SENTINEL

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

D8.1-Yearly project management report - first 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	D8.1- Yearly project management report- first version
Version	1.9
Date of Submission	31/05/2022
Main Editor(s)	Siranush Akarmazyan (ITML), Tatiana Trantidou (ITML), Anna Maria Anaxagorou (ITML)
Contributor(s)	Christos Dimou (ITML), Philippe Valoggia (LIST), Evangelia Kavakli, Yannis Skourtis (IDIR), Konstantinos Poulios (STS), Manolis Falelakis (INTRA), Manos Karampinakis (AEGIS), Giorgos Tsirantonakis (TSI), Thomas Oudin (ACS), Ruben Costa (UNINOVA), Christopher Konialis (CG), Daryl Holkham (TIG), Dimitra Malandraki (CECL), Eleni-Maria Kalogeraki (FP)
Reviewer(s)	Marinos Tsantekidis (AEGIS), Peri Loucopoulos (IDIR)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	08/04/2022	TOC	Confidential
1.1	14/04/2022	Draft	Confidential
1.5	20/05/2022	Draft	Confidential
1.6	27/05/2022	Draft	Confidential
1.8	30/05/2022	Draft	Confidential
1.9	31/05/2022	Final	Public

Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
CSA	Compliance Self-Assessment
CS	Cyber-Security
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
GA	Grant Agreement
GDPR	General Data Protection Regulation
IdMS	Identity Management System
ISMS	Information Security Management System
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
KoM	Kick-off Meeting
KPIs	Key Performance Indicators
KRs	Key Results
RE	Requirements Engineering
REA	Research Executive Agency
ROPAs	Records of processing activities
SME	Small – Medium Enterprise
ToC	Table of Contents
TRL	Technology Readiness Level
UI	User Interface
WG	Working Group
WP	Work Package

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 first 12 months period. Moreover, 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 and corrective actions for the Year 1 (Y1). Finally, it presents plans and next steps for the second year.

During the first 12 months of the project, all WPs and tasks were performed as described in the Grant Agreement (GA). Furthermore, within the first year, SENTINEL accomplished the Baseline Phase (M1-M8) resulting in a delivery of important outcomes for the project. It is worth mentioning that the phase is the driving force behind the project and provides direct input to the next phases of the project while serving also as a checklist for the whole work plan.

Though SENTINEL is in its early stage, (the project is approaching to the end of the first year of its life duration), all the actions performed during the first 12 months have managed to develop a more detailed and better-known image of SENTINEL. In this respect, the key achievements of the first year include:

- Setting up the project's baseline.
- Delivering the SENTINEL visuals (project website, promotional material, social media channels).
- Producing the project's handbook (first and interim versions).
- Producing the SENTINEL's experimental protocol and defining both functional and non-functional requirements and project's ambition.
- Revising the SENTINEL architecture by incorporating new capabilities through the use of plugin tools and new knowledge through external data sources.
- Performing market analysis and preliminary business modeling.
- Successfully delivering the SENTINEL Minimum Viable Product (MVP).
- Delivering the SENTINEL Data Management Plan and Ethics Manual.
- Establishing the Ethics Advisory and Data privacy Committee (EDAC).
- Producing risk identification, management and quality assurance plan.

During the first 12 months, 17 deliverables have been produced and successfully submitted to Research Executive Agency (REA). Nevertheless, there is still a very busy agenda to be implemented during the second year of the project, to reach the expected impact of SENTINEL. Currently, SENTINEL is at the Innovation Phase (M9-M18) conducting multiple parallel technical and non-technical activities aiming at the successful demonstration of the SENTINEL Minimum Viable Product during the 1st technical review meeting (M13), release of the 1st full featured SENTINEL technologies and services (M18). Regarding the non-technical activities, the phase includes the delivery of the initial report on pilot execution, dissemination strategy and exploitation activities. The milestone can be considered accomplished when the 1st integrated SENTINEL architecture is successfully delivered, the initial pilot execution and validation activities successfully accomplished and 13 more deliverables produced and submitted to the REA.

1. Introduction

1.1 Purpose of the document

The purpose of D8.1: Project Management Report (1st version) is to report on all the project activities executed during the first project year [from M1 (June 2021) to M12 (May 2022)] and present the planned activities for the second year of the project. 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 first 12 months, the SENTINEL consortium has managed to keep the initially defined time plan for all activities, in accordance with the plan specified in Annex 1 of the Grant Agreement. The partners of SENTINEL have paid their best efforts in all the WPs in which they have been involved in order to accomplish the expected tasks envisioned for the first project year. In this regard, this document is constructed in such a manner so as the reader can grasp key insights and get a complete image about the work carried out for all the work packages including the activities carried out per task and per beneficiary during the first 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.

The aim is to provide an overall overview of the project and help follow-up the different activities ongoing in the framework of the SENTINEL project. The release of such a document could serve as a reference point to get updates on the general status of the project, enabling visibility of the overall work accomplished by the whole team.

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 Y1 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, potential deviations and corrective actions for the reporting period.
- *Section 4* and *Section 5* cover the project main activities and achievements with respect to the expected impact, innovations, and communication, dissemination, and exploitation activities.
- *Section 6* wraps up the document with concluding remarks.

1.3 Intended readership

The report is part of WP8 “Project management” and is closely linked to all activities conducted in the SENTINEL WPs and tasks. It aims at reporting the progress and the consortium’s main

achievements within the first year towards the successful completion of all the project objectives, deliverables and milestones.

2. Project objectives: Explanation of the work carried out by the beneficiaries during the 1st 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 undertaken in WP2, WP3 and WP4, as well as the integration of respective components in WP5. More specifically, respective work during the first year of the project contributed towards the implementation of SENTINEL's unified privacy and personal data protection compliance self-assessment framework for GDPR compliance. The first version of GDPR Compliance Self-Assessment (CSA) was delivered via a module that performs an analysis of Processing Activities (PAs) to determine whether personal data are handled in accordance with data protection requirements. GDPR CSA provides SMEs with: a) GDPR Compliance Level of 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. In addition to this, work carried out in SENTINEL regarding its integrated IdMS was based on the decentralized MyData model for human-centric personal data management for SMEs/MEs, enabling a unified European Personal Data Space. The first version of the SENTINEL's IdMS was delivered. This is a first approach to IdMS ambitious goal to implement, among others, personal data portability and transparent vendor switching, among others. To this end, the SENTINEL MVP showcases a centralized identity management system with Single Sign-On capabilities for the SENTINEL end-users. The integration of the aforementioned tools into a platform that supports extensibility by design lays the foundation for the provision of a unified, end-to-end solution.

The table below provides a summary of the KRs related to Objective 1, including their status update, the activities conducted during Y1 and the strategy towards their successful completion.

Table 1. KRs status update - Objective 1

KR-1.1	**Successful integration and orchestration of SENTINEL technology offerings**	**In progress**
The refined architecture, as presented in D1.2, was designed to accommodate all SENTINEL offerings as well as providing the means for incorporating external ones in the form of plugins. Due to an integration-first approach that has been followed, interfaces and messaging formats as well as sequence diagrams have been defined and documented. As a result, we are very optimistic that all project technologies are going to be integrated successfully and on time. The MVP, described in D5.4 is the first integrated version of SENTINEL, with two more to follow in M18 and M30 and reported in D5.5 and D5.6 respectively. **Linked WP: 5; Owner: INTRA**		
KR-1.2	**40% improved compliance efficiency for SMEs/MEs**	**In progress**
This indicator is made of one variable which is still unknown, which is the average cost of compliance with data protection for SMEs. During the first year, we have conducted a thorough literature review to investigate the cost range for GDPR compliance for SMEs. This was proven to be a rather complex task, based on several factors; (a) GDPR compliance costs depend on the role of the SME (controller or processor), (b) existing studies solely focus on large companies, (c) GPRD compliance costs concern both implementation of OTMs and maintenance of GDPR compliance, and (d) GDPR costs do not only concern technical solutions, but also HR costs for training, etc. During the second year and		

after the launch of MVP, we plan to launch a survey aiming at determining what the average compliance with GDPR cost is. This survey will also be launched within the frame of the forthcoming SME-centric workshops, so that we can create a reference baseline for SENTINEL services pricing. Successful fulfilment of such indicator will then depend on the price of SENTINEL's services regarding compliance burden. **Linked WP: 2; Owner: LIST**		
KR-1.3	**Reduction of compliance – related costs by at least 40% against benchmarks defined by stakeholders and EU (International) initiatives.**	**In progress**
This KR is highly linked with KR-1.2. For this KR, it is essential to define the average cost of compliance for SMEs, before realising it. A forthcoming survey planned to be released after the MVP combined with literature data (already acquired during the first year of the project) will help us identify the average GDPR compliance costs for SMEs (see above description), which will also provide a baseline to compare with the SENTINEL services. Our intention is to leverage this survey in the forthcoming SME-centric workshops, as well as other relevant events. In addition to this, this KR will be evaluated once the validation phase kicks off. An important milestone towards this direction is the implementation of the MVP (M12), which can initiate a preliminary validation phase with end users. Nevertheless, this KR is expected to be achieved during Y3, after the validation phase is completed and a survey aiming at determining the average compliance with GDPR cost is fulfilled. **Linked WP: 6; 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.**	**In progress**
Regarding KR-1.4, SENTINEL has been organizing several events with the objective of raising awareness in SMEs/MEs all over the EU about GDPR compliance and PDP. Within this context, SENTINEL offerings have also been identified, with the objective to start motivating attendees using intelligent one-stop-shop solutions for compliance services. In this respect, the SENTINEL consortium has prepared a questionnaire to record user acceptance of SENTINEL offerings after the delivery of the two SME-centric workshops (September 2021 and May 2022), which is planned to serve as a baseline. SMEs that opted in for trialling SENTINEL offerings will be contacted again and asked to fill in the questionnaire again after using the SENTINEL services. This indicator will help us determine the acceptance before SENTINEL and any improvement after SENTINEL. This KR is planned to be achieved at the end of the project. **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**	**In progress**
This KR is directly connected with the expectations and goals of plugins, such as ACS's CyberRange and ITML's Security Infusion and thus will be 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 should first deploy our solution as part of a real use case and then perform 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. In Year 2 (Y2), these efforts will be intensified to be in a position to prove and/or demonstrate the applied protection mechanisms for at least 10 types of related threats and attacks to data storage and accessibility. This KR is planned to be fulfilled for the end of the project. **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 mostly realized through the work performed in WP2, WP3, and WP4. More specifically, during the first year of the project, the MVP version of the Data Protection Impact Assessment (DPIA) toolkit was designed, developed, and delivered. This module allows organizations to measure the exact risk and get recommendations for high-risk processing activities. The DPIA toolkit (MVP) consists of 19 questions created after a state-of-the-art review

on existing tools and questionnaires (e.g., CNIL, ICO etc.), measures the impact, likelihood, and risk based on the output of the questionnaire and provides the information to the end-user through the Self-Assessment Engine.

In addition, the first version of the GDPR Compliance Self-Assessment (CSA) module was designed and delivered. The GDPR CSA module performs an analysis of Processing Activities (PAs) to determine whether personal data are handled in accordance with data protection requirements. Thus, it 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 during Y1 and the strategy towards their successful completion.

Table 2. KRs status update - Objective 2

<table>
<tr><td>KR-2.1</td><td>Innovative customized RE-related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs</td><td>Achieved</td></tr>
<tr><td colspan="3">KR-2.1 has been successfully fulfilled within Y1 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 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.
Linked WP: 1; Owner: IDIR</td></tr>
<tr><td>KR-2.2</td><td>Accuracy of (distributed) machine (deep) learning algorithms facilitating intelligence in the recommendations for data compliance of more than 80%.</td><td>In progress</td></tr>
<tr><td colspan="3">A first implementation of the recommendation engine was implemented as part of D3.1. The purpose of these recommendations is to provide a list of recommended measures, plugins and trainings, so as to assist the organisation 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. During the next development phase of the Digital Core services (D3.2), machine learning algorithms will be explored as a more effective way to provide recommendations for data compliance. Validation of the integrated system in real-world settings via the SENTINEL use cases (WP6) will help us establish a baseline and assess the accuracy of the recommendation engine algorithms in terms of data compliance. Linked WP: 3; Owner: ITML</td></tr>
<tr><td>KR-2.3</td><td>Test GDPR compliance and digitalized DPIA self-assessment framework.</td><td>In progress</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, D2.3, D4.2 and D4.3 that are expected in M18 and M30 respectively. A lot of progress has been made already regarding this KR as part of D2.1 and D4.1 for which an MVP version of the GDPR CSA and DPIA self-assessment tools respectively has been designed and implemented. Both tools are</td></tr>
</table>

questionnaire-based and are integrated into the SENTINEL platform via API that they provide. The testing of the frameworks in real-world settings is going to be performed under WP6. **Linked WPs: 2; 4; Owner: STS**		
KR-2.4	**Offer robust and easy to adopt data access management, authentication, authorization and record keeping technologies to SMEs/MEs for GDPR compliance.**	**In progress**
Realisation of this KR during the first year was achieved through the implementation of SENTINEL integrated IdMS. IdMS first version for the MVP (D2.1) provides authentication, authorization and Single Sign-On services 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 next steps include the release of the full featured version of IdMS, including full compliance with the MyData model, 'one-click' integrations with existing SME/ME solutions for easier to adopt data access management, authentication and authorization, as well as ensuring no breaches are or duplication of sensitive data on premises (SMEs/MEs) is possible. With regard to the record keeping technologies, the SENTINEL platform is designed to store a Record Of Processing Activities (ROPA). This is stored under the organisation profile and is made available to the SENTINEL plugins (such as GDPR CSA and DPIA) as required. The GDPR CSA was developed as part of D2.1 MVP with the main functionalities to improve the compliance level of the record of processing activities (PA) for GDPR compliance. The current version of the GDPR CSA module includes determination of GDPR compliance of RECORD processes (a process that focuses on compliance with requirements related to PA description) and provision of recommendations to improve GDPR compliance level. The next version of GDPR CSA module is expected to (i) cover all processes of GDPR Process Assessment Model, (ii) link up GDPR CSA OTMs evidence with SENTINEL's OTMs database and (iii) define standard PAs, i.e., typical personal processing activities that an SME is likely to be responsible for. **Linked WP: 2; Owner: ITML**		
KR-2.5	**Ensuring the delivery, adoption, and utilization of a unified Identity Management System.**	**In progress**
This KR is tightly connected with KR-2.4 and is related to the delivery of an integrated IdMS. As mentioned above, during the first year the MVP version of the IdMS module was implemented based on an open-source solution (KeyCloak). The next steps include the release of the full featured version of IdMs, including full compliance with the MyData model, 'one-click' integrations with existing SME/ME solutions for easier to adopt data access management, authentication and authorization, as well as ensuring no breaches are or duplication of sensitive data on premises (SMEs/MEs) is possible. Adoption and widespread utilization of the unified IdMS will be determined during the validation phase (WP6) in the upcoming months, where the SENTINEL use case owners will trial the system in real-world settings. **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 in Y1 of the project, in the four main technical work packages: WP2 (which develops personal data protection and cybersecurity technologies key to SENTINEL), WP3 (which develops core components of the SENTINEL technical architecture specially focusing on recommending an appropriate policy based on earlier automated assessments) and WP4 (which is primarily responsible for SENTINEL's assessment & training context, including the SMEs' tailored profiling process, an automated DPIA and cyber range-based simulations and training), with overall integration work taking place in WP5.

This work primarily supports 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 shows a summary of these KRs, their current status, Y1 activities and the strategy for achieving them.

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.**	**In progress**

We consider the term services and tools within the wider concept of "capabilities" offered by the SENTINEL framework. During Y1, technical partners - as part of activities in WP2, WP3 and WP4- have developed from scratch and leveraged tried-and-tested tools and services, which are integrated for the MVP (see D5.4) and span across a number of capabilities in terms of PDP compliance, cybersecurity, data analytics, etc.

For example, FP's MITIGATE tool delivered the following services which will be available to the MVP through the Simulation Environment module:

- The Vendor 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
- 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
- The Threat Management service which provides to SMEs/MEs all threat-related information upon specific selected IT products
- The Attack Scenarios Simulation Environment service which gives the capability to SMEs/MEs to develop and experiment on attack scenarios upon selecting specific products and obtain knowledge on interrelations of corresponding threats and vulnerabilities for each specific product.

In addition, GDPR self-assessment services for PDP were provided by LIST which will be available to the MVP through the GDPR Compliance Self-Assessment module (CSA). These GDPR Compliance Self-Assessment (GDPR CSA) services analyse the Processing Activities (PAs) to determine whether personal data are handled in accordance with data protection requirements, and they are enlisted in the following:

- The RECORD GDPR Compliance Level service which analyses the user's Record of Processing Activities (ROPA) to determine the Compliance Level of RECORD of PAs of SMEs/MEs according to GDPR, Art. 30
- The Recommendations for GDPR Compliance service which supports a list of recommendations to improve the GDPR compliance level of PAs RECORD identified on SMEs/MEs
- The GDPR Assessment Scope service which determines the processes that have to be inspected according to the Privacy Risk Level of PA.

The Identity Management Service (IdMS), provided by ITML, supports single Sign-On capabilities for SENTINEL end-users. Another capability provided within Y1 was the implementation of a MISP instance to the MVP, supported by AEGIS, to promote threat intelligence services which will be further processed through the coming period. In addition to this, ACS's CyberRange simulation environment (testbed) has been linked with the SENTINEL platform under T4.1 activities, offering capabilities for testing systems before on-site integration, optimizing cyber-defence strategies or training the end-users.

Activities within WP3 have yielded several services that have either been incorporated within the MVP due in M12 (see D5.4) or will be incorporated in the next integrated version. These are:

- Continuous monitoring of an SME/ME's infrastructure, collection and reporting on any event that may be a security breach, vulnerability, threat, or attack through the Notification Aggregator module;

- Submission of incidents by the end-users, as they occur during the operations of an SME/ME, facilitated by the Incident Reporting module;
- Offering tailor-made, customised recommendations on measures, plugins and trainings for an SME/ME based on a thorough analysis of its processes, OTMs and profile, facilitated through the recommendation engine;
- Analysis and interpretation of the recommendations deployed by the recommendation engine and drafting tailor-made optimisation policies, facilitated by the policy drafting, enforcement and orchestration module.

The project's next steps will be to utilize and integrate more services or tools from diverse multi-domain technological areas to be applicable to SMEs/MEs environments to support their PDP via automation mechanisms which will be provided in the first and second prototype releases. Such services may be the following supported by the MITIGATE tool:

- The asset inventory service (online ISMS for SMEs/MEs), including asset interdependencies and security-related information
- The control's management service to keep SMEs/MEs information of security controls implemented on their assets and explore how these controls can mitigate either corresponding threats or vulnerabilities through the Simulation Environment.
- The risk appetite service to allow SMEs/MEs adjust the threat probability according to their conditional expectations and preferences.
- The provision of the Business Service for declaring SMEs/MEs assets operating in specific business processes.
- The risk assessment service to allow SMEs/MEs conduct cybersecurity risk assessment on their IT assets and review the reported results.

Concerning privacy and data protection future steps, the Data Protection Impact Assessment (DPIA) service is currently under development and supported by STS under T4.2. Future actions will involve the enhancement of the GDPR assessment scope service, as well with the provision of a Questionnaire that will be available to SMEs/MEs to answer in case the assessment scope is not limited to RECORD. Regarding the IdMS, next actions will be to enhance user management capabilities and apply these services to the personal data of the pilot SMEs/MEs end-users. In addition, data storing technologies will be utilized in the Observatory module in the context of T4.4 activities.

Future steps will also include the integration of external training services under T2.4 that will provide additional training capabilities to SMEs/MEs for topics that will be not covered by the other SENTINEL services. These actions will be supported through external plugins and open-source training modules that will be contributed by TSI. **Linked WPs: 2; 3; 4; Owner: FP**

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

All of the work and actions performed by the consortium partners in Y1, from setting the project's baseline (WP1), to delivering the first version of SENTINEL MVP (WP2-WP5) has directly contributed to this Key Result. Although the KR itself will not be quantifiable until later in the project, when the full-featured, and, subsequently, final versions of SENTINEL are released, by M12, the ground is already set for what will be the distinct innovative capabilities offered by SENTINEL for a) privacy and data protection (intelligent profiling, permanent processing activity records (ROPA), GPRD compliance self-assessment, Data Protection Impact self-assessment, privacy and PDP recommendations, trainings); b) cybersecurity (computer security simulation environments, the Cyber Range, a complete cyber asset inventory, threat assessment); c) integrated services (Security Notifications, Incident Reporting and Handling, the Observatory, the Policy Enforcement Monitoring Centre and the Compliance Centre). The initial version of the use cases for the SENTINEL Services in the use cases for a) SME profile including processing activities, b) self-assessment, c) acquiring policy recommendations and d) consulting the Observatory are already part of the MVP.

The upcoming period leading to M18 is critical for solidifying and quantifying this KR in the form of specific capabilities and services provided either by the integrated SENTINEL platform or its recommended tools, in the form of plugins. **Linked WP: 4; Owner: IDIR**

KR-3.3	**Upgrade ML/DL models to be realized as services in privacy-aware SMEs/MEs environments.**	**In progress**

As part of the SENTINEL services, the consortium aspires to leverage ML/DL models for anomaly detection; more specifically, SENTINEL plugins, such as ITML's Security Infusion are currently being advanced to identify events, items or observations, which differ significantly from standard behaviours or patterns. This is anticipated to significantly advance SENTINEL services in privacy-aware environments for SMEs/MEs. The envisioned service will be validated in two use cases in the upcoming months: (a) use case 4 - Receiving security notifications that showcase the Notifications Aggregator; and (b) use case 7 - Incident reporting and sharing that showcases the Incident Reporting module. Thus, this KR is still in progress and will be realised in future versions of the SENTINEL integrated framework. **Linked WP: 2; Owner: ITML**		
KR-3.4	**Accuracy and efficiency of the SENTINEL data privacy compliance recommendation engine at least 70%.**	**In progress**
A first implementation of the Recommendation Engine (RE) was implemented as part of D3.1. The purpose of these recommendations is to provide a list of recommended measures, plugins and trainings, so as to assist the organisation to address potential shortcomings and vulnerabilities in the realm of data protection and cybersecurity protection. For the purpose of the MVP (D3.1), 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. KR-3.4 will be validated during the next development phase of the Digital Core services (D3.2), where the recommendations on GDPR compliance and data protection in real-world settings will be evaluated for their accuracy and efficiency via the SENTINEL use case owners (WP6). **Linked WP: 3; Owner: ITML**		

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), naturally it will intensify during Y2, after the MVP is launched.

During the first year of the project, we have already identified seven (7) ways that a user can use and interact with the SENTINEL platform to showcase the framework's capability, which were based on a thorough requirements analysis performed in T1.1 and recorded in D1.1. These have been described in detail in D1.2 together with the respective experimentation protocols, including KPIs and related evaluation variables, as part of D1.3. With respect to experimentation variables, the methodology for validating the system has been initially defined in D1.3, it is currently being developed as part of T6.1 and will be further improved within WP6.

Towards experimentation execution, a number of relevant activities have already started, including definition of experimental setups and relevant infrastructure of the two use case owners, and will continue during Y2 of the project to meet the goal of executing at least two demonstrators in real-life settings. In the meantime, we have already secured the engagement of three (3) extra-consortium SMEs/MEs through Digital Innovation Hubs to trial the SENTINEL platform during the validation phase. An important milestone that was achieved as an enabling step towards this objective is the successful implementation of the MVP. Another important milestone towards this

direction is the definition of the SENTINEL main offerings that will shape the exploration of several aspects during the validation phase, such as “cost-efficiency”, “automation”, “intelligence”. The table below provides a summary of the KRs related to Objective 4, as defined in the GA, including their status update, the activities during Y1 and the strategy towards the 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.***	**In progress**
This KR is linked to the D6.3 in WP6, which will be delivered at the end of the project in M36. Currently, the MVP that has been designed and implemented provides functionality that collects data from SMEs/MEs to build their profile, provides assessments via the GDPR CSA and DPIA tools and policy recommendations via the policy recommendation engine. **Linked WP: 6; Owner: STS**		
KR-4.2	***Delivery of three (3) integrated versions of the SENTINEL framework.***	**In progress**
The MVP constitutes the first integrated version of the SENTINEL framework and has been delivered on time and reported in D5.4. Two more platform releases are expected to follow in M18 and M30 and reported in 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.***	**In progress**
Within Y1, the consortium has identified three additional demonstrators, in addition to the two pilots defined in the GA, as a result of T6.3 activities. Additionally, the consortium has organised two (2) SME-centric workshops, co-hosted under the 2nd and 3rd plenary meetings respectively, where SMEs from different application domains and different EU countries were informed about the SENTINEL offerings and were asked to trial the framework – when ready – for free. The participants were also asked to fill in a questionnaire to better reflect their needs, challenges, GDPR compliance obligation awareness and many more. This KR is still in progress as the use cases will be implemented and executed under WP6. INTRA – as integration leader – will monitor this KR under T5.2 to determine the percentage of tools validated in each demonstrator. **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.***	**In progress**
Within T1.1 and T1.3 of WP1, seven (7) use cases were identified, based on the pilots’ functional and non-functional requirements. The use cases are described in detail in D1.2. The KR is still in progress as the use cases will be implemented and executed under WP6. Based on the GA, SENTINEL has onboard two end-user partners, while we have already secured three more SMEs/MEs via Digital Innovation Hubs to trial the SENTINEL tools and services (as part of T6.3 activities). Considering that a trial refers to an end-to-end validation of one of the SENTINEL services, we anticipate having at least 10 trials in total for the already identified 5 end users. During Y2 and Y3 we will continue engaging end user via DIHs and focused SME-centric workshops towards achieving this KR. FP will monitor the KR under T6.1. **Linked WP: 6; Owner: FP**		
KR-4.5	***Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.***	**In progress**
Several remote meetings have been organized and carried out to define and implement the User Interface of the SENTINEL framework, 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 includes links to components that are 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 (more details in D5.1). Moving forward, work will continue to be comprehensive to refine and enrich the content of the UI by engaging and closely collaborating with end-users with diverse backgrounds under WP6, we will make sure to incorporate their feedback and implement a UI that offers high levels of usefulness and usability.		

All this effort will result in the intermediate and final versions of the MySENTINEL UI dashboard and will be documented in subsequent iterations of D5.1, namely D5.2 and 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 Y1, 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 a clustering webinar which was organized by the coordinator (ITML) and the dissemination manager (UNINOVA) of SENTINEL with 10 EU Horizon 2020 projects funded under the H2020-SU-DS-02 and H2020-SU-DS-03 topics. During this clustering webinar, the projects presented their main outcomes, offerings and innovations, while there was a very productive open discussion session, where the projects identified common pathways and potential joined synergies for the future. In addition to this, the consortium has organized two SME-centric workshops, as well as a Webinar on "A privacidade e a proteção de dados pessoais no panorama nacional das PMEs", with more than 100 attendees in total, including SMEs/MEs coming from different application domains and countries across the EU, in order to raise awareness of SENTINEL offerings and engage SMEs as future end users of the framework. The workshops were accompanied by a questionnaire that helped the consortium better understand the SMEs' needs, challenges, current OTMs, infrastructure and awareness of GDPR compliance obligations. SENTINEL has also engaged different DIHs, at national and EU level, namely Produtech, DIH4CPS and DIHWorld. The objective is to continue raising awareness through additional EU DIH in Y2.

Promotional material such as three (3) newsletters, the first promotional video of SENTINEL, flyer, brochure, business card, regular posts in social media (LinkedIn, Twitter) were produced during Y1 with SENTINEL attracting more and more attention as the project progressed. One paper produced by a SENTINEL partner (TSI) was published in a prominent European Workshop on Systems Security (EuroSec 2022), one conference paper was accepted and will be presented at the IEEE cyber security and Resilience (IEEE CSR) conference while one conference paper was submitted to 9th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE 2022) which is currently under review. More details can be found in Section 3.7 and Section 4.2.

For Y2, the consortium has already confirmed its participation in three major events, the FIC 2022 (International Cybersecurity Forum) and the IoT week 2022. The coordinator (ITML) will also present SENTINEL and its offerings to the upcoming Projects to Policy Seminar (PPS) event, invited by the European Research Executive Agency (REA).

The table below provides a summary of the KRs related to Objective 5, as defined in the GA, including their status update, the activities during Y1 and the strategy towards the successful completion. A more detailed description of the actions being addressed by SENTINEL towards Objective 5 are presented in Sections 3.7 and 4.2 of this report.

Table 5. KRs status update - Objective 5

KR-5.1	**All SENTINEL solutions, products and services aligned and harmonized with regulations and EU standards.**	**In progress**
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 EU and national legal and regulatory framework. **Linked WPs: 2, 8; Owner: CECL**		
KR-5.2	**Define a concrete dissemination strategy to raise awareness.**	**In progress**
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. This has been realised through a series of identified events and the creation of promotional material. Although the SENTINEL dissemination strategy will be reported in both deliverables D7.3 in M18 (intermediate version) and D7.4 in M36 (final version) respectively, the consortium has already undertaken a plethora of dissemination activities towards KR-5.2 during year 1, which are provided in detail in Sections 3.7 and 4.2 of this report. **Linked WP: 7; Owner: UNINOVA**		
KR-5.3	**Uptake more than (6) standards from several data privacy and compliance related technologies.**	**In progress**
Several developments during Y1 have taken into account important regulations and standards, such as the NIS Directive, alignment with ENISA's objectives, the eIDAS regulation, standards related to Information Security (e.g., ISO/IEC 27000) and standards related to Data protection and privacy (GDPR). At such a relatively early stage of the project (Y1), standards (other than GDPR) are not yet widely used by partners. STS is currently preparing a survey on the usage of standards and the interactions with standardisation bodies which will be distributed to all partners in Y2 in order to record the specific use of standards by all partners. Partners with active interactions with standardisation/regulation bodies are STS, TSI, CECL, LIST and UNINOVA and will drive this KR forward during Y1 and Y2. **Linked WP: 7; Owner: STS**		
KR-5.4	**More than (8) DIH engaged to further communicate and support SENTINEL offerings.**	**In progress**
UNINOVA is providing access to inNOVA4TECH – a DIH that supports the digitisation of companies (SMEs, MidCaps and large companies) - for a twofold purpose; (a) to engage SME end-users to trial the SENTINEL offerings during the project duration (M13-M36); and (b) to raise awareness of SENTINEL outcomes so as to ensure project sustainability beyond the end of the project (after M36). The potential of the inNova4TECH ecosystem can also be leveraged through the partnerships with Madan park and AISET, which account for more than 200 associate companies, more than 10 regional and national associations, and more than 10 thematic networks. UNINOVA has already engaged with Produtech, DIH4CPS and DIHWorld. The objective is to continue with such activities to address a much wider network. Additional DIHs have been already identified and interactions are being made for promoting SENTINEL in such ecosystems. SENTINEL is planning to engage with the European catalogue of DIHs, launched by the European Commission. A more detailed description of the actions being addressed by SENTINEL towards KR-5.4 during year 1 and the strategy towards the successful completion, are addressed in Sections 3.7 and 4 of this report. During Y2, the already connected DIHs will have a chance to trial SENTINEL as part of the validation phase (WP6), while efforts will be concentrated on bringing onboard the five (5) identified DIHs, towards realisation of this KR. **Linked WP: 6; Owner: UNINOVA**		

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 taken a series of actions; a sound preliminary business model was launched in M6 which defined – among others - SENTINEL target markets, customer segments, possible revenue streams, as well as individual exploitation plans and expected TRLs. 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 will reach 6-7, as expected. An important milestone achieved towards realising Objective 6 is the implementation of the MVP (D5.4) in M12. This will initiate the validation phase, as well as activate the project's exploitation activities and create opportunities for European-based SMEs to use SENTINEL offerings. It will also enable the initiation of further collaborations through the tangible trialling of SENTINEL offerings by third parties. Engagement of third parties has already been initiated by UNINOVA through inNOVA4TECH DIH.

The table below provides a summary of the KRs related to Objective 6, as defined in the GA, including their status update, the activities during Y1 and the strategy towards the 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).**	**In progress**
The SENTINEL MVP (D5.4) is the first step towards the integrated solution, while there have also been significant advancements in various individual solutions. The platform as well as the individual offerings are expected to become more mature though the validation and evaluation iterations that will follow as part of WP6 and provide inputs for improvements. **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**	**In progress**
SENTINEL is based on several mature – in terms of technology and market readiness- components (e.g., MITIGATE, Security Infusion, CyberRange, DPIA etc), which are already placed at a high TRL, while most of them (Security Infusion and CybeRange) are already launched in the market. In addition, newly developed tools during Y1 (IdMS, policy drafting, self-assessment workflow, GDPR CSA module) will also be further improved during Y2 and validated in real-world settings. The project's future steps will be to further advance tools brought by partners, as well as tools developed from scratch towards market readiness. Project activities will target the evolution of specific utilized SENTINEL technologies to develop a conceptual technical maturity framework for the elevation of their TRL. For instance, the GDPR CSA tool process model may be adjusted according to the SMEs/MEs specific technical characteristics and processes of the compliance assessment and privacy risk management tools may be modelled to be performed by automatic means. Moreover, the virtualization environment may be adjusted to the specific IT topology of SMEs/MEs. **Linked WPs: 2-5; Owner: FP**		
KR-6.3	**At least six (6) third-party collaborations to be established for further applicability verification.**	**In progress**
With respect to KR-6.3, SENTINEL has been (since day 1) interacting with several SMEs/MEs on a continuous basis under activities of T7.4, with the purpose of establishing partnerships for applicability and testing of the SENTINEL offerings. SENTINEL has organised two SME-centric workshops, 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 three (3) DIHs and has also created strong liaisons with five (5) other DIHs to trial or provide feedback to the SENTINEL offerings. A more detailed description of the actions being addressed by SENTINEL towards KR-6.3, during year 1 and the strategy towards the successful completion, are addressed in Sections 3.7 and 4 of this report. In Y2, the consortium will focus on bringing onboard potential end-users (from DIHs or other source) to trial the SENTINEL offerings as part of the activities of T6.3. In Y3, the consortium will focus on validating the utility of the proposed solution at a larger scale with a view to be adopted by several thousand European SMEs/MEs, being part of the activities of T5.3. Thus, we anticipate that this KPI will be achieved by the end of the project. **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.**	**In progress**

The design and development process of the integrated solution has already made various provisions related to the long-term sustainability. These include aspects such as extensibility and modularity of the architecture, software maintenance (organization of the code repositories, documentation of synchronous and asynchronous APIs), regular backups etc. As the project progresses, more sustainability aspects are to be considered to include ones related with the user feedback and the business landscape. **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.**	**In progress**
This KR is linked to WP7 "Ecosystem building, Exploitation and sustainability management" and more specifically T7.1 "Market continuous analysis and business planning for SENTINEL exploitation". T7.1 officially 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, we immediately started implementing the plan. As a first step to this plan, AEGIS organized a T7.1-related telco inviting all SENTINEL partners to further explain the rationale behind the plan presented. Additionally, AEGIS 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 that emerged from this process contributed to better understand and identify SENTINEL competitive advantage and value proposition and form the preliminary business modelling. This was presented in D7.2 titled "Market analysis and preliminary business modelling" in M6 of the project. Following the analysis of the inputs provided by all partners on the questionnaire in the context of designing and developing a collaborative business plan for SENTINEL, we were able to initiate preparations for D7.2 at an early stage. As a result, the D7.2 ToC was circulated among the SENTINEL members during M4. After the successful submission of the D7.2 "Market analysis and preliminary business modelling" AEGIS has 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. That being said, there is expected to be a revisit to the business planning based on the acceptance of the MVP as part of brainstorming, as well as based on the feedback we may receive. This involves cooperation between Tasks 7.1, 7.2 and 7.3 and will be documented in the final business model, market analysis and long-term sustainability report (D7.9) at the end of the project. **Linked WP: 7; Owner: AEGIS**		

3. Explanation of the work carried per WP during the 1st Year

3.1 WP1 – SENTINEL baseline: Setting the methodological scene

Leader: IDIR

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

Duration: M1- M6

3.1.1 Summary of results achieved during reporting period

WP1 was led by IDIR and started in M1. During the first six-month period, all the tasks involved in WP1 were successfully completed through the collaboration of all partners in a number of plenary and technical meetings.

The key achievements of WP1 include:

(i) Investigation of the parameters that drive the needs for data privacy and compliance processes for SMEs and the definition of a relevant Requirements Engineering (RE) methodology, contributing to D1.1, submitted in M4.

Concerning the needs of SMEs, D1.1 clearly identifies and discusses the specific challenges of SMEs that drive their requirements for an improved, customized and usable way of dealing with their CS for privacy. These challenges are discussed in the context of organizational, legal and technical concerns. Particular attention has been paid to the challenges presented to SMEs due to their increasing desire for migration towards the Cloud. The above analysis resulted in a set of major generic and specific requirements, which are presented in a concise tabular form. The tables are used to associate the SENTINEL components with system requirements and to inform the ontology for the overall Requirements Engineering methodology.

Concerning the definition of the SENTINEL RE methodology, D1.1 presents a methodology, developed for SENTINEL, which is innovative, generic, and dedicated to CS for the privacy needs of SMEs. The methodology is presented along two dimensions: its foundational concepts; and its process to be followed using these concepts. The backdrop to the way of working is a set of user-facing questions that link the methodology to the ENISA guidelines. To demonstrate its applicability the methodology was applied on the pilot cases identified in the GA.

D1.1 contributes to milestone 1 (‘Project’s baseline’ due M6).

(ii) Refinement of the architecture of the SENTINEL digital framework and definition of SENTINEL’s end-to-end architecture, leading to the delivery of D1.2 (“The SENTINEL technical architecture”) in M6.

The main goal of D1.2 was to revise and specify the technical descriptions provided in the GA and devise a solid technical architecture. It serves as a baseline for the development of the SENTINEL’s components in WP 2, 3 and 4, as well as their technical integration under WP 5. To this end, it describes the application of use cases and associated functional and non-functional requirements. These are represented using a common template and drive the subsequent design and specification of the architectural components. In particular, this design is based on the notion of contexts, i.e., groups of modules that operate under a common setting. A key decision that was made with respect to the GA was to separate the cybersecurity and personal data protection technology offerings from the core architecture, treating them as pluggable components. This choice decouples the offerings from the main system and thus fosters characteristics such as flexibility, extensibility and maintainability.

D1.2 contributes to Milestone 1 (‘Project’s baseline’ due M6).

(iii) Definition of the SENTINEL experimentation protocol and test cases. These contributed to the deliverable D1.3 (“The SENTINEL experimentation protocol”) which was successfully completed and submitted in M6.
In particular, D1.3 defines the experimentation process (phases and steps) and discusses the conditions for accessibility of participants in the actual experiments. Furthermore, it identifies relevant standards and benchmarks and defines the verification indicators and juxtapose these to the SENTINEL platform, as detailed in D1.2. Finally, it determines the validation indicators to

be used in the experiments involving the pilot cases, as detailed in D1.1 and defines the instruments (templates) to be used when the experiments are carried out and results are reported.

D1.3 contributes to milestone 1 ('Project's baseline' due M6).

3.1.2 Key WP1 achievements during reporting period at task level

Task 1.1 The SENTINEL requirements engineering methodology

T1.1 was led by IDIR, started in M1 and completed in M4. The aim of this task was to gain insight into the parameters that drive the needs for data privacy and compliance processes in SMEs/MEs and to define the relevant RE methodology. To this end, T1.1 contributed towards: (a) identification of generic SME requirements with respect to CS and personal data protection; (b) positioning of the technological and methodological assets of SENTINEL with respect to the above requirement; (c) development of a requirements engineering methodology specifically targeting SMEs needs and capabilities; and (d) demonstration of the feasibility of the above methodology.

T1.1 has contributed to the following WP1 objectives:

(i) Capture the detailed functional requirements and technical challenges for the envisioned framework and complete a thorough requirements analysis.
(ii) Determine the detailed functionality of the SENTINEL digital architecture according to the end-user (SMEs/MEs) needs and the state-of-the-art in privacy, personal data protection and compliance.
(iii) Describe in detail and continuously monitor the scientific (academic and industrial) and end-user needs and challenges for secure and trustworthy solutions for SMEs/MEs.
(iv) Synthesise and present the current state-of-the-art from the viewpoint of the project's highlighted problems.

The above comprise significant input to deliverable D1.1 ("The SENTINEL baseline", delivered M4), contributing also to milestone 1 ('Project's baseline') due in M6.

T1.2 Technology convergence: the SENTINEL offerings and updated architecture

T1.2 was led by INTRA, started in M3 and was completed in M6. The main objective of this task was to refine SENTINEL's end-to-end architecture, taking into account the state-of-the-art assets brought by the SENTINEL partners, as well as new assets to be developed within the project, and the requirements' analysis performed in T1.1. To that end, T1.2 has (i) closely monitored the high-level requirements being formed during T1.1, (ii) identified the capabilities of the distinct system components and (iii) worked towards the definition and elaboration of seven (7) use case scenarios that examine and expose the interplay among all components at an end-to-end level.

The refined SENTINEL architecture was designed, with particular focus on modularity and extensibility. The architecture is able to incorporate new capabilities through the use of plugin tools and incorporate new knowledge through external data sources. This was achieved through the close collaboration of technical partners in several technical meetings organized by the task leader and resulted in the timely submission of D1.2 ("The SENTINEL technical architecture") in M6.

T1.2 has contributed to the following WP1 objective:

(i) Design the technical framework and architecture of the integrated SENTINEL platform.

D1.2 contributes to Milestone 1 ('Project's baseline') due in M6.

T1.3 has contributed to the following WP1 objectives:

(i) Specify the test cases for the pilots including the verification and validation approach and develop a mapping of the architecture's mechanics.
(ii) Design and implement the SENTINEL demonstration protocol.

D1.3 also contributed to Milestone 1 ('Project's baseline') due in M6.

T1.3 The SENTINEL demonstration execution protocol

T1.3 was led by IDIR, started in M3 and was completed in M6. Informed by the preceding two tasks, T1.3 specified the SENTINEL experimentation protocol. The SENTINEL experimentation process, test cases and associated validation and verification variables have been defined in collaboration with the use case providers and technical partners in a number of bilateral meetings organized by the task leader. These contributed to the deliverable D1.3 ("The SENTINEL experimentation protocol") which was successfully completed and submitted in M6.

D1.3 also contributed to milestone 2 ('Innovation flame' due M12).

3.1.3 Work carried out in this work package per partner

ITML	Within the context of WP1, ITML has actively participated in all meetings towards the definition of the SENTINEL's baseline and high-level requirements. In addition, ITML has played a key role in facilitating the technical meetings towards refining the specification of the SENTINEL architecture alongside INTRA, while it participated in activities regarding the definition of the verification variables. Furthermore, ITML has contributed to the preparation of D1.1 (section 4.4.1), D1.2 (sections 4.3, 4.4 and 4.5.1.1) and D1.3 (section 4.2 and 4.3), as well as conducted the internal review of all of the aforementioned reports.
LIST	During the reference period, LIST has participated in all WP1 relevant meetings towards refining the specification of the SENTINEL architecture and definition of the verification variables. Furthermore, LIST has contributed to D1.1 (section 1), D2.1 (sections 3 and 4.5.1), D1.3 (section 4). Finally, LIST has reviewed D1.3.
The SHELL	For the first six-month project period, The SHELL has provided input for D1.1 and was actively involved in refining the SENTINEL architecture. **Since M6, the partner The SHELL has been terminated from ECAS.**
IDIR	Within the context of T1.1 IDIR coordinated all T1.1 activities. IDIR has developed appropriate questionnaires for eliciting the end-user needs as well as the existing and desired capabilities of technology providers. IDIR has participated in online meetings with end-users and technology partners towards the elicitation of the SENTINEL requirements and the definition of the SENTINEL RE methodology. In addition, IDIR led the delivery of D1.1, conducting explicit research and contributing material in most sections. Specifically, IDIR reviewed the state of the art, identified generic SME requirements, mapped the requirements to components of the SENTINEL architecture, defined the SENTINEL RE methodology and demonstrated it in two pilot cases. In T1.2, IDIR participated in technical meetings towards refining the specification of the SENTINEL architecture, providing key effort in initiating and coordinating the

	technical meetings towards refining the specification of the SENTINEL architecture alongside INTRA and ITML and contributed input to D1.2 sections 3 and 4.2. Finally, within T1.3, IDIR performed the coordination of task partners and the organization of several technical meetings towards the definition of the SENTINEL experimentation variables and test cases. IDIR has also led the delivery of D1.3, contributing key content for all sections.
INTRA	INTRA has participated in all meetings towards the definition of the SENTINEL's baseline and high-level requirements. INTRA reviewed available technologies and assets and contributed to section 2 of D1.1 with input related to requirements and challenges for privacy and cybersecurity for SMEs. Furthermore, INTRA led T1.2 towards the refinement of the SENTINEL architecture. The work performed within this task involved the coordination of technical partners through regular and ad-hoc technical meetings. INTRA also led the delivery of D1.2 and has contributed to sections 1, 3, 4.5, 5 and 6. Finally, INTRA participated in all technical meetings towards the definition of the verification variables, identified and evaluated relevant technical benchmarks and standards and contributed to D1.3 with input in sections 2 and 4.
STS	STS has participated in all WP1 meetings toward refining the specification of the SENTINEL architecture and verification of variables. Furthermore, STS provided content for D1.1 (section 4.4.5), D1.2 (sections 3 and 4.5.1) and D1.3 (section 4).
AEGIS	In the frame of WP1, AEGIS contributed to activities related to all tasks of WP1 according to the instructions and guidance of the task leader. AEGIS has participated in all technical meetings regarding the refinement of the SENTINEL architecture and the definition of the verification variables.
TSI	TSI participated in all technical meetings of WP1, additionally contributed to D1.1, D1.2 (sections 3 and 4.5.2) and finally D1.3 (section 4).
ACS	ACS has contributed to D1.1, in particular for the part related to the Simulation platform CyberRange. Furthermore, ACS has participated in technical meetings towards refining the specification of the SENTINEL architecture. Finally, ACS contributed to D1.2 by giving input to sections 3 and 4.5.1.
UNINOVA	UNINOVA has no effort in WP1. It conducted the internal review of D1.1
CG	CG has contributed with input to section 6 of D1.1, as well as participated in the relevant online meetings and discussions towards the definition of the experimentation cases and validation variables. Finally, CG contributed to D1.3 by providing input for section 5 of the document.
TIG	TIG has participated in technical meetings towards the definition of the experimentation cases and validation variables. It contributed to D1.2 and D1.3. Regarding the experimentation cases, TIG has proposed that Juventas Services, a TIG SME, will act as a pilot from which technical innovations can be implemented and trialled. However, the systems used by Juventas (i.e., MS OneDrive, SharePoint) have limited scope to offer significant insight. Therefore, following discussion with ACS partners, TIG will propose that another SME within the group, Dimensions Care, will assume pilot status. Dimensions Care uses an online Management Information System (MIS) known as CHARMS. The CHARMS system is commonly used within children's social care in the UK, particularly within the private sector. It is envisaged that engagement with Dimensions Care will provide a more effective platform for trialling SENTINEL technical innovations.

CECL	CECL participated in online meetings with the task leader and the partners and gave input on key principles to be followed in terms of privacy and data protection ethics, as well as an assessment of potential data protection risks and safeguards to mitigated them. CECL's input was incorporated in the SENTINEL baseline (see section 2 of D1.1) and has been followed thus far throughout the implementation of the project. Furthermore, the CECL team contributed to the development of the data protection methodology for the SENTINEL project, with emphasis on the pilot partners, general principles to be followed in accordance with the GDPR, and data anonymization. Data privacy indicators on compliance with the legal and regulatory framework were finalised in collaboration with the EDAC members – in particular the Ethics supervisor, with emphasis on the avoidance of breaches and other relevant safeguards.
FP	FP contributed to D1.1 and participated in online meetings with the task leader. FP in collaboration with all project's technical partners has contributed to the proper design process of the SENTINEL architecture components. FP has contributed to D1.1, D1.2, D1.3. In addition, FP provided the verification variables of the MITIGATE tool and undertook the activity to gather from technical partners information about the verification variables of the other SENTINEL platform assets, which were integrated in D1.3 in collaboration with IDIR.

3.1.4 Status of Deliverables and Milestones

The work done under T1.1, T1.2, and T1.3 contributed to reaching milestone MS1 and well-documented in three deliverables D1.1, D1.2 and D1.3.

Table 7. Status of WP1 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D1.1	The SENTINEL Baseline	IDIR	Report; Public; M4	Submitted
D1.2	The SENTINEL technical architecture	INTRA	Report; Public; M6	Submitted
D1.3	The SENTINEL experimentation protocol	IDIR	Report; Public; M6	Submitted
MS1	Project's baseline	IDIR	M6	Achieved

3.1.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D1.1, D1.2 and D1.3 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.2 WP2 – The SENTINEL privacy and personal data protection technologies

Leader: LIST

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

Duration: M7- M30

3.2.1 Summary of results achieved during reporting period

WP2 is led by LIST and kicked-off in M7, thus the reference period of this report covers the WP2 activities conducted in the M7-M12 period. The lineup of the WP2 has been adapted due to the termination of one of the participants “The SHELL”. ITML has accepted to take over the lead of task T2.2 and corresponding effort for the implementation of IdMS. Thanks to the expertise and experience of ITML, this modification did not impact WP2 expected results. All WP2 partners involved in WP2 worked intensively towards setting a solid ground for delivering the WP2 outcomes.

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 (performed by CECL) 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.

D2.1 contributes to milestone 2 (‘Innovation Flame’ due M12).

3.2.2 Key WP2 achievements during reporting period at task level

T2.1 The privacy and data protection compliance framework

T2.1 is led by LIST and started in M7. It aims at developing SENTINEL’s privacy and data protection compliance framework: GDPR Compliance Self-Assessment Module. The development concerns in digitalizing and automating the GDPR compliance assessment approach based on the ISO/IEC 330xx family standard. To this end, the task is divided into 3 sub-tasks.

Sub-task T2.1.1 concerns adapting a model for GDPR compliance assessment. During the reporting period, an analysis of existing GDPR compliance assessment for SME has been conducted to identify what are the main features incorporated in existing solutions. In parallel, experienced GDPR compliance assessors have been working on the 1) identification of information required to perform assessment; 2) specification of Organizational and Technical Measures that might meet data protection requirement; 3) definition of assessment rules regarding Privacy Risk Level of Processing Activities (PAs). Outputs of this task have been used to define SENTINEL’s Data Model.

Sub-tasks T.2.1.1, T.2.1.2 were synchronized to define the scope of the MVP functionality. It was decided to develop the following functionalities:

- **RECORD GDPR Compliance Level determination**: GDPR CSA MVP version module performs an analysis of user’s ROPA to determine Compliance Level of RECORD. Results provided are related to compliance with obligation to document Processing Activities (PAs) [Art. 30].

- **Provide recommendations to improve GDPR Compliance Level**: Based on assessment results, the module establishes a list of recommendations to improve RECORD compliance level (i.e., improving comprehensiveness and update of PA description).
- **Determine GDPR Assessment Scope**: The module also determines which processes have to be inspected with regard to Privacy Risk Level of PA. If assessment scope is not limited to RECORD, then the module sends to the user a set of questions to answer via the Questionnaire Engine. It should be noted that the latest will be implemented in Full Feature version of the module only.

Sub-task T.2.1.2 aims at automating GDPR compliance assessment. The work conducted within this task aims at both formalizing and coding “assessment rules”. Script allowing deployment of agreed MVP’s functionalities scope have been developed and tested. To this end, a set of PAs for testing purposes has been defined. Particular attention has been paid to documentation: in the code, script is explained; a GIT repository describes components of the GDPR CSA MVP module; additional documentation is developed to record assessment rules.

Sub-task T2.1.3 aims at ensuring integration of GDPR CSA MVP module within SENTINEL’s platform. The connection between SENTINEL's platform and GDPR CSA module is ensured via an Application Programming Interface (API). Instead of just deploying the code, all GDPR CSA module environment is deployed as well. An image docker container is then used to create, run and deploy application in container. As illustrated in Figure 1, Docker image contains application code ("assessment rules"), libraries and dependencies ("GDPR self-assessment"), and instructions related to data preparation (“json processing”).

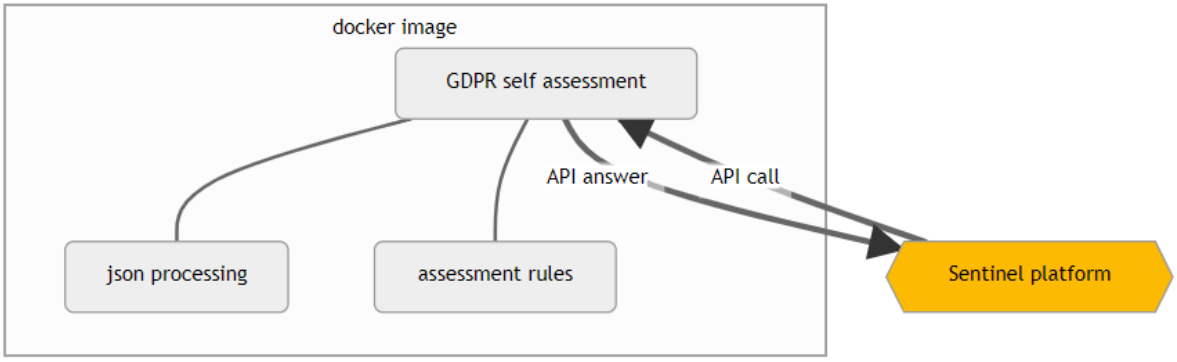

Figure 1. GDPR CSA docker image

T2.1 has contributed to the following WP2 objective:

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

The above comprises significant input to D2.1 (“The SENTINEL privacy & data protection suite for SMEs/MEs: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12.

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

T2.2 is led by ITML and started in M7. The main goal of Task 2.2 is 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. Within the context of this task, ITML presented an overview of the desired solution, requirements and constraints, as well as concrete steps that will deliver the first version of IdMS for the M12 MVP. More specifically, the proposed steps include 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 for the MVP. During the reference period, participating partners in this task discussed the overall ambition of the desired solution, challenges, and open issues, including size and scope of the IdMS component, seamless switching of service providers, data portability challenges and consent management issues. Additionally, meaningful use cases have been identified in collaboration with pilot owners and WP6 activities. The above proposed steps were organized and presented in a detailed time plan towards M12 MVP.

T2.2 has contributed to the following WP2 objective:

(i) 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 D2.1 ("The SENTINEL privacy & data protection suite for SMEs/MEs: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T2.3 Contributed cybersecurity components

T2.3 is 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 cyber risk assessment engine, which enables SMEs to build what-if scenarios on cyber-assets they may have on their infrastructure, or they are willing to invest. By providing the exact "vendor", "product" and "version" of the preferred asset SENTINEL, through MITIGATE, will automatically provide the following:

- a list of known vulnerabilities as these are registered and acknowledged on open vulnerabilities databases (i.e., NIST Vulnerability Management Database)
- a list of related threats, based on the attack taxonomy provided from CAPEC
- a list of possible attack scenarios
- the calculated risk for each one of the aforementioned attack scenarios

The above scenario is going to be included in the MVP version of the SENTINEL platform. In addition, FP implemented the first mitigate-adapter, which successfully provides all required integration services from the MITIGATE system and provides corresponding REST APIs to the SENTINEL internal components in order to implement the SENTINEL Simulation Environment.

T2.3 has contributed to the following WP2 objective:

(i) 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 will provide significant input to D2.2 (“The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version”, to be delivered in M18), contributing also to milestone 2 (‘Innovation Fire’), due in M18.

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

T2.4 is led by TSI and started in M7. Since the start of T2.3, TSI 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 draft on the type of information provided for each external plugin and training course. After discussion 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) 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 comprises significant input to D2.1 (“The SENTINEL privacy & data protection suite for SMEs/MEs: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12. Contribution included a first selection of external plugins and trainings and how they match with security capabilities.

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

T2.5 is led by CECL and started in M7. During Y1, 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. The topic was discussed during the 3rd plenary meeting.

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 to D2.1 (“The SENTINEL privacy & data protection suite for SMEs/MEs: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12.

3.2.3 Work carried out in this work package per partner

ITML	As task leader of T2.2, ITML provided a description of the IdMS solution required by SENTINEL, with a list of goals, requirements, and challenges, as well as a concrete proposal and time plan for the implementation of a first proof-of-concept demonstrator to be part of the M12 MVP. Furthermore, ITML participated in relevant meetings of T2.3 discussing the ways cybersecurity components (plugins) should be integrated in the SENTINEL framework, focusing on exposing APIs (if applicable), list of capabilities and configuration information. This task is also linked with T3.3 that ITML leads, addressing storage of the above information in the Plugins repository. ITML is contributing to T2.3 with the Security Infusion plugin, that will be used as one of the cybersecurity offerings of SENTINEL. Finally, ITML participated in relevant meetings discussing the way open-source solutions will be incorporated in the SENTINEL framework and participated in meetings for requirements and constraints and requirements set by relevant regulations and guidelines that SENTINEL should adhere to. ITML has also led the delivery of D2.1, contributing key content for all sections.
LIST	During Y1, as T2.1 leader, LIST has managed activities carried out in sub-task T.2.1.1, T.2.1.2, and T.2.1.3. 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. Finally, LIST has provided significant input for D2.1.
IDIR	In Y1, IDIR has participated in technical activities conducted in T2.1 by collaborating with LIST and other partners in the definition of the common SENTINEL data model for profiling, which is driven by privacy and personal data protection (GDPR) requirements and modelled to comply with standardised records of processing activities (ROPAs). This work is in direct exchange with T4.3 to establish a basis for SME profiling based on tailored requirements and the definition of the appropriate capabilities. Other activities performed, mostly within the last quarter of Y1, include an approach to estimate the risk associated with each processing activity with and without performing a complete DPIA, and to establish the basic data exchange between the GDPR compliance self-assessment and SENTINEL's Profile and Self-Assessment services, for the MVP release (M12).
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. STS has also participated in discussions regarding integration architecture patterns that could be applied to the cybersecurity components and their APIs.
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 MySENTINEL UI (see D5.1).
TSI	For T2.4, after meetings and discussions with partners a first list of capabilities to be matched by open-source solutions has been built by TSI. In addition, there has been planning on the metadata and information which will be produced for each external plugin and how this information will be transmitted. Additionally, TSI contributed to the section "Continuous management and integration of opensource technology offerings and solutions for D2.1 where a first set of external plugins and trainings was presented.

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. One development identified was the EDPB board opinion 1/2022, adopted on the 1st of February 2022, on the requirements for data protection certification criteria, which could be relevant to the SENTINEL branding and communication activities. The topic was discussed during the 3rd plenary meeting in Chania Crete (Greece) in M12.
FP	During this reporting period FP participated in all WP2 meetings as well as and other dedicated meetings for the self-assessment module development. Within these meetings and specifically for T2.3, FP has introduced a first approach for properly utilize and integrate the cybersecurity components contributed from the SENTINEL partners. This will be a step approach process based on which the first plugin that will offer services and functions will be the MITIGATE tool, through the SENTINEL simulation environment in which SMEs/MEs will be able to build cyber-security what-if scenarios providing information for their cyber-assets. Within this environment, SENTINEL (through MITIGATE) will automatically inform SME for potential vulnerabilities, threats and risks. FP, through its participation at all WP2 meetings, has also contributed to the design process based on which open-source solutions will be properly utilized within the SENTINEL context and offer services and functions. Finally, FP has participated in all meetings relevant directly or indirectly to T2.5 by discussing on 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. Finally, in the last three-month period (M10-M12), FP introduced the first Organization and Technical Measure (OTM) classification based on which many different SENTINEL components and WPs will be built upon. Our initial try 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 introduced 114 different OTMs grouped in 10 organization and 10 technical categories. These OTMs will be further considered from the SENTINEL privacy and data protection compliance framework (T2.1). The first mitigate-adapter was implemented for the realization of the SENTINEL Simulation Environment, which is introduced in the first (MVP) version of the SENTINEL platform.

3.2.4 Status of Deliverables and Milestones

The work conducted in WP2 contributed to reaching milestone MS2 and well-documented in deliverable D2.1.

Table 8. Status of WP2 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D2.1	The SENTINEL privacy & data protection suite for SMEs/MEs: MVP	ITML	Demonstrator; PU; M12	Submitted
MS2	Innovation Flame	ITML	M12	Achieved

3.2.5 Deviations from Work Plan

There were no deviations from the GA. Although the partner “The SHELL” has terminated its partnership with SENTINEL since M6, WP2 activities progressed as planned. ITML has accepted to take over the leadership of T2.2 and undertakes all the relevant activities.

The writing process of D2.1 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.2.6 WP2 planned activities for the next period

For the next project period the WP2 activities will be focused on the following aspects:

- Delivery of full-featured version of IdMS, including full compliance with the MyData model, ‘one-click’ integrations with existing SME/ME solutions.
- Investigation of external training services (through external plugins and open-source training modules) that will provide additional training capabilities to SMEs/MEs.
- Further enhancement of the GDPR CSA module to ensure personal data protection in accordance with respective requirements.
- Enrichment of the SENTINEL framework with plugins, such MITIGATE and Security Infusion, to boost the level of security within an organization.
- Further monitoring of various sources for developments in the data protection landscape.

The envisioned work will be reported in D2.2 and D2.4 in M18.

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 reporting period

WP3 is led by ITML and started in M7. The WP3 started with a kick-off meeting, during which task leaders presented the outline, goals and challenges for their respective tasks. The technical progress was notable for the open data security platforms (T3.1), the refinement of specifications for the Incident handling module and the Recommendation Engine (T3.2, T3.3) and a first draft of the inner workings of the Policy Drafting module and the corresponding policy templates (T3.4).

A high-level, overall planning for WP3 technologies is put in place, with a more detailed action items list set for the demonstration of these technologies in the upcoming MVP (M12).

During Y1, the key achievements of WP3 in terms of developed technologies include:

(i) **Open data security platforms** as accessed and used by the Observatory: For this module a mechanism and the corresponding infrastructure have been developed to access and monitor an instance of the Malware Information Sharing Platform (MISP) for retrieving information related to detected and well-known security threats and vulnerabilities.

(ii) Recommendation Engine: For this module, concrete responsibilities, along with its exposed interfaces, required inputs and delivered outputs have been defined. Additionally, the need for a supporting repository module has been identified.

(iii) Policy Drafting module as part of the Policy Drafting Use case: For this module, the required inputs retrieved from the Recommendation Engine have been defined. Additionally, a Policy Template that is based on a global terms taxonomy has been defined which is delivered as an output of this module to the SENTINEL end-user.

The functional details of the modules of the SENTINEL digital core, and their implementation details are explained in D3.1, which contributes to milestone 2 ('Innovation Flame' due in M12).

3.3.2 Key WP3 achievements during reporting period at task level

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

T3.1 is led by AEGIS and started in M7. AEGIS, as part of the preparatory work, made an investigation 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 with 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. This instance consumes open, public sources and feeds to receive updated information on current threats and vulnerabilities. In coordination with T4.4, a decision has been made on the data storing technology that can be used for the Observatory Knowledge Base. By combining the two approaches, it has been set up a base on which it will be able to build SENTINEL's threat intelligence platform, which will not only receive data from the community but also share and give back all relevant information. Additionally, it will be able to include other open security data sources and platforms, in order to give the end-user a more concrete approach to assess their organization's security.

T3.1 has contributed to the following WP3 objective:

(i) 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 D3.1 ("The SENTINEL digital core: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T3.2 The incident handling and sharing module

T3.2 is led by ITML and started in M7. This task was initiated within the WP3 kick-off meeting that set the outline and goals of incident handling and sharing modules. 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 end-users 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.

Although the incident handling service is not delivered as part of the MVP, within the context of WP3, initial suggestions for approaches, technologies and tools were discussed, including questionnaires and forms for the collection of incidents, automated tools for detecting potentially harmful events, as well as the inner workings of the proposed solution. In addition, for the needs of the SENTINEL's full-featured, the ITML's Data Fusion Bus (DFB) has been proposed as a SENTINEL offering that facilitates the collection, aggregation and streaming of predefined types of documents.

T3.2 has contributed to the following WP3 objective:

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

The above comprises significant input to D3.1 ("The SENTINEL digital core: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T3.3 The intelligent recommendation engine

T3.3 is led by ITML and started in M7. This task was initiated within the WP3 kick-off meeting that set the outline and goals of the Recommendation Engine. The participating partners discussed the required inputs and desired outputs of the Recommendation Engine. More specifically, its inputs depend heavily on previous steps that an SME may take while executing the Policy Drafting flow. 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. Within the context of these meetings, the relationship with T3.4 was discussed, as the outputs of the engine are directly consumed by the Policy Drafting module. The Recommendation engine is planned to be demonstrated as part of the M12 MVP, initially as a rule-based engine that provides sets of recommendations depending on cases of profile and risk level inputs.

T3.3 has contributed to the following WP3 objective:

(i) the SENTINEL Intelligent Recommendation Engine.

The above comprises significant input to D3.1 ("The SENTINEL digital core: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T3.4 Policy drafting, enforcement and orchestration module

T3.4 is led by FP and started in M7. The purpose of the Policy drafting module is to convert the list of tools provided by the recommendation engine into a meaningful, structured, and enforceable policy draft. While the recommendations list only provides the tools, by which a company may achieve its goals, 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. In essence, a policy draft provides both the tools and the methods for an SME/ME to address their security requirements.

As 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. In addition, to identify the template to structure the various draft tailor-made optimization policies and specify the units of the Organizational and Technical Measures (OTMs) upon which the policies will be 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).

Based on these OTMs, the raise score of the assessment process and the recommendations of the recommendation engine the policy drafting module will eventually build the required human readable policy that will be published at the MySENTINEL context. Considering this, FP designed and proposed an algorithm, upon which the policy drafting module will be able to utilize three different templates of policies: one for LOW, one for MEDIUM, and one for HIGH self-assessment scores.

Finally, FP designed and proposed a policy template which consists of the following main sections:

- Policy details: the section which consists of the main metadata of the policy (creation date, last modified date and time, etc.).
- Organization Info: the section which consists of the main information the organization has provided during registration of its profile.
- Processing Activities' Assessments: the section which lists one by one the processing activities with their assessment results.
- Recommendations: the section which includes all the recommendations based on the analysis performed from the SENTINEL platform.

The first version of the policy drafting module was implemented, considering the recommendations provided by the Recommendation Engine and based on these, it builds upon and generates a policy draft, which only consists of the recommended organization and technical measures. These measures come with a generic policy text, without considering additional factors such as asset ownership, asset locality etc.

T3.4 has contributed to the following WP3 objective:

(i) the SENTINEL Policy Drafting and Enforcement modules.

The above comprises preliminary input to D3.1 (“The SENTINEL digital core: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12. A more detailed presentation of this module will be presented in deliverable D3.2 (“The SENTINEL digital core: Full-featured version”, to be delivered in M18), contributing also to milestone 3 (‘Innovation Fire’), due in M18.

3.3.3 Work carried out in this work package per partner

ITML	As WP3 leader, ITML coordinated the discussions for the selection of external open data security platforms and participated in testing the suggested sources. ITML provided outlines, goals and specifications for the Incident Handling module and the Notification Aggregator. In addition, ITML provided a refinement of the initial specifications of the Recommendation Engine, while contributing to the discussions for the inputs and outputs of the engine. An initial suggestion of the inner workings of the engine for the upcoming MVP was also put forward. Taking into account the close relationship between T3.3 and T3.4, ITML participated in the design and specification of the Policy Drafting module and its dependency to the Recommendation Engine, as well as the initial interfacing of those components within the context of the MVP (M12). ITML has also led the delivery of D3.1, contributing key content for all sections.
IDIR	Within Y1 of the project, IDIR has contributed work in T3.3 and T3.4. In T3.3 the main body of this work focused on clarifying the data exchange between the Self-Assessment and Core contexts and the mapping between the ROPA/SME profile common data model and the potential inputs required by the Recommendation Engine. In T3.4, IDIR proposed a mapping between the cataloguing of organizational and technical measures detailed in D1.1 (Section 3), and the project’s base policy templates. Specifically, a direct mapping was proposed between the risk level associated with each personal data processing activity in the SME profile and the assigned policy template in two-tiered approach: (a) when only the initial assessment is executed the PAs are marked as either ‘potentially high risk’ or not, and the associated policy template (high or low) drafted or (b) when the GDPR CSA and/or DPIA assessments have been triggered, a low/medium/high or potentially ‘very high’-risk policy template applied. Work in these two tasks has matured the partners understanding of the interrelations between contexts and data and helped envision an end-to-end service towards SENTINEL’s proof of concept / MVP. Towards the end of Y1 (Q4), more detailed technical tasks were performed for the MVP integration, such as a) finalizing the Policy template and b) identifying the data exchange between the SA and Profile Services and the Recommendation Engine and Policy Drafting modules.
INTRA	INTRA has actively participated and contributed to all WP3 discussions. More specifically, and as part of T3.2, INTRA contributed to the definition of requirements and specifications of the Incident Reporting module. More specifically, the scenarios were the following: (i) the platform detects a security incident related to the SME infrastructure, either through a continuous auditing plug-in or via a public database and (ii) the SME wants to report an incident with appropriate response teams having being explored. Furthermore, INTRA contributed to the definition of the Recommendation Engine’s interconnection with the Self-Assessment and Policy Drafting modules in order to better define its capabilities and responsibilities in the pipeline of generating policy recommendations (T3.3). Finally, in T3.4 INTRA contributed to the mapping of risk levels identified in terms of processing activities

	onto the actual policy templates that will be proposed. Good practices were investigated and requirements for Organizational and Technical Measures were identified.
STS	STS has actively participated and contributed to all WP3 discussions. Best practices were investigated and contributions were made in determining the process to identifying the risk levels based on the processing activities captured during the initial assessment of the SME/ME. The outcome of this initial assessment will trigger either or both the GDPR and DPI assessments. Furthermore, the MVP version of the DPI self-assessment tool was designed and implemented. STS has contributed to the overall architecture discussions and how the DPIA tool would be integrated with the rest of the platform and its modules, such as the orchestrator and policy drafting modules.
AEGIS	During Y1, AEGIS had participated in all WP3 meetings and performed investigations for external open security data sources and gave to the rest of the consortium an outline of the most well-known. Furthermore, AEGIS has implemented a MISP instance for the MVP version of the platform. Furthermore, as a participant in the work related to T3.2, AEGIS participated in every related discussion and meeting and contributed to what was requested in accordance with the instructions provided by the task leaders as well as the Work Package leader. Finally, in collaboration with T4.4, AEGIS has chosen a data storing technology to be used for the Observatory Knowledge Base.
CECL	The CECL has participated in all WP3 related meetings taken place in the first project year, especially the ones focusing on T3.4 concerning the policy drafting module.
FP	During Y1, FP participated in all scheduled meetings and calls related to WP3. 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 design phase of the intelligent recommendation engine where critical decision support capabilities take place. Based on the initial approach of the SENTINEL architecture the recommendation engine is one of the core SENTINEL components the output of which is further processed by the Policy-Drafting to build and publish a human readable policy for the SME. Additionally, FP designed and proposed an algorithm, upon which the policy drafting module will be able to utilize three different templates of policies (one for LOW, one for MEDIUM, and one for HIGH self-assessment scores) for building the SME policies. 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 will be recorded and mapped to the processing activities and will be used at the building process of the human readable policy at a later stage. Finally, FP implemented the first version of the policy drafting module. This module considers the recommendations provided from the Recommendation Engine and based on these, it builds upon and generates a policy draft, which only consists of the recommended organization and technical measures and a generic policy text, for each one of them.

3.3.4 Status of Deliverables and Milestones

The work conducted in WP3 contributed to reaching milestone MS2 and well-documented in deliverable D3.1.

Table 9. Status of WP3 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D3.1	The SENTINEL digital core: MVP	ITML	Demonstrator; PU; M12	Submitted
MS2	Innovation Flame	ITML	M12	Achieved

3.3.5 Deviations from Work Plan

There were no deviations from the GA. Although the partner "The SHELL" has terminated its partnership with SENTINEL effective from M7, WP3 activities progressed as planned. ITML has conceived and submitted a mitigation plan, based on which AEGIS has taken over The SHELL's contribution in T3.1 and T3.2, and STS and FP took over their contribution in T3.4.

The writing process of D3.1 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.3.6 WP3 planned activities for the next period

After the successful release of the SENTINEL MVP, the WP3 activities will continue towards the enhancement of the technologies developed as part of the SENTINEL digital core. To that end, WP3 will

- Explore and incorporate more external open data sharing platforms (e.g., HELK, NIST NVD).
- Implement the Notification Aggregator Incident Handling modules using DFB.
- Collect more sample data from SMEs/MEs to expand the rule base of the Recommendation Engine.
- Design Policy Enforcement procedures.

The envisioned work will be reported in D3.2 in M18.

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 reporting period

WP4 is 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.

Within Y1, the key achievements of WP4 include:

(i) The design and implementation of SENTINEL's SMEs/MEs self-assessment services.

(ii) The establishment of a stable shared data model for the SME profile. In this regard, the design, implementation, and MVP deployment of the SENTINEL architecture has been based on two key components: The Profile Service and The Self-Assessment (SA) Service.
(iii) Simulations and training for SMEs/MEs, and integration of ACS's CyberRange platform in the SENTINEL environment.
(iv) Technical effort towards the development of the SENTINEL Observatory and knowledge base, including external data sources, data formats, storage technologies and user-facing collaborative tools.

Overall, the work leading up to M12 has enabled all partners to better understand user journeys, clarify roles and responsibilities, successfully release the SENTINEL MVP and bring the project closer to a feasible end-to-end technical solution.

The functional details of the SENTINEL services, and their implementation details are explained in D4.1, which contributes to milestone 2 ('Innovation Flame' due in M12).

3.4.2 Key achievements during reporting period at task level

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

T4.1 is 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 have 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. The functional details of the CyberRange and its integration within the SENTINEL platform are explained in D4.1 in more detail.

T4.1 has contributed to the following WP4 objective:

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

The above comprises significant input to D4.1 ("The SENTINEL Services: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T4.2 Data protection impact assessment and assurance

T4.2 is led by STS and started in M7. Since M7, there have been several 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, is 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 will be provided on the processing activities. A series of specific questions will be asked and organizational and technical measures (OTMs) will be mapped. Based on the answers provided the processing activity will be marked as potentially high risk and the relevant SA tool will be triggered.

The two SA tools will be API-driven, and a first attempt of the required APIs has been made. They are indented to be questionnaire based and no UI is required to be provided by these tools, in order to keep the solution to the users as simple as possible. A stable shared data model for the Organization profile is essential.

During the last quarter of the first year, STS was highly focused in the design and the implementation of the MVP version of the SENTINEL platform and the MVP version of the DPI self-assessment tool. STS was closely collaborating with the rest of the technical partners, attending weekly technical physical meetings in Athens on top of the regular planned calls to reach a satisfactory design of the MVP.

In addition, STS was chairing the weekly MVP Technical Meetings focused on the self-assessment service of SENTINEL 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 an Agile-based approach was followed. A project was created in GitHub and the period between 24th of March 2022 and the MVP demo date (31st of May 2022) was split in 7 sprints of 2 weeks duration each. Overall, this approach was proven to be very helpful as it was very clear which partner was working on what tasks and their dependencies. Their progress was 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 partners.

In terms of delivery, STS during this period, designed and delivered the MVP version of the DPIA toolkit, which is based on the state-of-the-art tools and questionnaires tailored to the needs of SENTINEL. It was designed to allow SMEs to identify and minimise the data protections risks of one or more processes involved within a project. 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.

The MVP version of the DPIA, consists 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.

T4.2 has contributed to the following WP4 objective:

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

A basic functional version of the DPIA plugin was included in D4.1 ("The SENTINEL Services: MVP", delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12. A more detailed description and further implementation will be presented in D4.2 ("The SENTINEL

Services: Full-featured version", to be delivered in M18), contributing also to milestone 3 ('Innovation Fire), due in M18.

T4.3 Tailor-made requirement analyses via self-assessment, training and RASE scoring

T4.3 is led by IDIR and started in M7. Since the launch of this task, significant work was accomplished towards designing and implementing SENTINEL's SMEs/MEs 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 profiling will store (a) the minimum amount of data required for the initial assessment such as structure, sector, and operating environment; (b) the personal data processing activities (ROPA) according to the GDPR principles and (c) infrastructure, cyber assets, goals, capabilities, and constraints of the organization. It has been established that, towards SENTINEL's MVP the self-assessment process will be GDPR (PDP)-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. Participant SMEs will be able to leverage SENTINEL's profiling as their official ROPA towards this end. A series of organizational and technical measures (OTMs) will also be recorded and mapped to the processing activities and then, the initial assessment will consider several privacy risk criteria against each process to establish a basic risk assessment which will be passed on to the Core context for recommendations and policy drafting. The SME profile will also (a) consider a number of Non-GDPR criteria such as cybersecurity assets and other requirements, and (b) store the results of the self-assessment plugins, namely the GDPR Compliance Self-Assessment, which many be triggered by any SME processing personal data and the Data Protection Impact Self-Assessment, 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. Major T4.3 achievements leading up to M12 have been:

- The establishment of a stable shared data model for the SME profile, which is common among core SENTINEL context and modules as well as plugins (Figure 2).
- 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. This work will influence the user journeys currently being designed towards the project's MVP.
- Detailed UI mockups to showcase the intended functionality, as well as the look and feel, of MySENTINEL.
- A 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 3). This model is implementation independent and intended for 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.
- The design, implementation and MVP deployment of two key technical components of the SENTINEL architecture:
  - The Profile Service
  - The Self-Assessment (SA) Service

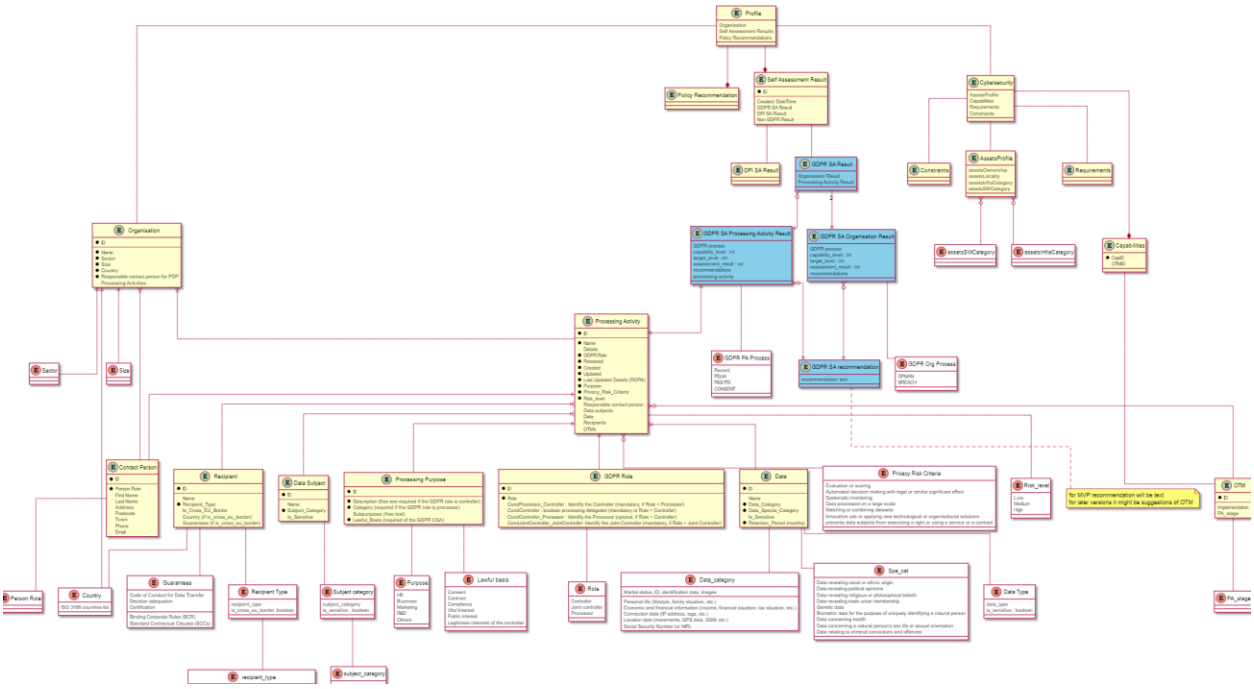

Figure 2. Updated common SENTINEL Organization Profile data model

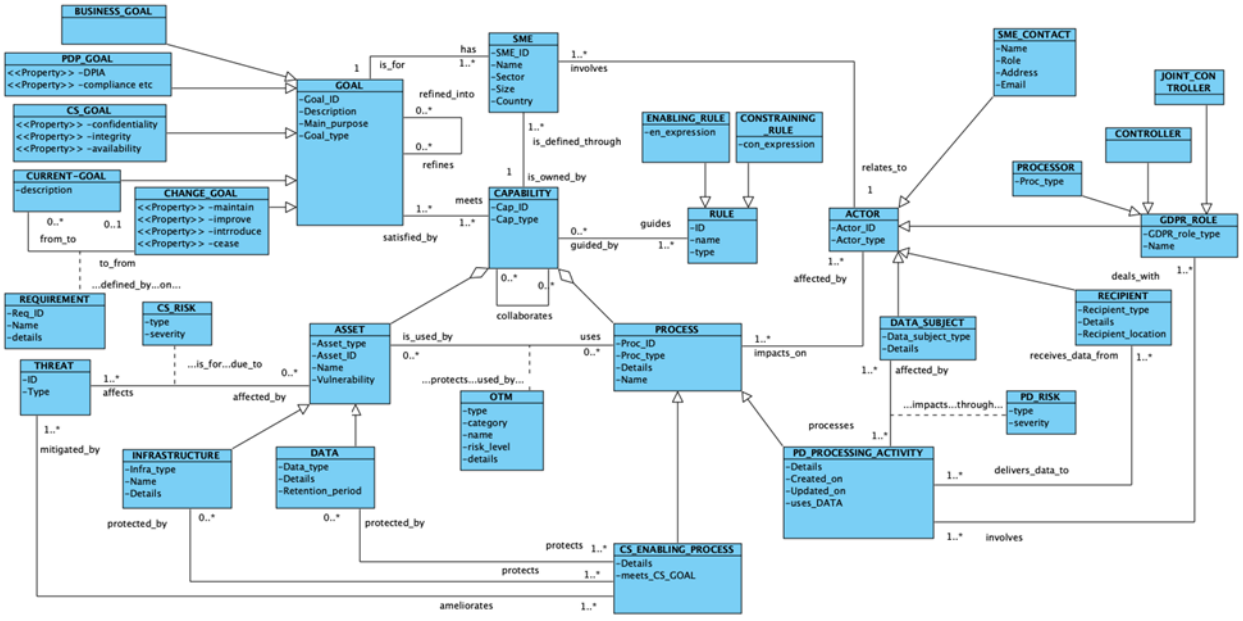

Figure 3. The conceptual metamodel for SME profiling

T4.3 has contributed to the following WP4 objective:

(i) 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).

The above comprises significant input to D4.1 (“The SENTINEL Services: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12.

T4.4 The SENTINEL Observatory

T4.4 is led by ITML and started in M7. ITML led the discussions that address all topics relevant to the Observatory, including external data sources, data formats, storage technologies and user-facing collaborative tools. The activity for selecting and using external data sources is directly linked with T3.1 where significant progress has been made for the selection and exploration of candidate open data security platforms. At this moment, the Policy data reuse module has not been examined, as it depends on the implementation of the Policy Drafting module in the context of T3.4. The rest of the above-mentioned topics are planned to be addressed and demonstrated in the M12 MVP, by showcasing the relevant use case of “Accessing the Knowledge Base”. To that end, a time plan has been outlined to provide an end-to-end service that gives the user the ability to navigate through and consult on security related information collected from external sources.

T4.4 has contributed to the following WP4 objective:

(i) the delivery of the SENTINEL Observatory and knowledge base.

An initial version of the Observatory was included in D4.1 (“The SENTINEL Services: MVP”, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12. Further development of this context will be presented in D4.2 (“The SENTINEL Services: Full-featured version”, to be delivered in M18), contributing also to milestone 3 (‘Innovation Fire’), due in M18.

3.4.3 Work carried out in this work package per partner

ITML	ITML participated in meetings about the initial definition, scope and contents of self-assessment trainings, as well as potential utilization of these offerings by the Recommendation Engine. Furthermore, as T4.4 leader, ITML has coordinated the discussions for the implementation of the Observatory, including selection of external data sources, data formats/structure, storage technologies, collaborative tools and UI issues. The outline of a proof-of-concept implementation and demonstration of the Observatory has been put in place. ITML has conducted the internal review of D4.1.
LIST	During Y1, LIST has contributed to T4.2 via eliciting requirements that are common to both GDPR compliance assessment and DPIA. In addition, LIST has started linking-up of common requirements with SENTINEL’s Organizational and Technical Measures Database.
IDIR	Within Y1 of SENTINEL, IDIR, as the T4.3 leader, has contributed key work towards technically maturing the proposed solutions in the project’s self-assessment context 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 the last three-month period, more concentrated and focused work led to i) the deployment of both the theoretical conceptual model for SME profiling based on tailored requirements, shown in Figure 2 in the above section and ii) the implementation of SENTINEL's core Profile and SA Services.
INTRA	Within Y1, INTRA actively participated in all Observatory-focused discussions as part of Task 4.4. Contributed to the formulation of the Observatory use case as well as its structure and interfaces.
STS	STS 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 was delivered the MVP version of the DPIA toolkit. STS, as T4.2 leader, but also actively involved in all the MVP related discussions, has been chairing the MVP 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), that describes the DPIA toolkit, which was designed and implemented for the MVP version of SENTINEL.
AEGIS	Within Y1 of the project, AEGIS participated in related discussion, and meetings and contributed to what was requested by the task leaders as well as by the WP leader. In more detail, in the period between M7 to M9 AEGIS participated in the discussions on the study for the establishment of new correlations of the Tasks of the Work Package with tasks of other work packages and based on the refined architecture that was presented in late November 2021. Additionally, as part of the T4.4, AEGIS collaborated with the partners involved in T3.1 to decide on the technology that will be used to store all data from the threat intelligence and sharing platform. Moreover, in the same context, AEGIS established communication between the Observatory Information Exchange module and the Observatory Knowledge Base.
ACS	As a leader of WP4, ACS led the KoM and 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. The development and implementation processes have been successfully launched.
FP	During Y1, 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. The core process is the SME profiling which consists of the data required for performing the initial assessment, the data processing activities, and the assets of the organization. At this process a number of organizational and technical measures are required also since based on these the Policy-drafting module will (later on) build the human readable policy for the SME. Furthermore, the tasks of this WP contribute to the proper utilization of the SENTINEL plugins (tasks T2.3 and T2.4 which FP leads and participates) since many of these require the list of processing activities and the list of the organizational assets.

	In the last three-month period (M10-M12) FP introduced the first version of the OTM classification. For each OTM a list of optional capabilities is mapped, upon which all plugins and training material will be also mapped. This mapping will allow the Recommendation Engine to generate the proper recommendations for each SME/ME.

3.4.4 Status of Deliverables and Milestones

The work conducted in WP4 contributed to reaching milestone MS2 and well-documented in deliverable D4.1.

Table 10. Status of WP4 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D4.1	The SENTINEL services: MVP	IDIR	Demonstrator; PU; M12	Submitted
MS2	Innovation Flame	ITML	M12	Achieved

3.4.5 Deviations from Work Plan

There were no deviations from the GA. Although, the partner The SHELL has terminated its partnership with SENTINEL effective from M7, WP4 activities progressed as planned. ITML has conceived and submitted a mitigation plan, based on which STS took over The SHELL's contribution in T4.2 and undertakes all the relevant activities since M7.

The writing process of D4.1 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.4.6 WP4 planned activities for the next period

WP4 will step up its processes towards the enhancement of the SENTINEL services driven by both WP2 and WP3 towards the full-featured version of the SENTINEL services in M18. In this context, WP4 will:

- Intensify its efforts to enhance the capabilities of the SENTINEL services with respect to i) privacy and data protection, ii) cybersecurity technologies and technologies already brought by partners (as plugins).
- Enrich the scenarios used for DPIA self-assessment tool, CyberRange tools based on additional requirements received from end-users as a results of first testing trials.
- Enhance the SENTINEL Observatory and knowledge base, including additional external data sources and data formats.

The envisioned work will be reported in D4.2 in M18.

3.5 WP5 – SENTINEL continuous integration and system validation

Leader: INTRA

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

Duration: M9- M36

3.5.1 Summary of results achieved during reporting period

WP5 is led by INTRA. It started in M9 with two tasks being active for the time being, i.e., T5.1 and T5.2, dealing with the SENTINEL front-end components and the overall system integration respectively.

Despite the recent start of the work package, there has been significant progress in both aforementioned fronts. More specifically, key achievements of WP5 are listed below:

(i) INTRA together with WP5 involved partners, worked on the development of concrete User Journeys, in order to help specify the interaction of the system with the SME representative and design the required User Interfaces (UI) as well as the communication with the other SENTINEL modules. To that end, initial sets of UI mock ups were developed and feedback has been collected during discussions in an iterative manner, resulting in various adjustments and improvements.

(ii) On a parallel track, we developed a process and set up the tools to facilitate continuous integration. Integration started by selecting the scenarios to be implemented as part of the SENTINEL MVP in M12. The selection was made based on the criterion of exposing as many modules as possible while at the same time demonstrating value to the user. To that end, use cases UC1 “SME registration and profiling”, UC2 “Completing a self-assessment workflow”, UC3 “Acquiring policy recommendations” and UC6 “Consulting the Observatory Knowledge Base”, as described in D1.2, were selected.

(iii) Subsequently, we defined more specific user journeys and scenarios and designed mock-ups to support them. Modules were mapped to these scenarios and the interfaces among them, including messages and data structures were specified. On a parallel track, after an initial sizing of the required infrastructure, we allocated and configured the Virtual Machines to host the platform and all supporting services. The actual deployments of modules started taking place as they were being delivered and incorporated to the docker compose environment. Finally, integration tests were conducted in a bilateral manner, which were subsequently followed by basic end-to-end tests.

Development towards the MVP was done in an agile manner. Starting from the beginning of March a series of meetings has been carried out where partners were asked to estimate all the individual pieces of work that needed to be carried out from their end to finalize the development of their respective modules, as well as to identify any potential dependencies from other partners’ work. 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 MVP deadline as a backup. Sprints were monitored on a weekly basis in dedicated meetings that combined retrospect and planning activities.

The aforementioned actions, together with the commitment of all technical partners resulted in the timely development and deployment of all major SENTINEL modules to an integrated platform, supported by the first version of the MySENTINEL UI, which accommodates all functionalities envisaged for the MVP.

The results are reported in D5.1 and D5.4, which both contribute to milestone 2 (‘Innovation Flame’ due M12).

3.5.2 Key WP5 achievements during reporting period at task level

T5.1 Interactive visualizations and front-end components

T5.1 is led by AEGIS and started in M9. An early planning for the task activities was presented during the 2nd plenary meeting of the project (January 2022). As part of the preparatory work for the task, AEGIS also presented a series of early mockups to initiate the 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 with an initial version for the User Journey. At the current stage, the MySENTINEL dashboard includes links to components that are 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 detail about the technical development of MySENTINEL dashboard.

Moving forward, work will continue to be comprehensive to refine and enrich the content of the UI. By conferring with the rest of the partners, through online teleconferences and physical meetings, AEGIS will include an increasing number of modules that play a pivotal role in the use-cases defined and detailed in D1.2. All this effort will result in the intermediate and final versions of the MySENTINEL UI dashboard and will be documented in subsequent iterations of D5.1, namely D5.2 and 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 D5.1 (“The SENTINEL visualization and UI component-first version, delivered in M12), contributing also to milestone 2 (‘Innovation Flame’), due in M12.

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

T5.1 is led by INTRA and started in M9. Within this task, a GitHub organization (https://github.com/SENTINEL-EU/) and subsequent repositories were set up to cater for code hosting and versioning, as well as a number of dedicated projects to facilitate tracking of action items and bugs towards the MVP release, and beyond. In terms of deployment, all modules are being delivered in a dockerized manner and automatically deployed on INTRA’s infrastructure using docker compose. A docker registry server has also been deployed to facilitate delivery and storage of docker images.

Embarking from the MVP, as the tools and processes put into place have proved to be rather efficient and effective so far, the plan is to continue using them. After M13, a retrospective session will be performed in order to facilitate any necessary adjustments reflecting on the feedback of the reviewers’ and the technical partners of the consortium. Furthermore, more tools (such as Jenkins and SonarQube) are considered to be introduced to further automate the integration and delivery pipeline, while deployment is planned to be taking place on Kubernetes.

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).

The above comprise significant input to D5.4 ("The SENTINEL Minimum Viable Product, delivered in M12), contributing also to milestone 2 ('Innovation Flame'), due in M12.

T5.3 From the prototype to the final solution

This task is led by UNINOVA and is planned to start at M31 according to the GA. No work has been carried out at this stage.

3.5.3 Work carried out in this work package per partner

ITML	ITML participated in the initial discussions relevant to MySENTINEL contributing with ideas on user journeys and flows. Furthermore, ITML provided support on integration of SENTINEL's components and the operation of the integrated framework. More specifically, ITML contributed 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. ITML has conducted the internal review of D5.1 and D5.4.
LIST	As a leader of GDPR compliance self-assessment module (see WP2/Task 2.1), LIST has developed an API to ensure its integration with the SENTINEL platform.
IDIR	In the last quarter of Y1 (M9-M12), IDIR has contributed with work in T5.2 towards preparing SENTINEL's technical integration approach, together with other technical project partners. The project's integration plan details the way in which the different components of SENTINEL's conceptual architecture come together and are adapted and integrated in one common framework. In this plan IDIR has also contributed tools, technologies, and methodologies for integration and for addressing system architecture, deployment, DevOps, interoperability, scalability, performance, and security, and participated in the discussions to clarify the release plan of the SENTINEL solution, towards its proof of concept / MVP.
INTRA	INTRA has organized and actively participated in all related calls and discussions. INTRA has set up and configured all the required infrastructure and processes to facilitate modules' integration as well as user journey definition. INTRA has coordinated and provided key content for D5.4.
AEGIS	As a leader of T5.1, AEGIS organized and coordinated several remote meetings to initiate discussion among technical partners and facilitate the development process. Additionally, AEGIS has delivered 3 different sets of mock-ups regarding the MySENTINEL Dashboard. At the current stage, the MySENTINEL dashboard includes links to components that are incorporated in the MVP. Organization Profile, Processing Activities, Contact Persons, Assets, Self-Assessment tools, Policy Recommendations and the Threat Intelligence platform comprise the modules offered to the end-user by the SENTINEL platform. AEGIS has also participated in discussions related to the SENTINEL integration activities. Finally, AEGIS has led D5.1 and delivered content for all sections of it, while it served as a reviewer for D5.4.
TSI	TSI has started to work on the integration of the repository which will contain the information of external plugins with other SENTINEL modules and has participated in all relevant telcos.

ACS	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.
UNINOVA	UNINOVA took part in all meetings associated with T5.2.
CG	CG participated in the meetings and discussions regarding the T5.2 activities and provided input to the integration leader (INTRA) and the individual technology providers to provide requirements and feedback, aiming at a better finetuning of SENTINEL services and tools.
TIG	Following initial engagement between AIRBUS and Juventas' IT provider it was agreed that there would be limited value in trialling technical innovations in respect of Juventas systems. Juventas use MS OneDrive and SharePoint to process and retain data/information. The structure of the system used by Juventas is bespoke. Therefore, TIG is in the process of engaging another SME, Dimensions Care, with whom it is anticipated that the testing of cyber range scenarios will be more effective.
CECL	Not involved in T5.1 and T5.2 and thus reporting is not relevant at this stage.
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 currently focused on the visualizations that are required to be delivered for the MVP phase of the project on M12. In a later phase more specific input will be given on the front-out outputs of the Policy Drafting and the Policy Enforcement modules. For the continuous integration towards the realization of a complete system (T5.2) FP focused on the proper integration of the MITIGATE plugin and how this will be realized in the MVP version of the SENTINEL system, enabling SMEs to build simulation computer security (CS) risk assessment scenarios for specific assets. In this context, the first version of the mitigate-adapter was successfully deployed, and the MVP version of the simulation environment was implemented and integrated with the first-mentioned. Additionally, the first version of the policy-drafting module was also implemented and deployed in the SENTINEL system.

3.5.4 Status of Deliverables and Milestones

The work conducted in WP5 contributed to reaching milestone MS2 and well-documented in deliverables D5.1 and D5.4.

Table 11. Status of WP5 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D5.1	The SENTINEL visualisation and UI component – first version	AEGIS	Demonstrator; PU; M12	Submitted
D5.4	The SENTINEL Minimum Viable Product	INTRA	Demonstrator; PU; M12	Submitted
MS2	Innovation Flame	ITML	M12	Achieved

3.5.5 Deviations from Work Plan

There were no deviations from the GA. Although the partner “The SHELL” has terminated its partnership with SENTINEL effective from M7, WP5 activities progressed as planned. ITML has conceived and submitted a mitigation plan, based on which IDIR took over The SHELL’s contribution in T5.2 and undertakes all the relevant activities since M9.

The writing process of D5.1 and D5.4 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

3.5.6 WP5 planned activities for the next period

For Y2, WP5 will aim at meeting SENTINEL’s milestone 3, i.e., the 1st version of integrated platform in M18. In this respect, WP5 will:

- Continue UI development with planned user flows beyond MVP.
- Facilitate the smooth and effective integration of the components by implementing an agile approach with iterations and development sprints.
- Closely monitor WP6 activities to collect feedback and requirements towards the definition of the specifications of the 1st complete prototype by M18.

These activities will be captured in corresponding deliverables, i.e., D5.2 and D5.5 in M18.

3.6 WP6 – Real-life experimental evaluations: SENTINEL pilots

Leader: CG

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

Duration: M10- M36

3.6.1 Summary of results achieved during reporting period

WP6 kicked-off in M10, thus the reference period of this report covers the WP6 activities conducted during the M10-M12 period. Based primarily 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, based on KPIs updated in T1.1.

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

CG, as a WP6 leader, kicked-off a SENTINEL pilot-focused meeting in M10 by inviting all the involved partners to discuss and understand the experimentation context of the project and ensure its requirements are met and facilitated by the infrastructure and the integrated platform.

A Key achievement of WP6 during the aforementioned period involve the refinement of the SENTINEL experimentation protocol (scoping and planning), including sub-systems and hardware components for demo purposes and utilization of simulation(s) in order to assess whether critical parts of the infrastructure are needed to accommodate and reflect the environments of the end-users engaged through the respective pilot cases (T6.1). To this end, and as an example, CG (Pilot Case 1) has already started providing the necessary information regarding its software/database infrastructure, i.e., the OS used, the database with the configuration used, schema of the database infrastructure, etc.

3.6.2 Key WP6 achievements during reporting period at task level

T6.1 SENTINEL experimentation protocol alignment and pilots' setup

T6.1 is led by FP and started in M10. To drive the task activities, initial talks about the main aim of the task (considering also input from previous tasks) were carried out during the dedicated session of WP6 monthly meeting. Moreover, through the 3rd plenary meeting which occurred in early May 2022, FP, as the leader of T6.1 highlighted the task's main objectives and proposed refinements for the experimental protocol and templates to be utilized for the experiments' specifications. In addition, FP initiated the discussion for the pilot operation setup action plan and time plan to be further commented and discussed with all the involved partners during the next respective WP6 meetings.

T6.1 has contributed to the following WP6 objective:

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

The above will comprise significant input to upcoming deliverable D6.1 ("SENTINEL Demonstration – initial execution and evaluation", to be delivered in M18), contributing also to milestone 3 ('Innovation Fire), due in M18.

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

This task is led by CG and is planned to start in M13. No significant achievements were addressed at this stage.

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

This task is led by UNINOVA and is planned to start in M13. No significant achievements were addressed at this stage.

T6.4 Evaluation and impact analysis

This task is led by STS and is planned to start in M22. No significant achievements were addressed at this stage.

3.6.3 Work carried out in Task 6.1 per involved partner

INTRA	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.
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.
CG	CG has kicked-off the WP6 monthly calls and supported the technical partners with the formulation of the end-user requirements. Furthermore, as a pilot case owner, CG has provided initial input regarding the specific challenges pertaining to the data handled by CG: • Personally Identifiable Information (PII) during the submission process • Cybersecurity protection of all stored data, etc. • Implementation of controls that limit any type of unauthorized access to the data In addition, to facilitate the ensuing operational trials, CG is in the process of finalizing the replication of CG's software infrastructure by providing the following information to all the involved technical partners: • the OS used • the database with the configuration used • schema of database infrastructure • the applications with the configuration used • the firewall, with the rules and • a network flow matrix
TIG	TIG has participated in the WP6 monthly call and by participating in all related discussions supported the technical partners with pilot requirements.
CECL	CECL took part 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. The interim Ethics manual, which will be part of the learning material, was finalised and discussed among the partners.
FP	As T6.1 leader, FP has illustrated the main task objectives to be followed and the activities to address T6.1 objectives and proposed directions for their execution to open discussions with all the partners involved in WP6 activities.

3.6.4 Deviations from Work Plan

There were no deviations from the GA. Although the partner “The SHELL” has terminated its partnership with SENTINEL effective from M7, WP6 activities are progressing as planned. ITML has conceived and submitted a mitigation plan, based on which AEGIS takes over The SHELL’s role in T6.2 and T6.3 and undertakes all the relevant activities.

3.6.5 WP6 planned activities for the next period

In the course of the second project year, CG together with TIG and UNINOVA will organize the pilot-focused meetings with technical partners to share information and to discuss on topics related to database infrastructure and storage, software/database infrastructure, integration,

visualization, demonstrators and evaluation starting from M13 towards the realization of the defined use cases. To this end, WP6 will:

- Finalize the pilot operation setup action plan and time plan.
- Collect solid information about the infrastructure regarding OTMs, software/database of each use case.
- Set up a plan for execution of operation trials on early version of the SENTINEL solution.
- Closely monitor WP5 activities in Y2 to collect information about the 1st complete prototype to be used and tested within each pilot scenario.

These activities will be captured in corresponding deliverable, i.e., D6.1 in M18

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 reporting period

WP7 is 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 Y1, WP7 activities focused on setting up of the fundamental communication and dissemination channels for the project. The project website (https://sentinel-project.eu/) has been designed and developed by ITML (see D7.1 submitted in M2). Currently it is fully operational and regularly updated.

The SENTINEL's LinkedIn and Twitter pages have been created, along with a YouTube channel, to promote awareness on the project and its results.

Promotional materials (three (3) newsletters, one (1) promotional video, one (1) brochure, one (1) poster as well as business card and a roll-up) 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 a preliminary business modelling, as part of D7.2 (submitted in M6).

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

- 1st Clustering Webinar with projects funded under the H2020-SU-DS02 and H2020-SU-DS03 topics
- Organization of Webinar "A privacidade e a proteção de dados pessoais no panorama nacional das PMEs", with the support of Produtech, DIH4CPS and DIHWorld

In addition to this, the partners have managed to submit three (3) conference papers

- Iosif Arvanitis, Grigoris Ntousakis, Sotiris Ioannidis, Nikos Vasilakis "A Systematic Analysis of the Event-Stream Incident" 15th EuroSec 2022, April 5 – 8 Rennes, France, **(accepted)**
- Tatiana Trantidou, George Bravos, Philippe Valoggia *et al.* "SENTINEL – Approachable, tailor-made cybersecurity and data protection for small enterprises" IEEE cyber security and Resilience, July 27-29, virtual **(accepted)**
- Evangelia Kavakli, Pericles Loucopoulos, Yannis Skourtis "Capability oriented RE for Cybersecurity and Personal Data Protection: Meeting the challenges of SMEs" 9th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE 2022), August 16, virtual **(submitted)**

The SENTINEL partners have already participated and presented the project in several events such as:

- CyberHOT summer school, 27-28 September 2021
- 5th NMIOTC Cyber Security Conference in the Maritime Domain, 29-30 September 2021
- Berlin Science Week 2021, 1-10 November 2021
- IDC Security Roadshow, 20th of April 2022
- Transferable Research & Laboratory Outcome, 29th of April 2022

while they have been accepted for participation in

- IoT Week 20222 workshop
- FIC 2022 International Cybersecurity Forum
- Projects to Policy Seminar (PPS) event invited by REA

SENTINEL has reached and secured the interest for further trialling of the SENTINEL framework of 3 Digital Innovation Hubs:

- DIH-WORLD
- PRODUTECH – Production Technologies Cluster
- DIH4CPS

while it has liaised with ten (10) EU projects

- PALANTIR-883335
- TRAPEZE-883464
- PUZZLE-883540
- ARCADIAN-IoT-101020259
- IRIS-101021727
- ERATOSTHENES -101020416
- IDUNN-101021911
- SECANT-101019645
- CyberKit4SME-883188
- CONCORDIA-830927

The exploitation activities will be intensified as soon as the MVP is released. Despite this, two important exploitation actions have been made in Y1. The project partners have organized two SME-centric workshops with a release of two SME engagement surveys.

D7.1 and D7.2 both contribute to milestone 1 (‘Project Baseline’ due M6).

3.7.2 Key achievements during reporting period 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. 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 has 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. That being said, there is expected to be a revisit to the business planning based on the acceptance of the MVP as part of brainstorming, as well as based on the feedback we may receive. This involves cooperation between Tasks 7.1, 7.2 and 7.3 and will be documented in the final business model, market analysis and long-term sustainability report (D7.9) at the end of the project.

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

The above comprise significant input to D7.1 (“Market analysis and preliminary business modelling”, delivered in M6), contributing also to milestone 1 (‘Project Baseline’), due in M6.

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

T7.2 is led by UNINOVA and started in M1. At the project kick-off meeting, the main objectives, short-term and long-term achievements were presented. The project website was officially launched within the M2 timeframe while a sneak peak was presented during the kick-off meeting, followed by the social media channels (LinkedIn, Twitter and YouTube).

With respect to the branding material, SENTINEL developed a project brochure, a business card, a poster and a roll-up. The SENTINEL newsletters have been released on a quarterly basis, where three issues have been released (M4, M7, M10). The SENTINEL promotional video has also been released in M12, and its available under the YouTube channel.

Considering attendance in events, SENTINEL participated in the "IDC Security Roadshow", held on the 20th of April, Lisbon, Portugal and also at the "Transferable Research & Laboratory Outcome", with one SENTINEL presentation, held on the 29th of April, UNINOVA, Lisbon, Portugal. SENTINEL was invited by the Embassy of Ireland in Berlin as part of the cooperation between the Irish (IDIR) and the German (AEGIS) partners, during the Berlin Science Week 2021, which was rigorously disseminated in their social media. Regarding upcoming events, SENTINEL will be present at a workshop within the "IoT week" conference, at the "International Cybersecurity Forum" with a booth in order to show its latest achievements related with the 1st release of the MVP and Projects to Policy Seminar (PPS) event invited by REA. 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.

With respect to academic publications, SENTINEL has submitted three (3) conference papers. Two papers have already been accepted, the third one is currently under review.

The WP7 monthly meetings are taking place regularly where all partners join and discuss actions for communication and dissemination activities. Finally, the SENTINEL social media channels, constantly being updated, increasing 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) above comprise significant input to deliverable D7.2 ("The SENTINEL website and visual identity", delivered in M2), contributing also to milestone 1 ('Project Baseline), due in M6.

Further actions towards achieving points (ii) and (iii) will comprise input for future deliverable, namely D7.3 ("Dissemination strategy and activities-interim version") to be delivered in M18, contributing also to milestone 3 ('Innovation Fire'), due in M18.

T7.3 Exploitation and standardization activities and best practices

This task is led by STS and is planned to start at M13. No achievements are to be reported at this stage.

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

T7.4 is led by UNINOVA and started in M1. Though at its early stage, the ecosystem building task has been very active during the first 12 months. With this respect the first attempt was made during the 1st plenary meeting, which took place in Guimarães, Portugal, 15-16 September 2021. when the 1st SENTINEL SME-centric workshop took place. Within the scope of the workshop

preparation, an online questionnaire was developed to collect insights from Portuguese SMEs that participated in the workshop. Also, the SENTINEL social media channels act themselves as enablers for the engagement of technology providers, as well as SMEs/MEs.

Another successful stakeholder engagement event was organized within the SENTINEL 3rd plenary meeting, held on the 6th of May in Chania, Greece, entitled "2nd SENTINEL SME-centric workshop", where we had the support of PRAXI Network in jointly inviting and engaging various business entities from Greece and other EU countries. The objective here was also to create awareness on GDPR compliance and personal data protection at the Greek SMEs ecosystem, present the SENTINEL offerings and register interest from the participant SMEs to trial SENTINEL services in the future.

Aligned with T7.2, a cluster webinar, involving several H2020 projects funded under the H2020-SU-DS-02 and H2020-SU-DS-03 topics was organized, representing ten (10) different EU projects. The webinar enabled SENTINEL to seek through other projects, ways to reach a wider audience of SMEs. The participation at the "International Cybersecurity Forum" and IoT Week, will also pave the way for reaching out to a wider audience of SMEs.

We've started our engagement with 3 digital innovation hubs (Produtech, DIH4CPS and DIHWorld). Such digital innovation hubs have supported the organization of a webinar entitled "*A privacidade e a proteção de dados pessoais no panorama nacional das PMEs*", held on the 13th of May 2022. This particular webinar was set to create awareness on GDPR compliance and personal data protection at the Portuguese SMEs ecosystem and present SENTINEL offerings. We had more than 70 registrations for this event. The highlights of the event are available at SENTINEL YouTube channel.

SENTINEL was present at the "Transferable Research & Laboratory Outcome" held on the 29th of April, UNINOVA, Lisbon, Portugal. In this event, there was a presentation of SENTINEL in one of the tracks dedicated to DIHs. During this event we have received an expression of interest from the "Digital Manufacturing Innovation Hub Wales", to collaborate with SENTINEL, in order to test and validate our offerings.

Within this task, SENTINEL is planning to engage with the European catalog of DIHs, launched by the European Commission. It is an online repository that includes more than 450 existing hubs across Europe. The plan is to use this network to disseminate SENTINEL offerings, promote events and liaise with different DIHs. SENTINEL has also initiated preliminary contacts with the following DIHs: INNOVA4TECH, Digital Manufacturing Innovation of Wales, INNOV TOURISM DIH, idD Portugal Defense, CONNECT5 and Madeira Digital Innovation Hub.

T7.3 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 INFO days.

The above will comprise significant input to D7.3 ("Ecosystem building and SMEs engagement report – interim version", to be delivered in M18), contributing also to milestone 3 ('Innovation Fire), due in M18.

3.7.3 Work carried out in this work package per partner

ITML	During Y1, ITML, has designed and delivered the project's website, which constituted the first deliverable of WP7 (D7.1). ITML has contributed to the T7.2 activities by producing, contributing and/or reviewing the project's communication material (such as newsletters, website updates, brochure, poster, promotional video). Furthermore, ITML has regularly created posts for communications on the project social accounts. Together with PRAXI Network, ITML has organized the 2nd SME-centric workshop co-hosted with the 3rd plenary meeting in Chania (Greece), while it has created the 2nd SME-centric questionnaire and contributed to the preparation of the questionnaire for the 1st SME-centric workshop (co-hosted with the 1st plenary meeting in Guimaraes, Portugal). In addition, ITML has coordinated the organization of the 1st Clustering Webinar with 9 other projects funded under the H2020-SU-DS02 and H2020-SU-DS03 topics. ITML took part in the "CyberHOT summer school" in September 2021. ITML has participated in all monthly and bilateral meetings regarding WP7 while it collaborated with the Dissemination Leader (UNINOVA), to seek synergies and collaborate with SMEs and business enterprises in order to promote the project offerings. ITML is going to disseminate the SENTINEL project in three upcoming events (IoT Week, FIC and PPS) that are going to take place in M13. In addition to these, ITML has prepared and released on a regular basis posts relevant to SENTINEL, GPDR compliance and data protection and security in SENTINEL's social media (LinkedIn, Twitter), as well as in its own media channels (social media and website).
LIST	During the first project year, LIST has attended the WP7 monthly meetings. LIST has also provided a description of the GDPR CSA module in a paper which describes SENTINEL's scope and objectives.
The SHELL	The SHELL has contributed to WP7 work through their participation in monthly WP7 calls (up until October). The beneficiary has also prepared, as part of their tasks for WP7, a post that was published in LinkedIn https://www.linkedin.com/feed/update/urn:li:activity:6836592765451730944/ and a post that was published in Twitter https://twitter.com/SentinelH2020/status/1431189622911082497 to raise awareness on SENTINEL's offering specifically with regard to cybersecurity readiness self-assessment services (total effort spent 0.2 PMs for WP7). **Since M6, the partner SHELL has been terminated from ECAS.**
IDIR	IDIR has participated at all three WP7 tasks active in the SENTINEL's Y1. Specifically, it has participated in all major WP meetings, contributed to social media content dissemination and creation; proposed and configured an email automation framework for automated newsletter content design, delivery and tracking; provided feedback on key dissemination content such as the newsletter (provided input about the SENTINEL baseline for the 2nd newsletter of SENTINEL) and the project video; driven the action to highlight the SENTINEL project activities, and specifically the cooperation between the Irish (IDIR) and the German (AEGIS) partners, during the Berlin Science Week 2021 through the Embassy of Ireland in Berlin, which was rigorously disseminated in their social media. Finally, IDIR is a key contributor in the common effort to define SENTINEL's business value for different stakeholder and customer personas and guide the outreach and early marketing efforts to make it approachable to its intended audiences. The initial feedback for this effort is gathered during the SME workshops and webinars organized during plenary meetings or independently.

INTRA	INTRA has participated in all meetings concerning the WP7 and provided input for the SENTINEL website. INTRA also regularly contributed to SENTINEL's social media dissemination and posted on the SENTINEL social media channels and provided input to produce the promotional material (Promotional Video Storyboard, SENTINEL newsletters). Finally, 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
STS	In Y1, STS participated in all WP7 relevant telcos and discussions. STS has reviewed the Exploitation Aspects Questionnaire gave input that was prepared and circulated by the T7.1 leader. Furthermore, STS reviewed and provided suggestions to the content used for designing the SENTINEL's website. In addition, STS has provided content for producing social media posts. Finally, STS supported SENTINEL in the International Workshop on Information & Operational Technology (IT & OT) Security Systems (IOSec 2022) that was co-organised by STS.
AEGIS	During the Y1 project period, AEGIS, as a leader of the T7.1, hosted T7.1 telcos for analytical presentation of the task planning as well as created and circulated the Exploitation Aspects Questionnaire. In addition, AEGIS has continued monitoring the market trends and investigated ways to identify further markets and/or targeted audiences. Furthermore, since January 2022 AEGIS has become a member of the WP7 Task Force alongside ITML and UNINOVA. The task force is focusing on coordinating efforts with respect to dissemination and communication activities that involve all the partners. Finally, AEGIS has participated in all discussions and meetings concerning T7.3 and T7.4 and contributed to what was requested by the task leaders as well as the Work Package leader.
TSI	TSI has participated in all WP7 meetings and discussions. In addition, TSI has made three (3) posts on SENTINEL's social media. TSI is continuously working on disseminating the project's results through paper publications and organization of events with other horizon projects. TSI has published a paper which was presented in European Workshop on Systems Security (EUROSEC '22).
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 provided input for the 2nd newsletter of SENTINEL about the CyberRange platform.
UNINOVA	During Y1, as the leader of the WP7 UNINOVA has conducted the following activities • Organization and leading of monthly WP7 telcos • Organization the 1st SENTINEL SME-centric workshop • Contribution to the exploitation questionnaire • Creation of SENTINEL contact point and social media channels (LinkedIn, Twitter, YouTube) • Continuously creating awareness, promoting SENTINEL through social media channels and providing content to social media on a regular basis • Design of the SENTINEL brochure • Engagement of relevant stakeholders through social media channels • Supporting the definition of the online questionnaire for collecting insights from Portuguese SMEs • Preparation of the SENTINEL newsletters • Support on preparation of the SENTINEL promotional video • Promotion on bilateral meetings with other EU projects, seeking potential synergies

	• Identification of possible projects for promoting the SU-DS03-2019-2020 cluster webinar • Preparation of the SENTINEL conference paper • Targeting industrial events for SME engagement • Assignment of series of partners interviews • Participation in "IDC Security Roadshow", "Transferable Research & Laboratory Outcome", FIC events
CG	CG has participated in all meetings regarding the WP7 and was actively following the SENTINEL social media profiles, while it also produced content for a post in SENTINEL's LinkedIn channel.
TIG	During Y1, TIG worked with relevant partners to fulfil the requirements of WP7 and participated in all meetings regarding WP7. Furthermore, it has reviewed newsletter #2 and created three (3) posts for the LinkedIn page. Finally, TIG has created the voice over for the 1st promotional video of the project.
CECL	CECL has participated in all meetings regarding the WP7. CECL has reviewed the 2nd Newsletter. 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.
FP	During Y1, FP has participated in all meetings regarding the WP7. FP created a short video, showing what FP does and how it's involved in SENTINEL. This was posted on SENTINEL's social media channels on 02/02 (https://www.linkedin.com/posts/sentinel-eu-project_driving-cyber-security-activity-6894582460827713536-cxtW). Furthermore, FP has reviewed the exploitation questionnaire and filled in with FP's respective information. In addition, FP has participated in two (2) dissemination events, boosting interested parties' acknowledgement about the project. • Event 1: "CyberHOT summer school" 27-28 September 2021 • Event 2: "5th NMIOTC Cyber Security Conference in the Maritime Domain" 29-30 September 2021 FP has provided feedback with regard to SENTINEL's promotional video storyboard, reviewed the 2nd Newsletter and provided input. FP has been active in social media of the project by creating new posts about the project.

3.7.4 Status of Deliverables and Milestones

The work done under T7.1 is well-documented in two deliverables D7.1 and D7.2.

Table 12. Status of WP7 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D7.1	The SENTINEL website and visual identity	ITML	R+ DEM; Public; M2	Submitted
D7.2	Market analysis and preliminary business modelling	AEGIS	Report; CO; M6	Submitted
MS1	Project's baseline	IDIR	M6	Achieved

3.7.5 Deviations from Work Plan

There were no deviations from the GA. Although the partner “The SHELL” has terminated its partnership with SENTINEL effective from M7, WP7 activities are progressing as planned. ITML has conceived and submitted a mitigation plan, based on which TSI took over The SHELL’s role in T7.2 and T7.3 and undertakes all the relevant activities since M7.

3.7.6 WP7 planned activities for the next period

In Y2, the SENTINEL project will intensify its activities, from a dissemination and communication, project exploitation as well as standardization point of view. In particular, WP7 will:

- Outline a detailed exploitation strategy and lay the ground for the long-term sustainability plan and next best actions for contribution to and leverage of relevant standards.
- Shape the “knowledge diffusion” phase of the SENTINEL dissemination strategy.
- Intensify event participation in both consortium level (such as the INFO Day for the MVP, the benchmarking event) as well as at a partner level (such as participation in conferences, workshops, forums etc.).
- Trigger engagement with other DIHs and boost the SENTINEL ecosystem building.

These activities will be captured in corresponding deliverables, i.e., D7.3, D7.5 and D7.7 due in M18.

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, is leading WP8, T8.1 and T8.2. During Y1, the WP8 activities have focused mainly on setting up the expected coordination bodies and procedures as well as building an efficient communication to ensure the smooth implementation of the project’s objectives and expected impact.

The key achievements of WP8 in Y1 include:

(i) Setting a day-to-day project management structure and procedures and establish collaborative tools to enable effective internal and external communication and decision making.

(ii) Preparation of the Ethics Manual and Data Management Plan (DMP). It has been elaborated technical and organizational procedures to handle research data consortium during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared/made open, and how data will be curated and preserved. In this respect, Ethics compliance, privacy, data protection and security of collected/processed/generated data are of the utmost importance for the success of the SENTINEL project.

(iii) Establishment of the External Advisory Board (EAB) and the Ethical & Data privacy Advisory Committee (EDAC).
(iv) Initiation and successful completion of the project's amendment process (submitted in February 2022) after The SHELL's termination notice in M6.
(v) Managing the preparatory activities towards the production of the present document as well as coordinating the preparation of the other seven (7) deliverables due in M12.

Throughout the whole first year project period, WP8 was dedicated to regular coordination activities. A tight control over the project activities has been established 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

In Y1, five (5) deliverables have been successfully produced and submitted, namely D8.4, D8.5, D8.8, D8.9, D8.10, while the present deliverable (D8.1) will be delivered in M12, as per the GA.

3.8.2 Key achievements during reporting period at task level

T8.1 Project Quality Planning and Monitoring

T8.1 is led by ITML and started in M1. The project quality planning and monitoring has been set up and reported since M3 first via D8.5 The SENTINEL QA plan and periodic monitoring report (first version) and then via D8.4 Risk identification and management & quality plan (M6). The main goal was to provide a reference point for all guidelines and procedures relating to the proper implementation of the project's risk management procedures, as well as the quality assurance of all SENTINEL deliverable documents, presentations, meeting minutes etc. D8.4 describes all steps of the SENTINEL risk management process including activities, processes (e.g., SENTINEL Risk Assessment List) and role assignments for the identification, assessment, mitigation and monitoring of project risks, as well as the results of the initial risk analysis. The quality assurance plan (D8.5) provides detailed description for the processes which have been established by the SENTINEL consortium for the production and reviewing of project deliverables, along with the involved partner roles and outputs are explicitly defined.

T8.1 has contributed to the following WP8 objectives:

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

The above comprise significant input to D8.4 ('Risk identification and management & quality plan', delivered in M6), and D8.5 ('The SENTINEL QA plan and periodic monitoring report - first version', delivered in M3), all contributing to milestone 1 ('Project Baseline'), due in M6.

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

T8.2 is led by ITML and started in M1. As part of the activities of task T8.2, the management structure and procedures and the consortium communication tools were set during M1-M3. Roles and responsibilities within the partnership were also established, including the setting up of the governing boards as per Grant Agreement and Consortium Agreement. During the second semester of Y1, the management procedures and the Consortium collaborative tools were updated and refined. The implementation of project monitoring and continual reporting processes has been completed. The analysis of the progress reports provided by each partner is being carried out on a quarterly basis. Project management bodies as well as risk identification processes have been reported in D8.4 and D8.5 (and comprise the main focus of T8.1). Also, a project handbook (D8.8 (first version) and D8.10 (second version)), summarizing the key project management procedures, has been prepared and made available to the Consortium.

During Y1, project coordination ha organized the following consortium meetings with the purpose of building a synergistic collaboration among partners and brainstorming on technical and management issues:

- 1 Kick-Off Meeting (hybrid)
- 3 Plenary Meetings (hybrid)
- 8 Monthly Scientific and Technical Meetings (started in M2)
- 1st Technical Review Meeting (envisioned for M13, logistics tasks in progress)

T8.2 has contributed 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 D8.1 (‘Yearly project management report -first version’, delivered in M12), D8.8 and D8.10 (‘The SENTINEL project handbook – first and second versions’, delivered in M4 and M6 respectively), and D8.9 (‘The SENTINEL data management plan, delivered in M6). D8.9 and D8.8 contributed to milestone 1 (‘Project Baseline’, due in M6), while D8.1 and D8.10 contribute to milestone 2 (‘Innovation Flame’), due in M12.

T8.3 Technical and innovation management

T8.3 is led by INTRA and started in M1. Starting from M2 (July 2021) INTRA has been organizing monthly Scientific and Technical meetings. The main purpose of this series is for the partners to align monthly with respect to the latest developments and achievements of the project, potential risks and future plans. 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, while the architecture updates were presented and discussed. Moreover, Key Results and Performance Indicators were revisited, discussed and responsible partners were assigned to them.

To facilitate the design and development of the SENTINEL platform by organizing more relevant and focused discussions the Working Groups (WGs) were introduced (MySENTINEL, Self-Assessment, Core and Observatory respectively). WGs held weekly meetings which helped to advance in respective fronts by bringing together closely related Tasks from different Work Packages and forming more coherent groups.

Finally, once the landscape in terms of the SENTINEL technological innovations and its architecture started taking a clearer form, T8.3 started discussions with WP6 and WP7 to align SENTINEL's business value with the needs of potential users. These discussions are expected to intensify after the delivery of the MVP.

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.

The above will comprise significant input to D8.12 ('The SENTINEL technical and innovation management report – interim version', to be delivered in M18), contributing also to milestone 3 ('Innovation Fire), due in M18.

T8.4 Ethics and Data Protection

T8.4 is led by CECL and started in M1. CECL has appointed Ass. Prof. Fereniki Panagopoulou as the project's Ethics Supervisor. Following the partnership's appointments of the rest of the Ethical and Data Privacy Advisory Committee's members, the Committee was officially established on the 15th of July 2021. Ass. Prof. Panagopoulou and her team already contributed to the drafting of deliverable D1.1 within the month of August and began the preparation of the Ethical and Legal issues template. EDAC finalized the first draft of the project's Ethics manual and sent it to partners for review. The manual contains information about the legal and ethical principles related to data protection, as relevant to the SENTINEL project, guidelines and proposed policies, a summary of issues related to the partners' data protection policies, as well as useful, ready-to-use tools and templates. The final version of the Ethics Manual (interim version) was finalised following input from all partners and will be delivered according to the plan initially defined in the GA.

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.

The above will comprise significant input to D8.14 ('Ethics manual and ethical controlling report – interim version', to be delivered in M18), contributing also to milestone 3 ('Innovation Fire), due in M18.

3.8.3 Work carried out in this work package per partner

ITML	During Y1 ITML has organized the SENTINEL KoM, M6 and M12 plenary meetings providing the minutes and the action items. ITML has created a NextCloud repository for the project-related entries (deliverables, minutes, reports, etc.) and created the project's mailing list. In addition, ITML has created the required templates for reports, deliverables, presentations, minutes, peer reviews. To manage and regularly monitor the status update of the project KPIs/KRs, ITML has also produced the SENTINEL KPI/KR evaluation matrix which is being updated on a regular basis. ITML followed all the necessary procedures for the establishment of the EAB and EDAC and kept regular communications with the respective members. ITML actively participated in the scientific-technical monthly teleconference meetings. ITML has established monthly meetings with the PO to create a solid communication channel between SENTINEL and the EU Commission. In addition, ITML has initiated, coordinated and prepared the amendment process after The SHELL termination, effective from M7. ITML is 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 is also 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 D8.4, D8.5, D8.8, D8.9 and D8.10 is currently finalizing D8.1 be submitted in M12.
LIST	LIST has participated in all WP8 relevant telcos, meetings and discussions.
IDIR	IDIR has participated in all Y1 project management and resource monitoring activities either standalone, as is the case when reviewing deliverables (e.g., D8.4, D8.5, D8.1 and D8.10 review) or collaboratively as in the participation in the SENTINEL Scientific and Technical monthly meetings and other administrative meetings, from M1 to M12.
INTRA	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.
STS	STS has participated in all WP8 relevant telcos.
AEGIS	AEGIS has participated in all scientific and technical meetings and plenary meetings. Apart from this, AEGIS has conducted an Internal review of deliverables D8.5 and D8.1, while it provided input for D8.1.
TSI	TSI participated in all project's relevant telcos, contributed quarterly reports and contributed to D8.1.
ACS	ACS participated in all relevant meeting related to T8.2. ACS contributed to D8.9 and has reviewed D8.10.
UNINOVA	UNINOVA has participated in all WP8 relevant telcos and discussions.
CG	CG participated in both scientific and technical telcos and in plenary meetings of the project.
TIG	TIG has participated in WP8 scientific and technical telcos and plenary meetings
CECL	CECL participated in project meetings. It has provided input for the amendment request and any additional information required by the PO; continued the day-to day management including internal financial control, resource monitoring and effort

	tracking. CECL has reviewed and provided feedback on D8.5 and D8.8. In addition, CECL has supported the establishment of EDAC of the project. Supported by EDAC and the ethics supervisor, CECL has drafted the ethical and legal issues template and organized the of 1st official EDAC meeting. After discussion on the draft template with EDAC, and following EDAC and consortium feedback, CECL has finalized the template and circulated it among partners. CECL has received final contributions from partners on the ethical and legal reporting forms, completed first draft of the Ethics manual and circulated draft document for comments. The final version of the Ethics Manual (interim version) was finalized following input from all partners and is expected according to the plan initially defined in GA.
FP	In Y1, FP has participated in regular meetings and discussions, reviewed project documents/deliverables that were assigned to FP, as well as monitored FP's activities based on project's quality assurance plan.

3.8.4 Status of Deliverables and Milestones

The work done under T8.1 and T8.2 are well-documented in six (6) deliverables listed below.

Table 13. Status of WP8 Deliverables and Milestones

Del/MS #	Del/MS name	Leader	Type; dissemination level; Due date	Status
D8.1	Yearly project management report – first version	ITML	Report, PU, M12	Prepared; To be submitted in M12
D8.4	Risk identification and management & quality plan	ITML	Report; CO; M6	Submitted
D8.5	The SENTINEL QA plan and periodic monitoring report	ITML	Report; PU; M3	Submitted
D8.8	The SENTINEL project handbook – first version	ITML	Report; PU; M4	Submitted
D8.9	The SENTINEL data management plan	ITML	Report; PU; M6	Submitted
D8.10	The SENTINEL project handbook – second version	ITML	Report; PU; M12	Submitted
MS1	Project's baseline	IDIR	M6	Achieved
MS2	Innovation Flame	ITML	M12	Achieved

3.8.5 Deviations from Work Plan

There were no deviations from the GA. Although the partner "The SHELL" has terminated its partnership with SENTINEL effective from M7, WP8 activities progressed as planned. The Amendment has been initiated and sent to the Project Officer by PC (see Section 3.8.7). Another item that is worth mentioning is related to the time plan for drafting the Ethics Manual. The timeline for the works of EDAC has slightly deviated from the one included in the project GA. Specifically, after the forming of the Committee and the discussion of their tasks, it was concluded that more time was required for the drafting of the Ethics manual, originally due by month 5 of the implementation (to be issued by M6), in accordance with the description of T8.4. By contrast, the Ethical controlling report did not require as much time as originally foreseen. It was, thus, decided – after consultation with the coordination core team – to move the internal due date of the Ethics manual to M9 of the implementation, while the due date for the Ethical controlling report was left unchanged, as were the due dates for the delivery of D8.14 and 8.15, due on months 18 and 36

respectively. As a result, the overall project timeline and activities will remain unaffected by the deviation.

3.8.6 WP8 planned activities for the next period

For Y2, ITML plans to continue along the same path and closely monitor the project's activities towards effective quality and overall project management. ITML, together with the PO, will proceed with all the necessary actions to organize the SENTINEL's Technical and Interim Review Meetings foreseen for M13 and M18 respectively. In terms of innovation management, the plan for Y2 is to boost its activities towards the project's Interim Review Meeting starting from M13.

3.8.7 GA Amendment

During Y1, the partner "The SHELL" has terminated its participation in the project, effective from M7. The coordinator together with the consortium have devised a mitigation plan to reallocate The SHELL's effort throughout the rest of the project. The table below summarizes the contingency plan and justification:

WP #	Start	End	Involved tasks	SHELL effort	Description of work	Proposed contingency actions	Justification
1	M1	M6	T1.1, T1.2	2 PMs	Contribution to the definition of requirements & specification of the SENTINEL framework architecture	Work within this WP has finished.	N/A
2	M7	M30	T2.2, T2.3, T2.5	25 PMs	T2.2: Leading the development of the IdMS T2.3, T2.5: Contributions	ITML takes over the development of the IdMS (T2.2) and the contribution in T2.5. Estimated effort: 30PMs FP Takes over the contribution in T2.3. Estimated effort: 1PM	During the period since proposal preparation (summer 2020) ITML has experienced a growth of ~40%; among others, engaging personnel that has been directly involved in the development and management of IdMS' deployment in large corporations. ITML has deployed identity management in data analytics during the development and refinement of its 3ACEs (Analytics-as-a-Service) product. Therefore, ITML has the capacity and resources to

							undertake all work in T2.2, and to support work in T2.5. FP, as task leader in T2.3, will undertake the expected contribution of SHELL in the relevant task.
3	M7	M30	T3.1, T3.2, T3.4	7 PMs	Contribution to the following: T3.1: Access and monitoring of open security data sharing platforms T3.2: Incident handling and sharing module T3.4: Policy drafting module	AEGIS takes over their contribution in T3.1 and T3.2 Estimated effort: 4 PMs STS and FP take over their contribution in T3.4 Estimated effort: 2 PM (1 PM each).	AEGIS, having a strong profile also in incident management, can take over the SHELL's expected contribution in T3.2 (estimated effort: 2 PMs). It can also take over its estimated contribution in T3.1, being task leaders (2 PMs). FP, as task leaders, will take over 1 PM of SHELL's expected contribution in T3.4. STS will take over the contribution related to support policy drafting in terms of ensuring the necessary assurance and compliance activities, as it is the partner mainly offering assurance – related services.
4	M7	M30	T4.2	2 PMs	Contribution to T4.2	STS takes over their contribution in T4.2 Estimated effort: 2 PMs	In line with the effort assigned in STS for T3.4, the same partner also takes over SHELL's expected contribution in T4.2, as task leaders.
5	M9	M36	T5.2	4 PMs	Contribution to the integration of tools/components from WP2-WP4 into the SENTINEL platform	IDIR take over their contribution Estimated effort: 4 PM (IDIR)	SHELL's expected contribution will be undertaken by IDIR (4 PMs, in T5.2 to further support ITML in the integration of the IdMS in the integrated solution).

6	M10	M36	T6.2, T6.3	2 PMs	Contribution to validation and testing of the SENTINEL offerings (T6.2, T6.3)	AEGIS takes over their contribution Estimated effort: 2 PMs	AEGIS will take over the contribution of SHELL in the 2 validation-related tasks, focusing mainly on the validation of the SENTINEL digital core offerings in the unified solution, as this partner also took over the relevant work in WP3.
7	M1	M36	T7.2, T7.3	3 PMs	Dissemination & exploitation activities, incl. communication and business planning activities.	TSI takes over their contribution Estimated effort: 3 PMs	TSI offered to take over SHELL's effort, combined with an amount for dissemination related-costs, in order to facilitate collaboration with the PRAXI network, aiming at further enhancing SENTINEL's efforts to engage SMEs and build a wide ecosystem of potential end users.
8	M1	M36	T8.2	1 PMs	Day-to-day management (project & financial control, resource monitoring)	N/A	N/A

The Amendment was approved by the European Commission. Thanks to the proactiveness of the coordinator and the careful and detailed mitigation actions undertaken by the consortium, all activities smoothly continued without delays since M7, when The SHELL was terminated.

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.

The activities in WP9 have focused on analyzing the ethical implications of the SENTINEL project, mainly from the perspective of data privacy aiming at safeguarding the rights of the data subjects. It also included the procedures and criteria to identify/recruit participants in the research activities, the informed consent procedures and the collection and treatment of collected data were defined.

The results of the ethical assessments are reported in the submitted D9.1“D9.1: POPD - Requirement No. 1” released in M4.

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 this work package

ITML	ITML has been working towards the preparation of D9.1. Towards this direction, ITML has organised bilateral discussions with the pilot partners (CG, TIG) to better understand their data protection policies, involvement in the project and any ethical requirements their involvement might raise during the project. ITML had bilateral discussions with the Ethics Manager of the project (CELC), who also chairs the EDAC and is actively managing ethics and monitoring all project activities to comply with legal and ethical requirements set in this project. The D9.1 POPD - Requirement No.1, has been submitted successfully in M4, by ITML.

3.9.3 Status of Deliverables and Milestones

Table 14. Status of WP9 Deliverables

Del #	Del name	Leader	Type; dissemination level; Due date	Status
D9.1	POPD - Requirement No. 1	ITML	Ethics; CO; M4	Submitted

3.9.4 Deviations from Work Plan

No deviations from Work plan.

3.9.5 WP9 planned activities for the next period

ITML, together with EDAC, will continue the management of ethics compliance for the project and strategy for addressing the ethics requirements as part of the overall project management of SENTINEL.

4. Impact

One of the main goals of SENTINEL apart from the scientific and technological advancements towards meeting the project objectives is also achieving the expected impacts. To do so, the SENTINEL consortium relies on 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 expected impact for the SENTINEL project is related to (i) the work programme, (ii) the innovation capacity, competitiveness, and growth, (iii) the other Public-Private Partnership (PPP) initiatives, (iv) standards, and (v) society. For each impact category, well-defined KPIs have been identified by the SENTINEL consortium aiming to monitor the progress within the course of the project and measure the respective achievements. 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 open-source engagements, a concrete exploitation strategy and management of knowledge and Intellectual Property.
Below, for each impact iKPI the status update, the activities during Y1 and the strategy towards the successful completion are reported. Moreover, the actions of the SENTINEL consortium with respect to the measure of impact maximization are summarized along with the main achievements of Y1.

4.1 Impact related to the work programme

Table 15. KPIs status update - Impact related to work programme

iKPI-1.1	At least four (4) privacy and personal data protection technologies delivered	In progress
Privacy and Data Protection technologies aim at supporting SMEs to comply with GDPR. Within the SENTINEL project, three technology-driven compliance services are developed according a 3 steps engineering approach that illustrates “readiness” of service (MVP, First Integrated version, Final Version): The three first services are: 1) GDPR Compliance Self-Assessment, 2) Integrated Identity Management System, 3) DPIA. The two first are managed in WP2, respectively T2.1 and T2.2. Last one is the expected outcome of T4.2. All these services are under development according project timeline. A fourth privacy and personal data protection technology has been introduced as part of the overall platform to support collection of data related to Processing Activities and required by GDPR CSA and DPIA services. Data are structured to comply with GPDR article 30 which is related to Processing Activity documentation. A first version of GDPR-CSA is effectively implemented in the MVP version of the SENTINEL platform, as presented in D5.4. **Linked WPs: 2, 4; Owner: LIST**		

iKPI-1.2	**At least six (6) standards, regulations and directive incorporated within SENTINEL**	**In progress**
This iKPI is directly linked with KR-5.3, please refer to Sec. 2.5; KR-5.3 **Linked WP: 7; Owner: STS**		
iKPI-1.3	**At least 40% improved privacy compliance efficiency for SMEs/MEs**	**In progress**
This iKPI is directly linked with KR-1.2, please refer to Sec. 2.1; KR-1.2 **Linked WP: 2; Owner: LIST**		
iKPI-2.1	**More than 20 entities CERTS / CSIRTS engaged by the end of the project**	**In progress**
TSI will track the CERTS / CSIRTS engaged by TSI and other partners for the duration of the project, TSI will aim to come in contact with such organization by the participation in academic events and through the INFO Day TSI will organize in M24. **Linked WP: 7; Owner: TSI**		
iKPI-2.2	**More than 8 Digital Innovation Hubs engaged by the end of the project**	**In progress**
This iKPI is directly linked with KR-5.4, please refer to Sec. 2.5; KR-5.4. **Linked WP: 6; Owner: UNINOVA**		
iKPI-2.3	**More than 20 novel services, tools and modules within the SENTINEL platform**	**In progress**
This iKPI is directly linked with KR-3.1, please refer to Sec. 2.3; KR-3.1. **Linked WPs: 2; 3; 4 Owner: FP**		
iKPI-3.1	**At least three (3) improved business model developed within the SENTINEL project**	**In progress**
The preliminary business model was presented in D7.2, as part of the ongoing process related to T7.1. Further outcomes of T7.1 and T6.4, will be reported in D7.9 “Final business model, market analysis and long-term sustainability report” (M36) and D6.3 “Assessment report and impact analysis” (M36). **Linked WP: 7; Owner: AEGIS**		
iKPI-3.2	**At least 40% reduction of compliance – related costs**	**In progress**
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)**	**In progress**
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**	**In progress**
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**	**In progress**
Regarding iKPI4.3, all the events described under the WP7 section of this deliverable are seen as activities to reach out to SMEs and third parties. The events organized by SENTINEL (1st and 2nd SME-centric workshops) and the Webinar on “A privacidade e a proteção de dados pessoais no panorama nacional das PMEs”, have reached more than 100 attendees in total. We truly believe that our participation in IoT week and FIC Forum events in June 2022, will strongly contribute towards this specific iKPI. Efforts to inform more SMEs about SENTINEL and reach out to a larger audience will be realised during Y2 – among others- through the upcoming Newsletters and possibly a LinkedIn campaign. **Linked WP: 7; Owner: UNINOVA**		
iKPI-9	**At least four (4) innovative technologies advanced within SENTINEL**	**In progress**
SENTINEL combines a set of tried-and-tested innovative solutions (MITIGATE, Security Infusion, CyberRange, etc) that are further advanced throughout the project, with a set of newly developed within the project (IdMS, policy drafting, self-assessment workflow, etc). During Y1, the consortium has made significant progress in advancing technologies such as the IdMS module for data portability, the GDPR CSA module, etc. In Y2 we anticipate that the continuous development of the newly developed technologies, as well as the technologies already brought by partners (as plugins) will lead to further advancements. This iKPI is obviously still in progress, as the project continues. **Linked WPs: WP2-WP4; Owner: ITML**		
iKPI-10	**At least five (5) cases testing and validating the innovative capacity of the SENTINEL’s offerings**	**In progress**
Concerning iKPI10, SENTINEL is already paving the way for an early test and validation of its offering through CG and TIG, which are the two end users in the consortium. From an external perspective, the collaboration with cluster projects (Clustering webinar organised by SENTINEL in May), also addresses		

this iKPI. The idea is to engage with SMEs from cluster projects consortia, able to test and validate the SENTINEL offerings. Also, in parallel, SENTINEL is already engaging with DIHs in order to attract other SMEs/MEs capable to test and validate the SENTINEL offerings. **Linked WP: 6; Owner: UNINOVA**		
iKPI-11.1	**At least 20 third-party entities (SMEs/MEs) directly using SENTINEL's tools/services**	**In progress**
To achieve this iKPI, SMEs (other than the ones included in the consortium) should first become aware of the SENTINEL services. Therefore, during Y1 the consortium has focused its dissemination activities on accomplishing this KPI. Within Y1, the consortium partners have approached SMEs in several targeted events (2 SME-centric workshops, several talks and events in DIHs -for more details see Section 3.7) outlining the project objectives and main project offerings. As a result, the consortium has secured 3 DIHs to trial SENTINEL offerings in the future, while it has identified 5 more DIHs as potential end users and plans to intensify outreach activities within Y2 (see KR-5.4 and KR-6.3). Following up the release of MVP in M12, the prototype and eventually the final results of the project, we are planning to intensify the efforts towards achieving this iKPI, given that the demos will facilitate SME's engagement. **Linked WP: 7; Owner: STS**		
iKPI-11.2	**At least 10% increase of market share for SMEs/MEs exploiting SENTINEL**	**In progress**
To monitor the project's impact on the market share, STS is planning to prepare a questionnaire to circulate among the project's technology providers and collect first insights about the basic financial figures of their companies. Similar questionnaire will be circulated before the end of the project in order to measure the achieved impact after the project completion. **Linked WP: 7; Owner: STS**		
iKPI-12.1	**At least four (4) start-ups and spin-offs boosted exploiting SENTINEL security services**	**In progress**
This iKPI necessitates that the SENTINEL complete suite of services is launched, trialled by end users and fully evaluated in terms of – among others - (i) usability, (ii) user acceptance, (iii) cost-efficiency, (iv) automation. There is no progress to be reported in terms of this iKPI, and we expect to realise this during Y3. **Linked WP: 7; Owner: STS**		
iKPI-12.2	**At least 15% increase in sales for the pilot partners exploiting the SENTINEL platform**	**In progress**
Similarly, to iKPI-12.1, this iKPI necessitates that the SENTINEL complete suite of services is launched, trialled by end users and fully evaluated in terms of – among others - (i) usability, (ii) user acceptance, (iii) cost-efficiency, (iv) automation. Increase in sales is an indicator that can be primarily measured in the long term. There is no progress to be reported in terms of this KPI. **Linked WP: 7; Owner: STS**		

4.2 Measures to maximize impact

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.

- **Mr Stephanos Camarinopoulos**, Director in RISA Sicherheitsanalysen GmbH, Berlin, Germany.

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, one internal and two external to the consortium:

- **Prof. Fereniki Panagopoulou,** Assistant Professor of Constitutional Law, Panteion University, Athens, Greece.
- **Dr Tanya Kyriakou,** Founding member of the Hellenic Association of Data Protection & Privacy (EDAC deputy member)
- **Dr. Christopher Konialis**, founder of ClinGenics (CG) and partner of SENTINEL.
- **Dr Tal Soffer**, Head of the unit of Technology and Society Foresigh, Tel Aviv University, Israel.

During Y1, EDAC has continuously been working towards drafting the Ethics Manual, which will comprise D8.14 in Y2. This process involved holding several meetings among the three EDAC members in order 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.

The first EAB meeting was successfully conducted on the 21st of January 2022, during the second day of the SENTINEL's 2nd plenary meeting, held in Athens, Greece. The meeting was hybrid, two of the EAB members joined the meeting physically, one joined online and one was absent. The purpose of the meeting was to introduce the SENTINEL project to the EAB members and present the main achievements up to M8, aiming to receive valuable feedback for the next steps. The meeting consisted of four parts: (i) SENTINEL project vision, objectives and outcomes, (ii) SENTINEL technical solution and innovations, (iii) SENTINEL use cases, and (iv) an overview towards implementing SENTINEL MVP. The EAB members through a fruitful discussion provided their feedback and recommendations aiming to ensure high quality and excellence in the project. Their comments were focused on the challenges that SENTINEL is facing related to the complexity of GDPR compliance, the two pilot cases, integration of all SENTINEL components, privacy preservation, data curation, etc. The table below includes several focused points and comments that the EAB members raised regarding specific aspects of SENTINEL, together with accompanying reply to summaries that will be further updated and enriched during the course of the project.

Table 16. SENTINEL EAB feedback

Name of the EAB member	Question/Comment/Suggestion	Reply summaries during the EAB meeting from the consortium
Toomas Lepik	Consider extra breaches to GDPR. For instance, Google Analytics can be considered as such (linking cookies to individuals).	We will consider including such pieces of information during the collection of the organisation profile and will incorporate it into the assessment tools.

João Mendonça	Need to define clear boundaries. For instance, are you focusing on the process of the companies (e.g., customers' data protection) or including their products too?	We only focus on the former. It will be extremely difficult to create generic-enough models for all companies' products.
João Mendonça	GDPR is extremely vast. Try to focus somewhere (for example the legal aspects).	For the preliminary version of the SENTINEL privacy & data protection suite, we have considered for the GDPR compliance Level a set of six processes, each of which is related to one specific aspect of data protection requirements.
João Mendonça	The two pilots seem to handle very sensitive data (genomics and children). You would benefit from also considering a simpler case, so that the process proposed is not always too complex.	We have already identified three additional use cases (as part of T6.3 activities) that concern simpler cases.
Toomas Lepik	It might be helpful to identify business sectors and target them specifically.	We strive to provide a more generic application area for SENTINEL services for a wider applicability. Nevertheless, this comment is indeed meaningful, when targeting business sectors with special needs.
João Mendonça	Make sure to curate the data, especially with respect to the Observatory, so that the quality is high enough.	We will curate the data of the Observatory, as this extracts data from multiple sources. For the MVP at the moment, we only consider one source (MISP), so we have not implemented this yet.
Rodrigo Diaz	Ask the following questions: Is there a way to achieve traceability of identity of data? For instance, can you tell where a data leak came from? Is that feasible to assess?	SENTINEL offerings (plugins) provide full logging capabilities that provide detailed information about detected events, including exact timestamp, origin, destination, username / user info, operational and/or any other details specific to detected events. For example, ITML's Security Infusion can trace changes in filesystem.
João Mendonça	Focus, focus, focus: Don't try to solve a problem for all SMEs. Rather use Personas and User Journeys to focus on specific needs. Be explicit about your goals.	We have identified 7 use cases, which we believe cover the full set of the SENTINEL offerings and have created User journeys and personas, as per the EAB member request, which were particularly

		useful for the MVP implementation.
Toomas Lepik	Consider offering possible consultancy services to very small companies for helping them troubleshoot, if they don't have IT personnel.	An important remark that might comprise part of the business model of SENTINEL.
Rodrigo Diaz	Consider digital twins for the infrastructure.	ACS' Cyber Range in a sense offers this capability already.
Rodrigo Diaz	Look at other related projects (such as GEIGER).	We have already liaised with GEIGER to explore common pathways and we are planning to invite them to the next clustering activities.
João Mendonça	Investigate how to contribute to the open-source community. Apart from releasing (parts of) the source code, try to enhance the functionality of existing tools.	An important attempt towards this direction is that SENTINEL establishes a 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 to open-source incident response platforms, as well as the continuous monitoring of such open data sets, ensuring a continuous aggregation of information for the SENTINEL knowledge base (T3.1).
Toomas Lepik	Useful links (related to cyberattacks, GDPR compliance, Data protection self-assessment tools) for further investigation https://getreadyforcyberessentials.iasme.co.uk/ https://www.ibm.com/data-responsibility/gdpr/self-assessment/ https://priviq.com/solutions-gdpr-software/ https://content.ketch.com/ketch-free https://www.dataprotection.ie/en/organisations/resources-organisations/self-assessment-checklist	We thank the EAB member for this useful material and we will take this into account for future developments.

The table is currently being processed and will be further updated to include the concrete actions of the consortium with respect to the comments received by the EAB members. The updated version will be included in the M18 technical project report. The goal of these tables is to better monitor the progress of the comments/feedback received by the EAB members.

For the second year of the project, the plan is to organise one more meeting with the EAB co-hosted with the SENTINEL's 4th plenary meeting (schedules in October 2022) and continue our efforts to fully address their comments.

Communication and dissemination plan and activities

The Communication and Dissemination activities of SENTINEL initiated in June 2021. More specifically, during the project's kick-off meeting, the main objectives, short-term and long-term plans have been presented. According to this plan the respective activities started with the release of the project's website (M1 timeframe) which was also demonstrated during the kick-off meeting.

After the project kick-off meeting, the SENTINEL's social media channels (LinkedIn and Twitter) were created, and the dissemination process started using mainly the social channels, where each different partner is responsible for providing at least one post per week. By the end of M3, the SENTINEL's website had reached 92 unique visitors, 70 followers on LinkedIn and 7 followers on Twitter.

The design and development of the 1st project brochure was initiated, were a final version of the brochure of the project was presented to all partners by the end of M3. Worth mentioning that additional marketing material was also developed, such as SENTINEL business cards, poster and roll-up.

Considering attendance in events, SENTINEL has participated in the "**CyberHOT summer school**", September 2021; "**5th NMIOTC Cyber Security Conference in the Maritime Domain**" September 2021; "**Berlin Science Week**" November 2021; "**IDC Security Roadshow**" April 2022 and "**Transferable Research & Laboratory Outcome**" April 2022.

Regarding the upcoming events, SENTINEL will be present at a workshop "**Identity, trust, and privacy in the intelligent, smart IoT word. Challenges and outcomes**" within the "**IoT week 2022**" conference, where the Project Coordinator - Dr. George Bravos - will act as a speaker, presenting the SENTINEL project. We were successfully accepted to provide a 45-min talk to **FIC 2022 International Cybersecurity Forum**, 7-9 June, Lille, France, about the SENTINEL project. SENTINEL will also set up a booth in FIC to show its latest achievements, including a demonstration of the 1st release of the MVP. The coordinator (ITML) will also present SENTINEL and its offerings to the upcoming **Projects to Policy Seminar (PPS)** event, invited by the European Research Executive Agency (REA).

For this reporting period, SENTINEL has also focused on promoting synergies with cluster projects, namely: Initial contacts and preliminary discussions have been started with ERATOSTHENES-101020416, CYBERKIT4SME-883188, SECANT- 101019645, TRAPEZE-883464, PUZZLE-883540, ARCADIAN-IoT-101020259, IRIS-101021727, PALANTIR-883335 and IDUNN-101021911. Such initiative resulted in the organization of a cluster webinar, held on the 12th of May, where each project had the opportunity to present its objectives and achievements. During the event, several ways of collaboration where discussed, at the communication and dissemination level, but also at a technical level. An idea of organizing a physical cluster meeting was also suggested. Also in this respect, a communication and dissemination task force has been created, with the objective to meet regularly and discuss possible way of synergies between the different projects.

Visibility of the project and transferability of the project outcomes has been promoted through the generation of promotional material. In this context, three (3) SENTINEL newsletters were released within this period, highlighting some of the SENTINEL components as part of the SENTINEL technical suite, but also dissemination and communication achievements. The SENTINEL promotional video was also released, and it is available under the SENTINEL YouTube channel. A plan to launch a series of podcast interviews is already on the table. The objective of these

podcasts is to invite project partners on a regular basis to present themselves and provide personal insights about the SENTINEL vision and beyond.

With respect to academic publications, SENTINEL has submitted three (3) conference papers. Two papers have already been approved, the third one is currently under review.

The WP7 monthly meetings, are also taking place regularly, where all partners are 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. Regarding the social media indicators, it is worthwhile to mention that we've reached more than 500 followers on LinkedIn, more than 170 followers on Twitter and the SENTINEL website with an activity of 77 visits per month on average.

The following table lists the dKPIs related to communication and dissemination activities and summarizes the progress for year 1. The aim of these KPIs is to measure the impact of the related activities.

Table 17. SENTINEL Website - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Achieved/In progress**
SENTINEL website	dKPI#1: Number of visitors	Monthly	≥ 100	In progress
	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 **932 number of visitors**, which is approximately **77 visitors monthly**. 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. This is one of the KPIs that has deviated compared to the initial plan and an adjustment for the future is needed. However, the consortium is optimistic that visibility will dramatically increase after the release of the MVP (M12) and the kick off of the exploitation actions. To better align this KPI with the following (dKPI#2), a new approach is identified, based on the results of the first year and the total goal as targeted by dKPI#2. Our consortium consists of 13 partners based in 10 different countries; therefore, our new approach is to engage 10 visitors/month/ country to aim for 1200 visitors annually.			
	dKPI#2: Number of page views	Annually	>5000	In progress
	To address this KPI, the approach was the same as in dKPI#1, since the two are highly related. The **number of the SENTINEL website views** was **4,502.** Here as well there is a deviation from the initial target, but we believe this is highly related to the fact that this was the first year of the project, where awareness and loyalty starts being built. We decide to keep the target and strive to reach it in the second and third year of the project.			
	dKPI#3: Number of downloads	Monthly	>500	In progress
	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 **total number of downloads** of our material is **109** at the moment of writing this report. Here as well there is a deviation from the initial target, but we believe this is highly related to the fact that this was the first year of the project, where not much material (especially publications) was produced to become available for download. We decide to keep the target and strive to reach it in the second and third year of the project.			

Table 18. SENTINEL Social Media:Twitter - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Achieved/In progress**

Twitter	dKPI#4: Number of followers	Monthly	>20	In progress
	The **number of followers** in Twitter during Y1 was **183**, which equals to approximately **15 monthly**. We believe this is highly related to the fact that this was the first year of the project, where awareness and loyalty starts being built. We decide to keep the target and strive to reach it in the second and third year of the project trying to produce content relevant to SENTINEL.			
	dKPI#5: Number of push announcements	Monthly	≥ 20	In progress
	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, we are planning to leverage more of our public content and keep up with this KPI.			
	dKPI#6: Number of unique visitors	Monthly	≥ 30	In progress
	In Y1 (M12 data) we recorded **2,313 twitter visitors (approximately 192 visitors monthly)**, although we had no unique visits on twitter. We believe this is highly related to the fact that this was the first year of the project, where awareness and loyalty starts being built. We decide to keep the target and strive to reach it in the second and third year of the project.			

We believe that within the 2nd period, some of these indicators can be improved, thanks to the release of the SENTINEL MVP and more involvement of SENTINEL in dissemination events. SENTINEL posts can be of different nature, therefore, creating more impact.

Table 19. SENTINEL Social Media: LinkedIn - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Achieved/In progress**
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**. This KPI was overachieved and we will keep monitoring this during Y2 and Y3.			
	dKPI#8: Number of push announcements	Monthly	≥ 20	In progress
	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 (M12 data). In Y2, we are planning to leverage more of our public content and keep up with this KPI.			
	dKPI#9: Number of unique visitors	Monthly	≥ 20	**Achieved**
	In Y1, we recorded approx. **60 visitors monthly** (M11 data)**.** This KPI was overachieved and we will keep monitoring this during Y2 and Y3.			

Table 20. SENTINEL Brand-building material - KPIs status update

	dKPI	**Frequency**	**Threshold**	**Achieved/In progress**
Brand-building material	dKPI#10: Number of distributed hard copies of the SENTINEL brochure	End of project	1000 distributed in ≥10 events	In progress
	Up to know, the SENTINEL consortium has produced SENTINEL brochures and has distributed approximately **80 brochures to more than 3 (physical) events**. Unfortunately, the COVID-19 pandemic has forced many events to be held online, thus this KPI experienced a deviation to the initial plan. However, we are optimistic that the situation is changing soon, and we can keep up with this KPI in Y2 and Y3.			
	dKPI#11: Number of electronic SENTINEL brochures	End of project	≥1000 downloads	In progress

	To address this KPI, the SENTINEL consortium has created a number of informative materials such as flyer, brochure, newsletters (all available in the SENTINEL's website). Based on the tendency of people and 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". Following up on this deviation, this KPI is on track with **426 views** of all our electronic material. We expect to increase the views once we have produced more material during the project in Y2.			
	dKPI#12: Regular newsletters	End of project	≥9 newsletters	In progress
	In Y1, we have released **3 high-quality Newsletters**, thus we believe we are on track towards achieving this KPI in the years to come.			
	dKPI#13: Number of SENTINEL videos and number of views	End of project	3 videos with >1000 views each	In progress
	In Y1, we have released the first promotional video of SENTINEL. However, since this was delivered in M12, we only recently uploaded it in our YouTube channel, thus no views are available yet. We will have the chance to promote the video through the project's social media, REA's media as well as partners' media, and we believe we will significantly increase visibility in Y2.			

Table 21. SENTINEL publications and conference presentations - KPIs status update

	dKPI	Frequency	Threshold	Achieved/In progress
Journal/ magazine publications and Presentations in International Conferences	dKPI#14: Number of international referred journal publications by SENTINEL partners	End of project	>6	In progress
	To address this KPI, the consortium relies a lot on the research and innovation teams of its partners. In Y1, the technical implementation has just kicked off, so we are expecting that the consortium will have produced a significant load of research material to be published in Y2 and thus keep up with this KPI. The consortium has created a focus group comprising academic partners, the project coordinator and the dissemination manager and occasionally meet to identify publishing opportunities in the time to come.			
	dKPI#15: Number of special issues in international referred journals	End of project	>2	In progress
	To address this KPI, the consortium relies a lot on the research and innovation teams of its partners. In Y1, the technical implementation has just kicked off, so we are expecting that the consortium will have produced a significant load of research material to be published in Y2 and thus keep up with this KPI. The consortium has created a focus group comprising academic partners, the project coordinator and the dissemination manager and occasionally meet to identify publishing opportunities in the time to come.			
	dKPI#16: Number of publications in international (printed or online) magazines	End of project	>6	In progress
	To address this KPI, the consortium relies a lot on the research and innovation teams of its partners. In Y1, the technical implementation has just kicked off, so we are expecting that the consortium will have produced a significant load of research material to be published in Y2 and thus keep up with this KPI. The consortium has created a focus group comprising academic partners, the project coordinator and the dissemination manager and occasionally meet to identify publishing opportunities in the time to come.			

	dKPI#17: Number of conference presentations by SENTINEL partners	End of project	≥12	In progress
	This KPI is accomplished within the first year of the project with 1 one publication is being presented in international conference, 1 one conference paper has already been approved, the third one is currently under review. The consortium has created a focus group comprising academic partners, the project coordinator and the dissemination manager and occasionally meet to identify publishing opportunities in the time to come.			

Table 22. SENTINEL Third-party events - KPIs status update

	dKPI	Frequency	Threshold	Achieved/In progress
Third-party events	dKPI#18: Number of events	End of project	≥15 events with >60 attendees	In progress
	To address this KPI, the consortium worked as a team and each partner utilised their network and individual dissemination plans. Within the first year of the project, SENTINEL participated in **5 large events with >60 attendees.** During Y2, we have already planned to participate in 3 large events in June (FIC 2022, IoT week 2022, Projects to Policy Seminar (PPS) June 2022), thus we anticipate that this KPI will be achieved by the end of the project.			
	dKPI#19: Number of audience contacts	End of project	≥50% of the participants	In progress
	To address this KPI in this difficult time where most of the events take place virtually, we utilise a combination of means such as online surveys, personal contacts and website statistics on the day of the event. For this type of events, the KPI was on average accomplished with approximately 60% of the participants registered as audience contacts. This KPI was accomplished, nevertheless, we will keep up monitoring this in Y2 and Y3.			
	dKPI#20: Number of participants interested in SENTINEL project	End of project	≥40% of the participants	In progress
	To address this KPI in this difficult time where most of the events take place virtually, we utilise 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. For this type of events, the KPI was on average accomplished with engaging approximately 60% of the participants and 1 DIH. We will keep monitoring this KPI in Y2 and Y3.			

Table 23. SENTINEL events - KPIs status update

	dKPI	Frequency	Threshold	Achieved/In progress
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	In progress
	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 plan to organise at least 2 large events, thus we anticipate that this KPI will be achieved by the end of the project.			
	dKPI#22: Number of audience contacts	End of project	≥50% of the participants	In progress
	To address this KPI in this difficult time where most of the events take place virtually, we utilise a combination of means such as online surveys, personal contacts and website statistics on the day of the event. For this type of events, the KPI was on average accomplished with engaging all participants as audience contacts. This KPI was accomplished, nevertheless, we will keep up monitoring this in Y2 and Y3.			
	dKPI#23: Number of participants interested in SENTINEL project	End of project	≥50% of the participants	In progress
	This KPI has already been achieved, after securing the interest of 60% of participants. SENTINEL is committed to increase the number of events within the 2nd year of the project. As an example, UNINOVA is working towards an EU summit event focusing on digital transformation to be held in Madeira, Portugal, scheduled for the last week of October 2022, where SENTINEL is planning to promote a satellite event.			

Table 24. SENTINEL Liaisons and networking - KPIs status update

	dKPI	Frequency	Threshold	Achieved/In progress
Liaisons and networking	dKPI#24: Number of SENTINEL members actively networking with other relevant projects	End of project	≥6	Achieved
	All SENTINEL consortium members are actively networking with other relevant projects. Tangible outcomes have already come from 6 partners (ITML, AEGIS, UNINOVA, FP, INTRASOFT, AIRBUS) who 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. Thus, this KPIS has already been achieved and we will continue to liaise with similarly themed projects and relevant stakeholders to intensify dissemination and exploitation actions.			

Table 25. SENTINEL Standardisation/regulation relevant activities- KPIs status update

	dKPI	Frequency	Threshold	Achieved/In progress
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
	We have achieved this KPI early in the project by securing the participation of 4 EAB members from the industry and academia. The first EAB meeting was held during the 2nd plenary meeting with an open discussion to obtain feedback, comments and recommendations.			

4.2.1 Exploitation strategy and plan for Year 2

Within the reference project period, the focus was on the design and development of the MVP, which will serve as the basis for all future exploitation actions. The dedicated T7.3 will kick off in Y2 (M13) of the project. Exploitation activities during Y1 focused on the following actions:

- Organizing 2 SME-centric workshops, where the consortium discussed with participating SMEs/MEs their challenges, needs, their view of SENTINEL offerings and asked for their willingness to trial future versions of the SENTINEL integrated solution.
- Drafting an SME-centric questionnaire distribute to the above SME/ME participants in order to better reflect aspects, such as their awareness of GDPR obligations, their needs, challenges, application domain, etc.
- Liaising with similarly themed projects from the H2020-SU-DS-02 and H2020-SU-DS-03 funded topics to explore common exploitation pathways and synergies. Separate discussions took place and the efforts culminated with a clustering webinar, where 10 projects presented their outcomes, offerings and innovations and discussed openly common exploitation & dissemination possibilities.

For Y2, we aim at preparing the ground for the SENTINEL exploitation plan. The exploitation manager will design a questionnaire and collect the renewed exploitation interest of the project partners. The objective of the survey will be to harvest data from partners and formulate the landscape of the customer segmentation, value propositions, revenue streams as well as innovation activities expected via the SENTINEL project. Based on the collected results, the SENTINEL exploitation can be separated into two routes: individual and joint. The first route seeks to enable each partner to take the project results and exploit them to their own ends while the second route will pursue to define a long-term vision for SENTINEL which partners can shape as they see fit. Whether it is industrial, commercial or research, the project partners identify 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 the upcoming D7.7 (M18) will illustrate updated exploitation strategies reported by all the SENTINEL partners including both current and future exploitation activities.

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 the 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 Y1 and after the MVP and distinct technologies have reached an adequate development stage, the consortium has made a first attempt to define SENTINEL offerings, which will provide the foundation for any innovation management and future exploitation activities. These offerings will be finetuned, as the project progresses in Y2.

The three main SENTINEL offerings that define the project's business value can be summarized below:

- **Educating SMEs in PDP and CS processes:** through a guided profiling process, GDPR requirements are laid clear to any SENTINEL framework user. SMEs are thus assisted to understand (a) why individual's data and privacy need protection; (b) how their processing activities affect the subject's privacy; and (c) what needs to be done in terms of OTMs in order to both improve privacy and achieve GDPR compliance.

- **Simplifying evidence-based GDPR compliance:** SENTINEL bridges the gap between cybersecurity and personal data protection (PDP) through providing a mapping between (a) privacy requirements; (b) measures/controls; (c) cyber assets; (d) configurations; (e) real time monitoring. A key innovation for SENTINEL is that it provides evidence for GDPR compliance.
- **Cutting costs through automation:** Automation in SENTINEL is achieved in multiple aspects, such as (a) GDPR compliance check; (b) Data Protection Impact Assessment; and (c) recommendations for the most suitable OTMs, policies, software tools, as well as education and training material for awareness based on the GDPR compliance check.

Following up on this initial assessment and taking into consideration the upcoming release of the MVP in M12, the SENTINEL consortium will further define its innovations and track their progress and evolution in M13, and every four months from then onward, utilizing the Innovation Radar Methodology[1] and leveraging the related questionnaire and instructions for its analysis. During the latest plenary meeting of the consortium, it was also decided that Innovations will be tracked on 4 aspects:

- Business model
- System
- Asset
- WP

Key internal milestones are considered to be the quarterly innovation reviews, the release of the SENTINEL 1st integrated solution (M18) and the final SENTINEL integrated solution (M30), where the SENTINEL technologies and concepts will be possible to be demonstrated and, therefore, assessed with regard to their innovativeness. Thus, KPIs linked with the aforementioned elements are going to be used for tracking innovation KPIs.

The output of these assessments will be used as input not only to the overall exploitation and long-term sustainability plan of the SENTINEL framework, but also to the individual exploitation plans of each consortium partner for their future developments and their contribution to the European Economy. Therefore, there is a strong link between innovations and activities within T7.1, T7.3, T7.4, as well as T5.3.

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

6. Conclusions

The SENTINEL project had several intensive activities in the first year M1-M12 (June 2021 to May 2022) in a sense of delivery of specific outcomes and achievements. During the reference period, the SENTINEL project has completed the Baseline Phase (M1-M8) and is currently on the Innovation Phase (M9-M18).

This deliverable represents the work conducted by the SENTINEL project partners during the first project year. It explains the advancements in relation to the project objectives and provides a detailed description of the technical progress in all the work packages including work carried out per task and per partner. Furthermore, it pinpoints the submitted deliverables, achieved milestones, potential deviations and corrective actions for the reference period. In addition, it provides an overview of the consortium plans for the second year. Finally, this report includes the project main activities and achievements in relation to the expected impact, innovations, and communication, dissemination, and exploitation activities.

The key first-year project achievements include:

- **SENTINEL baseline:** summarizing both the challenges that SMEs/MEs are facing and different approaches to meeting these challenges from both technological and methodological perspectives. Setting up the components to be utilized, and further developed using the SENTINEL architecture.
- **SENTINEL visuals:** Developing the project's visual identity (project website, social media, promotion material) to raise awareness about the project concept, developments and findings to all key actors.
- **SENTINEL Handbook (1st and interim versions):** describing the general management procedures of the SENTINEL project, including quality assurance and risk analysis.
- **SENTINEL experimental protocol:** Describing the use cases to be deployed by the SENTINEL pilot for the real-life field trials; describing their functional and non-functional requirements; defining the SENTINEL KRs/KPIs, identifying industry-validated benchmarks.
- **SENTINEL architecture:** Refinement of the SENTINEL architecture by incorporating new capabilities through the use of plugin tools and new knowledge through external data sources.
- **SENTINEL market potential:** Conducting market analysis and preliminary business modelling to assess the market potential of the knowledge, services, plugins and methodologies of the SENTINEL project.
- **SENTINEL MVP:** Successfully delivering the SENTINEL Minimum Viable Product.
- **SENTINEL Data Management Plan and Ethics Manual:** ensuring compliance with FAIR principles and outlines what data will be collected and processed, what methodology and standards will be applied, whether data will be shared/made open, and how data will be curated and preserved.
- **SENTINEL Ethics Advisory and Data privacy Committee (EDAC):** ensuring compliance with national legal and ethical requirements, addressing any rising research methodology ethical issues and identifying guidance with which SENTINEL should comply (in place since M3).

- **SENTINEL risk identification, management and quality assurance plan:** providing a reference point for all guidelines and procedures relating to the proper implementation of the project's risk management procedures as well as the quality assurance of all SENTINEL deliverable documents, presentations, meeting minutes etc.