs, etc. With the data collected, generic infrastructure has been created on the CyberRange, in order to exploit threats and play cyber-attack. Four (4) scenarios have been created to raise awareness of the SME, related to data storage and accessibility. In the Y2, these efforts have been intensified to be able to prove and demonstrate the applied protection mechanisms for eight (8) types of cyber threats. To achieve this, we used a new gaming interface of CyberRange. The covered cyber threats are phishing, malware attack, unsafely removed files, unencrypt disk files, social media presence, password guessing, password reused, and unprotected password. For Y3, we have collected feedback of end users to meet their needs, adapt and create		

more awareness scenarios based on the needs of SME's. From the most common attack vector the Phishing with Malicious URL that is an entry point for Malware Attack like Ransomware. We covered the Social Engineering part and show how this can compromise their personal and organizational data and security. We explained by practice how to be protected from several Cyber Threat by using common basic method like encrypt your disk file and used strong password protection. With this awareness we show how to protect SME environment from at least the 10 most common threats and attacks to data storage and accessibility. **Linked WP: 4; Owner: ACS**

2.2 Objective 2 - Provide scientific and technological advances in SMEs' and MEs' data protection compliance assessment, orchestrated and leaned towards the comprehensive digital Privacy and PDP compliance framework for SMEs/MEs

Objective 2 is realized through the work performed in WP1, WP2, WP3, and WP4. In Y3, the final version of Data Protection Impact Assessment (DPIA) toolkit was delivered. This module allows organizations to measure the exact risk and get recommendations for high-risk processing activities. The DPIA toolkit was created after a state-of-the-art review on existing tools and questionnaires (e.g., CNIL, ICO etc.). It measures the impact, likelihood, and risk based on the output of the final version of the DPIA questionnaire, which is based on the NOREA Guiding Principles and provides the information to the end-user through the Self-Assessment Engine.

In addition, the GDPR Compliance Self-Assessment (GDPR CSA) module was finalised. The GDPR CSA module performs an analysis of Processing Activities (PAs) to determine whether personal data are handled in accordance with data protection requirements. It thus provides SMEs with a) GDPR Compliance Level of Processing Activities (PAs) they are responsible for, and PAs they carry out on behalf of another company, and b) a list of recommendations to improve PA's GDPR Compliance Level.

The table below provides a summary of the KRs related to Objective 2, including their status update, the activities conducted in Y3 and the strategy towards their successful completion.

Table 2. KRs status update - Objective 2

<table>
<tr><td><b>KR-2.1</b></td><td><b>Innovative customized Requirements Engineering related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">KR-2.1 has been successfully fulfilled in the context of WP1 and in particular through the actions performed in T1.1 “The SENTINEL Requirements Engineering Methodology”. These involved:
• Identification of generic SME requirements with respect to Cybersecurity (CS) and personal data protection considering relevant challenges and threats as well as current state-of-the-art for assessing and managing risk for SMEs.
• Positioning of the technological and methodological assets of SENTINEL with respect to the above requirements.
• Development of a methodology whose purpose is to establish a generic process specifically targeting SMEs to address their needs and capabilities in such a way to enable these companies to yield the benefits of using the SENTINEL digital framework.
• Demonstration of the feasibility of the methodology through its application on two pilot cases.
The above is reported in D1.1 “The SENTINEL baseline”. <b>Linked WP: 1; Owner: IDIR</b></td></tr>
<tr><td><b>KR-2.2</b></td><td><b>Implement a dynamic rule insertion mechanism for the Recommendation Engine, providing predicates, variables and</b></td><td><b>Achieved</b></td></tr>
</table>

<table>
<tr><td></td><td><b>actions for forming rule expressions, addressing at least 135 organisational and technical measures (OTMs)</b></td><td></td></tr>
<tr><td colspan="3">The purpose of the Recommendation Engine (RE) is to provide recommendations in the form of Organisational and Technical Measures, plugins and trainings, so as to assist an SME to address potential shortcomings and vulnerabilities in the realm of data protection and cybersecurity protection. For the purpose of the MVP (D3.1), the Recommendation Engine was implemented following a rule-based approach to provide a set of recommendations depending on cases of profile and risk level outputs. Therefore, the RE leverages a pre-specified rule base to map Organisational and Technical Measures (OTMs) that correspond to a given risk assessment level with a list of plugins, trainings and other optional capabilities. At the FFV phase (work conducted in Y2), SENTINEL RE was further extended with 50 open – source tools and over 120 courses to increase flexibility and accuracy of recommendations. Additionally, and with the same goal in mind, asset ownership and locality were introduced in the calculations making the RE more accurate and realistic. In Y3, the RE mechanism was re-engineered following a more dynamic approach. In Final Product, recommendations are generated by a dynamic rule management system allowing effortless implementation of new rules, while upgrading the system to provide explanations to the user on the reasons behind the recommendations he receives. <b>Linked WP: 3; Owner: ITML</b></td></tr>
<tr><td><b>KR-2.3</b></td><td><b>Test GDPR compliance and digitalized DPIA self-assessment framework.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">The KR-2.3 is linked to WP2 and 4, and more specifically deliverables D2.1 and D4.1 due M12 and D2.2, D4.2 and D2.3, D4.3 due in M18 and M30 respectively. This KR has been realised through the final versions of the GDPR CSA and DPIA self-assessment tools which were respectively designed and implemented throughout the duration of the project. Both tools are fully integrated into the SENTINEL platform via APIs and can be executed for one processing activity at a time, providing a score that is visible to the user via MySentinel UI. The testing of the frameworks in real-world has been performed under WP6 and details can be found in D6.3. A conformity assessment of the GDPR CSA Assessment Model with CARPA’s data protection requirements has been performed, while in parallel assessments of the GDPR CSA Method, Framework and Model have been performed with ISO/IEC 33002, ISO/IEC 33003 and ISO/IEC 33002 respectively. <b>Linked WPs: 2; 4; Owner: STS</b></td></tr>
<tr><td><b>KR-2.4</b></td><td><b>Offer robust and easy to adopt data access management, authentication, authorization and record keeping technologies to SMEs/MEs for GDPR compliance.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">This KR is mainly tackled by SENTINEL’s Identity Management System (IdMS) as well as the record-keeping capabilities provided by its Profile Service. The IdMS provides authentication, authorization and Single Sign-On capabilities to SENTINEL end users, based on an open-source solution (Keycloak), towards adopting the MyData model, whose core idea is that data owner should have an easy way to see where personal data goes, specify who can use it, and alter these decisions over time. The SENTINEL IdMS is offered as-a-service, where SMEs can use it to verify, and manage attributes and entitlements that are necessary for the creation and maintenance of digital identities for all users accessing third party applications EU-wide. This includes functionalities and flows like user registration, account recovery, profile management, credentials management, and consent management. In terms of record keeping, SENTINEL offers the capability of storing versatile organisation-wide information, as well as storage of activities that involve processing of personal data. Furthermore, it offers the capability of keeping a formal, immutable and auditable Record of Processing Activities (ROPA) that helps companies comply with Art.30 of the GDPR. All records are persisted in the Profile Service and are made available to SENTINEL plugins (such as GDPR CSA, DPIA and CSRA) as required. <b>Linked WP: 2; Owner: ITML</b></td></tr>
<tr><td><b>KR-2.5</b></td><td><b>Ensuring the delivery, adoption, and utilization of a unified Identity Management System.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">This KR is tightly connected with KR-2.4 and is related to the delivery of an integrated IdMS. As mentioned above, the IdMS is offered as-a-service that provides a range of functionalities to the SME/ME including i) Central, EU-wide, self-service identity management, ii) Credentials and access tokens management that allow Authentication (AuthN) of the above identities, iii) Role Based Access Control (RBAC), iv) Federation with 3rd party applications, based on protocols that allow scalable expansion according to the needs of SMEs/MEs wanting to leverage SENTINEL IdMS, v) My Data,</td></tr>
</table>

data management scheme for secure, GDPR compliant storage and access of user data, vi) Governance. Adoption and widespread utilization of the unified IdMS have been verified as part of WP6 activities, where the SENTINEL use case owners and external SMEs have tested the system in operating conditions. **Linked WP: 2; Owner: ITML**

2.3 Objective 3 - Provide novel tools and services for enabling highly automated PDP compliance in SMEs/MEs

Objective 3 maps to key technological achievements which enable the project's advertised automation in the sense of minimizing the involvement of costly human experts in cybersecurity and personal data protection processes such as compliance checks, assessments and recommendations. This technical work has been carried out up to M30 of the project, in the four main technical work packages: **WP2** - which develops personal data protection and cybersecurity technologies key to SENTINEL, namely the GDPR compliance self-assessment, the cybersecurity risk assessment, the IdMS and others; **WP3** - which develops core components of the SENTINEL technical architecture specially focusing on formulating, formatting and presenting an appropriate human-readable set of recommendations (the "policy"), in the form of collections of (a) organizational and technical measures, (b) plugins, tools and software, and (c) cyber awareness and PDP trainings and educational material; and **WP4** - which is primarily responsible for (a) SENTINEL's tailored SME Profiling process including the Profile Service and the Self-Assessment Service, (b) the detailed capturing of personal data processing activities, including an auditable ROPA, (c) an automated DPIA, (d) deploying advanced Cyber Range -based simulations and training, and (e) developing the SENTINEL Observatory; overall integration work takes place in **WP5**.

The SENTINEL MVP was initially released in M12. In the ensuing 6 months, significant effort was dedicated to technical developments leading to SENTINEL's full-featured version in M18, in which functioning and demonstrable versions of all of SENTINEL's functionalities, tools and services were developed, which contribute to Objective 3. These novel tools and services were further refined for the project's final integrated version in M30. In more detail:

- The detailed cyber asset capturing and inventorying, based on the MITIGATE framework, which allows for cybersecurity risk assessments (CSRA) at a single-asset or whole processing activity (business process) level has been finalised. The CSRA is now SENTINEL's third self-assessment tool, after the GDPRCSA and the DPIA.
- The integration of the SCORE metamodel into the SME profiling process, including the convergence of the input of the two PDP-related self-assessment tools (the GDPRCSA and the DPIA) with the existing personal data processing activity capturing process (eventually allowing unified SME profiling) is now completed.
- SENTINEL's read-only, immutable, auditable and GDPR compliant Record of Processing Activities (ROPA) is now completed, with full PA versioning capability.
- A revised and more detailed global organizational and technical measures (OTMs) classification, complete with selection taxonomies for the recommendation engine and user-facing policy metadata has been implemented. Specifically, the sixth organisational measures category (O6) of the classification has been renamed to "Managing GDPR compliance" and enriched with over 30 low, medium and high-risk measures targeting data protection requirements. This important work has taken place between M25 and M30.

- A complete user manual, with a getting-started guide, a glossary and per-page inline help has been developed in wiki format, greatly simplifying the user journey and flattening the solution's learning curve.
- Enhanced the policy recommendations considering detailed cyber asset data and available tools (plugins) and trainings.
- The Policy Enforcement monitoring, in the form of tracking the implementation status of OTMs, also considering their recommendation status, is now complete.
- The Observatory's expansion with a knowledge base and additional sources / feeds is now final.
- The Identity Management System (IdMS) is also finalised.
- The GDPR compliance self-assessment plugin (GDPRCSA) is also finalised to consider all six aspects of GDPR compliance: (a) Record (carried forward from the MVP), (b) Personal Data Lifecycle Management, (c) Rights Management, (d) Consent Management, (e) Data Protection Management, and (f) Personal Data Breach Notification.
- The Gamification Interface of the Airbus Cyber-Range, addressed to the average SME employee and based on realistic SME scenarios is now final.
- The use cases 4 and 7, for: (a) receiving security notifications, and (b) reporting and sharing cybersecurity incidents (e.g. data breach notifications) are now final, implementing basic usage scenarios.
- The profiling process for Processing Activities has been enriched with Templates functionality, which is now finalised with four (4) key high-usage templates for SMEs: Marketing, HR, and more.
- The transition into a fully-fledged rule-based Recommendation Engine is now also complete. The new rule engine is based on the Drools business rule management system and framework, and is already implementing a number of custom rules, so the system can recommend measures, tools and trainings based not just on risk but on custom and complex profiling rules.

The achievements above which, as of M30, are concluding the technical work foreseen for the project, primarily support key results KR3.1 to KR3.4 which will be achieved by the project's end and describe specific and quantified indicators for the technologies, tools and capabilities made available.

The table below provides a summary of the KRs related to Objective 3, including their status update, the activities conducted in Y3 towards their successful completion.

Table 3. KRs status update - Objective 3

KR-3.1	**More than (20) novel services and tools utilized and integrated from diverse multi-domain technological areas and applied in SMEs/MEs environments.**	**Achieved**
We consider the term services and tools within the wider concept of "capabilities" offered by SENTINEL. During Y3, technical partners - as part of activities in WP2, WP3, WP4 and WP5 – have finalised the development of tools and services, which are integrated in the Final SENTINEL platform (see D5.6) and span several capabilities. - The MITIGATE framework, provided by FP, and integrated within the SENTINEL's platform, delivers a number of user-facing tools and services: (1) The Vendor and Product Management service which delivers a CPE-based catalogue of vendors' products. It enables SMEs/MEs to identify and select specific versions of products from vendors that correspond to their IT assets aiming to search for		

security-related information on these products. (2) The asset inventory service (online ISMS for SMEs/MEs), including asset interdependencies and security-related information. (3) The Vulnerability Management service which allows SMEs/MEs to capture information of all vulnerabilities along with their attributes and severity scores identified for the selected products. (4) The Common weaknesses management service which is realized through the Common Weakness Enumeration specification of MITRE and provides a common language of discourse for discussing, finding, and dealing with the causes of software security vulnerabilities as they are found in code, design, or system architecture. (5) The Threat Management service which provides to SMEs/MEs all threat-related information upon specific selected IT products. (6) The Simulation Environment which enables SMEs/MEs to experiment with attack scenarios by selecting specific vendors' products and obtain knowledge on interrelations of corresponding threats and vulnerabilities. All these MITIGATE services are integrated in SENTINEL via the (7) CyberSecurity Risk Assessment (CSRA) tool, available to users via MySentinel (Cybersecurity), enabling SMEs to assess assets grouped under Processing Activities (PAs).

- Another novel service is the (8) GDPR Compliance Self-Assessment (GDPRCSA) developed by LIST. GDPRCSA allows SMEs/MEs to determine their compliance level with GDPR and provides a set of recommendations to improve it. GDPRCSA covers all six data protection capabilities (Record, Personal Data Lifecycle Management, Rights Management, Consent Management, Breach notification management, and Data Protection Management System).
- The (9) Data Protection Impact Assessment (DPIA) API-based service, provided by STS, allows SMEs to identify (through assessment) and minimise (through recommendations) the data processing-related risks and is invoked for processing activities that are likely to result in a high risk to individuals.
- (10) Security Infusion (SI) is an all-in-one solution provided and supported by ITML, which implements data collection and management services in order to address the need for control baseline of Information and Communications (ICT) operations with integrated risk mitigation and regulatory compliance capabilities. Another indicative example of the SENTINEL platform novel services is the (11) Identity Management Service (IdMS), also provided by ITML, which supports self-service EU-wide and MyData-compliant identity management and data governance with Single Sign-On capabilities.
- SENTINEL also provides robust cybersecurity data retrieval, management and dissemination leveraging custom tools that actively connect the (12) Observatory Information Exchange (supported by ITML) with external cybersecurity and open-source threat intelligence, such as MISP, HELK and NIST for browsing, searching, and filtering. Within the same context, the (13) Observatory Knowledge Base is hosting third-party content for cybersecurity and personal data protection, fetched from i) Information Exchange, ii) MITIGATE and iii) open-source content and training material.
- SENTINEL's OTM recommendations are accompanied with (14) Open-Source software/plugins and educational or training material, curated by TUC, which helps users better understand, design and implement security and data protection controls within their organization. A major SENTINEL offering is (15) the CyberRange, contributed by ACS, enabling (a) simulation environments (testbeds) and (b) a gamification interface with realistic and SME-focused scenarios, for testing cybersecurity setups before on-site integration for optimizing defences and training end-users.
- To the above services we should add core offerings of the integrated SENTINEL platform for cybersecurity and personal data protection. The platform enables users to (16) receive security notifications, through the integration of Security Infusion (SI) with the SENTINEL Notification Aggregator; (17) handle and share cybersecurity incidents and data breaches, as they occur, leveraging the Incident Reporting module; (18) create and edit a data protection-oriented organisational profile, complete with a global asset profile, MITIGATE-modelled asset inventory and a complete Processing Activities data capturing model shared with the self-assessment tools; (19) record their processing activities in a permanent, immutable and auditable ROPA, thus satisfying Art. 30 of the GDPR; (20) obtain tailor-made recommendations of measures (OTMs), software and trainings, based on thorough analysis of every aspect of their profile and processes facilitated through an intelligent synergy of SENTINEL's Recommendation Engine (RE) and Policy Drafting (PD) modules, and, finally, monitor the progress of the enforcement (implementation status) of the aforementioned recommendations through the (21) Policy Enforcement tool, integrated with each policy draft.

Details on individual progress and functionalities of these tools and services in the final version of the SENTINEL integrated solution can be found in deliverables D2.3, D3.3, D4.3 and D5.6. **Linked WPs: 2; 3; 4; 5; Owner: FP Linked WPs: 2; 3; 4; 5; Owner: FP**

<table>
<tr><td><b>KR-3.2</b></td><td><b>At least (10) tools and services related to data protection, data privacy management, security assurance and compliance.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">The technical work (WP2-WP5) completed by the consortium leading up to the final version (M30) has directly contributed to this Key Result. The final SENTINEL tools and services for cybersecurity, data protection and compliance are now identified as such:
1. Organisation profiling (SENTINEL Core)
2. Cyber asset inventorying (SENTINEL Core/MITIGATE).
3. Personal data processing activities capturing (SENTINEL Core)
4. GDPR compliant recording of PAs (SENTINEL Core /ROPA).
5. GDPR compliance self-assessment (GDPRCSA).
6. Data protection impact assessment (DPIA).
7. Cybersecurity risk assessment (CSRA/MITIGATE).
8. Policy recommendations for OTMs, software and training material (SENTINEL Core).
9. Policy enforcement monitoring: tracking the implementation status of OTMs (SENTINEL Core).
10. Cyber Range simulations and gaming with realistic SME scenarios (CyberRange).
11. Identity management system (SENTINEL Core/IdMS).
12. Cyber incident reporting and handling (SENTINEL Core/Observatory).
13. Receiving security notifications with Security Infusion (SENTINEL Core/SI/FVT).
14. Observatory Knowledge Base (SENTINEL Core/Observatory).
15. Observatory Information Exchange (SENTINEL Core/Observatory).
Some of the above not only support the integrated SENTINEL solution as a whole but are supported by partner-contributed components. These tools and services are the essential constituent offerings of SENTINEL’s final version (M30); their maturity and completion status allow us to measure this KR both qualitatively and quantitatively. <b>Linked WPs: 2; 3; 4; 5; Owner: IDIR</b></td></tr>
<tr><td><b>KR-3.3</b></td><td><b>Update and enrich the SENTINEL OTMs classification and their mappings to adapt to the dynamic properties of the SENTINEL Recommendation Engine.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">In the final platform release, SENTINEL’s Common Service is enriched with around 50 open-source tools and over 120 courses from the full-featured phase, and an overall number of 171 organisational and technical measures (OTMs) including 37 new GDPR measures. The above have been reported in D3.3 “The SENTINEL digital core: Final product” and is anticipated to significantly advance SENTINEL services in privacy-aware environments for SMEs/MEs. <b>Linked WP: 3; Owner: ITML</b></td></tr>
<tr><td><b>KR-3.4</b></td><td><b>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.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">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. <b>Linked WP: 3; Owner: ITML</b></td></tr>
</table>

2.4 Objective 4 - Facilitate an efficient exploration of cost-efficient, intelligent, and automated PDP compliance and Identity Management full potential in SMEs/MEs environments and realize societal and economic opportunities by validating SENTINEL framework in real-world settings via use cases driven by complementary industries

This objective’s main focus is planning to and ultimately engaging users from different industries and with different needs and requirements in terms of data protection and privacy to validate and provide feedback to the SENTINEL framework. As this objective refers to validation and is mainly related to WP6, as well as WP7 (for further engagement and exploitation), related work has intensified in Y2.

During the first year of the project, we have already identified seven (7) ways (use cases) that a user can use and interact with SENTINEL which were based on a thorough requirements analysis performed in T1.1 “SENTINEL baseline: Setting the Methodological Scene” and recorded in D1.1 “The SENTINEL baseline”. These have been described in detail in the architecture in D1.2 "The SENTINEL technical architecture" together with the respective experimentation protocols, including KPIs and related evaluation variables, as part of D1.3 "The SENTINEL experimentation protocol". With respect to experimentation variables, the methodology for validating the system that has been initially defined in D1.3, has been finalised as part of T6.1 and recorded in D6.1 “SENTINEL Demonstration - initial execution and evaluation”.

Towards experimentation execution, in Y2, piloting-related activities have seen progress, including the definition and refinement of experimental setups and relevant infrastructure of the two use case owners. In the meantime, the project has secured the engagement of six (6) extra-consortium SMEs/MEs through Digital Innovation Hubs (DIHs) to trial the SENTINEL platform during the validation phase. A critical milestone achieved as an enabling step towards this objective has been the successful implementation of the MVP. The MVP was demonstrated to internal and external stakeholders and its functionality, usability and performance characteristics were internally evaluated by the SENTINEL user partners. The results informed the development of the FFV in Y2.

Y3 saw the main implementation stage for Objective 4-related tasks with the completion of the project’s final version and the execution of at least five demonstrators in real-life settings, including the evaluation of central aspects such as “cost-efficiency”, “automation” and “intelligence”. The identification of user personas has assisted this user-centric validation process.

Y3 work culminated in a significant milestone, reached in February 2024, during a 2-day meeting when one day was entirely devoted to external users from SMEs and MEs from different industrial and commercial sectors. During this day users, after receiving an introduction of the objectives of SENTINEL, the advantages of SENTINEL to SMEs and an introduction to the SENTINEL platform were engaged in a full walkthrough of all the functionalities of the platform making sure that their experience using the system was grounded on real situations from their domain of expertise. This is further discussed under the WP6 heading.

The table below provides a summary of the KRs related to Objective 4, including their status update, the activities conducted in Y3 towards their successful completion.

Table 4. KRs status update - Objective 4

KR-4.1	***Successful collection of data for recommendations of personal data protection technologies and GDPR compliance procedures in complementary SMEs/MEs environments.***	**Achieved**
The SENTINEL platform (since it’s MVP version) is fully integrated and provides functionality that successfully collects data from SMEs/MEs to build their profile, provide assessments via the GDPR CSA and DPIA tools and policy recommendations via the policy recommendation engine. The DPIA toolkit underwent improvements to account for the implemented OTMs during the FFV, while FFV of GDPR CSA provides a set of recommendations to improve SMEs/MEs compliance levels. In the final version during Y3, the DPIA questionnaire was reintroduced with a more complete set of questions based on the NOREA Guiding Principles. Finally, GDPR CSA module has been improved regarding		

the accessibility of questionnaires, proposed answers, and proposed improvement. **Linked WP: 6; Owner: STS**		
KR-4.2	***Delivery of three (3) integrated versions of the SENTINEL framework.***	**Achieved**
All three versions of the platform (MVP, FFV and Final Version) were successfully delivered in time and reported in D5.4, D5.5 and D5.6 respectively**. Linked WP: 5; Owner: INTRA**		
KR-4.3	***Execution of five (5) demonstrators in complementary SMEs/MEs' industries and environments, together validating at least 95% of tools.***	**Achieved**
Apart from the two (2) pilots defined in the GA, the consortium has identified additional SMEs to participate in the SENTINEL testing and evaluation process, as a result of T6.3 activities. In Y2, four demonstrators (CG, TIG pilots and 2 external SMEs) successfully tested the SENTINEL MVP and provided valuable feedback. After the SENTINEL FFV release in M18, the SENTINEL pilot partners (CG and TIG) started the end-to-end validation of the SENTINEL platform as part of WP6 activities. In particular, CG conducted trials of SENTINEL FFV during M23-M27, whereas 3 demonstrators from TIG (i.e. Dimensions Care, Beyond Limits and Sportfit) conducted trials of SENTINEL FFV during M25-M29. 10 additional demonstrators executed trials of SENTINEL FFV during M28-M29 engaged via UNINOVA (DIH Pilot). Eventually, in M30, the project reached MS5 'Demonstration Fire' and by that **time 14 demonstrators** carried out an end-to-end validation of SENTINEL tools. To this aim, INTRA – as an integration leader –monitored this KR under T5.2 to determine the percentage of tools validated in each demonstrator. Additional effort was considered in M33 via the SME user-centric workshop which engaged **11 additional demonstrators** and EAB members. This brings in **total 25 demonstrators** who conducted an end-to-end validation towards the SENTINEL tools during the three Pilots operations and the physical final SME-centric workshop. **Linked WPs: 5, 6; Owner: CG**		
KR-4.4	***More than ten (10) trials to demonstrate SENTINEL tools' applicability and performance within real-world environments.***	**Achieved**
A trial refers to an end-to-end validation of one of the SENTINEL services. As mentioned in KR-4.3, as part of the work conducted in WP6 (during the pre-pilot phases), **short-run tests were executed by the two end-user partners CG and TIG** right after the SENTINEL MVP release (M12) and **4 initial trial executions** were conducted for the evaluation of the SENTINEL MVP within M16-M17 period, involving CG and TIG internal pilot partners and 2 external SMEs engaged via Digital Innovation Hubs (DIHs) and provided initial feedback. After the SENTINEL FFV release the main pilot phase was commenced in M18 and within M23-M27 Clingenics performed two (2) trial executions by **two (2) CG end-users** who tested the SENTINEL FFV (1st prototype) under specific PA experiments relying on the healthcare sector. Moreover, the TIG pilot activities have started in M24, and four **(4) additional trial executions** conducted by TIG pilot end-users (i.e. 2 end-users engaged from Dimensions Care on PA experiments related to social care, one (1) end-user from Beyond Limits and one (1) end-user from Sportfit on performing generic PA experiments to test the SENTINEL FFV. During M28-M29, the DIH pilot activities were running. In this context, 10 trials conducted by **10 external SMEs** recruited by DIHs. Eventually, in M33 a physical final SME-centric workshop carried out where eleven (11) trials executed by **eleven (11) external SMEs**, recruited under T6.3 for the workshop, **two (2) CG end-users**, **two (2) end-users engaged via TIG** (i.e., one **(1) Dimensions Care end-user and one (1) Sportfit end-user)** and **three (3) EAB members** to test and validate the SENTINEL final integrated solution (2nd prototype). In **total 42 trials** occurred concerning the testing of SENTINEL 1st and 2nd prototypes. **Linked WP: 6; Owner: FP**		
KR-4.5	***Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.***	**Achieved**
Several meetings have been carried out to define and implement the User Interface (UI) of the SENTINEL platform, namely MySentinel. As part of these meetings, updated versions for the mock ups were presented to the consortium alongside an initial version for the User Journey. Continuous work has been carried out on the UI since the start of the project. By M12, the MySentinel dashboard included links to components that were incorporated in the MVP, as well as the relevant pages. Organization Profile, Processing Activities, Contact Persons, Assets, Self-Assessment tools, Policy Recommendations and a Threat Intelligence Platform (TIP) comprised the modules offered to the end-user by the SENTINEL platform in the MVP phase (more details in D5.1).		

By M18, the MySentinel dashboard already included links to components and modules that were incorporated in the first complete prototype, as well as the relevant pages. This means that apart from the MySentinel dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts were also included in the second version of the platform. Additionally, feedback from collaborating end-users with diverse backgrounds (under WP6) was taken into consideration in the platform.

By M24, several elements of the MySentinel UI in several different pages were updated. Additionally, a number of bugs/glitches identified by the technical team and/or the end-users were fixed. Furthermore, the UI was integrated fully with the backend modules. Moreover, the Cyber Range Gaming Interface, offered by ACS, was integrated into the platform.

In the final period of the relevant task T5.1 (M25-M30), we continued to do comprehensive work in order to refine and enrich the content of the UI by constantly engaging and closely collaborating with end-users (under WP6), incorporating their feedback and implementing a UI/UX which offers true usability. Additionally, made all adaptations required in the communication of the UI with all modules as their development progressed. This effort resulted in the final version of the MySentinel UI and was documented in the subsequent iteration of D5.1 and D5.2, namely D5.3. **Linked WP: 5; Owner: AEGIS**

2.5 Objective 5 - Consolidate international and European links, raise awareness, collaborate with standardization bodies and ensure the technology transfer of the project's results via EU digital innovation hubs

During Y3, the consortium has undertaken a plethora of dissemination and exploitation activities to (a) raise awareness, (b) collaborate with international and EU links and (c) promote the technology transfer of the project's results. In particular:

Activities towards the aforementioned targets included the organization of the Cyber Security and Data Protection Synergies – Joint Cluster Event held on the 16th and 17th of October 2023 at UNINOVA facilities. The agenda included various presentations made by invited sister project representatives together with open discussion on relevant topics of the cyber security and data protection domain. SENTINEL co-hosted the following 10 projects: **IDUNN, KRAKEN H2020, Electron, Secant, CROSSCON, TRUSTaWARE, IRIS H2020, SPATIAL, ERATOSTHENES** and the **ARCADIAN-IoT**.

In addition to this, the consortium has organized its 4th SME-centric workshop (online) on the 25th of September 2023. with the main scope of demonstrating the SENTINEL platform within the third pilot of the project engaged through Digital Innovation Hubs (DIHs) as part of D6.3. The workshop was held online gathering 48 participants and engaging 24 SMEs in total. A full guide of instructions has been shared to the participants in order to proceed correctly with the evaluation and trial of the platform.

The 5th and final SME-centric workshop was held in Athens, Greece, on the 27th of February during the 2nd day of the 7th SENTINEL plenary meeting. The event aimed to present the main achievements reached within the scope of the project, demonstrate the SENTINEL platform and elaborate on the innovation capacities of the project. It covered topics related to GDPR, personal data protection and cyber security and how these aspects can affect the SMEs' core business activities. The SENTINEL platform was presented to the audience highlighting its innovation capacities, and how an SME can utilize them to leverage its privacy and cybersecurity. The workshop welcomed **11 additional companies** from the private sector, small and medium-sized enterprises (SMEs), startups, and Small Business Entities.

Finally, SENTINEL was jointly organised its final event with Arcadian-IoT project which was held on the 9th of April 2024 in Stockholm, Sweden. It was a comprehensive in-person event dedicated to demonstrating the innovation capacities of both projects towards integrated and automated IoT Cybersecurity and Personal Data Protection, which gathered more than 40 physical participants.

During this period, SENTINEL has also engaged with additional DIHs, at national and EU level, namely ATTRACT, Südwestfalen EDIH and AIP (*Associação Industrial Portuguesa*).

In Y3, the SENTINEL exploitation, standardization and ecosystem building activities has been intensified by focusing on following activities:

- Finalising the SENTINEL offerings and value proposition.
- Updating individual and formulating the ground for joint exploitation.
- Boosting standardisation activities.

From communication perspectives, additional promotional material such as four more (4) newsletters, five (5) videos, three (3) SENTINEL podcasts, 1 SENTINEL booth mock-up for INFOSHARE event, regular posts in social media (LinkedIn, Twitter), were produced during Y3 attracting more and more attention as the project progressed.

Four (4) more papers have been presented in three (4) different conferences including the EuroSPI 2023 on the 30th of August in France, the IEEE CSR-CRE 2023 on the 31st of July 2023 to 2nd of August 2023 (online), the IEEE Symposium on Computers and Communications (ISCC) on the 9th to 12th in Tunisia, and the International World Wide Web Conference 2024 (WWW), on the 13th to 17th of May in Singapore**.** These papers (except the last paper) have already been published and are openly accessible to the general public. In addition, the partners have managed to publish 1 electronic journal paper, 1 journal paper in Internet of Things Journal, 2 already accepted journal papers in “Journal of Surveillance, Security and Safety” and “International Journal of Information Security”, submitted 1 journal paper and currently are working on 2 journal papers to be submitted by the end of the project.

Finally, the consortium has participated the following major events and conferences: PUZZLE‘s Cybersecurity Conference, Final Event of the CitySCAPE project, 28th IEEE Symposium on Computers and Communications, IEEE International Conference on CSR, CyberHOT Summer School 2023, 30th EuroSPI Conference, ATTRACT EDIH public presentation, AIP Roadshow I&D, Data Protection Day, CTI Workshop, INFOSHARE Conference.

The table below provides a summary of the KRs related to Objective 5, including their status update, the activities conducted in Y3 and the strategy towards their successful completion.

Table 5. KRs status update - Objective 5

KR-5.1	**All SENTINEL solutions, products and services aligned and harmonized with regulations and EU standards.**	**Achieved**
From an early point, all the linked deliverables from a data protection/privacy standpoint have been reviewed by the consortium. CECL, as the owner of this KR, gave input on applicable standards, where relevant, and provided feedback to ensure all solutions proposed in SENTINEL were in line with the		

<table>
<tr><td colspan="3">EU and national legal and regulatory framework. In this respect, the CECL scientific officer in collaboration with the project’s Ethics Supervisor, updated the partnership on EDPB and national DPAs’ opinions, relevant to the SENTINEL scope, in real time, as well as through its regular reporting obligations and updated the respective deliverable (see D2.5 “Continuous data privacy legislation compliance monitoring and guidelines - final version”) that was successfully submitted in M30. <b>Linked WPs: 2, 8; Owner: CECL</b></td></tr>
<tr><td><b>KR-5.2</b></td><td><b>Define a concrete dissemination strategy to raise awareness.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">From an early point of the project, the consortium has defined a structured methodology to disseminate the project’s offerings and preliminary outcomes and raise awareness of SENTINEL’s potential. The SENTINEL dissemination strategy has been already established and documented in D7.3 (M18). Furthermore, the strategy was successfully realised through a plethora of dissemination and communication activities conducted during Y1 and Y2. In Y3, SENTINEL has increased awareness and disseminated the SENTINEL outcome among wider audiences by following the methodologies and strategy already defined in D7.3 and D7.4. <b>Linked WP: 7; Owner: UNINOVA</b></td></tr>
<tr><td><b>KR-5.3</b></td><td><b>Uptake more than (6) standards from several data privacy and compliance related technologies.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">During Y2 SENTINEL successfully applied for the first open call of the Horizon Standardisation Booster, aiming to provide standardization support for H2020 projects (application made on the 5th of July 2022). Through series of meetings the expert assigned by HSBooster.eu assisted SENTINEL to (i) analyse CARPA’s requirement (conformity assessment of GDPR CSA Assessment Model), (ii) identify extent of existing and additional measures required for CARPA (based on current CSA and ISO standards being followed) and (iii) identify relevant current and upcoming standards that SENTINEL can take advantage of. SENTINEL implement partly or fully the following standards:
1. ISO/IEC 29100 – Privacy Framework
2. ISO/IEC 27701 – Privacy Information Management
3. ISO/IEC 27001 Information security management systems
4. ISO/IEC 29190 – Privacy capability assessment model
5. ISO/IEC 27035 Information security incident management
6. ISO/IEC 27552 – Privacy-specific application of ISO/IEC 27001 Requirements (PIMS)
7. ISO/IEC 29151 – Code of practice for personally identifiable information protection
8. ISO/IEC 29134 – Privacy Impact Assessment methodology
Other relevant standards that have been considered as well as a study of CARPA are as follows.
1. ISO/IEC 27002 — Information security, cybersecurity and privacy protection
2. ISO/IEC 27003 — Information security management system implementation guidance
3. ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation
4. ISO/IEC 27005 — Guidance on managing information security risk
5. ISO/IEC 27040 — Storage security
6. ISO/IEC 27557 — Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management
7. IEC 31010:2019 Risk management – Risk assessment techniques (related to risk management)
8. ISO/IEC TR 27550:2019 Privacy engineering for system life cycle processes (related to risk management and DPIA). <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>KR-5.4</b></td><td><b>More than (8) DIH engaged to further communicate and support SENTINEL offerings.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">During Y3, SENTINEL kept maintaining direct connections with the DIHs already contacted and engaged with two (2) new DIHs. As a result, by the end of Y3, UNINOVA had engaged ten (10) DIHs namely: <b>Produtech</b>, <b>DIH4CPS</b>, <b>DIHWorld</b>, <b>Madeira DIH</b>, <b>Digital Manufacturing Innovation Hub Wales</b>, <b>DataLife DIH</b>, <b>Images-et-reseaux DIH</b>, <b>ICE RWTH DIH</b>, <b>ATTRACT</b>, and <b>Südwestfalen EDIH</b>. The collaboration with these DIHs has extensively helped to invite its members (the SMEs/MEs) to trial SENTINEL as part of the validation phase (WP6). <b>Linked WP: 6; Owner: UNINOVA</b></td></tr>
</table>

2.6 Objective 6 - Boost the effectiveness of the EU data economy by offering high TRL solutions (TRL 6-7).

Towards achieving this objective, the SENTINEL consortium has progressed in Y3 by finalising its business model which initially was launched in Y1 and updated in Y2. In particular, among others, SENTINEL value proposition, main offerings, target markets, customer segments, possible revenue streams, individual and joint exploitation plans and expected TRLs have been finalised. SENTINEL is based on several mature – in terms of technology readiness- components (e.g., MITIGATE, Security Infusion, CyberRange, etc) which are already placed at a high TRL, thus ensuring that the end product TRL has reached 6-7, as expected. In Y3, two important milestones were achieved towards realising Objective 6 is the release of the FFV final version of SENTINEL, described in D5.6 (M30) and the best practices for maintaining and operating the system in the long-term, described in D5.7 (M36). This consolidated the SENTINEL validation phase as well as activated the project's exploitation activities towards creating opportunities for European-based SMEs to use SENTINEL offerings. It enabled further collaborations through the tangible trialling of SENTINEL offerings by third parties. Engagement of third parties was accomplished by UNINOVA through the different networks of DIH previously identified.

The table below provides a summary of the KRs related to Objective 6, including their status update, the activities conducted in Y3 and the strategy towards their successful completion.

Table 6. KRs status update - Objective 6

KR-6.1	**Ready to market integrated solution for the overall security compliance framework and independent privacy and security enhancing solutions (TRL 7).**	**Achieved**
Through its three release cycles, the SENTINEL platform and its constituting components have been developed, tested and improved. The solutions were successfully validated and positively evaluated by external SMEs through the activities conducted as part of WP6. **Linked WP: 5; Owner: INTRA**		
KR-6.2	**At least four (4) SENTINEL tools reach market readiness level (8) at the end of the project**	**Partially achieved**
The initial evaluation of TRLs and MRLs of the SENTINEL platform and its components have been already conducted and reported in D7.7 and D8.12. More technical enhancements on the SENTINEL tools were performed progressively within the ongoing project's development works taking into account the feedback that is gradually received from the trials/pilots' execution evaluators. To this aim, different types of personas have been identified from SMEs end-users which were grouped by specific criteria to better profile the targeted users and thereby improve the linkage between the technical work on the system architecture and the user-centric approach. By utilizing this persona-based validation, we aimed at facilitating the identification and development of technical improvements (e.g. UI/UX improvements) which can increase the commercial readiness of the SENTINEL tools towards the current needs of SME markets. This KR was monitored successively on the technical enhancements carried out after each pilot from the lessons learned. As a result, SENTINEL offers three (3) mature – in terms of technology and market readiness - components (**MITIGATE**, **Security Infusion**, **CyberRange**), which are placed at a high TRL and MRL, while Security Infusion and CyberRange are already launched in the market. In addition, tools/services newly developed in the project (e.g., IdMS, policy drafting, self-assessment workflow, GDPR CSA module) were further improved in Y3 and validated in real-world settings. The final calculation of the market readiness level reached by the SENTINEL tools is assessed and provided in D8.13 "The SENTINEL technical and innovation management report - final version". **Linked WPs: 2-5; Owner: FP**		
KR-6.3	**At least six (6) third-party collaborations to be established for further applicability verification.**	**Achieved**

With respect to KR-6.3, SENTINEL has been interacting with several SMEs, since the beginning of the project, under activities of T6.3 and T7.4, with the purpose of establishing partnerships for applicability and testing of the SENTINEL offerings. SENTINEL has organised five (5) SME-centric workshops in total (2 during Y1, one during Y2 and two during Y3), bringing onboard SMEs/MEs from different application domains that are interested in learning more about GDPR compliance and PDP, as well as trialling the SENTINEL framework. In parallel, UNINOVA has engaged ten (10) DIHs so that their associates (the SMEs) can trial the SENTINEL platform and provide feedback on the SENTINEL offerings. As a result, **23** third-party companies participated in the SENTINEL testing and applicability validation activities. **Linked WPs: 5; 6; 7; Owner: UNINOVA**		
KR-6.4	**More than ten (10) critical aspects (e.g., maintenance and software updates) will be addressed to ensure long-term sustainability of the solution.**	**Achieved**
The design and development process of the platform made various technical provisions related to long-term sustainability. These include aspects such as extensibility and modularity of the architecture, software maintainability in terms of proper organisation of code repositories, naming conventions in code, common objects libraries, documentation of synchronous and asynchronous APIs), regular backups and automated deployments. Its long-term sustainability was also enhanced by improvements in the explainability, the UI as well as a clearer focus in the Unique Value Proposition that was elicited by user feedback and research. Finally, all appropriate ethical considerations were also taken into account to ensure the longevity prospects of the solution. **Linked WP: 5; Owner: INTRA**		
KR-6.5	**A concrete business plan for business continuity (including joint exploitation plans, alliances and collaborations) will be released at the end of the project.**	**Achieved**
This KR is linked to WP7 and T7.1. Activities within this task have been ongoing since the start of the project. As a first step, all consortium partners contributed to the rationale which became the basis for the exploitation plan. Additionally, a questionnaire was created and circulated for gathering insights from many different perspectives including academia, large industries, technology providers and SMEs. These insights contributed to understanding and identifying SENTINEL's value proposition and supporting its business modelling. This was presented in D7.2 titled "Market analysis and preliminary business modelling" in M6 of the project. Following submission of D7.2, information gathering, and observation of market trends continued for changes that could affect the elaboration of the joint business plan presented in the deliverable. In this context, as part of the continuous market observation, an intermediate analysis was carried out resulting in an updated business strategy [value proposition, business model (canvas)] which was included in D7.7, submitted in M18. After D7.7, we continued monitoring and analysing the market to provide updates to the (i) market analysis, (ii) business model, (iii) business model canvas and (iv) value proposition. In Y3, the business planning was revisited based on the acceptance of the SENTINEL platform and feedback we received from end-users. This involved the cooperation between T7.1, T7.2 and T7.3 and is documented in the final business model, market analysis and long-term sustainability report (D7.9). **Linked WP: 7; Owner: AEGIS**		

3. Explanation of the work carried per WP during the 3rd Year

3.1 WP1 – SENTINEL baseline: Setting the methodological scene

Leader: IDIR, Involved Partners: IDIR, ITML, LIST, The SHELL, INTRA, STS, AEGIS, TUC, ACS, CG, TIG, CECL, FP

Duration: M1- M6

The activities of WP1 have been successfully completed in Y1 and already reported in D8.1.

3.2 WP2 – The SENTINEL privacy and personal data protection technologies

Leader: LIST

Involved Partners: LIST, ITML, IDIR, STS, AEGIS, TUC, CECL, FP

Duration: M7- M30

3.2.1 Summary of results achieved during Y3

WP2 is led by LIST and kicked-off in M7. The reference period of this report covers the WP2 activities conducted in the M25-M30 period. All WP2 partners worked intensively towards setting a solid ground for delivering the WP2 outcomes. As part of this work package, Final Product version of self-assessment module for GDPR compliance (i.e., GDPR Compliance Self-Assessment), integrated Identity Management System, and standards-based risk management tool (i.e., MITIGATE) have been released in M30.

The key achievements of WP2 include:

(i) Delivering the Self-Assessment module for GDPR compliance.

(ii) Delivering the integrated Identity Management System.

(iii) Delivering state-of-the-art security- and privacy-enhancing modules to meet individual specific needs of participants.

(iv) Continuous monitoring of various sources in order to meet the core objectives of GDPR and other legal data protection regulations and to steer the project for continuous compliance across every task.

During Y3, two (2) deliverables have been prepared and submitted namely: D2.3 “The SENTINEL privacy & data protection suite for SMEs/MEs: Final Product Version” and D2.4 “Continuous data privacy legislation compliance monitoring and guidelines - final version” (delivered in M30). These deliverables contributed to milestone 5 “Demonstration Fire”, planned in M30.

3.2.2 Key WP2 achievements during Y3 at task level

T2.1 The privacy and data protection compliance framework

Led by LIST, T2.1 aims at developing SENTINEL’s privacy and data protection compliance framework that takes the form of a GDPR compliance self-assessment tool: the GDPR Compliance Self-Assessment (GDPR CSA) module. GDPR CSA is a rules-based engine derived from ISO/IEC 330xx family standard compliant expert-based GDPR compliance assessment approach. GDPR CSA is inspired by an expert-based data protection capabilities assessment approach developed by LIST in accordance with requirements established in ISO 330xx family standards on process assessment. The standard provides requirements for: a) assessment model (ISO/IEC 33004), b) measurement scale (ISO/IEC 33003), and c) Assessment method (ISO/IEC 33002).

During the reference period, a new version of GDPR CSA (aka GDPR CSA final product) has been released. The final product version of GDPR CSA is based on the same architecture developed for Full-Featured version (technological description of GDPR CSA is available in deliverable 5.6). The final release of GDPR CSA introduces a set of improvements to two key functionalities: ASSESS and IMPROVE.

ASSESS functionalities were improved to consider the comments made during the project review. Indeed, reviewers emphasized the importance of clarifying to future users that GDPR CSA assessment results should not be confused with a traditional conformity assessment. It means that even assessment results are good, it does not mean that personal data are handled in conformance with GDPR. To avoid this possible confusion, two actions were taken. The first one concerns the GDPR CSA assessment model. It was confronted with two established GDPR requirements models (GDPR-CARPA certification criteria and ISO/IEC 29100:2011 – Privacy framework) to verify relevance of GDPR CSA assessment criteria, and to identify missing ones. Some of missing requirements were incorporated to the new version of the assessment model. For the requirements that were not integrated, they are now listed in the wiki allowing users to know what is considered by GDPR CSA. The second action taken to avoid confusion with GDPR CSA's results was related to the assessment measurement framework. The evaluation now focuses on the level of accountability, rather than the level of compliance (see D2.3 for more details).

The GDPR CSA final product version brings a major improvement of IMPROVEMENT by integrating OTMs defined in SENTINEL's OTMs taxonomy. The purpose was to link GDPR CSA's recommendations with SENTINEL's OTMs, allowing SMEs/MEs to identify which measures to implement to satisfy a requirement. This mapping allowed to determine that SENTINEL's OTMs did not meet all requirements included in GDPR CSA's assessment model. It was then decided to complete SENTINEL's OTMs taxonomy with new OTMs dedicated to meet specific data protection requirements.

T2.1 has contributed to the following WP2 objective:

(i) Deliver SENTINEL's unified privacy and personal data protection compliance self-assessment framework for GDPR compliance.

The work described above is detailed in D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product", contributing to milestone 5 "Demonstration Fire", due in M30.

T2.2 The integrated Identity Management System: enabling a unified European Personal Data space

T2.2 was led by ITML and started in M7. The main goal of Task 2.2 was to deliver SENTINEL's IdMS that meets the objectives and requirements set by initiatives such as the MyData operator, with special attention to personal data portability and consent management. For the MVP version of IdMS, ITML presented an overview of the desired solution, requirements and constraints, including the detailed examination of the MyData Operator, selection and testing of state-of-the-art security technologies to support the solution, as well as a bottom-up approach to build the initial version of the IdMS, starting from the minimum set of the most fundamental requirements to provide a proof-of-concept demonstrator.

During Y2, for the FFV version, we designed and reported on the expansion and transformation of the IdMS module to a standalone IdMS as a service module that provides the above features as a service. It is based on six main pillars, related to the robust management of EU-wide user access and GDPR compliant data management that is easily available for third-party SMEs.

1. Central, EU-wide, self-service identity management.
2. Credentials and access tokens management that allow Authentications of the entities.
3. Role based access control.
4. Federation with third-party systems.
5. MyData, data management for secure GDPR compliant storage and access of user data.
6. Governance.

During Y3, for the Final Product, a new registration process has been designed while the SENTINEL UI has been updated so the users being capable of exporting their data after registering in the platform. Those improvements are bridging the gap between our data management system the directives of MyData.

T2.2 has contributed to the following WP2 objective:

(i) Deliver SENTINEL's integrated Identity Management System, based on the decentralized MyData model for human-centric personal data management for SMEs/MEs, enabling a unified European Personal Data Space.

The above comprises significant input to D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product", contributing to milestone 5 "Demonstration Fire", submitted in M30.

T2.3 Contributed cybersecurity components

T2.3 was led by FP and started in M7. Since M7, FP designed and presented the first integration scenario of the cybersecurity components contributed from the project's partners. Specifically, this first scenario is based on the MITIGATE platform, which is a standards-based risk management tool, providing a collaborative, evidence-driven risk assessment approach, delving into the technical specificities and security particularities of an organisation's infrastructure, analysing assets' interdependencies, detecting all cyber threats and assets' vulnerabilities, and calculating all cyber risks related to the underlined infrastructure, including potential cascading effects.

The proper realization of this scenario required the implementation of the SENTINEL mitigate-adapter, which successfully offers all required integration services from the MITIGATE system and provides corresponding REST APIs to the SENTINEL internal components to implement the following:

- The SENTINEL cyber-asset definition, which allows the detailed specification of the vendor, the product, and the exact version of a cyber-asset, respecting the SENTINEL asset model.
- The SENTINEL cybersecurity risk assessment, which is available at the *Processing Activity (PA)* level, when at least one SENTINEL cyber-asset assigned has a proper *Common Platform Enumeration (CPE)* identifier and offers a detailed summary of the calculated risks for each abovementioned cyber-asset.
- The SENTINEL simulation environment, which offers a friendly user interface, where the SME/ME representative, using the SENTINEL platform, may set experiments on specific cyber-assets and automatically identify possible attack scenarios and risks.

These are realized through the following functionalities:

- The vendor and product management, which is based on the CPE catalogue of National Institute of Standards and Technology (NIST). The catalogue is parsed for the embedded vendor names and products along with their CPE identifier, name, version, and edition, which are then extracted and assigned with a unique id.
- The vulnerability management, which allows the exact vulnerabilities related to the declared SENTINEL cyber-asset to be automatically inherited, based on the selected CPE identifier and the vulnerability records, that are replicated in the persistence engine from the *National Vulnerability Database (NVD)*.
- The common weaknesses management, which utilizes the *Common Weakness Enumeration (CWE)* [4] specification, allowing the automated identification of relations with specific vulnerabilities, identified on the selected cyber-assets.
- The threat management, which allows the identification of the threat landscape the underlined organisation's IT infrastructure may be exposed to, from the *Common Attack Pattern Enumeration and Classification (CAPEC*) of MITRE[5].

For the final reporting period, FP worked in close collaboration with WP2 partners on designing and implementing the final integration scenario of the cybersecurity components. More specifically, this scenario improves and properly enhances the first one as follows:

- Significantly enrich the current reports of the Cyber-Security Risk Assessment (CSRA) process.
- Optimize the MITIGATE adapter upon which the integration with the MITIGATE tool is based.
- Enhance the information provided for each data-entity (i.e., vulnerability, threat).

All these are realized through the MITIGATE system and help SME/MEs to better realize the nature of their assets' risks as well as what specific actions are available in order to properly mitigate them.

T2.3 has contributed to the following WP2 objective:

(i) Deliver a curated collection of self-serving, state-of-the-art security- and privacy-enhancing modules, both open-source and contributed by consortium partners, which will be selected to meet individual specific needs of participants.

The above provided significant input to D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final Product".

T2.4 Continuous management and integration of open-source technology offerings and solutions

T2.4 was led by TUC and started in M7. Since the start of T2.4, TUC presented a first list of capabilities not currently covered by the SENTINEL modules and how these can be addressed by open-source solutions, also established some minimal requirements for the proposed open-source solutions such as maturity and long-term sustainability. Additionally, created a first version on the type of information provided for each external plugin and training course. After discussion

[4] https://cwe.mitre.org/
[5] https://capec.mitre.org/

with partners, it was decided how the external plugins and training repository will fit in the overall architecture and how the information it contains will be transmitted.

T2.4 has contributed to the following WP2 objective:

(i) Deliver a curated collection of self-serving, state-of-the-art security- and privacy-enhancing modules, both open-source and contributed by consortium partners, which will be selected to meet individual specific needs of participants.

During Y2, the implementation of Task 2.4 produced an enriched list with open-source tools and trainings to be used as external plugins that will be recommended by the SENTINEL platform. These include around 54 tools and 117 training elements, covering a wide range of security/privacy technologies and concepts.

- For the tools, the offered functionality includes compliance self-assessment or privacy policy creation for private data protection legislations (e.g., CCPA, CalOPPA, PIPEDA, UK GDPR, and Australia's Privacy Act), DPIA, data anonymization models, fair and transparent use of personal data, analytics, vulnerability scanners, secure code inspection, IDS/IPS, SIEM, monitoring and incident response, threat intelligence and information sharing, penetration testing and digital forensics, security protection mechanisms (e.g., firewalls, antivirus), secure remote access, identity and access management, password management, disk/data encryption, secure data deletion, data recovery, and backup.
- For the training elements, this involves courses, webinars, articles, talks, and other online training material for various levels of expertise (ranging from beginners to experts). The training topics cover several concepts, such as privacy, security, combination of privacy and security, safety, ethics, as well as the implications from emerging technologies of Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, surveillance systems, and many others. The user can learn from fundamental concepts of privacy and security up to very technical and research aspects. Training for all privacy and security principles (such as confidentiality, integrity, availability, non-repudiation, authentication, authorization, anonymity, pseudo-anonymity, etc.) is offered, as well as technology-oriented perspectives (like network monitoring, system administration, personal cybersecurity, ethical hacking and penetration testing, digital forensics, etc.). Also, there are complete courses that can prepare experts to assert professional certification for the examinations of ISC2 SSCP, CompTIA, and ISACA CISA.

In addition, the external plugins were mapped to the respecting OTMs, which occurred during the technical SENTINEL meetings. The implementation of Task 2.4 was presented as part of the deliverable D2.2 “The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version”, which was submitted in M18.Also, this information was processed by the Recommendation Engine in order to make targeted suggestions to the SENTIENL user.

Within Y3, the two lists were further enhanced based on the project’s needs and the pilot evaluations. More specifically, the following updates have been performed during this period:

- Search for methodologies that assess the security of opensource projects.
- Follow these approaches to evaluate the security of the examined opensource tools and verify that the selected ones are the best in their category.

- Update the SENTINEL Wiki with links to these external tools and training materials.
- Use the field ‘Main OTM covered’ to improve the recommendation process of tools or training materials in comparison to the first versions of the platform where a long list of elements may be suggested to a user, taking equally into account all involved OTMs.
- Check on the links for tools’ tutorials and download sites, as well as the links for the external sources and training materials.

The last version of the lists (tools and training elements) was documented in the final iteration of the task in the Deliverable D2.3 “The SENTINEL privacy & data protection suite for SMEs/MEs: Final product”, due in M30.

T2.5 GDPR and data protection regulations continuous monitoring and guidelines

T2.5 was led by CECL and started in M7. Since the launch of T2.5, the CECL team has been continuously monitoring various sources for developments in the data protection landscape. These include legal and policy developments, opinions issued by the European Data Protection Board (EDPB), national DPAs, literature and publications. As part of its monitoring activities, CECL identified relevant developments, consulted with the Ethics supervisor, and relayed the relevant information to the coordinator and the partners. One development identified was the EDPB board opinion 1/2022, adopted on 1 February 2022, on the requirements for data protection certification criteria, which could be relevant to the SENTINEL branding and communication activities.

Using the same methodology, CECL carried on its monitoring activities in Y2 and Y3 as well which eventually resulted in production of D2.4 and D2.5. The corresponding compliance report codifies relevant opinions of the EDPB and national DPAs, as well as legal and policy developments at the EU level (such as the adoption of the New Standard Contractual Clauses (SCCs) for transfers of personal data from the EU and the European Economic Area (EEA) to third countries). The report emphasises developments relevant to SMEs and MEs and is used to inform the SENTINEL outputs and the content of current and future tasks. Regarding specifically D2.5, additional decisions on SMEs compliance with the GDPR were included. These Decisions were mainly from the Hellenic and Spanish Data Protection Authorities.

T2.5 has contributed to the following WP2 objective:

(i) Monitoring of GDPR and other legal data protection regulations, to steer the project for continuous compliance across every task.

The above provided input D2.4 ‘Continuous data privacy legislation compliance monitoring and guidelines - interim version’ as well as to milestone 3 “Innovation Fire”, due in M18 and D2.5 “Continuous data privacy legislation compliance monitoring and guidelines - final version” which was submitted in M30.

3.2.3 Work carried out in WP2 per partner

ITML	As a task leader of T2.2, ITML participated in relevant meetings discussing the way open-source solutions are incorporated in the SENTINEL platform. During Y3, ITML contributed to the design of My Account page as part of the effort for the IdMS to make one step towards MyData paradigm. This work has been reported in D2.3, for which ITML has provided valuable feedback as an internal reviewer.

LIST	In Y3, as WP2 leader, LIST has organised coordination meetings with work package task leaders. LIST was also the representative of work done in this WP for plenary meetings. LIST ensured coordination with other work packages. In addition, as T2.1 leader, LIST has managed the development and release of GDPR CSA final product version. LIST was also the representative of this task within coordination meetings and activities conducted within WP2. LIST has actively contributed to tasks T2.2, T2.3. LIST was also responsible for Deliverable D2.3.
IDIR	In Y3, IDIR has contributed technical work in T2.1 by collaborating with LIST and other technical partners in the further refinement of the project's domain model for profiling, in direct exchange with T4.3. Since Y3 saw the development and the release of the project's final version in M30, along with the verification and validation activities, this work was primarily focused in the development and enrichment of the OTM classification with GDPR-related OTMs, the introduction and merging of category O6 (Managing GDPR compliance) and the testing and provision of feedback of the GDPRCSA interface.
STS	STS participated in all T2.3 related discussions and meetings aiming at exploring ways of cybersecurity components that can be integrated in the overall solution and how and when these tools can or should be triggered. Additionally, STS played a significant role in deliberations concerning the integration architecture patterns suitable for the cybersecurity components and their associated APIs. Furthermore, STS made valuable contributions to Deliverable 2.2.
AEGIS	AEGIS has contributed to the development of SENTINEL's Data Model and participated in all the relevant discussions and contributed to what was requested in accordance with the instructions provided by the task leaders as well as the WP2 leader. Furthermore, AEGIS developed a sample API to be used by the relevant cybersecurity components and modules to communicate with the front-end. The mentioned modules are integrated within the MySENTINEL UI (see D5.1, D5.2 and D5.3). Finally, AEGIS participated in all WP2-relevant telcos. Finally, during Y3, AEGIS has conducted the internal review for D2.5.
TUC	Within Y3, TUC further updated the contents of the list with the trainings and third-party open-source tools to be offered by the SENTINEL platform, as external plugins. This was driven by the technical progress of the platform (i.e., integration with the Recommendation Engine for better suggestions to the user), as well as the evaluation from the piloting environments regarding the appropriateness of the recommended tools and trainings. Moreover, the SENTINEL Wiki was updated with links to these external tools and training materials in order to provide more explanatory resources to the user for the various terms and technologies that are used under the SENTINEL solution. There was also research concerning the security evaluation of open-source software. All suggested tools are supported by an active community and are considered safe for use, without severe security issues being known. All these activities have been documented under the deliverable D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product".
CECL	The CECL team, being the T2.5 leader, has been continuously monitoring various sources for developments in the data protection landscape. As part of its monitoring activities, CECL identified relevant developments, consulted with the Ethics supervisor, and relayed the relevant information to the coordinator and the partners. Within the M25-M30 project period, CECL carried on its monitoring activities using the same methodology described above and successfully reported monitoring activities in D2.5. The corresponding compliance report codifies relevant opinions of the EDPB and national DPAs, as well as legal and policy developments at the EU level (such as the adoption of the New Standard Contractual Clauses (SCCs) for

	transfers of personal data from the EU and the European Economic Area (EEA) to third countries). The report encompasses additional decisions, whereby fines have been imposed on SMEs for their non-compliance with the GDPR from national DPAs (such as HDPA 50/2022, HDPA 51/2022, HDPA 45/2022, AEPD – PS-00097-2022, AEPD – PS-00310-2022, AEPD – PS-00158-2022, AEPD – PS-00200-2023 etc.) and emphasises developments relevant to SMEs and MEs and is used to inform the SENTINEL outputs and the content of current and future tasks.
FP	During Y3 FP participated in all WP2 meetings for the self-assessment module development. Within these meetings and specifically for T2.3, FP has finalized the proper utilization and integration of the cybersecurity components contributed from the SENTINEL partners. FP continued to participate in all meetings relevant directly or indirectly to T2.5 by discussing how to align all technologies and solutions developed in the context of SENTINEL with the GDPR, and other EU regulations or best practices dedicated to privacy assessment and personal data protection. FP led the process of finalization of the Organization and Technical Measure (OTM) classification, based on which many different SENTINEL components and WPs are built upon. Through this classification our focus was to avoid complicated formal policy and procedures and simplify (as much as possible) our approach to make it approachable, understandable, affordable, and practical for smaller enterprises, selectively adopting, however, world-wide accepted and known standards, frameworks, and best practices. Towards this and in accordance with T2.5, in SENTINEL we were based on the hierarchy of the ISO/IEC 27001:2013 standards and ENISA's risk-based approach to protecting data and we built upon these. Towards this, we defined 175 different OTMs grouped in 10 organization and 10 technical categories. These OTMs are further considered from the SENTINEL privacy and data protection compliance framework (T2.1). Upon successfully delivering the final version of the SENTINEL platform, FP led the proper design and implementation of the final integration scenario, which was realized through the MITIGATE adapter and system. FP reported all this effort in D2.3.

3.2.4 Status of Deliverables and Milestones

The work conducted in WP2 in Y3 contributed to reaching milestone MS5 and is well-documented in deliverables D2.3 and D2.5.

Table 7. Status of WP2 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D2.3	The SENTINEL privacy & data protection suite for SMEs-MEs - final product	LIST	Demonstrator; PU; M30	Submitted
D2.5	Continuous data privacy legislation compliance monitoring & guidelines - final version	CECL	Report, PU, M30	Submitted
MS5	Demonstration Fire	INTRA	M30	Achieved

3.2.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D2.3 and D2.5 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.3 WP3 – The SENTINEL digital core

Leader: ITML

Involved Partners: ITML, IDIR, INTRA, STS, AEGIS, CECL, FP

Duration: M7- M30

3.3.1 Summary of results achieved during Y3

WP3 was led by ITML and started in M7. Since the first demonstration of WP3 activities (MVP delivered in M12) SENTINEL core has been upgraded to its FFV (delivered in M18), after a set of improvements and changes implemented to its comprised modules. The final version of SENTINEL core including the final changes and improvements was delivered in M30.

The key achievements of WP3 in terms of developed technologies, from M25-M30, include:

Open data security platforms as accessed and used by the Observatory: Redesigned the Observatory and its Knowledge Base to include guidelines for the Sentinel user to browse through the platform as well as helpful articles to get familiar with GDPR, PDP and CS concepts.

The incident handling and sharing module: Updates have been applied to SENTINEL UI to improve the user experience on incident reporting and handling functionality.

Recommendation Engine: This module has been implemented to provide recommendations to the users in the form of OTMs, trainings and tools. Within Y3, the recommendation process has been re-engineered with a dynamic rules system allowing the users to be aware of the reasons that they receive specific recommendations, while the rule-based system enables potential implementation of additional rules in the future.

In addition, Policy Drafting, enforcement and orchestration module has been further expanded to include 171 organisational and technical measures including 37 new GDPR measures.

Technical details of each module of the final version are explained in D3.3 “The SENTINEL digital core: Final product” delivered in M30.

3.3.2 Key WP3 achievements during Y3 at task level

T3.1 Access and monitoring of open security data sharing platforms

T3.1 was led by AEGIS and started in M7. AEGIS, as part of the preparatory work, investigated for external open security data sources and presented an outline of the most well-known and widely used to the rest of the consortium. Additionally, functionality of T3.1 and system requirements were identified and discussed with the consortium.

As a result of a series of WP3 meetings since the launch of T3.1, AEGIS alongside the participants of T3.1 examined the external open security data sources presented more thoroughly to select the most relevant sources. Experimenting with concrete data and developing a series of examples was also a part of the procedure described above. As a result of the aforementioned process, we were able to narrow our options down to three alternatives that can be exploited within the scope of T3.1.

After examining the characteristics of the last three alternatives with regard to external open-source threat intelligence and sharing platforms, it has been decided to implement a MISP instance for the MVP and the first complete prototype. This instance consumes open, public sources and feeds to receive updated information on current threats and vulnerabilities. In coordination with T4.4, a decision was made on the data storing technology that can be used for the Observatory Knowledge Base. By combining the two approaches, a base has been set up on which we were able to build SENTINEL's threat intelligence platform, which not only receives data from the community but also shares and gives back all relevant information. Additionally, it includes other open security data sources and platforms, in order to give the end-user a more concrete approach to assess their organization's security. Furthermore, the user is able to submit incidents identified in their own organization, through a form created for this exact purpose.

T3.1 has contributed to the following WP3 objective:

Continuous access and monitoring of open security data sharing platforms that will facilitate (a) the deployment of the SENTINEL knowledge base; and (b) the establishment of a dependable two-way communication channel cross open security platforms and data aggregators for gathering security (e.g., threats) data and the escalation of data and privacy breaches and incidents, as handled by SENTINEL's incident reporting components.

The above comprises significant input to D3.3 “The SENTINEL digital Core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

T3.2 The incident handling and sharing module

T3.2 was led by ITML and started in M7. Within the refinement of the SENTINEL architecture, the participating partners decided that this module should be split into two complementary modules to provide the desired services in an effective way:

a) the Incident Reporting that permits the end-users to submit incidents as they occur during the operations of an SME/ME.
b) the Notification aggregator that continuously monitors an SME/ME's infrastructure, collects and reports on any event that may be a security breach, vulnerability, threat or attack.

In Y3 the incident handling service was further enhanced in terms of improved user interface on the specific services. As in Y2, the report was separated in two (2) use cases:

1. Receiving security notification which discusses the way the various SENTINEL plugins are sending notifications through the plugin adapter and the notification aggregator to the SENTINEL UI (i.e the user) and
2. Reporting security incidents, where the user is given the option to report security incidents observed internally to the organization to open security platforms in order to share knowledge with anybody interested.

T3.2 has contributed to the following WP3 objective:

(i) Deliver the SENTINEL Data Fusion mechanisms for data breach incident handling and sharing.

The above comprises significant input to D3.3 “The SENTINEL digital core: Final product” in M30 and milestone 5 “Demonstration Fire”.

T3.3 The intelligent recommendation engine

T3.3 was led by ITML and started in M7. The intelligent recommendation engine developed in the framework of T3.3 and the main input of the Recommendation engine is the result of the Self-assessment engine that operates on the initial assessment and potential subsequent assessments realized within SENTINEL. Therefore, the inputs and roles of the Recommendation engine were touched upon during discussions related to Self-assessment, while the progress of these discussions were reported during the monthly WP3 meetings. The outputs of the engine are directly consumed by the Policy Drafting module to produce human bespoke policy drafts.

Since M25, hard-coded rules have been replaced with a mechanism that produces recommendations based on a Business Rule Management System. Drools environment provides a rule engine that is responsible for evaluating and executing rules based on data and conditions specified by developers or business requirements providers. The updated recommendation mechanism empowers Sentinel platform by raising the awareness of the users on the reasons behind the recommendations they may receive. This last version of the RE is still highly performant and available (>99% requests satisfied, <3 sec latency), even though the complexity of the rules has significantly increased.

T3.3 has contributed to the following WP3 objective:

(i) Deliver the SENTINEL Intelligent Recommendation Engine.

The above comprises significant input to D3.3 “The SENTINEL digital core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

T3.4 Policy drafting, enforcement and orchestration module

T3.4 was led by FP and started in M7. The purpose of the Policy drafting module was to convert the list of tools provided by the recommendation engine into a meaningful, structured, and enforceable policy draft. The output policy draft is enriched with organization measures to be taken, specific enforceable and actionable security policies and policy data patterns that are provided by both the Policies repository and the Observatory of the SENTINEL architecture.

As a leader of the task, FP has provided the challenges that have to be considered and some first action points concerning the identification of the SENTINEL policy drafting module (i.e., brainstorm on its basic content and operations, the SME’s/ME’s monitoring upon policy enforcement, orchestration mechanisms) and recognized interrelations (i.e. inputs/outputs) with other modules of the SENTINEL Digital Core. Based on this, this task designed and released the SENTINEL template policy model, which is based on various sections:

- Section 1: **Policy details**, which consists of the metadata of the SENTINEL policy (i.e. generation date and time of policy).
- Section 2: **Organization Info**, which includes the most important organization profile details (i.e. name, sector, size, etc.).

- Section 3: **Global Recommendations**, which reports the recommendations that concern the whole organization regardless of the information provided in each one of the Pas.
- Section 4: **PA specific Recommendations**, which reports the recommendations for each completed PA.

Section 3 and 4 consist of the following:

- The *Organizational and Technical Measures (OTMs)* classification upon which the policies are constructed to guide the SME's/ME's through meeting the data protection requirements according to their risk appetite, relevant EU and international guidelines, good practices and approaches are investigated (i.e., ENISA risk-based approach and guidelines for personal data processing, NIST Privacy Framework, Cyberwatching GDPR Risk Temperature approach).
- The implementation status of each recommended OTM.
- The list of recommended software / tools for addressing each recommended policy / measure.
- The list of recommended training materials that are relevant or may help the SME/ME properly address each recommended policy / measure.

Based on these, the RASE score of the assessment process and the recommendations of the RE and the policy draft module are eventually building the required human readable policy that are published at the MySENTINEL context.

The final version (full featured version) of the SENTINEL platform reports on 96 organization and 79 technical (175 total) measures, further analysing these recommendations while considering the following factors:

- The risk level of the organization.
- The ownership of the assets (as registered in the organization profile).
- The locality of the assets (as registered in the organization profile).

Therefore, for each proposed organization and technical category, SENTINEL performs the following:

- Considers the calculated risk level of the organization and gathers all available measures that need to be recommended to the SME/ME.
- Filters the list of available measures based on the ownership of organization assets.
- Considers the locality of the organization assets recommending the proper policy text for each case.

In the last reporting period effort was spent on the proper enhancement of the OTMs included in the "Managing GDPR Compliance" organization category. This category counts 31 measures in low risk level, 8 in medium risk level, and 7 in high risk level. In parallel all existing measures and specifically the recommended policy text was properly tuned in order to properly consider the different options of assets' ownership and assets' locality.

The above comprises significant input to D3.3 "The SENTINEL digital core: Final Product", delivered in M30.

3.3.3 Work carried out in WP3 per partner

ITML	As WP3 leader, ITML continued coordinating the discussions for the selection of external open data security platforms and participated in testing the suggested sources. Considering the close relationship between T3.3 and T3.4, in Y3, ITML has continued its active participation in the design and deployment of the Policy Drafting module and its dependency to the Recommendation Engine, as well as interfacing of those components within the context of the Final product (M30). Finally, ITML has also led the delivery of D3.3, contributing key content for all sections.
IDIR	In Y3, IDIR has finalised their contributions to both T3.3 and T3.4, ahead of SENTINEL's final release and piloting activities (M30). In T3.3, Y3 work has been about testing the fully functional rule-base engine and, specifically, validating how risk-based OTM selection works, along with custom admin-defined rules. In T3.4, Y3 work has finalised the mapping between OTMs and policy templates. This mapping, for which FP has led the work, has been recorded as SENTINEL's global classification sheet, which, in the technical architecture, resides in the Common Repository. IDIR has (a) helped enrich this classification with OTMs, additional metadata (columns), selection rules and other data.
INTRA	In Y3, INTRA has actively participated and contributed to all WP3 discussions. INTRA contributed to the specification of the rule-based recommendation engine as well as the elicitation, specification and refinement of the rule set. Moreover, it contributed to the definition of risk levels with regards to the Organizational and Technical Measures as well as the incorporation of new OTMs regarding Personal Data Protection that pertain to the O6 category.
STS	In Y3, STS has actively participated and contributed to all WP3 discussions. In particular, the final version of DPIA was delivered and fully integrated within the SENTINEL platform. Additionally, STS has contributed to D3.3.
AEGIS	During Y3, AEGIS continued to work on and maintain the implementation of MISP on the SENTINEL platform, by updating the external open security data sources and redesigning and updating the form that the user can use to contribute relevant information back to the community. This effort has been reported in D3.3.
CECL	In Y3, CECL has continued to participate in all WP3 related meetings and discussions taken, especially the ones focusing on T3.4 concerning the policy drafting module.
FP	During this last project year, FP participated in all scheduled meetings and calls related to WP3 as well as to meetings and activities related to the proper design and implementation of the SENTINEL platform and its components. FP contributed to the design of the Data Fusion Bus which is required to allow a trustworthy way of transferring data between the SENTINEL internal and external components. FP also participated in the finalization of the rules required to be implemented from the intelligent recommendation engine where critical decision support capabilities take place. FP has also investigated relevant EU and international guidelines, good practices and approaches (i.e., ENISA risk-based approach and guidelines for personal data processing, NIST Privacy Framework, Cyberwatching GDPR Risk Temperature approach). A series of organizational and technical measures (OTMs) were defined based on ENISA's structured framework for assessing information security requirements for protecting privacy and personal data using a risk- based approach. These OTMs are recorded and mapped either to the organization profile of the SME/ME and the processing activities and are used at the building process of the human readable policy. FP reported these efforts in D3.3.

3.3.4 Status of Deliverables and Milestones

The work conducted in WP3 in Y3 contributed to reaching milestone MS5 and is well-documented in deliverable D3.3.

Table 8. Status of WP3 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D3.3	The SENTINEL digital core: Final product	ITML	Demonstrator; PU; M30	Submitted
MS5	Demonstration Fire	INTRA	M30	Achieved

3.3.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D3.3 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.4 WP4 – The SENTINEL services

Leader: ACS

Involved Partners: ACS, ITML, LIST, IDIR, INTRA, STS, AEGIS, FP

Duration: M7- M30

3.4.1 Summary of results achieved during Y3

WP4 was led by ACS and started in M7 with a kick-off meeting to present the WP4 and the different tasks followed by monthly WP4 meetings to regularly report the work done within the work package.

In Y2, the key achievements of WP4 include:

- The design and implementation of SENTINEL's FFV of self-assessment services.
- The establishment of a stable shared data model for the SME Profile Service focusing on both PDP aspects (PAs and ROPA) and organization aspects. This data model is common among core SENTINEL modules as well as plugins.
- Simulations and training for SMEs/MEs, integration of ACS's CyberRange platform and new gaming interface in the SENTINEL environment.
- Technical effort towards the development of the expanded SENTINEL Observatory and knowledge base, including external data sources, data formats, storage technologies and user-facing collaborative tools.

Overall, the work leading up to Y2 has enabled all partners to better understand user journeys, clarify roles and responsibilities, successfully release the SENTINEL FFV and bring the project closer to a feasible end-to-end technical solution.

In Y3, based on the feedback received from the SENTINEL FFV version further work have been done to update and create more user-friendly experience to the SME. Update have been made to the CyberRange gaming interface, and a Wiki was created for the new SENTINEL users to help them in the first step on the SENTINEL platform. Final version of the questionnaire for the DPIA was completed and testing, and the profile service was adapted to fulfil the requirement for the Final Product.

Final contribution has been reported in D4.3 “The SENTINEL services: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

3.4.2 Key achievements during Y3 at task level

T4.1 Advanced CyberRange simulations and training for SMEs/MEs

T4.1 was led by ACS and started in M7. This task is responsible for integrating and delivering the advanced, fully featured and scalable CyberRange platform. Aiming at providing an educational, collaborative platform for simulating real-life cybersecurity scenarios, user accounts for the SENTINEL partners have been created on the CyberRange platform, and a presentation of the capability of the platform has been made. A meeting with SMEs to present the CyberRange and involve them in the development process has also taken place. Technical aspects regarding development and implementation of simulation scenarios have been discussed among all involved partners. Furthermore, discussions on how to integrate the CyberRange testbed within SENTINEL have been initiated. Multiple possibilities have been discussed aiming to offer the best user experience for the SMEs. As a result, to comply with the SENTINEL project scope, a solution-based on OpenID Connect was selected as a rational option with the authentication process from the SENTINEL user to the CyberRange platform. On the CyberRange, generic infrastructure of SME has been created, in order to replicate the way most SMEs operate nowadays. Scenarios have been created with Cyber-attack to exploit vulnerabilities, and misconfiguration.

The above comprises significant input to D4.2 “The SENTINEL Services: Full-featured version”, delivered in M18, contributing also to milestone 3 “Innovation Fire”, due in M18.

In Y2, a simplified version of CyberRange has been decided to be developed to be used by non-IT experts. For this reason, by keeping the core CyberRange functionalities for IT experts, we have developed a new way to interact with the CyberRange via a new Gaming Interface. The new Gaming interface provides a novel training approach based on the CyberRange to raise awareness of end users. In such a manner, the users can learn in an interactive way the best practice to better protect personal and sensitive data. Four (4) scenarios that demonstrate mechanisms of protection for at least eight (8) threats related to data storage and accessibility have been created to raise awareness of the SME. The covered cyber threats are phishing, malware attack, unsafely removed files, unencrypted disk files, social media presence, password guessing, password reused, and unprotected password. The integration of the Gaming Interface in the SENTINEL platform has been made with OpenID solution. The SENTINEL users can directly be connected to the gaming interface from the SENTINEL platform.

In Y3 based on the feedback received from the SME end users, improvement have been realised. A new version, of the Gaming interface was released to offer a more smoothly user experience. The gaming session is now automatically created, and accessible from the SENTINEL platform, without the need of external assistance. End users are able to start their session when they want, do the training and fulfilled the gaming objectives for cyber awareness as they wish. The immersive scenarios have been updated, and are based on the most common attack vector, threats and attacks to data storage and accessibly that the SME environment and employees are facing.

T4.1 has contributed to the following WP4 objective:

(i) Design and deliver the SENTINEL cyber range testbeds for simulations and training.

All the above-mentioned activities have been described in D4.3 “The SENTINEL services: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

T4.2 Data protection impact assessment and assurance

T4.2 was led by STS and started in M7. Since M7, there have been regular weekly meetings that STS has chaired during this period and significant progress has been achieved in the design of the Self-Assessment overall solution and related components. One of the key achievements within this task, was the first version of the Organization Profile model, also known as the “SME Profile”. The creation of the Organization Profile is the core process of the Self-Assessment service, which is enhanced by the results of the two core SA tools, namely the GDPR CSA and the DPIA. It has been agreed amongst the involved partners that regarding the SENTINEL’s MVP, the self-assessment process will be GDPR (PDP)-driven.

The first step of the self-assessment is the creation of the organization profile by the SME/ME, during which information is provided on the processing activities. A series of specific questions are asked, and organizational and technical measures (OTMs) are mapped. Based on the answers provided the processing activity is marked as potentially high risk and the relevant SA tool is triggered.

SENTINEL’s DPIA Toolkit is responsible for constructing the DPIA questionnaire and subsequently, calculating the risk based on the responses to it. The questionnaire includes 19 questions, where each question can have one or more (1..*) options. Each option has a specified impact and likelihood. After a SENTINEL end-user submits the questionnaire, the DPIA Toolkit is responsible to calculate the risk (based on the likelihood and impact of the selected options per question), as well as provide some qualitative, and quantitative metadata.

In terms of delivery, STS was closely collaborating with the rest of the technical partners, attending weekly technical physical meetings on top of the regular planned calls to reach a satisfactory design of DPIA toolkit. The aim was to allow SMEs to identify and minimise the data protection risks of one or more processes involved within a project.

As a result, the MVP version of the DPIA was released (M12), consisting of two main components, (a) the DPIA toolkit, and (b) the DPIA database. The former is responsible to generate the DPIA questionnaire, get the DPIA response, and calculate the risk, while the latter stores the questionnaire, and the results of the DPIA process.

During M13-M18 the FFV of the DPIA toolkit was delivered, which has an enhanced algorithm, taking into consideration the OTMs that have been implemented for the specific PA that it is executed. The input of the data that DPIA is processing has changed. Instead of receiving a set of Q&As it is now parsing through the full set of data collected for a specific Processing Activity. It has also better integration with the SENTINEL platform utilising a unified stable shared data model across the core SENTINEL modules and plugins. The DPIA toolkit codebase was re-engineered to adapt to the updated domain model and is now harmonized with ROPA, GDPRCSA and CSRA.

Throughout the period between M7-M30 STS has been chairing a series of weekly MVP/FFV Technical Meetings which all the technical partners were attending and were reporting on the progress of their activities. For the smooth delivery and planning of the MVP, FFV and the final version of SENTINEL, an agile-based approach is being followed. Overall, this approach has been proven to be very helpful as it is very clear which partners are working on what tasks and their dependencies. Their progress is easy to track, sharing comments, files and having a history on every task (GitHub issue). A Slack channel was utilized in parallel for a more immediate communication among technical partners.

T4.2 has contributed to the following WP4 objective:

(i) Design and deliver the SENTINEL data protection impact assessment (DPIA) framework.

In Y3 STS improved the functionality and accuracy of the DPIA toolkit results by reintroducing a questionnaire, which was based on the NOREA Guiding Principles[6].

T4.3 Self-assessment and RASE scoring engine

T4.3 was led by IDIR. To provide some background for the work carried out during Y3, this task was concerned with designing and implementing SENTINEL's **profiling and self-assessment services**, based on tailored requirements. The core process of this context has been labelled 'SME profiling' which, in turn, drives the Initial Assessment, a recording and evaluation of the data recording during this profiling. In summary, the profile stores (a) the minimum amount of data required for the initial assessment such as structure, sector, and operating environment; (b) the personal data processing activities (PAs) according to the GDPR principles and (c) infrastructure, cyber assets, goals, capabilities, and constraints of the organization. It has been established during Y1 that the self-assessment process will be GDPR (data protection)-driven, with organizational and operational details gathered per processing activity, in a way that is consistent with the legal and technical definition of a GDPR-compliant Record of Processing Activities. SMEs will be able to demonstrate additional GDPR compliance by using a SENTINEL-powered permanent, immutable and auditable record of the PAs, *the ROPA*. Additional cybersecurity-specific assessment capabilities were added during Y2 (M13-M24), in the form of the cyber asset inventory (implemented in the Profile) which provides the necessary data, grouped in PAs, for the MITIGATE-based cybersecurity risk assessment (CSRA). A series of organizational and technical measures (OTMs) were also recorded and mapped to PAs, in Y2, which the Self-Assessment Engine considers along with several privacy risk criteria against each process to establish a basic risk assessment which is then passed on to the Core context for recommendations and policy drafting. The Profile now (a) considers a number of non-GDPR criteria such as cybersecurity assets and other requirements, and (b) stores the results of the SA-tools (self-assessment plugins), namely:

- the GDPR Compliance Self-Assessment (GDPRCSA), which may be triggered by any SME processing personal data.

[6] https://www.norea.nl/uploads/bfile/a344c98a-e334-4cf8-87c4-1b45da3d9bc1

- the Data Protection Impact Self-Assessment (DPIA), which will be triggered when at least one processing activities is flagged as 'potentially high-risk' based on the evaluation of the aforementioned privacy risk criteria and
- the Cybersecurity Risk Assessment (CSRA), which may be run at will for any processing activity with at least one (1) cyber asset assigned to it, from the inventory.

Y3 achievements related to this task and leading up to M30 have been:

- The finalisation of the domain model for the SME profile (shared data structures), focusing on both data protection aspects (PAs and ROPA) and organization aspects (such as organisation attributes and cyber asset inventory). This data model is common among core SENTINEL modules as well as plugins (Figure 1). The final (Y3) domain model is theoretically grounded on a number of flowcharts and sequence diagrams which illustrate the user flow and data exchange among different Self-Assessment context modules and participants. It has been agreed that the self-assessment context will utilize an API-first approach and not encourage deploying separate UIs for the different contexts or plugins.
- Final updates to the UI mockups, which drive front-end development, including the platform's UI/UX-optimized dashboard and a number of other aspects such as accompanying risk score calculations and recommendations with reasons for the sake of explainability and transparency.
- The finalisation of the theoretical conceptual model, defining the "universe of discourse" for organization profiling, for CS and PDP which will inform the aforementioned data model and provide the basis for tailored requirements elicitation and analysis (Figure 2). This model is based on the fine-tuning of work conducted during Y2 and accommodates any SENTINEL tool and for any SME scenario. It also supports the possibility of deploying the notion of patterns, together with a template for production rules to utilize instances of patterns, a work which had been proposed as early as Y1.
- The completion and final deployment (M25-M30) of the two key technical components of the SENTINEL architecture associated with T4.3:
  - ○ The Profile Service
  - ○ The Self-Assessment (SA) Service

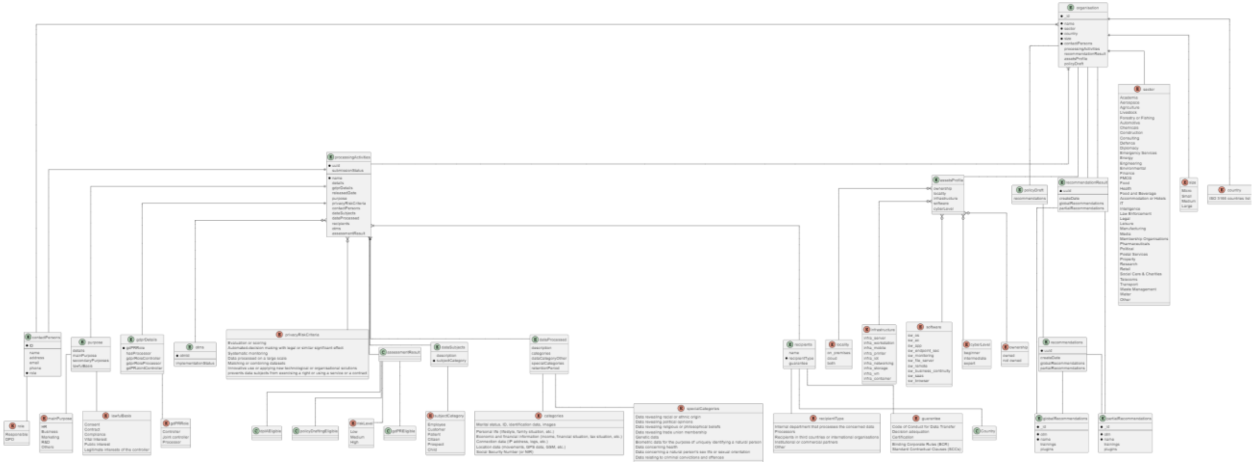

Figure 1. Updated common SENTINEL Organization Profile data model

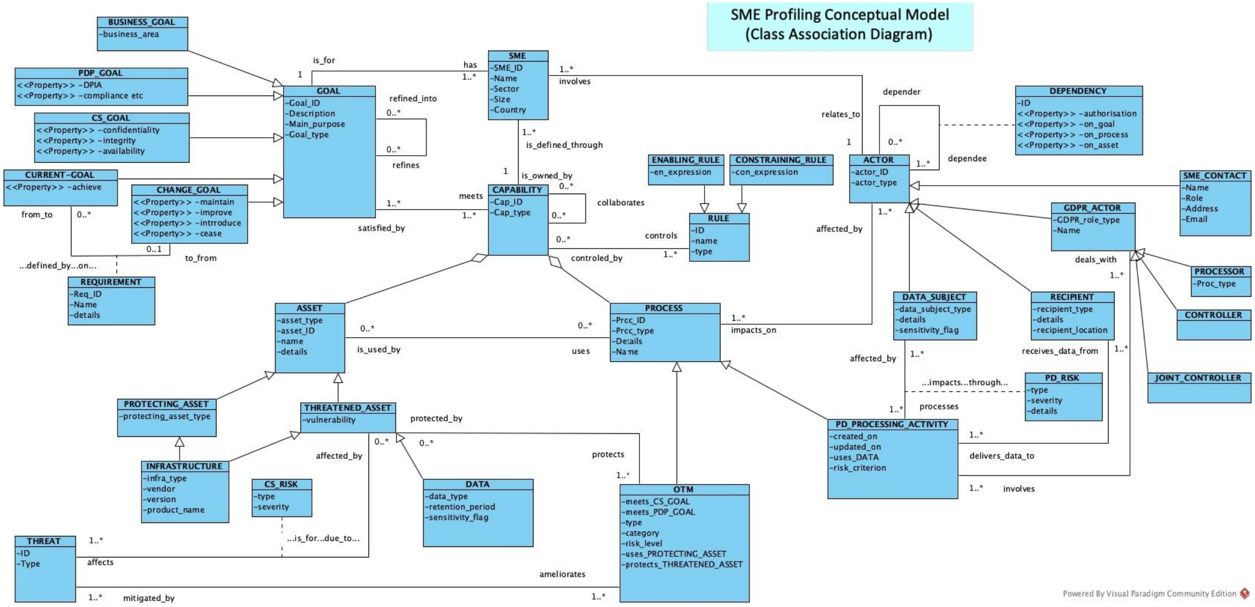

Figure 2. The conceptual metamodel for SME profiling

T4.3 has contributed to the following WP4 objective:

(i) Design and deliver thorough, tailor-made and intelligent requirements analyses, followed by the design and deployment of the necessary training sessions and a smart self-scoring mechanism (risk assessment for small enterprises – RASE).

Overall, T4.3 work during Y3 has provided key input to deliverable D4.3 "The SENTINEL services: Final version" (M30). It has also contributed to Milestone 5 "Demonstration Fire", delivered in M30.

T4.4 The SENTINEL Observatory

T4.4 was led by ITML and started in M7. After delivering the MVP version of the observatory, ITML led the efforts for the FFV reported in D4.2. During Y2 additional external sources identified in T3.1 were integrated (i.e CONCORDIA MISP) as well as capabilities for automatic feed update. Most importantly it reports on the development of the observatory service, which in essence is an API that includes 3 endpoints:

- Endpoint 1: Allows to GET events from the Observatory Information Exchange.
- Endpoint 2: Ingests data from the Observatory Information Exchange (MISP instance) to the Observatory Knowledgebase (Elasticsearch instance).
- Endpoint 3: Adds events to Observatory Information Exchange (related to incident reporting).

In Y3, the main updates include the redesign and expansion of the Observatory Knowledge base from the user perspective. A wiki page that provides access platform guidelines and educational material has been integrated in the system.

T4.4 has contributed to the following WP4 objective:

(i) Design and deliver the SENTINEL Observatory and knowledge base.

The final version of the Observatory was included in D4.3 “The SENTINEL services: Final product” due in M30.

3.4.3 Work carried out in WP4 per partner

ITML	In Y3, as T4.4 leader, ITML has initiated and coordinated the discussions for the implementation of the Observatory as part of Final Product of the platform, including selection of external data sources, data formats/structure, storage technologies, collaborative tools and UI issues. The implementation and demonstration of the Observatory has been successfully executed while the achieved results have been thoroughly reported in deliverable D4.3.
LIST	In Y3, LIST has extended SENTINEL’s OTMs taxonomy by defining and integrating organisational and technical measures that are specific to compliance with GDPR.
IDIR	In Y3, IDIR, as T4.3 leader, has contributed technical work towards finalizing SENTINEL’s Profiling and Self-Assessment modules, along with the leaders of T4.2 and T2.1 which are the key participants. Key contributions towards this end have been (a) participating in key meetings and decisions towards the technical direction of the respective tasks (b) defining and refining a shared data model for the SME profile and the GDPR-compliant ROPA, which is common among core SENTINEL context and modules as well as plugins; (c) proposing a feasible SME profiling and initial assessment process requirements; (d) collaborating towards establishing the appropriate user flow and sequencing among context modules; (e) clarifying organizational and technical measures (OTMs) structure and role and (f) defining the data exchange (inputs and outputs) between the participating self-assessment plugins, namely the GDPR Compliance Self-Assessment (T2.1) and the Data Protection Impact Self-Assessment (T4.2), as well as between SENTINEL’s SA context and the Core context. In M25-M30, technical work and refinements were provided by IDIR to T4.3, related to (a) the finalisation of the ROPA (Profile Service), (b) the finalisation of the detailed cyber asset inventory as a prerequisite for the cybersecurity risk assessment (CSRA) (Profile Service), (c) the finalisation of the algorithm which assigns a preliminary risk level to both the Pas and the organisation as a whole, every time a PA is saved, by examining specific risk criteria (Self-Assessment Engine), and (d) the unification of the SME profile with the GRPDCSA and DPIA inputs (Profile Service), all towards the final version of the platform. In the last months (M28-M30) the work intensified to keep up with the feedback received from the verification and validation (piloting) activities running in parallel in WP6. Furthermore, T4.3 oversaw the finalisation of the mockups riving front-end development and the design, population and deployment of the user help and documentation aspects of the platform which were released as the *SENTINEL Wiki*, and, specifically the Introduction, Getting Started Guide, Glossary, OTM and rules listings, and a page-by-page help and support wizard guiding users along each workflow with screenshots and descriptive text. Finally, IDIR has conducted the internal review of D4.3.
INTRA	Within Y3, INTRA actively participated actively participated in all WP4 discussions contributed to the formulation of the Observatory use case, and the new Observatory Knowledge Base. INTRA also contributed content into the SENTINEL wiki that covers the general domain-specific terminology used by the platform as well as documentation and instructions to help the user complete the company profile efficiently.
STS	STS, as a T4.2 leader, has managed and coordinated the work among the technical partners through which the overall SENTINEL solution has technically matured. STS worked closely with the technical partners that are responsible to provide deliverables

	related to the Self-Assessment tools, the GDPR and the DPIA to design the integration of these tools within the SENTINEL platform following an API-driven approach. In this respect, STS delivered the MVP version of the DPIA toolkit. STS, was actively involved in all the MVP and FFV related discussions, has been chairing the MVP/FFV Technical weekly calls, managing the Agile based approach, coordinating with the rest of the technical partners. Actively contributed to the design of the APIs that would be provided by the self-assessment plugins, GDPR and DPIA, so that they can easily be consumed by the front end through the orchestrator module. Finally, STS has contributed to D4.1 (Section 3) as well as led the production of D4.2. In Y3, STS continued leading the relevant technical discussions with the aim of sustaining the positive momentum achieved during the first 2 years of the project and further advance the maturity of the SENTINEL platform. Finally, STS provided contributions to D4.3.
AEGIS	AEGIS participated in related discussion, and meetings and contributed to what was requested by the task leaders as well as by the WP leader. Additionally, as part of the T4.4, AEGIS collaborated with the partners involved in T3.1 to decide on the technology that is used to store all data from the MISP TIP. Moreover, in the same context, AEGIS performed maintenance on the communication channel between the Observatory Information Exchange module and the Observatory Knowledge Base (KB) and maintained the integration of MISP with the Observatory KB.
ACS	As a leader of WP4, ACS led the monthly meetings of this work package. As part of T4.1, ACS made the CyberRange platform available for the SENTINEL users by creating user accounts on the CyberRange testbed. Following this ACS presented the CyberRange platform to the SENTINEL partners. Several meetings took place with SME end users to show the CyberRange capabilities and try to involve them in the process to create relevant content adapted to their needs. ACS led and participated in discussions on how to integrate the CyberRange in the SENTINEL environment. For the CyberRange a solution-based on OpenID Connect was selected for the interconnection with the SENTINEL platform. Finally, generic SME infrastructure has been created on the CyberRange, with scenarios including cyber-attack to exploit vulnerabilities and misconfiguration. In Y2, the gaming interface has been adapted and integrated with the SENTINEL platform with OpenID connection. Four (4) complete scenarios have been created for at least eight (8) threat related to data storage and accessibility design to raise awareness of the SME. Development has been made to provide better user experience for SME's. Finally, in Y2 the gaming interface was successfully presented to the SENTINEL partners and end users. In Y3, based on the feedback received from the SME end users, improvement have been realised. A new version, of the Gaming interface was released to offer a more smoothly and immersive user experience.

FP	In this last reporting period, FP participated in all scheduled meetings and calls related to WP4 and led many of the processes required to be implemented in all main components of the SENTINEL platform. Specifically, FP actively participated in the finalization of the SME profiling process, which consists of the data required for performing the initial assessment, the data processing activities, and the proper definition of the organization assets in which the MITIGATE system participates through the mitigate-adapter. Effort was spent on the introduction of the SENTINEL OTM classification with their selection criteria when generating the SENTINEL policy recommendations. For each OTM a list of optional capabilities was mapped, upon which all plugins and training material were also mapped. This mapping allows the Recommendation Engine to generate the proper recommendations for each SME/ME, mainly based on the risk level of the organization. Furthermore, the tasks of this WP contribute to the proper utilization of the SENTINEL plugins (tasks T2.3 and T2.4 in which FP leads and participates correspondingly) since many of these require the list of processing activities and the list of the organizational assets.

3.4.4 Status of Deliverables and Milestones

The work conducted in WP4 contributed to reaching milestone MS5 and is well-documented in deliverable D4.3.

Table 9. Status of WP4 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D4.3	The SENTINEL services: Final product	ACS	Demonstrator; PU; M30	Submitted
MS5	Demonstration Fire	INTRA	M30	Achieved

3.4.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D4.3 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.5 WP5 – SENTINEL continuous integration and system validation

Leader: INTRA

Involved Partners: INTRA, ITML, LIST, IDIR, STS, AEGIS, TUC, ACS, UNINOVA, CG, TIG, CECL, FP

Duration: M9- M36

3.5.1 Summary of results achieved during Y3

WP5 was led by INTRA. It started in M9 with two tasks i.e., T5.1 and T5.2, dealing with the SENTINEL front-end components and the overall system integration respectively. Both tasks were completed on time in M30, leaving the floor to T5.3 that was carried out in the last six months of the project.

WP5 that includes system integration (as part of T5.2) as well as the development of the UI (as part of T5.1) has been instrumental in driving enhancements across all releases of the platform, including the latest and final iteration. Building on concrete foundations and with the platform fully integrated, WP5 continued to support its evolution and accommodate advanced features, bug fixes and adjustments dictated by the feedback received from the validation and verification activities of WP6. In particular, after the delivery of the FFV, WP5 continued supporting the evolution of the platform in order to accommodate new features to cater for the reviewers' comments and the feedback being received by the SENTINEL, which are both to be developed in conjunction with other features, fixes and adjustments planned for the final release. The two main goals of the final release are to improve the user experience and make the platform more approachable to the stakeholders and to increase transparency of the policy drafting process by introducing explainability into the recommendations. To that end, WP5 continues to operate in an agile manner, organizing meetings and prioritizing tasks as necessary and further improves the automations in deployment and testing to facilitate incorporation of new functionalities both in the front-end and the back-end.

In that context, significant efforts were directed towards enhancing user experience and streamlining the platform's functionality. These improvements focused on three main areas: the introduction of a user-friendly Dashboard offering summaries of organizational processing activities, ROPA status, module assessments, and recommendations; the provision of pre-filled templates for Processing Activities to simplify profile completion for users unfamiliar with technical terms; and the incorporation of extensive contextual help features including an introductory page, a glossary, and contextual help within each SENTINEL screen.

Another major aspect of improvement revolved around refining recommendation mechanisms and policy items for users. This involved refining the collection of Organisational and Technical Measures (OTMs) to provide better coverage of Personal Data Protection aspects, evolving the Recommendation Engine (RE) into a flexible mechanism supported by a Business Rule Management System (BRMS), and integrating additional recommendation types from plugins, such as those enhancing GDPR compliance and cyber threat mitigation strategies.

Furthermore, this version of SENTINEL introduced various other enhancements, including a redesigned Observatory and Knowledge Base accessible through contextual help menus, a more intuitive user registration and organization creation process, and technical enhancements aimed at ensuring platform sustainability and security. These technical improvements encompassed refactoring domain classes, redesigning APIs and message queues, implementing security enhancements, and maintaining up-to-date documentation while ensuring compliance with Web Content Accessibility Guidelines.

Development towards the final version, in a similar fashion to the previous ones, was done in an iterative and agile manner. All the work items were captured as issues on GitHub and responsible partners were defined. The issues were then divided into bi-weekly development sprints, reserving one sprint before the deadline of each respective release as a backup. Sprints were monitored on a weekly basis in dedicated meetings that combined review and planning activities. Moreover, shorter and more concise low-level meetings (similar to daily Scrum) were carried out three times per week (Monday, Wednesday and Friday) in the final month before the final release (November 2023).

The aforementioned actions, together with the commitment of all technical partners resulted in the timely development and deployment of the final version of all SENTINEL modules, supported by the MySENTINEL UI in M30. The results of T5.1 and T5.2 are reported in D5.3 and D5.6, respectively which contribute to milestone 5 “Demonstration Fire”, due M30, while the results of T5.3 were reported in D5.7, contributing to milestone 6 “Consolidation” due M36.

3.5.2 Key WP5 achievements during Y3 at task level

T5.1 Interactive visualizations and front-end components

T5.1 was led by AEGIS and started in M9. An early planning for the task activities was presented early in the project. As part of the preparatory work for the task, AEGIS also presented a series of early mockups to initiate discussions and brainstorming with reference to the front-end components and visualization of the SENTINEL solution from the end-user perspective. Several remote meetings took place where updated versions for the mockups were presented to the consortium alongside an initial version for the User Journey. At the MVP stage, the MySENTINEL dashboard included links to components that were incorporated in the MVP, as well as the relevant pages. Organization Profile, Processing Activities, Contact Persons, Assets, Self-Assessment tools, Policy Recommendations and a Threat Intelligence platform comprise the modules offered to the end-user by the SENTINEL platform. D5.1 presents more details about the technical development of the MySENTINEL dashboard in the MVP phase.

Moving forward, the MySENTINEL dashboard included links to components and modules that were incorporated in the first complete prototype, as well as the relevant pages. This means that apart from the MySENTINEL dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts were also included in FFV of the platform. Additionally, several elements of the MySENTINEL UI in several different pages were updated and a number of bugs/glitches identified by the technical team and/or the end-users have been fixed. Furthermore, the UI was integrated fully with the backend modules. Moreover, the Cyber Range Gaming Interface, offered by ACS, was integrated into the platform.

At the last stage, work continued to be comprehensive to refine and enrich the content of the UI by constantly engaging and closely collaborating with the project’s end-users with diverse backgrounds (under WP6). We made sure to continue incorporating their feedback and implement a UI that offers high levels of usefulness and usability. Additionally, we made all adaptations required in the communication of the UI with all modules as their development progressed. All this effort resulted in the final version of the MySENTINEL UI dashboard and was documented in the subsequent iteration of D5.1 and D5.2, namely D5.3.

T5.1 has contributed to the following WP5 objective:

(i) Ensuring the seamless integration of SENTINEL components into a unified toolkit, usable by SMEs/MEs.

The above comprises significant input to D5.2 “The SENTINEL visualisation and UI component – second version”, delivered in M18 contributing also to milestone 3 “Innovation Fire” due in M18. Major contributions were provided in D5.3 “The SENTINEL visualisation and UI component – final version”, contributing to milestone 5 “Demonstration Fire”, both due in M30.

T5.2 Continuous integration towards the realization of a complete system

T5.2 was led by INTRA and started in M9. Within this task, a GitHub organization (https://github.com/SENTINEL-EU/) and 22 subsequent repositories were set up to cater for code hosting and versioning, as well as 6 dedicated projects to facilitate tracking of action items and bugs towards all three platform releases of M12, M18 and M30 respectively. In terms of deployment, all modules are being delivered in a dockerised manner and automatically deployed on INTRA's infrastructure using docker-compose on two deployment environments to cater for development and staging purposes. A docker registry server (JFrog artifactory) has also been deployed to facilitate delivery, storage and deployment of docker images. Corresponding Jenkins pipelines have also been created in order to automate the release process.

The tools and processes put into place have proved to be rather efficient and included retrospective sessions after each release where feedback on the development process was provided by software engineers and managers. This resulted in the collection of technical debt and pending issues that needed to be tackled as well as various organizational aspects of the integration process such as the frequency and focus of recurring meetings. Moreover, the feedback of the reviewers as well as the technical partners of the consortium has been incorporated into the backlog of the product, and the work has been broken down in sprints as with previous releases.

T5.2 has contributed to the following WP5 objectives:

(i) Ensuring the seamless integration of SENTINEL components into a unified toolkit, usable by SMEs/MEs.
(ii) Continuously optimizing the SENTINEL platform through an iterative process (testing-improvement-testing).
(iii) Supporting the project's sustainability by putting into place automations and monitoring mechanisms.

The above comprises significant input to D5.6 "The SENTINEL integrated solution – final version", delivered in M30 contributing also to milestone 5 "Demonstration Fire" of the project.

T5.3 From the prototype to the final solution

This task was led by UNINOVA and started in M31 according to the GA. The main objective of this task was to develop and describe the end-user guide to best practices for maintaining and operating SENTINEL platform in the long-term. Within this respect, the user guide was divided into the following main areas:

- Internal testing procedure, with the objective to describe the methodology used for the internal testing procedure, also include an analysis of different "bugs" found during the SENTINEL validation and verification of third-party end-users.
- Scalability, accessibility and evolving user requirement, focusing on the technical aspects of SENTINEL which need to be addressed in the face of potential market adoption and scaling up of the system. These aspects primarily address scalability, accessibility and addressing evolving business requirements.
- Legal, Ethical and Operational dimension of SENTINEL platform,
- SENTINEL user manual, focusing on providing a description of SENTINEL wiki.

With the conclusion of Task 5.3, the comprehensive testing and validation phases have demonstrated SENTINEL platform's robustness and adaptability. The internal testing enabled to identify and correct issues, enhancing usability and effectiveness. This process confirmed the platform's capabilities in real-world scenarios and pinpointed areas for future improvement. SENTINEL platform can move towards full-scale implementation and broader market integration. The findings of T5.3 enabled to define next steps, which include refining the platform based on feedback from upcoming testing phases and user engagement, ensuring compliance with evolving regulations and standards. Additionally, the platform can expand its features and functionalities to address new cybersecurity threats and challenges.

3.5.3 Work carried out in WP5 per partner

ITML	ITML provided support on integration of SENTINEL's components and the operation of the integrated framework contributing with ideas and experience on continuous integration processes, testing methods, quality assurance tools and infrastructure sizing. Additionally, ITML participated in the configuration and use of the Github project for issue tracking. Finally, ITML has contributed to the D5.3 and D5.6 deliverables.
LIST	In Y3, the contribution of LIST to WP5 consisted in ensuring integration of GDPR CSA Final product Version with the SENTINEL's platform. The core challenge was the alignment of GDPR CSA questionnaire with SENTINEL's OTMs taxonomy. In addition, LIST has contributed to D5.6.
IDIR	During Y3, IDIR contributed work in T5.2, together with other technical project partners, in the timeframe of the deployment of the final SENTINEL platform (M25-M30), with various tools, technologies, and methodologies for integration and for addressing system architecture, deployment, DevOps, interoperability, scalability, performance, and security.
INTRA	In Y3, INTRA has organized and actively participated in all related calls and discussions. INTRA has set up and configured all the required infrastructure, tools and processes to facilitate modules' continuous integration and delivery. Moreover, INTRA participated in the engineering of business requirements, the definition of user journeys and the design of the User Interfaces. INTRA has coordinated the preparation of and provided key content to deliverable D5.6.
STS	STS has been actively involved in the WP5 discussions and integration activities related to its DPIA component and has made significant contributions towards enhancing the integration solution and patterns. STS has provided contributions to D5.4, D5.5, D5.6, D5.7 and conducted the internal review of D5.1
AEGIS	In Y3, work continued to be comprehensive to refine and enrich the content of the UI by constantly engaging and closely collaborating with the project's end-users with diverse backgrounds (under WP6). We made sure to continue incorporating their feedback and implement a UI that offers high levels of usefulness and usability. Additionally, we made all adaptations required in the communication of the UI with all modules as their development progressed. All this effort resulted in the final version of the MySENTINEL UI dashboard and was documented in the subsequent iteration of D5.1 and D5.2, namely D5.3. Additionally, AEGIS provided input to deliverable D5.6 and D5.7.
TUC	For Y3, TUC further enhanced the content of the lists with the external plugins (open-source tools and trainings) based on feedback from the application of SENTINEL to the piloting environments regarding the appropriateness of the suggested tools and training. Towards this goal, the models and metadata of the two lists were slightly

	updated in an attempt to assist the Recommendation Engine and its decision making to derive more targeted recommendations for the end user. Also, the content of the two lists was included under the SENTINEL Wiki. TUC contributed to deliverable D5.6.
ACS	In Y3, ACS participated in the meeting and discussion regarding the work on T5.1 and T5.2. In addition, ACS has participated in the discussion on how to integrate the CyberRange platform on the SENTINEL architecture. ACS has also contributed to D5.3 and D5.6, while conducted an internal review of the deliverable D5.3.
UNINOVA	In Y3, UNINOVA was deeply involved WP5 leading T5.3 – "From the prototype to the final solution". UNINOVA was responsible for setting-up the internal testing procedure used to analyse and address the technical bugs which were identified within the validation phase by third-parties SMEs, during the 4th SME-centric workshop. UNINOVA was responsible for coordinating and contributing to the development of deliverable D5.7.
CG	In Y3, CG users continued to collaborate with technical partners for the improvement and refinement of the SENTINEL platform to address their needs in an iterative process. Furthermore, the CG pilot users have actively participated in the SENTINEL FFV Demonstration workshop, successfully executed 2 experiments, and filled out a questionnaire by providing new suggestions regarding the FFV of the SENTINEL platform. During the last project year, CG's extended its activities in Work Packages 5 by actively participating in all WP5 related meetings and discussions. Furthermore, CG partners actively participated in the final SENTINEL platform testing activities and filled out a questionnaire by providing final feedback on the SENTINEL platform.
TIG	Throughout Y3, TIG has actively participated in WP5 related calls and discussions. Attendance has been regular and timely. As consistent with Y2 activities, TIG has participated in testing and reviewing the SENTINEL platform to: • Assess usability, checking the use of language and structure for SME users who may have limited knowledge and understanding of GDPR, particularly regarding compliance requirements. • Identify any areas for development in terms of user experience. Two further TIG SMEs (Beyond Limits & Sportfit) were introduced to SENTINEL, whilst work continued with Dimensions Care. • Dimensions care and Sportfit participated in the ATHENS plenary, providing a valuable opportunity to extend their experience of the platform in a bespoke workshop with developers. Finally, TIG has conducted the internal review of D5.6.
CECL	In Y3, CECL work on ensuring the compliance of SENTINEL system with relevant laws and regulations governing data privacy, security, and other pertinent areas as part of T5.3. Legal reviews were conducted by the EDAC to identify any legal risks or compliance gaps within the system.

FP	FP participated in all meetings regarding T5.1 and contributed to the building process of the interactive visualizations and front-end components. Specifically, this effort has been mainly focused (i) on the visualization of the SENTINEL policy, (ii) the monitoring of the OTMs implementation status, and (iii) the visualization of the results of the cybersecurity risk assessment. In addition, FP, as WP6 leader, contributed to T5.1 UI/UX enhancements of the SENTINEL platform by promoting a close and perpetual collaboration with pilot end-users and providing the feedback gained from their testing, organised under WP6 pilot evaluation activities. This facilitated the continuous process of the development and refinement of "MySentinel UI" to develop a clearer and more functional version of the front-end of the platform following SMEs user perspectives. For the continuous integration towards the realization of a complete system (T5.2) FP focused on the proper integration of the MITIGATE plugin, enabling the SENTINEL platform to build upon its functionalities, allowing SME/MEs on one hand to build simulation computer security risk assessment scenarios for preferred cyber-assets, and on the other to perform cybersecurity risk assessments on one or more processing activities. In this context, the final version of the mitigate-adapter was successfully deployed, offering all required integration services from the MITIGATE system and providing corresponding REST APIs to the SENTINEL internal components. Additionally, the final version of the policy-drafting module and the policy enforcement component were also implemented and deployed in the SENTINEL system. As part of the internal platform testing procedures of T5.3, FP representatives contributed by self-testing the SENTINEL functionalities and providing feedback for the platform's final technical refinements. In addition, FP communicated the results from the final pilot event occurred in February 2024 (M33) which were considered in the technical works of maintaining and operating the SENTINEL final solution. FP participated in all WP5 related meetings and contributed to the deliverables D5.3, D5.6 and D5.7.

3.5.4 Status of Deliverables and Milestones

The work conducted in WP5 in Y3 contributed to reaching milestone MS5 and is well-documented in deliverables D5.3, D5.6 and D5.7.

Table 10. Status of WP5 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D5.3	The SENTINEL visualisation and UI component – final version	AEGIS	Demonstrator; PU; M30	Submitted
D5.6	The SENTINEL integrated solution - final version	INTRA	Demonstrator; PU; M30	Submitted
D5.7	Best practices for maintaining and operating the system in the long-term - TRL 7	UNINOVA	Report, PU, M36	Submitted
MS5	Demonstration Fire	INTRA	M30	Achieved
MS6	Consolidation	STS	M36	Achieved

3.5.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D5.3, D5.6 and D5.7 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.6 WP6 – Real-life experimental evaluations: SENTINEL pilots

Leader: FP

Involved Partners: CG, ITML, LIST, IDIR, INTRA, STS, AEGIS, TUC, ACS, UNINOVA, TIG, CECL, FP

Duration: M10- M36

3.6.1 Summary of results achieved during Y3

WP6 kicked-off in M10 and continued until the end of the project (M36). Based on the guidelines and parameters formulated in D1.3, the main objectives of WP6 are the following:

- Ensure the finalization of the experimentation protocol based on end-users' requirements
- Realize real-life demonstrators based on both consortium members and on external entities engaged via DIHs
- Provide detailed validation and evaluation of the SENTINEL platform, from a usability and end-user point of view.

WP6 involved four distinct phases: scoping and planning (the two definition phases) as well as execution and analysis (the two operational phases). All four phases were inter-connected and required continuous feedback.

WP6 key achievements during M10-M24 have been presented in Y1 and Y2 reports, i.e., D8.1 and D8.2 respectively.

During Y3 (M25-M36) the following MS have been accomplished

- MS5 Demonstration Fire (M30)
- MS6 Consolidation (M36)

with the contribution of WP6 activities, summarized below:

- During M25-M30: the main SENTINEL pilot phase was running with testing and validation activities carried out under T6.2 and T6.3 activities in the context of three major pilots, i.e. the Clingenics Pilot on Genomics (CG Pilot), the Tristone investment Group on social care (TIG Pilot) and the SMEs/MEs engaged via Digital Innovation Hubs (DIH Pilot). Within this period, the SENTINEL Full Featured Version (FFV, 1st prototype) was demonstrated to pilot end-users who tested and validated the platform under focused Processing Activity (PA) experiments in the fields of Genomics and socialcare, whereas additional generic PA experiments carried out. They provided fruitful feedback which was considered in the technical development activities and led to the SENTINEL Final Integrated Solution (2nd prototype) released in M30. All pilot testing and validation activities of this period are reported in D6.2. UI/UX improvements in the SENTINEL platform based on the pilot feedback received are reported in D5.3.

- During M31-M36: a final testing and validation conducted via an SME physical workshop in Athens (M33) under T6.3 activities to evaluate the utility of the proposed solution which engaged internal pilot owners, external SMEs and the External Advisory Board (EAB). The feedback gained was considered in the technical refinements and maintenance-operational works of the platform which occurred under T5.3. All these WP6 related activities were reported in D6.3.

Throughout the current reporting period (M25-M36), the evidence from all pilot activities was collected and studied under T6.4 activities as a continuous process which drove the overall assessment and evaluation of the platform and led to the conduction of an impact analysis with respect to the experimentation protocol identified in T1.3 and finalized in T6.1. Moreover, KPIs were continuously monitored for each pilot demonstrator both in operational (cost, service levels, etc) and technical terms (performance of solution), while validation and verification variables, identified under the works of T1.3 and T6.1 were utilised to measure them. Eventually, an overall KPIs/KRs assessment was conducted. The SENTINEL evaluation outcomes and impact analysis were reported in D6.3.

All WP6 activities carried out in this period were coordinated through WP6 biweekly meetings and additional focused telcos between WP6 partners were needed.

3.6.2 Key WP6 achievements during Y3 at task level

T6.1 SENTINEL experimentation protocol alignment and pilots' setup

T6.1 was led by FP. It started in M10 and completed in M18.

T6.1 has contributed to the following WP6 objective:

(i) Ensure the finalization of the experimentation protocol based on end-users' requirements.

In addition, under T6.1 the overall SENTINEL user-centric evaluation methodology was defined, the training process and types of educational material utilised during the pilots identified, directions for the execution of sanity checks were given and pilots time/action plans were set providing significant input to D6.1 (M18). All T6.1 activities were thoroughly reported in D8.1 and D8.2.

T6.2 Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care

This task was led by CG. It started in M13 and completed in M36. In Y3 (M25-M36) the following activities carried out:

- Concerning the CG Pilot on genomics, the two (2) CG end-users completed the trials execution in the SENTINEL platform under the scope of two (2) pilot experiments addressing two (2) PAs on normal operations of Clingenics micro-enterprise (ME) company which resides in the Healthcare sector. The CG end-users filled out the online

SENTINEL User Evaluation Questionnaire and provided additional textual feedback via an excel evaluation form to further address additional technical issues of the SENTINEL FFV (1st prototype) and suggestions which were considered in the technical implementation activities for the SENTINEL Final Integrated Solution (2nd prototype) released in M30.

- Regarding the TIG Pilot on Social care, TIG engaged Dimensions Care, an SME that provides residential care to children, to test and validate the SENTINEL FFV. After the SENTINEL FFV demonstration, occurred in M24, two (2) Dimensions Care end-users executed trials on the platform in two rounds (during M25-M28) by performing two (2) experiments addressing PAs related to childrencare, utilised by the company in their daily normal operations to manage personal data processes. The Dimensions Care end-users provided their feedback by completing the online SENTINEL User Evaluation Questionnaire. Furthermore, in M29, TIG engaged two (2) additional SMEs from its portfolio (i.e. Beyond Limits and Sportfit related to social care to participate in the pilot testing and evaluation activities of SENTINEL FFV (1st prototype). A digital demonstration workshop carried out to present the SENTINEL platform to two (2) end-users who represented those companies respectively. The two (2) end-users tested the SENTINEL platform in the context of two (2) PA generic experiments involving employee and prospect data and provided feedback by filling out the online SENTINEL User Evaluation Questionnaire which was again considered in the technical development of the SENTINEL Final Integrated Solution
- In addition, the two (2) CG end-users and two (2) end-users coming from Dimensions Care and Sportfit accordingly participated in the SENTINEL final SME workshop, occurred in M33 under the activities of T6.3. The end-users tested and validated the SENTINEL Final Integrated Solution (2nd prototype) and the collected input was considered in the technical works of the platform conducted under T5.3 activities

Both Pilots aimed at i) testing and validating the SENTINEL functionalities under real-life operation scenarios and providing feedback considering their personal experience gained after performing the trials considering various validation criteria (e.g. usability, performance, user satisfaction, UI/UX, speed, flexibility, quality, efficiency), ii) testing how SENTINEL addresses privacy, personal data protection and cybersecurity requirements of different PAs performed in the context of the SMEs operations. All input collected was analysed under the activities of T6.4.

T6.2 has contributed to the following WP6 objective:

(i) Realise real-life demonstrators based on both consortium members and on external entities engaged via DIHs.
(ii) Provide detailed validation and evaluation of the SENTINEL platform, from a usability and end-user point of view.

All of the above activities were reported in D6.2, D6.3.

T6.3 Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs

This task was led by UNINOVA which started in M13 and completed in M36. UNINOVA, as a task leader, has been in close contact with several DIHs in order to engage European SMEs willing to use and validate the SENTINEL platform. Such engagement activities were performed through webinars and workshops aiming to present the SENTINEL platform to different SMEs.

In Y3, SENTINEL engaged with three additional ATTRACT EDIH, Südwestfalen EDIH and AIP (Associação Industrial Portuguesa), although the last one is not an EDIH, we consider relevant to engage with AIP mainly because it represents the Portuguese SME ecosystem, with more than 6.000 associates. Such contacts enabled to recruit additional SMEs in Y3 to use and validate the SENTINEL offerings throughout the several SME-centric workshops organized. To this aim, a virtual SENTINEL FFV Demonstration workshop (The Shields Workshop), conducted in M28 in the context of DIH Pilot, with the participation of 24 SMEs. During M28-M29 ten (10) end-users coming from ten (10) SMEs conducted trials to test and validate the SENTINEL platform. The obtained feedback was considered in the technical progress of the SENTINEL Final Integrated Solution. In addition, during M33, an SME physical workshop in Athens was conducted (the 5th and final SME-centric workshop) where apart from CG, Dimensions Care and Sportfit engaged under T6.2 activities and 11 additional SMEs were engaged under T6.3 activities. The EAB members participated in the workshop as well. After the demonstration of the SENTINEL platform, all these workshop attendees tested and validated the SENTINEL Final Integrated Solution (2nd prototype) in an interactive manner. The feedback gained was considered in the technical refinements of the platform under the activities of T5.3.

Evaluation results retrieved from the current task were analysed as part of T6.4 works. All of the above activities were reported in deliverables D6.2, D6.3 and D7.6.

T6.4 Evaluation and impact analysis

This task was led by STS; started in M22 and completed in M36. In Y3, a persona-based approach was formulated and used during the demonstration, testing and validation of the SENTINEL FFV. The SENTINEL persona-based approach assisted in the design of user experiments (creation of scenarios representing how different personas might interact with the system) and guided the identification of UI/UX improvements (by reconsidering user flows and define appropriate help to meet the requirements of the diverse groups represented by the personas). The main instrument for collecting information from end-users was the user evaluation questionnaires filled by the 3 Pilots participants.

As part of the SENTINEL evaluation process, STS monitored KR templates to be completed and regularly updated for each KR. In M30, after the final execution of the three demonstrators each KR was evaluated and they were re-evaluated at the end of the project (M36) as well. During the current reporting period, STS utilised questionnaires to collect and analyse data and feedback received from end-users participated in the three Pilots (T6.2, T6.3) and in the final SME workshop (T6.3) occurred in M33 (including the EAB members) following the SENTINEL user-centric evaluation methodology (T6.1). All collected evidence was processed through descriptive analysis and respective diagrams, pies and charts were developed to visualize the results. Impact analysis carried out with respect to the experimentation protocol (T6.1) and verification and validation variables utilised to measure business, operational and technical aspects from input collected via the end-users trials execution and from technical testing occurred in laboratory environments by technical partners. In addition, the SENTINEL platform was evaluated towards its capability to address application requirements and SMEs business requirements, identified in D1.2. The SENTINEL persona-based approach and the evaluation results derived from the three

Pilots were reported in D6.2. The evaluation outcomes of the final SME-centric workshop and the overall SENTINEL assessment and impact analysis were reported in D6.3, led by STS.

3.6.3 Work carried out in WP6 per partner

ITML	In Y3, ITML has participated in all WP6 related discussions providing inputs and valuable insights on the execution of both the SENTINEL FFV trials. Furthermore, ITML has facilitated the organization of the FFV demonstration workshops by inviting and engaging external SME representatives (pilot 3) and giving short presentations during these sessions. ITML has contributed to D6.2 and D6.3. Finally, ITML has facilitated the successful achievement of MS5 “Demonstration Fire” and MS6 “Consolidation” in M30 and M36 respectively.
LIST	In Y3, LIST was involved in the different Pilots and Workshop dedicated to introducing and testing the SENTINEL platform. More precisely, LIST was in charge to introduce to participants the main concepts coined by GDPR. In addition, LIST was involved in the analysis of test results and contributed to both D6.2 and D6.3.
IDIR	In Y3 (M25-M36) IDIR has continued providing updates, rolling over the work from T6.1, regarding the verification variables concerning two SENTINEL main system components (the Profiling service and the Self-Assessment engine) and associated KPIs. IDIR helped define user test cases, apply the methodology to identify user personas and finalise user evaluation questionnaires leading up not just to internal piloting activities but also the final SME-centric workshop. Overall, during Y3 IDIR participated in the monthly telcos and discussions of WP6, for the implementation of the demonstration and evaluation activities with particular focus on the Final SME-centric Workshop in M33 (February 27, 2024). In particular, IDIR played an active role in defining the demonstration workflow of the SENTINEL platform and contributed to the definition of the interactive survey that was used during the workshop. Also, IDIR actively participated in the workshop itself, assisting the demonstration and hands on testing of the platform from the attendees. Finally, IDIR provided input concerning the SENTINEL impact analysis according to the SENTINEL demonstration protocol.
INTRA	In Y3, INTRA participated in all related discussions providing inputs on the evolving system architecture and functionalities to help align the experimentation protocol in terms of validation and verification as well as related benchmarks and standards. Moreover, INTRA conducted the demonstration workshops for Final Versions of the platform to onboard internal users and external SMEs participating in the platform evaluation.
STS	STS has participated in all WP6 monthly telcos and discussions as a leader of T6.4. Furthermore, STS helped organising the SME workshop recruiting an SME to participate testing and validating the SENTINEL platform. Additionally, STS provided updates to the online questionnaire to better reflect the user personas. Finally, STS contributed to D6.2 and led the delivery of D6.3.
AEGIS	AEGIS participated in all related discussions providing inputs on the evolving system architecture and functionalities. In addition, AEGIS has contributed to the deliverable D6.1. In Y3, AEGIS contributed to the validation of the SENTINEL offerings to SMEs and its evaluation through Digital Innovation Hubs as requested by the relevant task leaders, while participating in all related discussions. Furthermore, AEGIS contributed to the deliverables D6.2 and D6.3.
TUC	TUC has participated in all WP6 monthly telcos and discussions (mainly for T6.2 and T6.3). TUC also contributed to D6.1 and D6.2. The main contributions were focused on the recommendation of external tools and trainings, which could potentially assist the pilots to improve their security/privacy status. Currently, the suggestions are

	mostly based on covering missing functionality and OTMs. A wide list of recommendations is given to the user, who then has to select the most suitable of them. In Y3, TUC collected feedback from the pilots, concerning the appropriateness of the recommended external tools and training elements. The goal was to assist the operation of the Recommendation Engine in order to make tailored and fruitful suggestions to the end user. TUC contributed to D6.3 by conducing also the review of this report.
ACS	ACS has participated in the WP6 monthly call and initiated discussions with SENTINEL pilot owners (TIG, CG) to engage them in the development of CyberRange scenarios. ACS has provided the gaming interface of the CyberRange with four scenarios to be used by the SME's. In Y3, the end-users have used the gaming interface of the CyberRange and have provide feedback that was used to improve the solution and user experience. In addition, ACS has contributed to the deliverables D6.2 and D6.3.
UNINOVA	In Y3, UNINOVA has participated in WP6 regular calls and has provided input to D6.2 namely on the pilot 3 FFV demonstration workshop and also on D6.3, focusing on the 5th SME-centric workshop preparation and recruiting.
CG	In Y3, CG persisted its validation, trial executions and the analysis of CG pilot results. Furthermore, the CG users were active participants in the final SME-centric workshop by testing the final SENTINEL platform and providing significant insights through the designated forms and reports. Concurrently, CG dedicated efforts to the refinement of verification and validation variables, along with their corresponding Key Results (KRs) needed for the impact assessment of the project. This work has been reported in D6.2 where CG had a leading role as well as in D6.3 where CG was an active contributor.
TIG	Throughout Y3, TIG participated in the WP6 monthly calls and related discussions supported the technical partners with pilot requirements. In addition to Dimensions Care's involvement as a pilot, TIG were able to secure two further SMEs from within the TIG portfolio. Therefore, the TIG piloting contributions encompassed: • Beyond Limits (Adult Social Care) • Dimensions Care (Children's Social Care) • Sportfit (Children's Social Care & Education) Additionally, DH (TIG) engaged in the ATHENS plenary SME workshop, along with the DPOs from Dimension's Care and Sportfit. The following items remain the most important requirements to be addressed by the SENTINEL platform: • Enhance the measures taken to protect sensitive information about service users and those significant to them. • Improve upon the robustness of security measures in place to counter potential threats from ransomware and malware that could result in serious disruption to day-to-day operations, such as the locking of essential communication systems. • Reduce the potential for vulnerable service users to access inappropriate sites and social media platforms that have the potential to cause harm. TIG has continued to be involved in the pilot preparatory actions, by actively participating in a further Demo Workshop provided for Beyond Limits and Sportfit. Finally, TIG has contributed to D6.2 and D6.3.
CECL	In Y3, CECL participated in WP6 relevant discussions by providing valuable insights about legal and ethics topics. Furthermore, CECL gave input relevant to training on

	privacy and data protection. Moreover, the EDAC started working on the finalisation of the Ethical Controlling Report (D8.15), which offers a more detailed comparison of the partners' (especially the SMEs partners) data protection policies. In particular, a detailed questionnaire was drafted and distributed to all partners with particular focus on SMEs partners in order to record their legal and ethical policies in terms of personal data protection. Both documents will be used as valuable sources and learning materials for pilot partners.
FP	FP led all WP6 activities and organised biweekly WP6 meetings and several focused telcos between partners whenever needed to coordinate all required procedures. As WP6 leader, FP supervised all pilot and evaluation activities (T6.2, T6.3) to ensure their alignment with the SENTINEL user-centric evaluation methodology and experimentation protocol. FP, in collaboration with ITML, organised the pilot demonstration workshops and the SME-centric workshop in M33. In addition, FP in collaboration with ITML, STS and IDIR provided updates to the online questionnaire to better reflect the user personas (T6.4). Moreover, FP prepared all SENTINEL instructions utilised in each pilot and described the Processing Activity (PA) experiments reported in D6.2. FP also collected the pilot evaluation results and provided analytics (e.g. charts, pies, diagrams) in D6.2. Furthermore, FP guided the activities for the SENTINEL platform assessment towards the validation and verification metrics and assisted in evaluating SENTINEL capabilities against the business and application requirements identified in D1.2 and in presenting the overall evaluation outcomes (T6.4) reported in D6.3. Concerning the final SME-centric workshop conducted in M33, FP recruited two SMEs to participate who tested and validated the SENTINEL platform (T6.3). In addition, FP communicated to technical partners the end-user feedback received from the Pilots which was considered in the technical refinements of the platform undertaken as part of T5.3 works. An FP representative together with CG was the main editor of D6.3, whereas another FP representative was one of the internal reviewers of the deliverable.

3.6.4 Status of Deliverables and Milestones

The work conducted in WP6 in Y3 is well-documented in deliverables D6.2 and D6.3 which also contributed to reaching milestone MS5 and MS6.

Table 11. Status of WP6 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D6.2	SENTINEL Demonstration - final execution	CG	Report; PU; M30	Submitted
D6.3	Assessment report and impact analysis	STS	Report; PU; M36	Submitted
MS5	Demonstration Fire	INTRA	M30	Achieved
MS6	Consolidation	STS	M36	Achieved

3.6.5 Deviations from Work Plan

No deviations occurred in the current reporting period. The writing process of D6.2 and D6.3 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.7 WP7 – Ecosystem building, Exploitation and sustainability management

Leader: UNINOVA

Involved Partners: All

Duration:M1-M36

3.7.1 Summary of results achieved during Y3

WP7 was led by UNINOVA and started in M1. It is a horizontal work package that will be active during the entire lifetime of the project, and it is composed of four (4) tasks.

During Y3, WP7 activities focused on updating and maintaining the fundamental communication and dissemination channels for the project. In addition, SENTINEL has produced additional dissemination materials: four (4) newsletters, five (5) videos, three (3) SENTINEL podcasts, which have been prepared and electronically distributed via the established online channels and in physical meetings.

The consortium partners have conducted a thorough market analysis and have released an updated business modelling and the well-defined list of offerings as part of Task7.1 activities.

Furthermore, the project's dissemination activities continued via seeking potential synergies among relevant EU projects and other initiatives. This led to the organization of the

- 4th SME-centric Workshop, 25 September 2023
- Cyber Security and Data Protection Synergies – Joint Cluster Event, 16-17 October 2023
- 5th SME - centric Workshop, 27 February 2024
- SENTINEL Final Event, 9 April 2024

In addition to this, the partners have managed to submit and present four (4) additional publications in conference proceedings.

- Stephane Cortina, Michel Picard, Samuel Renault, Philippe Valoggia "Digitalizing process assessment approach: An illustration with GDPR Compliance Self-Assessment for SMEs", European Conference on Software Process Improvement, (EuroSPI) 2023, 30 August – 01 September 2023 France, France https://link.springer.com/chapter/10.1007/978-3-031-42310-9_9
- George Hatzivasilis, Sotiris Ioannidis, Cataldo Basile, et al. "Continuous Security Assurance of Modern Supply Chain Ecosystems with Application in Autonomous Driving: The FISHY approach for the secure autonomous driving domain", IEEE International Conference on Cyber Security and Resilience (IEEE CSR) Workshop on Cyber Resilience and Economics (CRE) 31 July 2023 - 02 August 2023, Virtual DOI: http://dx.doi.org/10.1109/CSR57506.2023.10224971.
- Eva Papadogiannaki, Ioannidis Sotiris "Pump Up the JARM: Studying the Evolution of Botnets using Active TLS Fingerprinting", IEEE Symposium on Computers and Communications (ISCC 2023), July, Virtual, http://doi.org/10.1109/ISCC58397.2023.10218210

- Andreas Theofanous, Eva Papadogiannaki, Alexander Shevtsov, Sotiris Ioannidis “Fingerprinting the Shadows: Unmasking Malicious Servers with Machine Learning-Powered TLS Analysis”, International World Wide Web Conference 2024 (WWW), May 2024, DOI: https://doi.org/10.5281/zenodo.10655329

The partners have managed to publish 1 electronic journal paper, 1 journal paper in Internet of Things Journal, 2 already accepted journal papers in “Journal of Surveillance, Security and Safety” and “International Journal of Information Security”, submitted 1 journal paper and currently are working on 2 journal papers to be submitted by the end of the project.

- Fereniki Panagopoulou, “Data Protection for SMEs”, e-politeia Journal, April 2024, https://www.epoliteia.gr/e-journal/2024/04/22/e-politeia-teyxos-10-aprilios-iounios-2024/
- Dimitrios Tyrovolas, Nikos A. Mitsiou, Thomas G. Boufikos, Prodromos-Vasileios Mekikis, Sotiris A. Tegos, Panagiotis D. Diamantoulakis, Sotiris Ioannidis, Christos K. Liaskos, and George K. Karagiannidis, “Energy-aware Trajectory Optimization for UAV-mounted RIS and Full-duplex Relay” IEEE Internet of Things Journal, April 2024, DOI: 10.1109/JIOT.2024.3390767 (**published**).
- Eleni-Maria Kalogeraki and Nineta Polemi, “A Taxonomy for Cybersecurity Standards”, Special Issue "Industrial Control Systems Security and Privacy Issues”, Journal of Surveillance, Security and Safety (**accepted**).
- George Hatzivasilis, Eftychia Lakka, Manos Athanatos, etc. “Swarm-Intelligence for the Modern ICT Ecosystems”, International Journal of Information Security – Special Issue on Cybersecurity in Healthcare, Springer (**accepted**).
- George Hatzivasilis, et al. “Review of Smart Home Security using IoT”, Electronics, MDPI, Special Issue on New Challenges in Information Security and Privacy and Cyber Resilience (**submitted**).

In Y3, the SENTINEL partners have participated and presented the project in events and conferences:

- PUZZLE‘s Cybersecurity Conference, 21 June 2023.
- Final Event of the CitySCAPE project, 28 June 2023.
- 28th IEEE Symposium on Computers and Communications, 09 -12 July 2023.
- IEEE International Conference on CSR, Workshop on Cyber Resilience and Economics (CRE), 31 July – 02 August 2023.
- 30th European Conference on Software Process Improvement, (EuroSPI) Conference, 01 September 2023.
- CyberHOT Summer School, 29 September 2023
- ATTRACT EDIH public presentation, 10 January 2024
- Data Protection Day, 29 January 2024
- AIP Roadshow I&D, 29 February 2024
- Cyber Threat Intelligence: Empowering IoT Security Workshop- CTI Workshop, 06 March 2024
- International World Wide Web Conference 2024 (WWW), 13-17 May 2024
- INFOSHARE Conference, 22-23 May 2024

In addition, SENTINEL has reached and secured the interest for further trialling of the SENTINEL platform of two (2) additional Digital Innovation Hubs:

- ATTRACT EDIH
- Südwestfalen EDIH

In Y3, SENTINEL has continued to liaise and execute joint dissemination and communication activities with 14 projects joined under the SecureCyber Cluster. In particular, SENTINEL has contributed to two policy briefs released and jointly worked on four (4) newsletters released by the SecureCyber Cluster.

- The cybersecurity needs of the EU industry, Policy Brief, April 2023
- CTF Policy brief (to be released in May 2024)

During Y3, the project partners organized two SME-centric workshops with a release of the SME engagement survey, which, in conjunction with the final SENTINEL platform release, has triggered the intensification of the exploitation activities. Furthermore, we gave training for the SENTINEL end-users and showcased the Cyber Security and Data Protection Synergies – Joint Cluster Event.

The above was comprised significant input to D7.4 “Dissemination strategy and activities - final version”, D7.6 “Ecosystem building and SMEs engagement report - final version”, D7.8 “Exploitation strategy, standardisation activities and best practices - final version” and D7.9 “Final business model, market analysis and long-term sustainability report” due in M36. Furthermore, D7.4, D7.6, D7.8 and D7.9 contributed to milestone 6 “Consolidation” due in M36.

3.7.2 Key achievements during Y3 at task level

T7.1 Market continuous analysis and business planning for SENTINEL exploitation

T7.1 is led by AEGIS and started with the start of the project in June 2021. Following the official presentation of the task plan at the Kick-Off meeting at the end of June, AEGIS has immediately started implementing the plan. As a first step to this plan, AEGIS organized a Task 7.1 related telco inviting all SENTINEL partners to further explain the rationale behind the plan presented. In this context, AEGIS has created and circulated a questionnaire that all partners were kindly requested to fill in. The design of the questionnaire was aimed at gathering insights from many different perspectives including Academia, large industries, technology providers and SMEs. The insights emerged from this process were contributed to better understand and identify SENTINEL competitive advantage and value proposition and form the preliminary business modeling that was successfully presented in D7.2 titled “Market analysis and preliminary business modeling” in M6 of the project.

After the successful submission of the D7.2 “Market analysis and preliminary business modelling”, AEGIS continued to gather information and follow the observation of market trends for any changes that could affect the elaboration of the joint business plan presented in the deliverable. As part of the continuous market observation, an intermediate analysis was carried out for M18 resulting in an updated business strategy [value proposition, business model (canvas)] which was included in D7.7 “Exploitation strategy, standardisation activities and best practices - interim version”. As expected, there was a revisit to the business planning based on the acceptance of the MVP and the FFV as part of brainstorming, as well as based on the feedback we received. This involved cooperation between Tasks 7.1, 7.2 and 7.3 and is documented in the final business model, market analysis and long-term sustainability report (D7.9) due in M36.

T7.1 has contributed to the following WP7 objectives:

(i) To develop the SENTINEL business model and strategies for incentivizing/promoting project adoption by various stakeholders within the SMEs/MEs ecosystem during and after the project.

(ii) Create a marketing strategy that focuses on commercialization including the products costs (TCO), benefits (TBO), and return on investment.

The above comprise significant input to D7.7 "Exploitation strategy, standardisation activities and best practices – interim version", delivered in M18), contributing also to milestone 3 "Innovation Fire", due in M18. Major contributions are provided in D7.9 "Final business model, market analysis and long-term sustainability report", contributing to milestone 6 "Consolidation", due in M36.

T7.2 Dissemination and communication strategy to trigger awareness and new business opportunities

T7.2 is led by UNINOVA and started in M1. With respect to dissemination and communication activities in Y3, SENTINEL has released four (4) new newsletters (M25, M29, M34 and M36), five (5) videos, three (3) SENTINEL podcasts, 1 SENTINEL booth mock-up for the INFOSHARE conference, updated the SENTINEL poster as well as produced regular posts in social media (LinkedIn, Twitter),

Considering attendance at events, SENTINEL was present at different events, as already presented previously. In parallel to participation in multiple events, SENTINEL has also organized webinars and workshops aiming to invite and engage target audiences and potential end-users. The full list of activities and events conducted in Y3 is described under D7.4" Dissemination strategy and activities - final version".

With respect to academic publications, SENTINEL has published four (4) conference papers, 1 electronic journal paper, 1 journal paper in Internet of Things Journal. In addition, 2 journal papers are accepted to be published in "Journal of Surveillance, Security and Safety" and "International Journal of Information Security", 1 journal paper already submitted and currently the consortium is working on 2 journal papers to be submitted by the end of the project.

The WP7 bi-weekly meetings take place regularly where all partners join and discuss actions for communication and dissemination activities. Finally, the SENTINEL social media channels, constantly being updated, increase the number of visitors and followers daily.

T7.2 has contributed to the following WP7 objectives:

(i) Develop the project's visual identity, including conventional information material, tools (project website, social media) and audio-visual material (e.g., videos).

(ii) To raise awareness about the project concept, developments and findings to all key actors (the cybersecurity and data protection industry, SMEs/MEs, academics, policy makers, general public) by participating and organising outreach activities, international events (e.g., conferences and seminars) and INFO days.

(iii) To develop the dissemination and communication strategy of the project, including social presence, participation in EU events, collaboration with other related projects, and implement it.

Points (i) and (ii) mentioned above are mainly covered in Y1 and Y2. In Y3, we updated the project's visual identity (where needed), continued raising awareness about the project, developed the project's dissemination and communication strategy and proceeded in implementing the main aspects mentioned in point (iii). The respective activities are well demonstrated in D7.4 "Dissemination strategy and activities – final version", delivered in M36.

T7.3 Exploitation and standardization activities and best practices

T7.3 commenced in M13 and was led by STS. Within the scope of designing and developing the exploitation strategy and standardisation activities for SENTINEL, STS distributed a 2nd exploitation questionnaire, and all partners were kindly requested to complete it.

This questionnaire focused on Key Exploitation Results (KERs) where each partner provided updated data about the KERs that they owned, the Technology Readiness Level (TRL) and Market Readiness Level (MRL). They also described any innovations introduced, the market relevant market trends, the competitors and the target audiences by additionally providing updates on the Intellectual Property (IP) status and their IP protection strategies.

Furthermore, as part of this questionnaire, the SENTINEL partners examined their individual exploitation plans, gave details about completed exploitation actions in the second half of the project and detailed their short/long- term future exploitation plans and long-term sustainability plans. They also described the standardisation activities they are engaged in and their expected impact, all of which were reported in the D7.8 report, submitted successfully within the given timeline.

Valuable insights were collected from many different perspectives including Academia, large industries, technology providers and SMEs. The insights emerged from this process contributed to better understanding and identifying SENTINEL exploitation results, current and future exploitation and standardisation activities and form the project's expected impact and long-term sustainability plan.

Towards the end of Y2 and in the early months of Y3, SENTINEL engaged the Horizon Standardisation Booster[7] to aid in identifying relevant current and upcoming standards that could benefit the project. Several meetings were held with the assigned expert, and based on these discussions, the expert prepared a report filled with valuable suggestions and recommendations. More details can be found in D7.8, section 6.2.

Additionally, later in Y3, STS applied for and benefited from two modules under Service 1, "Portfolio Dissemination and Exploitation Strategy," of the Horizon Results Booster[8]. This initiative aimed to strengthen SENTINEL's dissemination and exploitation strategy and maximise the project's impact. The main objectives of Module A included identifying complementary results among a group of research projects formed as part of the module, grouping them into Key Exploitable Results, analysing and prioritising key stakeholders, and preparing for joint dissemination actions. More details on this can be found in D7.4, section 2.7. Module C was focused on assisting SENTINEL to improve its existing exploitation strategy. It aimed to enhance the review and revision of key project results, refine exploitation plans, identify relevant stakeholders, and provide support for risk analysis in the exploitation process.

[7] HSbooster.eu
[8] https://www.horizonresultsbooster.eu/

One recommendation from Module C was for SENTINEL to apply for the Horizon Results Booster's Business Plan Development (BPD) service[9]. STS submitted this application in December 2023, and the service was successfully executed in the early months of 2024. The service aimed to help SENTINEL beneficiaries market project results by offering guidance and tailored training in developing business plans, analysing markets and competitors, and identifying start-up operations and funding options. More details on this can be found in D7.8, section 2.3.

T7.4 SENTINEL ecosystem building: Continuous engagement of technology providers, SMEs/MEs

T7.4 was led by UNINOVA and started in M1. The ecosystem building task continued to be very active in the reference period. In particular in Y3 two (2) successful SME-centric workshops were organized. The fourth SME-centric workshop was held online in September 2023 while the fifth and final workshop was held in person in February 2024.

We accounted 35 SMEs in both workshops witnessing for more than 80 people attending. During these workshops, all participants participated in our SME questionnaire, and had the possibility to test and validate the SENTINEL platform. The focus of SME-centric workshops was to present the SENTINEL project to European SMEs and to collect feedback on the SENTINEL features and services as well as to gather impressions on platform’s usability, UI/UX and assess the participants’ acceptability and interest on investing on services similar to SENTINEL.

Aligned with T7.2, the SENTINEL project has organised and participated in the “Cyber Security and Data Protection Synergies – Joint Cluster Event”. The event took place at UNINOVA premises, in Portugal, on the 16th and 17th of October 2023 inviting also external participants to join a training session held on the 2nd day of the event. The agenda included various presentations made by invited sister project representatives together with open discussion on relevant topics of the cyber security and data protection domain. The projects co-hosted the event were: the IDUNN Project, KRAKEN H2020, Electron Project, Secant project, CROSSCON, TRUSTaWARE, IRIS H2020 Project, SPATIAL Project, ERATOSTHENES PROJECT and the ARCADIAN-IoT. The event kicked off by the Dissemination Manager of SENTINEL. Also, a keynote presentation took place in the beginning of the agenda the Project Adviser of the SENTINEL project.

During Y3, SENTINEL was able to establish contacts with the following EDIHs: ATTRACT EDIH and Südwestfalen EDIH.

T7.4 has contributed to the following WP7 objective:

(i) To raise awareness about the project concept, developments and findings to all key actors (the cybersecurity and data protection industry, SMEs/MEs, academics, policy makers, general public) by participating and organizing outreach activities, international events (e.g., conferences and seminars) and workshops.

The above comprised significant input to D7.6 “Ecosystem building and SMEs engagement report – final version”, delivered in M36, contributing also to milestone 6 “Consolidation”, due in M36.

[9] https://www.horizonresultsbooster.eu/ServicePacks/Details/7

3.7.3 Work carried out in WP7 per partner

ITML	In Y3, ITML has participated in all monthly and bilateral meetings regarding WP7 while it collaborated with the Dissemination and Exploitation Leaders (UNINOVA and STS), to seek synergies and collaborate with SMEs and business enterprises to promote the project offerings. In this respect, ITML participated in all the crucial discussions conducted among all partners towards building a thorough joint exploitation and business strategy aligned with market needs. As part of T7.2 and T7.4, ITML has hosted the **5th SME-centric workshop** (27th of February 2024) and actively supported the organisation of the **4th SME-centric Workshop** (25 September 2023), by presenting and promoting the project's offerings among external SME representatives. With the ARCADIAN-IoT coordination team ITML has supported the organisation of **"ARCADIAN-IoT and SENTINEL Symposium and Showcase"** event on the 9th of April 2024. In Y3, ITML has presented the SENTINEL project in "**Cyber Security and Data Protection Synergies – Joint Cluster Event"**, "**Cyber Threat Intelligence: Empowering IoT Security Workshop" "Cyber Security and Data Protection Synergies – Joint Cluster Event"** and "**InfoShare Conference"**. ITML has prepared and released posts in SENTINEL's social media (LinkedIn, Twitter), as well as kept updating and maintaining the smooth operation of the SENTINEL website. ITML has reviewed all the SENTINEL newsletters released within this period. Finally, ITML has provided input for all deliverables of WP7 and conducted a review process wherever assigned. In this regard, ITML, worked on and contributed to the deliverables D7.4, D7.6, D7.8 and D7.9.
LIST	In Y3, LIST has presented the SENTINEL project in the "The Data Privacy Day 2024" event in January 2024 and participated in the Arcadian-Sentinel Symposium organised in April 2024. LIST also presented a paper describing GDPR CSA and providing its conformity assessment with ISO/IEC 330xx family standard.
IDIR	In Y3, IDIR has followed all WP7 telcos and discussions. IDIR has also contributed to the writing of two publications, one led by FP, regarding the validation and evaluation of the SENTINEL project's platform through multiple real-world settings and a second, led by IDIR, regarding the evolution of the RE methodology within SENTINEL. In addition, IDIR has actively participated in the organization and implementation of the SENTINEL Final SME-centric Workshop. IDIR participated in the SENTINEL's Final Event, the ARCADIAN-IoT and SENTINEL Symposium and Showcase (April 2024) in Stockholm, Sweden. Finally, IDIR has conducted the internal review of the deliverable D7.9.
INTRA	In Y3, INTRA participated in all the meetings concerning the WP7. Occasionally, input for the SENTINEL website and SENTINEL social media channels (e.g., newsletters) has been provided also. INTRA has participated in meetings and discussions dedicated to dissemination and exploitation strategy. Within this period, INTRA has demonstrated the SENTINEL platform in SENTINEL events/workshops such as the Arcadian-IoT / SENTINEL joint workshop as well as the InfoShare 2024 event. Furthermore, INTRA contributed to the definition of the business value of SENTINEL, portraying its main virtues and helping the consortium find pitching points for engaging external SMEs. In addition, INTRA has participated in meetings concerning T7.3, regarding the standardisation activities and in crucial discussions which occurred in Y3 focusing on exploitation strategy. Finally, INTRA contributed to D7.4, D7.8, D7.9 and conducted the internal review process of D7.9.

STS	In Y3, STS participated in all WP7 relevant telcos, discussions and provided content for producing social media posts. In addition, STS supported SENTINEL in the InfoShare 2024 event and talked about the project during the SENTINEL Podcast #10. Furthermore, STS has circulated an exploitation questionnaire by collecting updates about KERs and exploitation activities of the SENTINEL partners conducted in the last project year. This helped to prepare and submit D7.8. In addition, STS has engaged with Horizon standardisation Booster (HSbooster.eu) to seek help in Identifying relevant current and upcoming standards that SENTINEL can take advantage of. Within Y3, STS has applied for Plan Development (BPD) service provided by the Horizon Results Booster (HRB) to strengthen the exploitation strategy by preparing the project's results for the market.
AEGIS	In Y3, as part of the continuous market observation, AEGIS carried out the final market analysis resulting in the final business strategy which is included in D7.9 "Final business model, market analysis and long-term sustainability report". AEGIS has participated in all discussions and meetings concerning WP7 and contributed to what was requested by the task leaders as well as the Work Package leader. Finally, AEGIS participated in the InfoShare 2024 event, promoting SENTINEL and its offerings to a wide audience.
TUC	In Y3, TUC has participated in all WP7 meetings and discussions. TUC assisted again in the organization of the CyberHOT summer school of 2023. The SENTINEL poster was presented, and flyers were disseminated to the participants. Moreover, TUC assisted the organization of workshops under scientific conferences, focusing on conferences where CERTs can be reached. TUC invited 3 SMEs and 1 CERT in various SENTINEL workshops and evaluation Workshops. TUC published 3 conference/workshop papers, 1 journal paper and submitted 2 journal papers. TUC is also organizing a Special Issue on 'New Challenges in Information Security and Privacy and Cyber Resilience', under the MDPI Electronics journal. Finally, TUC contributed to the deliverables D7.4 and D7.8.
ACS	ACS has participated in the WP7 monthly meetings. ACS has contributed to the social media publication by posting several times in the SENTINEL LinkedIn channel. ACS has contributed to D7.8 by providing updates regarding the company's exploitation activities conducted also the review process of the same deliverable.

UNINOVA	During Y3, as the leader of the WP7, UNINOVA has conducted the following activities. • Organization and leading of bi-weekly WP7 telcos. • Organization the 4th SENTINEL SME-centric workshop. • Recruitment of SMEs to participate in the 4th and 5th SME-centric workshops. • Contribution to the exploitation questionnaire. • Continuously creating awareness, promoting SENTINEL through social media channels and providing content to social media on a regular basis • Engagement of relevant stakeholders through social media channels. • Supporting the definition of the online questionnaire for collecting insights from EU SMEs. • Preparation of the SENTINEL newsletters. • Leading the creation of the SENTINEL podcast series. • Promotion on bilateral meetings with other EU projects, seeking potential synergies. • Targeting industrial events for SME engagement. • Participation in several EU events aiming to disseminate SENTINEL achievements. • Preparing and submitting D7.4 and D7.6 deliverables.
CG	In Y3, CG has participated in all meetings regarding the WP7 and was actively following the SENTINEL social media profiles. It also produced content for Newsletter #8 regarding the pilot studies and posts in SENTINEL's LinkedIn channel.
TIG	During Y3, TIG continued work with relevant partners to fulfil the requirements of WP7. TIG participated in all WP7 meetings.
CECL	CECL has participated in all meetings regarding the WP7. During Y3 CECL has contributed to the Exploitation strategy and standardisation activities questionnaire needed to prepare D7.8. Furthermore, it has created LinkedIn posts for SENTINEL's social media and has been active in sharing the social media posts of the SENTINEL project. Finally, CECL has prepared a scientific article that was published in the e-politeia magazine[10].
FP	In Y3, FP has regularly participated in all meetings regarding WP7. In addition, FP has participated in the "CyberHOT" summer school (29 September 2023), boosting interested parties' acknowledgement about the project. FP researchers joined the ARCADIAN-IoT clustering event "Symposium and Showcase: Integrated and automated approaches for IoT Cybersecurity and Privacy compliance" which occurred on 9th April 2024 in Stockholm and presented some parts that FP is responsible for the SENTINEL project. FP has actively engaged with the project's social media platforms by generating new posts and promoting events in which SENTINEL participates or presents. Additionally, FP has contributed content for the newsletter, particularly related to WP6. Within Y3, FP has submitted the paper: E.-M. Kalogeraki and N. Polemi "A Taxonomy for Cybersecurity Standards", Special Issue "Industrial Control Systems Security and Privacy Issues", Journal of Surveillance, Security and Safety (accepted). Furthermore, FP has coordinated the preparation of 2 additional papers in collaboration with other project partners that are currently under preparation. Eventually, FP has contributed to deliverables D7.4, D7.8 and reviewed D7.6 as FP was one of the assigned internal reviewers for this deliverable alongside with AEGIS.

[10] https://www.epoliteia.gr/wp-content/uploads/2024/04/teyxos_10_meletes_1.pdf

3.7.4 Status of Deliverables and Milestones

The work done under WP7 is well-documented in three deliverables D7.4, D7.6, D7.8 and D7.9.

Table 12. Status of WP7 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D7.4	Dissemination strategy and activities - final version	UNINOVA	Report; PU; M36	Submitted
D7.6	Ecosystem building and SMEs engagement report - final version	UNINOVA	Report; PU; M36	Submitted
D7.8	Exploitation strategy, standardisation activities and best practices - final version	STS	Report; CO; M36	Submitted
D7.9	Final business model, market analysis and long-term sustainability report	AEGIS	Report; PU; M36	Submitted
MS6	Consolidation	STS	M36	Achieved

3.7.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D7.4, D7.6, D7.8 and D7.9 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.8 WP8 – Project Management, coordination and quality assurance

Leader: ITML

Involved Partners: All

Duration: M1-M36

3.8.1 Summary of results achieved during reporting period

ITML, as the coordinator of SENTINEL, led T8.1 and T8.2 tasks. Following the same manner already established in Y1 and Y2, during Y3 the WP8 activities have focused on updating the expected coordination bodies and procedures (if needed) as well as maintaining the efficient communication among the project partners and ensuring smooth implementation of the project's objectives and expected impact.

The key achievements of WP8 in Y3 include:

(i) Maintaining the day-to-day project management structure and procedures already established.

(ii) Ensuring the existence of collaborative tools to enable effective internal and external communication and decision making.

(iii) Keeping constant communication with the External Advisory Board (EAB) and the Ethical & Data privacy Advisory Committee (EDAC).

Within Y3, WP8 was dedicated to regular coordination activities. A tight control over the project activities has been taking place regularly by organizing and executing regular meetings at different levels:

- project-wide consensus and organizational activities have been monitored by the Quality Assurance Team of the project.
- project development activities have been monitored via monthly scientific and technical meetings with all the project partners.
- project management and risk assessment activities have been monitored by the Scientific-Technical-Innovation Manager and the Quality Assurance Team of the project.

Four (4) deliverables of WP8 were planned to be released due M36. These reports are D8.3 (present document), D8.7, D8.13 and D8.14 and which are currently under preparation.

3.8.2 Key achievements during Y3 at task level

T8.1 Project Quality Planning and Monitoring

T8.1 was led by ITML, and it has been an active task since the beginning of the project. In Y3, the project's quality planning and monitoring has been further updated in D8.7 "The SENTINEL QA plan and periodic monitoring report – final version" in M36. This report provides updates on the project's organization, procedures, roles and responsibilities in addition to the management, coordination, control and quality assurance activities of the SENTINEL project that were previously presented in D8.6 "The SENTINEL QA plan and periodic monitoring report – second version". In addition, it contains updates regarding the production and reviewing of project deliverables, along with the involved partner roles and outputs.

In Y3, T8.1 has continued to contribute to the following WP8 objectives:

(i) Establish/update a strong project management scheme.
(ii) Conduct continuous quality assurance activities for the operation of the project and the production of its scientific and technical results within its lifespan.
(iii) Ensure continuous monitoring of the project's progress and timely initiation of corrective actions (if needed).
(iv) Perform risk analysis.

The above comprise significant input to D8.7 "The SENTINEL QA plan and periodic monitoring report – final version" due in M36.

T8.2 Day-to-day management, project & financial control and resource monitoring

T8.2 was led by ITML and started in M1. As part of the activities of task T8.2, ITML has been actively monitoring all the activities of the project in Y3 within all WPs and tasks to ensure that the time plan is well-followed by providing clarifications (when needed) and ensure the SENTINEL partners follow the same project mission towards the fulfilment of the project's objectives as defined in the GA. Furthermore, together with the project PO, ITML has initiated the final review meeting (M36) preparation activities.

Finally, D8.3 (current document due in M36) has been prepared by presenting the work accomplished during the last project year. It elaborates on the advancements in relation to the project objectives and provides an in-depth description of the technical progression in all the WPs including work carried out per task and per partner, submitted deliverables, achieved milestones, potential deviations and corrective actions.

In Y3, project coordination has organized the following consortium meetings with the purpose of ensuring a synergistic collaboration among partners and brainstorming on technical and management issues:

- The 6th Plenary meeting, hosted by UNINOVA in Almada, Portugal, on 11-12 October 2023.
- The 7th Plenary meeting (together with the 5th SME-centric workshop), hosted by ITML in Athens, Greece, on 26-27 February 2024.
- 4 Scientific and Technical Meetings (up to M30) and 5 Monthly Consortium Meetings (after M30).
- The Final Review Preparation meeting (**21st of June** 2024, online).
- The Final Review Official Rehearsal meeting (**2nd of July 2024**, online).
- Final Review Meeting (**5th of July 2024**, online).

T8.2 has continued to the following WP8 objectives:

(i) Establish a strong project management scheme.
(ii) Establish the appropriate communication and reporting channels to the European Commission.
(iii) Ensure successful achievement of the project objectives on time and within budget.
(iv) Establish an efficient electronic service for communications, and document exchanging.
(v) Coordinate the organization and execution of the various project meetings, and/or participation of the project in various external or self-organized events.

The above comprise significant input to D8.3 “Yearly project management report - final version” delivered in M36.

T8.3 Technical and innovation management

T8.3, led by INTRA, started in M1 and continued until the end of the project. During Y3, INTRA continued the organization of monthly Scientific and Technical meetings on a regular basis. The main purpose of this series was for the partners to align monthly with respect to the latest developments and achievements of the project, potential risks and future plans. To facilitate the design and development of the final version of the platform, during the Scientific and Technical meetings, the roles and expected contributions of each partner were clarified and key technology assets were presented by their owners. Moreover, Key Results and Performance Indicators were revisited and discussed defining their quantitative progress for the reference period.

Moreover, T8.3 kept in sync with the activities of WP6 and WP7, aligning SENTINEL’s business value with the needs of potential users. These discussions were intensified as the project progressed towards its conclusion and led to the production of D8.13 “The SENTINEL technical and innovation management report – final version”. This report, being an update of D8.12, set the common rules that will govern the exploitation and commercialization of SENTINEL results, including the management of IPR and the relative competitiveness of the end results. It presents the strategic plans for innovation assurance, including coordination and management procedures of the technical evolutions within the project, as well as the project progress in terms of achieved innovation, evolving market needs/changes and business models linked to the project objectives.

T8.3 has contributed to the following WP8 objectives:

(i) Achieve a common scientific and technical direction within the project.
(ii) Realize synergies amongst the project members and effective exploitation of the project's' results.
(iii) Ensure successful achievement of the project objectives on time and within budget.
(iv) Realize synergies amongst the project members and effective exploitation of the project's' results.

Delivery of D8.13 contributed to milestone 6 - "Consolidation", which was due in M36 of the project.

T8.4 Ethics and Data Protection

T8.4 was led by CECL and started in M1. Within Y3, the Ethical and Legal Issues template was drafted by the SENTINEL Project's Ethics Supervisor, Ass. Prof. Fereniki Panagopoulou (chair of EDAC) and Dr Tania Kyriakou (EDAC deputy member). The template was intended to serve as a blueprint for the project partners to record their legal and ethical policies in terms of personal data protection. The outcome of this questionnaire helped to update and release D8.15 "Ethics manual and ethical controlling report - final version", which contains a detailed comparison of the partners' data protection policies against the standards identified in the Ethics Manual, assesses the level of data protection currently and whether this level has changed over the course of the SENTINEL project.

T8.4 has contributed to the following WP8 objectives:

(i) Achieve a common scientific and technical direction within the project.
(ii) Ensure successful achievement of the project objectives on time and within budget.

3.8.3 Work carried out in WP8 per partner

ITML	In Y3, ITML has organized the SENTINEL final plenary meeting, Final Review preparation and official meetings creating the agenda, minutes and the action items. ITML has maintained the smooth operation of the NextCloud repository for the project-related entries (deliverables, minutes, reports, etc.) and the project's mailing list. To manage and control the status update of the project KPIs/KRs, ITML has also facilitated the updating process of the SENTINEL KPI/KR evaluation matrix. It followed all the necessary procedures for keeping regular communications with the project Officer and the respective members of the EAB and EDAC. In addition, ITML proceeded with all the necessary actions to organise the final review report. In detail, it initiated all the procedures to collect input for the report (cost claims, technical report (PART A and PART B). ITML has been constantly monitoring the quality of the deliverables through a thorough final quality review process before the final submission based on its established Quality Assurance Plan. Apart from this, ITML has also been contributing to T8.3 by discussing with INTRA the time plan and the monitoring means that will be used for the innovation tracking. Finally, ITML has produced and successfully

	submitted the D8.7, D8.3 (current document), contributed to D8.13 and D8.15 and reviewed D8.13.
LIST	In Y3, LIST has participated in all WP8 relevant telcos, meetings and discussions as well as plenary meetings and scientific and technical meetings. ILIST has contributed to D8.3 (current document), D8.13 and reviewed D8.15.
IDIR	During Y3, IDIR has participated in all project management and resource monitoring activities either standalone, as is the case when reviewing deliverables (e.g., the D8.3 and D7.9 review) or collaboratively as in the participation in the SENTINEL monthly meetings, the monthly WP meetings and other administrative work, between M25 and M36.
INTRA	In Y3, INTRA coordinated the technical advancements of the project, organised the respective Scientific and Technical meetings on a monthly basis and actively participated in all other related telcos and physical meetings to ensure the scientific soundness, technical integrity and innovation potential of the SENTINEL platform. INTRA has conducted the internal review of the deliverable D8.7, provided input for D8.3 and produced D8.13.
STS	STS has actively participated in all relevant telcos, scientific, and plenary meetings associated with WP8, and has chaired most of the technical weekly calls. Additionally, STS contributed to deliverable D8.3, D8.13 and conducted the internal review of D8.3.
AEGIS	AEGIS has participated in all scientific and technical meetings and plenary meetings. Apart from this, during Y2 AEGIS has conducted an internal review of the deliverable D8.12, while it provided input for D8.2. In Y3, AEGIS participated in all scientific and technical meetings and plenary meetings. Additionally, AEGIS provided input to deliverables D8.3 and D8.13.
TUC	In Y3, TUC participated in all project's relevant telcos (e.g., scientific and technical telcos), plenary meetings and contributed to quarterly reports as well as deliverables D8.3 and D8.13.
ACS	ACS participated in all relevant meetings related to T8.2. ACS contributed to D8.3 and reviewed D8.13 deliverables.
UNINOVA	UNINOVA has participated in all WP8 relevant telcos and discussions. Contributed to D8.3.
CG	In Y3, CG actively participated in all plenary & technical meetings and discussions of the project organised by the project coordinator as well as scientific, technical and innovation manager of SENTINEL. CG has also contributed to as well as conducted the internal review of D8.15.
TIG	TIG has attended and contributed towards WP8 scientific and technical telcos, as required throughout the project year (Y3). In addition, TIG has provided the necessary contribution for D8.3.
CECL	In Y3, CECL participated in project meetings. Furthermore, as part of T8.4 activities, the CECL completed the Ethics Manual following input from all partners and delivered to the coordinator for submission one month ahead of schedule. Furthermore, CECL has executed the internal review process of D8.7.
FP	During Y3, FP has participated in regular meetings (telcos, plenary meetings, technical meetings, etc) and discussions, reviewed project documents/deliverables that were assigned to FP, as well as monitored FP's activities based on the project's

	quality assurance plan. Furthermore, FP provided the necessary input for D8.13 and D8.15.

3.8.4 Status of Deliverables and Milestones

The work done under WP8 in Y3 is well-documented in four (4) deliverables listed below.

Table 13. Status of WP8 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D8.3	Yearly project management report – third version	ITML	Report, PU, M36	Prepared, to be submitted in M36
D8.7	The SENTINEL QA plan and periodic monitoring report - final version	ITML	Report; PU; M36	Submitted
D8.13	The SENTINEL technical and innovation management report - final version	INTRA	Report, CO, M36	Submitted
D8.15	Ethics manual and ethical controlling report - final version	CECL	Report; CO; M36	Submitted
MS6	Consolidation	STS	M36	Achieved

3.8.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D8.3, D8.7, D8.13 and D8.15 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.8.6 WP8 planned activities for the next period

ITML, together with the PO, will proceed with all the necessary actions to organize the SENTINEL's Final Review Meeting planned on the 5th of July, 2024, finalise and submit the final review report.

3.9 WP9 – Ethics requirements

Leader: ITML

Involved Partners: -

Duration: M1-M36

3.9.1 Summary of results achieved during reporting period

ITML is the only partner involved in this WP.

Within Y3 the project mainly focused on monitoring all the activities to comply with all the pre- and post-grant ethics and legal requirements as described in D9.1.

D9.1 has contributed to the following WP9 objective:

(i) Ensure compliance with the 'ethics requirements' set out in this work package.

3.9.2 Work carried out in WP9 package

ITML	ITML is leading WP9 and within Y3 closely collaborated with CECL to continuously monitor all the project activities by providing guidance and assistance to all partners related to ethics issues and ensuring that the project fully complies with all legal and ethical requirements set in this project.

3.9.3 Status of Deliverables and Milestones

No deliverables to report in Y3.

3.9.4 Deviations from Work Plan

No deviations from Work plan.

4. Impact

Apart from the scientific and technological advancements towards meeting the project objectives, SENTINEL is allocating considerable effort to achieving the project's expected impacts. In this regard, the SENTINEL consortium has established an impact maximization strategy that is based on three fundamental elements:

1) **Openness:** open-access sharing of knowledge and cross-fertilization with other relevant EU funded programmes and communities for cybersecurity, personal data protection and GDPR compliance (WP1, WP7 – T7.2, T7.3)
2) **Sustainability:** invest in research and innovation to produce new knowledge and advance existing one, ensuring sustainable growth for the technological advancements (WP6 - T6.4, WP7-T7.2, T7.3)
3) **Ecosystem engagement:** Engage SMEs and MEs through DIHs and other activities and secure their support in order to promote breakthrough innovation.

The impacts that SENTINEL will achieve by the end of the project are related to the following pillars:

- the work programme.
- the innovation capacity, competitiveness, and growth.
- the other Public-Private Partnership (PPP) initiatives.
- standards and society.

Aiming to monitor the progress and measure the respective achievements, well-defined iKPIs have already been identified by the SENTINEL consortium since Y1. Moreover, we rely on specific measures aiming to maximize the impact of SENTINEL. The measures include the establishment of the External Advisory Board (EAB) and the External Ethics and Data Advisory Committee (EDAC), communication and dissemination plan and activities, continuous stakeholder engagements, a concrete exploitation strategy and management of knowledge and Intellectual Property. The activities towards the successful completion for each impact iKPI conducted in Y3 are reported below.

4.1 Impact related to the work programme

Table 14. KPIs status update - Impact related to work programme

iKPI-1.1	**At least four (4) privacy and personal data protection technologies delivered**	**Achieved**
Within the SENTINEL project, technology-driven compliance services are developed according to a 3 steps engineering approach that illustrates "readiness" of service (MVP, First Integrated version, Final Version). Although the platform as a whole provides an integrated and extendable solution for multiple privacy and data protection technologies, the four most significant contributions to that end are: 1) GDPR Compliance Self-Assessment, 2) Integrated Identity Management System, 3) Data Protection Impact Assessment and 4) the Record of Processing Activities, as required by GDPR article 30. The two first are managed in WP2, respectively T2.1 and T2.2, while the third one is the expected outcome of T4.2. Finally, the fourth privacy and personal data protection technology has been introduced as part of the overall platform, so can be considered as an outcome of T5.2. All these services have been already successfully released. **Linked WPs: 2, 4, 5; Owner: LIST**		
iKPI-1.2	**At least six (6) standards, regulations and directive incorporated within SENTINEL**	**Achieved**

<table>
<tr><td colspan="3">This iKPI is directly linked with KR-5.3, please refer to Sec. 2.5; KR-5.3 <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-1.3</b></td><td><b>At least 40% improved privacy compliance efficiency for SMEs/MEs</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-1.2, please refer to Sec. 2.1; KR-1.2 <b>Linked WP: 2; Owner: LIST</b></td></tr>
<tr><td><b>iKPI-2.1</b></td><td><b>More than 20 entities CERTS / CSIRTS engaged by the end of the project</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">TUC tracked the CERTS/CSIRTS engaged with SENTINEL for the duration of the project. In this context, TUC and other SENTINEL partners contacted several H2020 European projects (e.g., CONCORDIA, JCOP, CyberExchange) and promoted the dissemination of the project’s results. A considerable number of the liaised organizations including CERT/CSIRT teams approached are 21 which are presented below:
- JCOP project
o Hellenic Ministry of Digital Governance (NCSA)
o Digital Security Authority of Cyprus (DSA)
o Norwegian National Security Authority (NSM)
- CyberExchange project
o CZNIC CSIRT.CZ
o Directoratul National De Securitate Cibernetica (DNSC)
o Slovak Computer Emergency Response Team (SK-CERT)
o Computer Incident Response Center Luxembourg (CIRCL)
o FORTHcert
- CONCORDIA project
o DFN CERT
o CERIT Scientific Cloud (CERIT-SC)
- CERTS/CSIRTS engaged during CyberHOT 2022, 2023 summer schools
o SPACE HELLAS
o Mediterranean Shipping Company (MSC)
o AEGIS
o AIRBUS
o PDMFC
o Focal Point (FP)
- CERTS/CSIRTS engaged during other SENTINEL events
o Bournemouth CERT (BU-CERT)
o GRNET
o Raven Cybersecurity
o Dienekes
o ZELUS
Also, TUC members are members of the Forum of Incident Response and Security Teams (FIRST), where more CERTs can be reached. <b>Linked WP: 7; Owner: TUC</b></td></tr>
<tr><td><b>iKPI-2.2</b></td><td><b>More than 8 Digital Innovation Hubs engaged by the end of the project</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-5.4, please refer to Sec. 2.5; KR-5.4. <b>Linked WP: 6; Owner: UNINOVA</b></td></tr>
<tr><td><b>iKPI-2.3</b></td><td><b>More than 20 novel services, tools and modules within the SENTINEL platform</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-3.1, please refer to Sec. 2.3; KR-3.1. <b>Linked WPs: 2; 3; 4 Owner: FP</b></td></tr>
<tr><td><b>iKPI-3.1</b></td><td><b>At least three (3) improved business model developed within the SENTINEL project</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">The preliminary business model was presented in D7.2, as part of the ongoing process related to T7.1. An intermediate update of the market analysis and the business model was performed in the context of D7.7 “Exploitation strategy, standardisation activities and best practices – interim version” (M18). In Y3, further outcomes of T7.1 and T6.4 have been collected and reported in D7.9 “Final business model, market analysis and long-term sustainability report” (M36) and D6.3 “Assessment report and impact analysis” (M36). <b>Linked WP: 7; Owner: AEGIS</b></td></tr>
</table>

iKPI-3.2	**At least 40% reduction of compliance – related costs**	**Achieved**
This iKPI is directly linked with KR-1.3, please refer to Sec. 2.1; KR-1.3; **Linked WP: 6; Owner: STS**		
iKPI-4.1	**At least 4 tools reach market readiness level eight (8)**	**Partially achieved**
This iKPI is directly linked with KR-6.2, please refer to Sec. 2.6; KR-6.2; **Linked WPs: 2-5; Owner: FP**		
iKPI-4.2	**More than 10 critical aspects addressed to ensure long-term sustainability**	**Achieved**
This iKPI is directly linked with KR-6.4, please refer to Sec. 2.6; KR-6.4; **Linked WP: 5; Owner: INTRA**		
iKPI-4.3	**10.000 smaller enterprises entities and third parties reached**	**Achieved**
Regarding iKPI4.3, all the dissemination and communication activities conducted since M1, are seen as actions to reach out to SMEs and third parties. In particular, the events organized by SENTINEL (1st, 2nd, 3rd SME-centric workshops, 1st clustering webinar, MVP demonstration workshop, “A privacidade e a proteção de dados pessoais no panorama nacional das PMEs” webinar) have reached more than **200 participants** in total. We believe that our participation in major events (such as IoT week, Madeira digital transformation summit, FIC Forum (both in 2022 and 2023)) strongly contributed towards this iKPI as well. For example, the FIC event reports more than **13.000 participants** every year while the last edition of IoT week attracted about **1.600 participants**. The Madeira digital transformation summit has received more than **300 registrations** the Infoshare 2024 reported more than **6.500 attendees.** Regarding the outreach of third parties through the SENTINEL social media, the numbers indicate good progress towards this KPI as well: in LinkedIn, we reached more than **1500 unique visitors,** in Twitter, we’ve reached more than **12000 visits,** in our YouTube channel we reached around **3000 views** while in the SENTINEL Zenodo Community we recorded more than **670 views.** Considering such numbers for the entire project duration, we can estimate that we successfully achieve this KPI. **Linked WP: 7; Owner: UNINOVA**		
iKPI-9	**At least four (4) innovative technologies advanced within SENTINEL**	**Achieved**
SENTINEL combines a set of tried-and-tested innovative solutions (MITIGATE, Security Infusion, CyberRange, GDPR CSA etc) that are further advanced throughout the project, with a set of components/modules newly developed within the project (IdMS, DPIA, etc). During Y2, the consortium has made significant progress in advancing at least six technologies by integrating them within the 1st integrated version of the SENTINEL platform and anticipates that both the newly developed technologies, as well as the technologies already brought by partners will lead to further advancements. During Y3 the advancement activities of these technologies continued and finalised in M30 when the 2nd version of the SENTINEL platform is released. The work has been reported in D2.3; D3.3; D4.3 and D5.6. **Linked WPs: WP2-WP4; Owner: ITML**		
iKPI-10	**At least five (5) cases testing and validating the innovative capacity of the SENTINEL’s offerings**	**Achieved**
As mentioned previously in KR-4.3, in the frame of WP6 activities, SENTINEL has managed to connect with **25 demonstrators** who conducted an end-to-end validation towards the SENTINEL tools during the three Pilots operations and the physical final SME-centric workshop. These demonstrators have created 12 Processing Activities (PAs) by validating the innovation capacity of the SENTINEL platform. The respective activities are thoroughly presented in D6.2 and D6.3 **Linked WP: 6; Owner: UNINOVA**		
iKPI-11.1	**At least 20 third-party entities (SMEs/MEs) directly using SENTINEL’s tools/services**	**Achieved**
Since the launch of the project the consortium partners have approached SMEs in several targeted events (5 SME-centric workshops, several talks and events co-organised with DIHs and relevant projects) outlining the project objectives and main project offerings. Aiming to intensify the SME’s engagement, in Y2, UNINOVA has engaged with three (3) and in Y3 two (2) more DIHs in addition to previously engaged five (5) by increasing the number of potential channels for inviting more SMEs to test the final release of the SENTINEL platform. As a result, two successful SME-centric workshops were organised in Y3. The fourth SME-centric workshop was conducted online in September 2023, and the fifth and final workshop was held in person in February 2024. Across these five (5) workshops, **twenty-three (23)** third-party companies participated in the SENTINEL applicability validation activities, by testing and providing feedback on the SENTINEL tools/services. **Linked WP: 7; Owner: STS**		

<table>
<tr><td><b>iKPI-11.2</b></td><td><b>At least 10% increase of market share for SMEs/MEs exploiting SENTINEL</b></td><td><b>Partially achieved</b></td></tr>
<tr><td colspan="3">By nature, this ambitious iKPI cannot be completed within the timeframe of the project as it reflects a long-term vision of the SENTINEL project. Nevertheless, in Y3, during the final SME-centric workshop the external SMEs/MEs members were asked to comment on the project’s possible future impact on their companies’ market share. Based on the collected responses approx. 42% of SME representatives anticipated that exploiting SENTINEL could potentially increase their organisation’s market share from 5% up to 15% in the coming years. In more detail
• 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%.
These findings suggest that the exploitation of SENTINEL, particularly when coupled with reallocating budgets to other areas like marketing, can, in some instances, increase sales and, consequently, market shares. <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-12.1</b></td><td><b>At least four (4) start-ups and spin-offs boosted exploiting SENTINEL security services</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">One way of interpretation that a start-up or a spin-off is boosted exploiting SENTINEL security services, is by gaining security, GDPR and data protection awareness, which can contribute to enhancing their business's overall security and GDPR compliance. Below are 4 start-ups and spin-offs that have been boosted by their participation in the various SENTINEL workshops, as evidenced by their relevant feedback confirming this:
1. DOT SYNTAX (https://www.dotsyntax.gr/)
2. DIENEKES (https://www.dienekes.eu/)
3. CYBERALYTICS (https://cyberalytics.com/)
4. Knowledgebiz (https://knowledgebiz.pt/)
<b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-12.2</b></td><td><b>At least 15% increase in sales for the pilot partners exploiting the SENTINEL platform</b></td><td><b>Partially achieved</b></td></tr>
<tr><td colspan="3">By nature, this ambitious iKPI cannot be completed within the timeframe of the project as it reflects a long-term vision of the SENTINEL project. Nevertheless, the SENTINEL platform was thoroughly trialled and evaluated by two pilot partners of the project, CG and TIG. Both partners completed a questionnaire based on the premise that exploiting SENTINEL would lead to reduced compliance costs, thereby freeing up budget for their organisations to allocate elsewhere. The potential areas they collectively identified for reallocating the freed-up budget include:
1. Marketing and Advertising: Invest in targeted advertising campaigns, social media marketing, search engine optimization (SEO), and other promotional activities to increase brand visibility and attract more customers.
2. Sales Training and Development: Provide additional training and resources for sales teams to improve their skills, enhance customer engagement, and increase conversion rates.
3. Product Development: Allocate funds towards research and development to introduce new products or improve existing ones, catering to evolving customer needs and preferences.
4. E-commerce and Online Presence: Enhance the organization's e-commerce platform, website, and digital infrastructure to facilitate smoother transactions, improve user experience, and capture a larger share of online sales.
5. Market Research: Conduct thorough market research to identify emerging trends, understand customer preferences, and stay ahead of competitors, enabling targeted strategies to boost sales.
6. Customer Service Enhancement: Allocate resources towards improving customer service channels, response times, and overall satisfaction levels, fostering positive word-of-mouth and repeat business.
Additionally, they both strongly agreed that “with the expertise and capabilities gained through SENTINEL, they are poised to provide more secure and GDPR-compliant services and products, which</td></tr>
</table>

we plan to highlight in our advertising campaigns." Considering all the above, one of the partners anticipates that exploiting SENTINEL will result in a minimum increase in sales in the upcoming years by 20%. TIG SMEs anticipated 5% increase in sales in the upcoming year. Due to the specific nature of their business, TIG does not believe that their increase in sales can be impacted by these kinds of factors. However, it is important to recognise that SENTINEL will provide critical assurance of compliance with the GDPR for commissioning purposes, as defined by UK Government (Part O: Data Protection). Therefore, SENTINEL offers TIG SMEs enhanced diligence and oversight in managing GDPR responsibilities, which helps to secure tendering opportunities with local authorities. **Linked WP: 7; Owner: STS**

4.2 Measures to maximize impact

4.2.1 External Advisory Board (EAB) and Ethical & Data privacy Advisory Committee (EDAC)

The main task of the SENTINEL External Advisory Board is to provide external, independent analysis and recommendations on the project achievements and to bring additional competencies towards a full achievement of the SENTINEL objectives. The responsibilities and duties of the EAB include connecting the project outcomes with potential users of the developed solutions, other projects and research initiatives, policy makers, and standardisation bodies, following the project development and providing necessary feedback, and contributing significantly with fresh ideas regarding the challenges and opportunities from the emerging research and from an industrial perspective. The SENTINEL External Advisory Board consists of four (4) independent members external to the SENTINEL consortium:

- **Mr Rodrigo Diaz,** Head of Cybersecurity Unit in ATOS Research & Innovation department, Barcelona, Spain.
- **Mr Toomas Lepik**, Senior Information Security expert, SME owner of IT Kool Ja Konsultatsioonid OÜ, Brussels, Belgium.
- **Prof. João Mendonça**, Ass. Professor in the Department of mechanical Engineering at the University of Minho (Portugal) with a strong link with SMEs.
- **Ms. Georgia Panagopoulou**, privacy ICT auditor at the Greek Data Protection Authority, Athens, Greece.

Apart from the EAB, SENTINEL has also established the SENTINEL Ethical & Data privacy Advisory Committee (EDAC). The main task of the EDAC members is to oversee, advise, assess and, when applicable, raise concerns to the PC and consortium partners on relevant ethical issues within the project, with a special focus on the processing of personal data. Another important aspect is to identify guidance and regulations with which SENTINEL should comply, such as Data Protection Policy, Informed Consent Form policy, ETSI guidance notes, ISO/IEC 17799 data security. The SENTINEL EDAC consists of three (3) independent members.

- **Prof. Fereniki Panagopoulou:** Assistant Professor of Constitutional Law, Panteion University, Athens, Greece.
- **Dr. Tania (Konstantina) Kyriakou**: Dr. Kyriakou has a well-demonstrated track record on data protection law, EU law and cultural heritage law. Dr. Kyriakou has a full membership of EDAC, as she has already worked on several tasks for the EDAC as a deputy member.
- **Dr. Tal Soffer**: Head of the unit of Technology and Society Foresigh, Tel Aviv University, Israel.

During Y3, EDAC has successfully updated the Ethics Manual and Ethical Controlling reports, which comprised D8.15 delivered in M36. For this purpose, the EDAC team has prepared and shared the Ethical and Legal Issues template partners to record their legal and ethical policies in terms of personal data protection. The process involved also holding several meetings among the three EDAC members to draft the Ethical and legal controlling form, which was distributed to all SENTINEL partners. The form aimed to serve as a blueprint for the SENTINEL partners to record their legal and ethical policies in terms of personal data protection.

In Y3, the final EAB meeting took place during the second day of the SENTINEL's 7th plenary meeting, gathering three (3) out of four EAB members. The purpose of the meeting was to present the main achievements and after life demonstration of the final SENTINEL platform, receive feedback on the work conducted. The meeting took place right after the Final-SME centric workshop helping the EAB members to participate the workshop and act as end-users so to provide feedback and valuable recommendations after testing the SENTINEL platform. The feedback received was extremely positive. Several recommendations received are mainly towards the advancement of the SENTINEL platform with respect to UI/UX and other topics, so the value of the project is well understood among interested parties. As the EAB members tested and acted as end-users their feedback and recommendations are presented and elaborated in D6.3 in more detail.

4.2.2 Communication and dissemination activities conducted in Y3

In Y3, SENTINEL social media channels have been engaging with different users almost daily (please refer to the dissemination dKPIs identified in the tables below). The 3rd year resulted in the consolidation of our SENTINEL YouTube channel, which has been used to promote SENTINEL videos and the SENTINEL podcast series.

As previously mentioned, in Y3 SENTINEL has participated in eleven (11) events: the PUZZLE's Cybersecurity Conference, Final Event of the CitySCAPE project, 28th IEEE Symposium on Computers and Communications, IEEE International Conference on CSR, CyberHOT Summer School 2023, 30th EuroSPI Conference, ATTRACT EDIH public presentation, AIP Roadshow I&D, Data Protection Day, Cyber Threat Intelligence: Empowering IoT Security Workshop and INFOSHARE Conference.

Regarding the organization of events, SENTINEL has organized four (4) additional events: 4th and 5th SME-centric Workshops, Cyber Security and Data Protection Synergies – Joint Cluster Event and the SENTINEL Final Event.

In Y3 SENTINEL has continued promoting synergies with cluster projects with fourteen (14) projects engaged. With this respect, besides the organization of physical meetings, we also promote the development of two (2) joint publications on policy priorities, four (4) joint newsletters and joint training sessions on projects technical innovations.

The visibility of the project and transferability of the project outcomes has been promoted through the generation of promotional material. In this context, four (4) additional SENTINEL newsletters were released within Y3, highlighting some of the SENTINEL components as part of the SENTINEL technical suite, but also dissemination and communication achievements. Several SENTINEL videos and podcasts were also released and are available under the SENTINEL YouTube channel.

With respect to academic publications, SENTINEL has published four (4) conference papers, 1 electronic journal paper, 1 journal paper in Internet of Things Journal. In addition, 2 journal papers are accepted to be published in "Journal of Surveillance, Security and Safety" and "International Journal of Information Security", 1 journal paper already submitted and currently the consortium is working on 2 journal papers to be submitted by the end of the project.

The WP7 bi-weekly meetings also take place regularly, where all partners were requested to join and discuss actions for communication and dissemination activities. The SENTINEL social media channels are also constantly being updated, increasing the number of visitors and followers daily.

The following table lists the dKPIs related to communication and dissemination activities and summarizes the progress in Y3 and main achievements during the entire lifespan of the project.

Table 15. SENTINEL Website - KPIs status update

<table>
<tr><td rowspan="7"><b>SENTINEL website</b></td><td><b>dKPI</b></td><td><b>Frequency</b></td><td><b>Threshold</b></td><td><b>Status</b></td></tr>
<tr><td>dKPI#1: Number of visitors</td><td>Monthly</td><td>≥ 100</td><td><b>Achieved</b></td></tr>
<tr><td colspan="4">To address this KPI, digital content was regularly created and partners were encouraged to share with their local network to enhance the number of visitors and widen the demographic area of visibility. During Y1, we had <b>932 number of visitors</b>, which is approximately <b>77 visitors monthly</b>. Most of the users were from the coordinator's country (EL) with a significant number of users coming from the United States, Portugal, United Kingdom and China, showing a relatively broad impact area for SENTINEL. In the second year (<b>M13-M24</b>) we had <b>1544 number of visitors</b>, which is approximately <b>128 visitors monthly.</b> In the third year (M25-M36), we had <b>2633 number of visitors</b>, which is approximately <b>219 visitors monthly</b>. In average we had <b>141 visitors monthly in the duration of project.</b></td></tr>
<tr><td>dKPI#2: Number of page views</td><td>Annually</td><td>&gt;5000</td><td><b>Achieved</b></td></tr>
<tr><td colspan="4">To address this KPI, the approach was the same as in dKPI#1, since the two are highly related. In the first year (<b>M1-M12</b>), the <b>number of the SENTINEL website views</b> was <b>4,502.</b> This was highly related to the fact that it was the first year of the project, where awareness and loyalty starts being built. For the second year of project (<b>M13-M24</b>) the <b>number of the SENTINEL website page views increased significantly by reaching to 6.498</b>, and the project achieved more than the expected KPI with 11.000 page views in total. During the Y3 (<b>M25-M36</b>) the <b>number of the SENTINEL website page views</b> increased significantly by reaching <b>36,000.</b> The overall result is <b>15.500 views annually.</b></td></tr>
<tr><td>dKPI#3: Number of downloads</td><td>Monthly</td><td>&gt;500</td><td><b>On track</b></td></tr>
<tr><td colspan="4">To address this KPI, all scientific material, presentations, as well as public deliverables, were made available on the website for the audience's reference and easy access. The <b>total number of downloads</b> of our material is <b>120 in Y1.</b> In the second year (<b>M13-M24</b>), we had <b>285 files downloaded</b>, totalizing 4<b>05 downloads</b> since the beginning of the project. During the Y3, the communication regarding the material downloads toward events, mails and social media was increased, resulting in a great progress in this KPI. The number of downloads during the Y3 was <b>15,000 downloads</b>. The consortium also took advantage of the Zenodo Open Access repository[11] as well and made all scientific material, presentations, and public deliverables available for the audience's reference via this channel too. The overall result is <b>16,500 downloads</b> in total. This impressive growth highlights the influence of SENTINEL's publications within the scientific community, the effectiveness of the project's dissemination activities and its active presence in social media channels in the last project year. This KPI is considered to be well on track in Y3 and ~95% achieved since the launch of the SENTINEL website.</td></tr>
</table>

Table 16. SENTINEL Social Media:Twitter - KPIs status update

<table>
<tr><td rowspan="3"><b>Twitter</b></td><td><b>dKPI</b></td><td><b>Frequency</b></td><td><b>Threshold</b></td><td><b>Status</b></td></tr>
<tr><td>dKPI#4: Number of followers</td><td>Monthly</td><td>&gt;20</td><td><b>On track</b></td></tr>
<tr><td colspan="4">The <b>number of followers</b> in Twitter during Y1 was <b>183</b>, which equals to approximately <b>15 monthly</b>. This was highly related to the fact that it was the first year of the project, where awareness and loyalty starts being built. In Y2, <b>the number of followers</b> in twitter was <b>287,</b></td></tr>
</table>

[11] https://zenodo.org/communities/sentinel-h2020/search?page=1&size=20

	which equals to approximately **23 monthly.** In Y3, **the number of followers** in twitter was not possible to properly report for the entire M25-M36 period associated with Twitter to X changes. Nevertheless, we recorded **132 additional followers** during Y3**,** which equals to approximately **11 monthly.** In average we had 17 followers monthly counting ~85% completion since the launch of the SENTINEL twitter page.			
	dKPI#5: Number of push announcements	Monthly	≥ 20	**Achieved**
	To address this KPI, we tried to curate interesting and relevant content. However, this was not always possible; therefore, the average **number of tweets** per month deviated from the target and was approximately **9** for Y1 (M12 data). In Y2, the **number of tweets** per month was approximately **17**. In Y3 the **number of tweets** per month was approximately **34**. The overall result is ~20 tweets monthly**.**			
	dKPI#6: Number of unique visitors	Monthly	≥ 30	**Achieved**
	Although the twitter analytics provide no information about unique visits, we keep monitoring the total number of visitors via this channel. In Y1, we recorded 2,313 twitter visitors (approximately **192 visitors monthly**). In Y2 (M13-M23 data) we recorded approx. 3,500 twitter visitors (approximately **290 visitors monthly).** In Y3, the Twitter analytics changed to X, and this metric (visitors) was not reported by the platform. Considering the previous results, this KPI was 100%.			

Table 17. SENTINEL Social Media: LinkedIn - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Status**
LinkedIn	dKPI#7: Number of followers	Monthly	>20	**Achieved**
	The **number of followers** in LinkedIn during Y1 was 534, which accounts for approximately **44 monthly**. In Y2, the **number of follower**s in LinkedIn was **272**, which accounts for approximately **22 monthly**. In Y3, the **number of follower**s in LinkedIn was **177**, which accounts for approximately **15 monthly**. The overall result is **27 monthly**.			
	dKPI#8: Number of push announcements	Monthly	≥ 20	**Achieved**
	To address this KPI, we tried to curate interesting and relevant content. However, this was not always possible; therefore, the average **number of push announcements** per month deviated from the target and was approx. **11** for Y1. In Y2, we achieved approx. **18** (M24 data). In Y3, with event participation and the Secure Cyber Cluster group, we produced relevant content for the audience, and we achieved approx. **31**. The overall result is **20 push announcements monthly**.			
	dKPI#9: Number of unique visitors	Monthly	≥ 20	**Achieved**
	In Y1, we recorded approx. **60 visitors monthly** (M11 data)**.** In Y2, we recorded approx. **45 unique visitors monthly**. In Y3, we recorded approx. **29 unique visitors monthly**. The overall result is **44 monthly unique visitors**.			

Table 18. SENTINEL Brand-building material - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Status**
Brand-building material	dKPI#10: Number of distributed hard copies of the SENTINEL brochure	End of project	1000 distributed in ≥10 events	**Achieved**
	Up to now, the SENTINEL consortium has produced SENTINEL brochures and has distributed approximately **80 brochures** to more than **three (3) physical events**. Unfortunately, the COVID-19 pandemic has forced many events to be held online in Y1. In Y2, we participated in more than eight **(8) physical events** and were able to distribute more materials through participants, which totalized more than **480** distributed brochures in the second year. During Y3, SENTINEL has organized **3 physical events** and has participated in seven **(7) third-party events** by distributing approx. **500 brochures**. In total, SENTINEL distributed **>1000 brochures** in more than **18 events**.			

	dKPI#11: Number of electronic SENTINEL brochures	End of project	≥1000 downloads	**Achieved**
	To address this KPI, the SENTINEL consortium has continued to create a number of informative materials such as flyer, brochure, newsletters (all available in the SENTINEL's website) in Y3 as well. Based on the tendency of people to read and "save" whatever they are most interested in terms of interesting material, we decided that "views" is a more relevant aspect to track for this KPI compared to "downloads". This KPI was recorded **426 views** of all our electronic material in Y1 and **555 views** in Y2. In Y3, the consortium took advantage of the Zenodo Open Access repository[12] and made all informative materials available for the audience's reference via this channel too. As a result, we achieved more than **1,300 views/downloads** for the entire project duration.			
	dKPI#12: Regular newsletters	End of project	≥9 newsletters	**Achieved**
	In Y1 and Y2, we have released six (**6) high-quality newsletters**, while in Y3 we released **four (4)** additional newsletters. Thus, reaching a total number of **10 newsletters.**			
	dKPI#13: Number of SENTINEL videos and number of views	End of project	3 videos with >1000 views each	**Achieved**
	In Y1, we released the first promotional video of SENTINEL. In Y2, we released more than 14 video materials (including the SENTINEL podcasts) on our channel, with a total of **535 views**. For Y3, we released 5 videos and 3 podcasts and releasing **23 video materials with >3000 views** in total.			

Table 19. SENTINEL publications and conference presentations - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Status**
Journal/ magazine publications and Presentations in International Conferences	dKPI#14: Number of international referred journal publications by SENTINEL partners	End of project	>6	**Achieved**
	In Y3, the consortium worked hard in order to prepare and publish scientific publications and dissemination the SENTINEL outcome in relevant scientific communities. As a result, we have published 2 journal papers, submitted 3 papers among which two (1) are already accepted and currently working on two (2) papers to be submitted by the end of the project.			
	dKPI#15: Number of special issues in international referred journals	End of project	>2	**Achieved**
	Regarding this dKPI, we achieved 2 special issues in well-acclaimed international journals in Y3.			
	dKPI#16: Number of publications in international (printed or online) magazines	End of project	>6	**Achieved**
	In Y1 and Y2 SENTINEL has published **four (4) different conference proceedings.** In Y3 we have published four (4) papers in four conference proceedings. In total we have published eight (8) conference papers.			
	dKPI#17: Number of conference presentations by SENTINEL partners	End of project	≥12	**Achieved**
	Regarding this KPI, SENTINEL has participated in **seven (7) conferences** in Y1 and Y2. In Y3, SENTINEL was presented in **four (4)** SENTINEL scientific conferences, and we've made 1 project presentation in **one (1) industrial conference.**			

Table 20. SENTINEL Third-party events - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Status**

[12] https://zenodo.org/communities/sentinel-h2020/search?page=1&size=20

Third-party events	dKPI#18: Number of events	End of project	≥15 events with >60 attendees	**Achieved**
	To address this KPI, the consortium worked as a team and each partner utilised their network and individual dissemination plans. Within the first and second years of the project, SENTINEL participated in **15 large events** with > 60 attendees. In the 3rd year SENTINEL participated in **seven (7) additional events** with >60 attendees.			
	dKPI#19: Number of audience contacts	End of project	≥50% of the participants	**Achieved**
	During Y3 we keep on engaging with the different audience participants in the several events where we have participated. The KPI was on average accomplished with approximately 50% of the participants registered as audience contacts.			
	dKPI#20: Number of participants interested in SENTINEL project	End of project	≥40% of the participants	**Achieved**
	Similar to dKPI#19, to address this KPI we utilised a combination of means such as online surveys, personal contacts and website statistics on the day of an event or at any other occasion where we made contact with potential SENTINEL stakeholders. The KPI was on average accomplished during Y1 and slightly overachieved during Y2 with approximately 45% of participants demonstrating their interest in SENTINEL. In Y3, we kept monitoring this dKPI and recorded our stakeholders' attitude during the 4th and 5th SME-centric workshops as presented in D7.6.			

Table 21. SENTINEL events - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Status**
SENTINEL Events	dKPI#21: Number of events organised by SENTINEL partners	End of project	≥8 events with ≥60 attendees and 3 events with ≥100 attendees	**Achieved**
	The consortium worked as a team and each partner utilised their network and individual dissemination plans. Within the first year of the project, SENTINEL has organized **two (2) SME-centric workshops** and **1 (one) clustering webinar** with **≥60 attendees.** Furthermore, our collaboration with DIHs supported the organization of **one (1)** more webinar entitled "A privacidade e a proteção de dados pessoais no panorama nacional das PMEs" where we had **≥ 70 registrations** for the event. During Y2, we organised the **3rd SME-centric** workshop, **one (1) Workshop**/Training session with SMEs for MVP demonstration with **≥100 registrations** in total. Furthermore, with AI4HealthSec and HEIR H2020 projects we co-organized **an international workshop** on Information & Operational Technology (IT & OT) Security Systems took place on the 23rd – 26th of August 2022. This workshop took place in conjunction with the 17th International Conference on Availability, Reliability, and Security (ARES 2022). The event reported ≥**100 attendees**. During Y3, we have organized the **two (2)** additional SME-centric workshops (**4th and 5th workshops**) with **≥80 actual participants. One (1) Joint Cluster Event** and the **SENTINEL Final Event** engaging approx. 100 participants.			
	dKPI#22: Number of audience contacts	End of project	≥50% of the participants	**Achieved**
	To address this KPI we utilised a combination of means such as online surveys, personal contacts and website statistics on the day of the event. This KPI was on			

	average accomplished with approximately 50% of the participants registered as audience contacts.			
	dKPI#23: Number of participants interested in SENTINEL project	End of project	≥50% of the participants	**Achieved**
	In Y2 during the 3rd workshop where the SENTINEL MVP demonstration took place 42% of attendees expressed interest about the SENTINEL project by answering that they could consider investing in tools/services similar to SENTINEL within the next 2 years. In Y3 during the 4th and 5th SME-centric workshops where the SENTINEL FFV demonstration took place more that 50% of attendees expressed interest about the SENTINEL project by answering that they could consider investing in tools/services similar to SENTINEL within the next 2 years.			

Table 22. SENTINEL Liaisons and networking - KPIs status update

	dKPI	Frequency	Threshold	Status
Liaisons and networking	dKPI#24: Number of SENTINEL members actively networking with other relevant projects	End of project	≥6	**Achieved**
	For this dKPI tangible outcomes observed since Y1. All SENTINEL partners have leveraged their network and participation in other projects and facilitated the 1st Clustering Webinar, which was organised by SENTINEL and hosted other **9 EU Horizon projects**, funded under the H2020-SU-DS-02 and H2020-SU-DS-03 topics. As a result, we started actively negotiating with 10 SENTINEL relevant projects since Y1. In addition to this, in Y2, we engaged with **four (4)** and in Y3 with **three (3) more** new projects. In total, SENTINEL actively collaborated with **17 projects.**			

Table 23. SENTINEL Standardisation/regulation relevant activities- KPIs status update

	dKPI	Frequency	Threshold	Status
Standardisation and regulation	dKPI#25: Number of "EAB" members monitoring and ensuring compliance with relevant regulations	End of project	At least two (2) members of EAB	**Achieved**
	In the project we have secured the participation of four (4) EAB members from the industry and academia. The first EAB meeting was held in Y1 while the second EAB meeting took place in Y2 during the 5th plenary meeting. In Y3 we've conducted a EAB meeting during the 7th plenary meeting. All meetings had a special open discussion session where we obtained feedback, comments and recommendations. Furthermore, the Ethics Advisory and Data privacy Committee (EDAC) of SENTINEL kept regular monitoring and undertakes necessary activities to ensures that SENTINEL (deliverables, innovation activities etc.) meets national legal and ethical requirements aligned with relevant regulations.			

4.2.3 Exploitation strategy and activities conducted in Y3

The SENTINEL exploitation activities have deeply intensified in Y3. Particularly in Y3 the SENTINEL exploitation activities were focused on the following actions:

- Organisation of further SME-centric workshop and engagement with potential SMEs for further exploration of the SENTINEL platform. In Y3, the 4th and 5th SME-centric workshops took place aiming at showcasing the SENTINEL platform and revealing external SMEs willingness/intention to adopt and use the SENTINEL integrated solution.

- Creating an SME-centric questionnaire distributed to the above SME/ME participants to better reflect aspects, such as their awareness of GDPR obligations, their needs, challenges, application domain, etc.
- Liaising with similarly themed projects to ensure common exploitation pathways and synergies. Like Y2, special communications and discussions took place in Y3 as well and the efforts culminated with one (1) clustering webinar, where more than 10 project representatives elaborated on outcomes, offerings and innovations of their projects and discussed openly common exploitation & dissemination possibilities.
- Further exploration of individual components and technology offerings provided by the project partners.

In Y3, we have culminated the SENTINEL exploitation strategy and plan. The exploitation manager released the 2nd exploitation questionnaire and collected partners exploitation activities conducted in the last project period as well as renewed exploitation interest of the project partners. Based on the collected results, the SENTINEL individual exploitation plans were updated and finalised. Furthermore, the SENTINEL joint exploitation strategy was formulated by defining a long-term vision for SENTINEL and identifying the consortium partners' interests in collaborating for the commercial exploitation of SENTINEL. Whether it is industrial, commercial or research, the project partners spotted various opportunities to leverage the project's outcomes in their ongoing and/or future activities. To highlight these opportunities, technology and knowledge transfer actions from the individual viewpoint perspective D7.8 illustrates updated exploitation strategies reported by all the SENTINEL partners including both current and future exploitation activities as well as outlines the terms and conditions under which the project's will be leveraged to tap into commercial business opportunities for the post-project phase.

Regarding our activities supported by the Horizon Results Booster initiative, after successfully realizing the two modules **Module A** "Identifying and creating the portfolio of R&I project results" and **Module C** "Assisting projects to improve their existing exploitation strategy" as part of Service 1 "Portfolio Dissemination & Exploitation Strategy" the exploitation manager has applied for **Business Plan Development (BPD) service**[13] aiming at getting guidance and support to SENTINEL's consortium in preparing the project results for the market. As a result, we received advice and guidance from exploitation experts on how to prepare the ground for exploiting the SENTINEL platform and its services and to enhance partners' competence in enriching their exploitation strategy. The outcome of this service has been reported in D7.8 "Exploitation strategy, standardisation activities and best practices – final version".

[13] https://www.horizonresultsbooster.eu/ServicePacks/Details/7

5. Innovations

SENTINEL innovations have been described in a number of deliverables already within the first year of the project; D1.1 stated SENTINEL's consortium's intention to go beyond SOTA in a number of technologies and methodologies. D1.2 gave an overview of the TRL of the current SENTINEL modules, contexts and plugins to be used as a benchmark for what we aim to achieve. D7.2 provided a high-level overview of the business model to be used to exploit SENTINEL.

During Y2, and after the SENTINEL MVP release, the consortium has proceeded with respect to the project's product definition by updating the SENTINEL business model and value proposition elaborating on the project's main offerings, which provides the foundation for innovation management and exploitation activities. These offerings have been investigated more in parallel with the project's technical developments. The SENTINEL consortium has further defined its innovations and track their progress utilizing the Innovation Radar Methodology[14] and leveraging the related questionnaire and instructions for its analysis. As a result, a preliminary Technology and Innovation Radar was constructed based on the technologies and innovations identified with respect to their potential and maturity. Key internal milestones to construct the Radar were the release of the SENTINEL 1st integrated solution (M18-MS3) and the initial demonstration and assessment of the SENTINEL platform and technologies (M24-MS4). Consequently, we delivered D8.12 which presents i) the list of technological innovations and their convergence in SENTINEL, ii) Technical and Innovation Strategy Plan, iii) innovation management approach including a thorough assessment framework of project innovation. It is worth mentioning that this work was used as input not only to manage innovation strategy of the project but also for the overall exploitation and long-term sustainability plan as well as for the individual exploitation plans of each consortium partner for their future developments and their contribution to the European Economy. To this end, D7.5, D7.7 and D5.5 (in addition to D8.12) have been prepared and released showing a strong link between innovations and activities within T7.1, T7.3, T7.4, T8.3 as well as T5.3.

In the last project year, the SENTINEL Innovation Radar has been revisited to decide on whether the technologies and innovations identified in the project progressed and moved further in terms of maturity. This analysis was facilitated through the 2nd exploitation survey launched within the scope of T7.3 "Exploitation and standardisation activities and best practices towards a holistic privacy-by-design European solution" (details on the questionnaire are available in D7.8 "Exploitation strategy, standardisation activities and best practices – final version"). Based on the final assessment of the Innovation Radar, we concluded that, beside the SENTINEL integrated solution, other twelve (12) innovative candidates of the SENTINEL project can be exploited independently as Key Exploitation Results. Furthermore, several KIRs moved to the **"Assess"** stage: indicating that they have become promising, and it is worth exploring with the goal of understanding their impact in the near future. While some KIRs are currently in the **"Trail"** phase are worth pursuing and it is worth investigating these KIRs further to understand their weaknesses and strengths. The consortium partners are committed to keep on working on these KIRs to better-shaped innovations beyond the scope of the SENTINEL project since they are in line with their research and commercial interests.

[14] https://www.innoradar.eu/methodology

A detailed description of technical and innovation progress, innovation management results as well as final technology and innovation radar are presented in D8.13 “The SENTINEL technical and innovation management report - final version”.

6. Conclusion

This document presents the work accomplished mainly during the third year of the project [M25-M36 (June 2023 to May 2024)]. It provides an overview of the consortium work achieved in the third and final year of the project elaborating on the project's main achievements regarding the project's objectives, key results, expected impact, innovations, communication, dissemination, and exploitation activities. The SENTINEL project had several intensive activities during this period in a sense of delivering tangible results and achievements. In particular, it illustrates i) activities that the SENTINEL project successfully accomplished in the Demonstration Phase (M19-M30) and Consolidation & Sustainability Management Phase (M31-M36).

In Y3, the project reached MS5 “Demonstration Fire” (M30) and MS6 “Consolidation” (M36) by delivering the final version of the SENTINEL integrated framework together with its technologies and services. In this regard, MS5 was accomplished by producing and successfully submitting nine (9) deliverables within WP2, WP3, WP4, WP5 and WP6 due M30 and MS6 was addressed by submitting ten (10) additional deliverables within WP5, WP6, WP7 and WP8.

During the final project phase (Consolidation & Sustainability Management Phase) the project partners joined their forces to conduct the final framework's evaluation and impact assessment, confirming the platform's effectiveness and providing a solid foundation for future improvements and innovations.

Furthermore, the partners conducted final dissemination and exploitation activities and deliver the corresponding final reports. In this regard, the SENTINEL partners organised two additional workshops (4th SME-centric and 5th SME-centric workshops) gathering very positive feedback on the SENTINEL offerings by highlighting a growing readiness among SMEs/MEs to adopt the SENTINEL solution. Moreover, SENTINEL has jointly organised its' final event together with the ARCADIAN-IoT project and had an outstanding performance in the final event at the InfoShare 2024 Industrial Conference. In Y3, we have culminated in the SENTINEL exploitation activities. An important milestone was successfully achieved by leveraging the Horizon Results Booster and Horizon Standardisation Booster initiatives that helped to formulate the SENTINEL joint exploitation plan and strengthen the project standardization activities. In this respect, the SENTINEL joint exploitation strategy helped to define a long-term vision for SENTINEL and outline the consortium partners' interests in collaborating for the commercial exploitation of SENTINEL. Whether it is industrial, commercial or research, the project partners spotted various opportunities to leverage the project's outcomes in their ongoing and/or future activities.

An important milestone was the finalisation of the SENTINEL business model. With the Business Model Canvas, we have visualised the SENTINEL's unique selling proposition and outlined initial financial analysis aligned with future activities that can be examined by the consortium towards the commercialisation of the SENTINEL offering.

The SENTINEL project, with its dedicated and ambitious partners, has made significant steps for bridging the security, privacy, and data protection gap. The project demonstrates accountability in handling personal data, in alignment with GDPR compliance and data protection impact assessments. Well-aligned with the initial expectations, SENTINEL primarily addresses the needs and challenges of SMEs of all industries in Europe although it can be useful also for larger enterprises, public authorities or any organisation which processes personal data.