SENTINEL

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

# D8.2 - Yearly project management report - second 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 | D8.2 - Yearly project management report- second version |
| Version | 1.2 |
| Date of Submission | 24/05/2023 |
| Main Editor(s) | Siranush Akarmazyan (ITML) |
| Contributor(s) | Stavros Rafail Fostiropoulos (ITML), Anna Maria Anaxagorou (ITML), Philippe Valoggia (LIST), Yannis Skourtis (IDIR), Konstantinos Poulios (STS), Manolis Falelakis (INTRA), Marinos Tsantekidis (AEGIS), George Hatzivasilis, Papadogiannaki Evangelia, Kontogiorgakis Ioannis, Shevtsov Alexander (TSI), Thomas Oudin (ACS), Ruben Costa (UNINOVA), Mihalis Roukounakis (CG), Daryl Holkham (TIG), Dimitra Malandraki, Zoe Kasapi (CECL), Eleni-Maria Kalogeraki, Thanos Karantjias, Natalia Christofi (FP) |
| Reviewer(s) | Manolis Falelakis (INTRA), Peri Loucopoulos (IDIR), Evangelia Kavakli (IDIR) |

| Document Classification | | | | | | | |
|---|---|---|---|---|---|---|---|
| Draft | | Final | X | Confidential | | Public | X |

| History | | | |
|---|---|---|---|
| **Version** | **Issue Date** | **Status** | **Distribution** |
| **1.0** | 07/04/2023 | TOC | Confidential |
| **1.1** | 15/05/2023 | Draft released for internal review | Confidential |
| **1.2** | 24/05/2023 | Final report | Public |

# Table of Contents

## List of Tables

## List of Figures

# Abbreviations

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

# Executive Summary

This document presents the project's main activities and achievements in relation to the project objectives, expected impact, innovations, communication, dissemination, and exploitation activities conducted during the second year of the SENTINEL project. 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 further actions for the third year (Y3). Finally, it presents plans and next steps that the partners will undertake during the final third year.

Within the second year of the project, the **Innovation Phase (M7-M18)** was accomplished resulting in tangible results and achievement of major milestones for the project. In this respect, the SENTINEL project has delivered its interim full-featured platform together with its tools and services such as GDPR Compliance Self-Assessment (GDPR CSA) module, Identity Management System (IdMS), Data Protection Impact Assessment (DPIA) toolkit, GDPR compliant recording of PAs (ROPA), Cybersecurity risk assessment (CSRRA/MITIGATE), Cyber Range simulations, Policy recommendation and enforcement, Cyber incident reporting and handling, Observatory. During the 2nd project year, the tools and services targeted above participated in all seven (7) use cases that were initially defined in the SENTINEL project.

Furthermore, piloting-related activities have seen progress, including the definition and refinement of experimental setups and relevant infrastructure of the two use case owners of the project.

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

Presently, followed by the Innovation Phase, SENTINEL is in the middle of the **Demonstration Phase (M19-M30).** This stage includes two important milestones (MS4 "Demonstration Flame" and MS5 "Demonstration Fire") and requires the completion of the 1st round of pilot execution (M24), delivery of the final integrated SENTINEL architecture as well as successful execution of all pilot cases. The phase can be considered accomplished when all the above-mentioned activities are reported in nine (9) deliverables and successfully submitted to the REA (M30).

# 1. Introduction

## 1.1 Purpose of the document

The purpose of D8.2: Yearly Project Management Report (second version) is to report on all the project activities executed during the second project year [from M13 (June 2022) to M24 (May 2023)] and present the planned activities for the final 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 reference period, the SENTINEL consortium has continued to keep the initially defined time plan for all activities, in accordance with the proposal specified in Annex 1 of the GA. Following the same approach applied in the previous Yearly Project Management Report (D8.1), this document presents the key insights of SENTINEL by providing updates on the general status of the project, enabling visibility of the overall work accomplished by the whole team. In such a manner, the reader of this report can get a complete image of the work carried out for all the work packages including the activities carried out per task and per beneficiary during the second project year. Furthermore, it provides an overview of all submitted deliverables, achieved milestones, core achievements with respect to project objectives, expected impact, innovations, communication, dissemination, and exploitation activities. Although the report is focused mainly on the Y2 project activities, the goal is to provide an overall overview of the project and help follow-up the different activities ongoing in the framework of the SENTINEL project.

## 1.2 Structure of the document

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

- **Section 1** outlines the purpose of this report, its relation to other tasks and deliverables, and a brief description of the methodology followed.
- **Section 2** presents the main scientific and technical achievements in Y2 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.
- **Section 4** and **Section 5** cover the project's main activities and achievements with respect to the expected impact, innovations, and communication, dissemination, and exploitation activities.
- **Section 6** summarizes the document with concluding remarks.

## 1.3 Intended readership

The report is part of WP8 "Project management" and is directly linked to all activities conducted in the SENTINEL WPs and tasks. It reports the progress and the consortium's main achievements within the second year towards the successful completion of all the project objectives, deliverables and milestones. This document serves as an interim version for the final version 'D8.3 – Yearly project management report -third version (due in M36), which will provide a complete overview of the SENTINEL activities and main achievements. It is primarily addressed to the members of the project consortium while it may serve as an informative report for any external party interested as it is a public report.

# 2. Project objectives: Explanation of the work carried out by the beneficiaries during the 2nd Year

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

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

In Y2, a major contribution towards Objective 1, is the delivery of the Full-Featured Version (FFV of GDPR Compliance Self-Assessment module (GDPR CSA) which was integrated as a plugin within the SENTINEL platform. GDPR CSA performs a thorough analysis of different Data Protection Capabilities to determine the compliance level with data protection requirements. Specifically, it considers, and assesses, the compliance of both individual Processing Activities and the Organisation as a whole, on six different data management aspects: (i) Record (ii) Personal Data Lifecycle (iii) Rights (iv) Consent, (v) Data Protection and (vi) Breach. For each aspect, the GDPR CSA provides a) the compliance level and b) a list of recommendations to improve compliance.

In addition to the above, there has been significant work carried out towards the development and integration of an Identity Management System (IdMS), based on the decentralized MyData model for human-centric personal data management, enabling a unified European Personal Data Space. Similar to GDPR CSA, the FFV of the SENTINEL's IdMS was delivered in Y2. The SENTINEL FFV showcases a central identity management system with Single Sign-On (SSO) capabilities for end-users. The IdMS is deployed as-a-service, independently, it offers the creation of centralized, trusted digital identities for individuals and relates these identities with specific roles and access rights, allowing for secure lifecycle personal data governance to satisfy SMEs / vendor / controller / processor compliance requirements.

More information on the design, architecture and operation of the IdMS system and the GDPR CSA can be found in D2.2 "The SENTINEL privacy and data protection suite for SMEs/MEs: Full featured version".

The table below provides a summary of the KRs related to Objective 1, including their status update, the activities conducted in Y2 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 throughout the project development, interfaces and | | |

messaging formats as well as sequence diagrams have been defined and documented. As a result, we are confident that all project technologies are going to be integrated successfully and on time. This was reflected on the MVP, presented in D5.4, as well as the Full-Featured Version (FFV), described in D5.5. The latter successfully integrated all SENTINEL components and technology offerings. The final version is to be delivered in M30 and reported in D5.6. This KR is considered ~80% achieved. **Linked WP: 5; Owner: INTRA**

| | | |
|---|---|---|
| **KR-1.2** | **40% improved compliance efficiency for SMEs/MEs** | **In progress** |

Efficiency indicates how consistently things are done right. Applied to SENTINEL, measuring efficiency requires calculating the rate at which an SME can complete the assessment of all their personal data processing activities (PAs), which, in turn requires comparing the number of PAs for which compliance with GDPR has been established/assessed to the total of PAs the company is accountable for. This is calculated as follows:

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

By providing innovative and user-centric data protection services such as the ROPA, GDPR CSA and DPIA, SENTINEL is expected to boost compliance efficiency by at least 40 percentage points. Practically speaking, improving compliance efficiency implies then to increase the number of PAs that have been described, recorded in SENTINEL's ROPA, and assessed through either GDPR CSA or DPIA. To establish this KR, it is first necessary to compare for each user of SENTINEL evolution of their compliance efficiency rate. To do so, compliance efficiency will be measured twice: before using SENTINEL (t0), and after a period of use (t1). KR-1.2 will result in the average of the variation of compliance efficiency rate of SENTINEL users (n).

$$KR - 1.2 = \frac{\sum_1^n Compliance\ efficiency\ (t1) - Compliance\ efficiency\ (t0)}{n}$$

After the release of FFV of the SENTINEL platform, within M22-M24 under the works of WP6, CG pilot activities were carried out during which two engaged end-users from CG tried and tested the ROPA, GDPRCSA and DPIA services of the platform upon specific pilot experiments of three different personal data PAs utilised in the company's normal operations. Initial evaluation results have been already provided from these two trials indicating that SENTINEL can be used to improve the GDPR compliance efficiency of the PAs used in the pilot experiments. In addition, within M24, TIG pilot activities commenced, and a dedicated workshop conducted to demonstrate the SENTINEL FFV to relevant pilot end-users deriving from the Socialcare sector. Respective trials are currently in progress, in the context of the TIG pilot, to assess the GDPR compliance of the SME's PAs related to socialcare using the SENTINEL compliance services abovementioned. The assessment of compliance efficiency that SENTINEL can provide to SMEs/MEs is an ongoing process that follows the SENTINEL technical progress. Specifically, SENTINEL compliance services are planned to be tested in Y3 by a set of additional trials organised by CG and TIG and external SME end-users engaged through on critical periods of project's technical developments (e.g. during M28-M30 close to the final platform release). This approach will allow the consortium to measure the compliance efficiency that SENTINEL can provide to the engaged SMEs after distinct periods of use and make comparisons with the efficiency rate the SMEs had obtained before using SENTINEL by utilising the compliance efficiency indicators presented above.

This KR is considered ~60% achieved in the sense that the services (ROPA, GDPR CSA and DPIA) and methodologies that are going to be used to measure the compliance assessment efficiency have been implemented and initial testing activities have been launched. Within Y3 the corresponding measures will continue to take place (mainly as part of WP6 activities) to monitor and assess this KR. **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 combined with literature data (already acquired

<table>
<tr><td colspan="3">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 against the SENTINEL offerings. Our intention is to leverage this survey in all of the forthcoming SME-centric workshops, as well as other relevant events. This KR will be evaluated during the validation phase. An important milestone towards this direction is the validation of the SENTINEL offerings through the test cases in the pilots, which will provide a basis for evaluation and verification. 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 during Y3. This KR is considered ~40% achieved. <b>Linked WP: 6; Owner: STS</b></td></tr>
<tr><td><b>KR-1.4</b></td><td><b>30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">Regarding KR-1.4, SENTINEL has organized three (3) SME-centric workshops (September 2021, May 2022 and October 2022), with the objective of raising awareness in SMEs/MEs all over the EU about GDPR compliance and PDP. Within this context, in Y2, the SENTINEL offerings have been identified, so as to start motivating attendees and grasping their attention towards the project's tools and compliance services. Based on the established list of offerings, the SENTINEL consortium has prepared a questionnaire to record user acceptance of SENTINEL offerings which will serve as a baseline. It is worth to mention, that during the 3rd workshop where the SENTINEL MVP demonstration took place 29% of participants accepted that SENTINEL can be a potential solution to be implemented in their companies, 42% have answered that they could consider investing in tools/services similar to SENTINEL within the next 2 years, while 54% choose that the "Automated GDPR compliance, recommendation and real-time monitoring" are the most useful services among the SENTINEL tools to be used in their own business. More in-depth analysis of the responses can be found in D7.5 "Ecosystem building and SMEs engagement report - interim version". SMEs that opted in for trialling the SENTINEL offerings will be contacted again and asked to fill in the questionnaire again after using the SENTINEL services integrated within the SENTINEL platform. This indicator will help us determine the acceptance before SENTINEL and any improvement after SENTINEL. So far, we achieved 30% of this specific KR while it will be fully achieved at the end of the project. <b>Linked WP: 7; Owner: UNINOVA</b></td></tr>
<tr><td><b>KR-1.5</b></td><td><b>Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">This KR is directly connected with the expectations and goals of plugins, such as ACS's CyberRange and ITML's Security Infusion and thus is addressed in that context. The goal is to provide a quantitative measurement of the final results of this task with regard to data integrity and confidentiality. On that note, we first deployed our solution as part of a real use case and then performed the evaluation with respect to the objective of KR-1.5. During Y1, ACS has conducted several meetings with the project's end users to get information such as identify a list of threats that could potentially occur and respectively be avoided, their infrastructure with regard to OTMs, etc. With the data collected, generic infrastructure has been created on the CyberRange, in order to exploit threats and play cyber-attack. Four (4) scenarios have been created to raise awareness of the SME, related to data storage and accessibility. In the Y2, these efforts have been intensified to be able to prove and demonstrate the applied protection mechanisms for eight (8) types of cyber threats. To achieve this, we used a new gaming interface of CyberRange. The covered cyber threats are phishing, malware attack, unsafely removed files, unencrypt disk files, social media presence, password guessing, password reused, and unprotected password. For Y3, we will collect feedback of end users to meet their needs and adapt or create more awareness scenarios based on the needs of SME's. This KR is planned to be fulfilled at the end of the project and currently is considered ~70% achieved. <b>Linked WP: 4; Owner: ACS</b></td></tr>
</table>

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

Objective 2 is realized through the work performed in WP1, WP2, WP3, and WP4. In Y2, 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 was 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 GDPR Compliance Self-Assessment (GDPR 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. It thus provides SMEs with a) GDPR Compliance Level of Processing Activities (PAs) they are responsible for, and PAs they carry out on behalf of another company, and b) a list of recommendations to improve PA's GDPR Compliance Level.

The table below provides a summary of the KRs related to Objective 2, including their status update, the activities conducted in Y2 and the strategy towards their successful completion.

*Table 2. KRs status update - Objective 2*

<table>
<tr><th>KR-2.1</th><th>Innovative customized Requirements Engineering related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs</th><th>Achieved</th></tr>
<tr><td colspan="3">KR-2.1 has been successfully fulfilled in the context of WP1 and in particular through the actions performed in T1.1 "The SENTINEL Requirements Engineering Methodology". These involved:<br>• Identification of generic SME requirements with respect to Cybersecurity (CS) and personal data protection considering relevant challenges and threats as well as current state-of-the-art for assessing and managing risk for SMEs.<br>• Positioning of the technological and methodological assets of SENTINEL with respect to the above requirements.<br>• 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.<br>• Demonstration of the feasibility of the methodology through its application on two pilot cases.<br>The above is reported in D1.1 "The SENTINEL baseline". This KR is considered 100% achieved.<br><b>Linked WP: 1; Owner: IDIR</b></td></tr>
<tr><td><b>KR-2.2</b></td><td><b>Implement a dynamic rule insertion mechanism for the Recommendation Engine, providing predicates, variables and actions for forming rule expressions, addressing at least 135 organisational and technical measures (OTMs)</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The purpose of the Recommendation Engine (RE) is to provide recommendations in the form of Organisational and Technical Measures, plugins and trainings, so as to assist an SME to address potential shortcomings and vulnerabilities in the realm of data protection and cybersecurity protection. For the purpose of the MVP (D3.1), the Recommendation Engine was implemented following a rule-based approach to provide a set of recommendations depending on cases of profile and risk level outputs. Therefore, the RE leverages a pre-specified rule base to map Organisational and Technical</td></tr>
</table>

<table>
<tr><td colspan="3">Measures (OTMs) that correspond to a given risk assessment level with a list of plugins, trainings and other optional capabilities. At the FFV phase (work conducted in Y2), SENTINEL RE was further extended with 50 open – source tools and over 120 courses to increase flexibility and accuracy of recommendations. Additionally, and with the same goal in mind, asset ownership and locality were introduced in the calculations making the RE more accurate and realistic. This KR is considered ~70% achieved. <b>Linked WP: 3; Owner: ITML</b></td></tr>
<tr><td><b>KR-2.3</b></td><td><b>Test GDPR compliance and digitalized DPIA self-assessment framework.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The KR-2.3 is linked to WP2 and 4, and more specifically deliverables D2.1 and D4.1 due M12 and D2.2, D4.2 and D2.3, D4.3 due in M18 and M30 respectively. A lot of progress has been made already regarding this KR as part of MVP and FFV versions of the GDPR CSA and DPIA self-assessment tools respectively were designed and implemented. Both tools are integrated into the SENTINEL platform via APIs and can be executed for one processing activity at a time, providing a score that will be visible to the user via MySentinel UI. The testing of the frameworks in real-world settings is going to be performed under WP6. Activities have already been planned to perform a conformity assessment of the GDPR CSA Assessment Model with CARPA’s data protection requirements, while in parallel assessments of the GDPR CSA Method, Framework and Model have been performed with ISO/IEC 33002, ISO/IEC 33003 and ISO/IEC 33002 respectively. This KR is considered ~75% achieved. <b>Linked WPs: 2; 4; Owner: STS</b></td></tr>
<tr><td><b>KR-2.4</b></td><td><b>Offer robust and easy to adopt data access management, authentication, authorization and record keeping technologies to SMEs/MEs for GDPR compliance.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">This KR is mainly tackled by SENTINEL’s Identity Management System (IdMS) as well as the record keeping capabilities provided by its Profile Service. The IdMS provides authentication, authorization and Single Sign-On capabilities to SENTINEL end users, based on an open-source solution (Keycloak), towards adopting the MyData model, whose core idea is that data owner should have an easy way to see where personal data goes, specify who can use it, and alter these decisions over time. The SENTINEL IdMS is offered as-a-service, where SMEs can use it to verify, and manage attributes and entitlements that are necessary for the creation and maintenance of digital identities for all users accessing third party applications EU-wide. This includes functionalities and flows like user registration, account recovery, profile management, credentials management, and consent management. In terms of record keeping, SENTINEL offers the capability of storing versatile organisation-wide information, as well as storage of activities that involve processing of personal data. Furthermore, it offers the capability of keeping a formal, immutable and auditable Record Of Processing Activities (ROPA) that helps companies comply with Art.30 of the GDPR. All records are persisted in the Profile Service and are made available to SENTINEL plugins (such as GDPR CSA, DPIA and CSRA) as required. This KR is considered ~70% complete and on track to be achieved in M30. <b>Linked WP: 2; Owner: ITML</b></td></tr>
<tr><td><b>KR-2.5</b></td><td><b>Ensuring the delivery, adoption, and utilization of a unified Identity Management System.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">This KR is tightly connected with KR-2.4 and is related to the delivery of an integrated IdMS. As mentioned above, the IdMS is offered as-a-service that provides a range of functionalities to the SME/ME including i) Central, EU-wide, self-service identity management, ii) Credentials and access tokens management that allow Authentication (AuthN) of the above identities, iii) Role Based Access Control (RBAC), iv) Federation with 3rd party applications, based on protocols that allow scalable expansion according to the needs of SMEs/MEs wanting to leverage SENTINEL IdMS, v) My Data, data management scheme for secure, GDPR compliant storage and access of user data, vi) Governance. Currently, adoption and widespread utilization of the unified IdMS are being verified as part of WP6 activities, where the SENTINEL use case owners trial the system in real-world settings. KR is considered ~70% complete and will be achieved in M30. <b>Linked WP: 2; Owner: ITML</b></td></tr>
</table>

## 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 and Y2 of the project, in the four main technical work packages: **WP2** - which develops personal data protection and cybersecurity technologies key to SENTINEL, namely the GDPR compliance self-assessment, the cybersecurity risk assessment, the IdMS and others; **WP3** - which develops core components of the SENTINEL technical architecture specially focusing on formulating, formatting and presenting an appropriate human-readable set of recommendations (the "policy"), in the form of collections of (a) organizational and technical measures, (b) plugins, tools and software, and (c) cyber awareness and PDP trainings and educational material; and **WP4** - which is primarily responsible for (a) SENTINEL's tailored SME Profiling process including the Profile Service and the Self-Assessment Service, (b) the detailed capturing of personal data processing activities, including an auditable ROPA, (c) an automated DPIA, (d) deploying advanced Cyber Range -based simulations and training, and (e) developing the SENTINEL Observatory; overall integration work takes place in **WP5**.

After the successful release of the SENTINEL MVP (M12) significant effort has been dedicated to technical developments leading to SENTINEL's full-featured version (M18). Specifically, functioning and demonstrable versions of the functionalities, tools or services below have been developed in Y2, all of which are contributing towards Objective 3:

- Detailed cyber asset capturing and inventorying, based on the MITIGATE framework, which allows for cybersecurity risk assessments (CSRA).
- Maturing of the MVP's cybersecurity simulation environment into a full-fledged cybersecurity risk assessment (CSRA), serving as SENTINEL's third self-assessment tool.
- Further utilization of the SCORE metamodel into the SME profiling process, including the convergence of the input of the two PDP-related self-assessment tools (the GDPRCSA and the DPIA) with the existing personal data processing activity capturing process, eventually allowing unified SME profiling.
- The deployment of a GDPR compliant, permanent and immutable record of processing activities (ROPA).
- A revised, enriched and more detailed global organizational and technical measures (OTMs) classification, complete with selection taxonomies for the recommendation engine and user-facing policy metadata.
- Enhanced policy recommendations considering detailed cyber asset data and available tools (plugins) and trainings.
- Policy enforcement monitoring in the form of tracking the implementation status of OTMs, also considering their recommendation status.
- An expanded Observatory with a knowledge base and additional sources / feeds.
- An Identity Management System (IdMS) with proof-of-concept SSO functionality.
- The deployment of the updated GDPR compliance self-assessment plugin (GDPRCSA) which considers all six aspects of GDPR compliance: (a) Record (carried forward from the

MVP), (b) Personal Data Lifecycle Management, (c) Rights Management, (d) Consent Management, (e) Data Protection Management, and (f) Personal Data Breach Notification.
- Implemented a series of trainings in the Cyber-Range (new gamification interface), based on realistic SME-focused scenarios (Post FFV, M18-M24).
- Technical developments, providing a proof of concept for the use cases 4 and 7, for: (a) receiving security notifications, and (b) reporting and sharing cybersecurity incidents (e.g. data breach notifications).
- Preparatory work (M18-M24) for improving SENTINEL's user experience with redesigned user flows, inline help, a quick-start guide and tutorials (by M30).
- Preparatory work (M18-M24) for supporting Processing Activity templates (by M30).
- Preparatory work (M18-M24) and sample rules for transitioning into a rule-based Recommendation Engine (by M30).

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 provides a summary of the KRs related to Objective 3, including their status update, the activities conducted in Y2 and the strategy towards their successful completion.

*Table 3. KRs status update - Objective 3*

| **KR-3.1** | **More than (20) novel services and tools utilized and integrated from diverse multi-domain technological areas and applied in SMEs/MEs environments.** | **In progress** |
|---|---|---|
| We consider the term services and tools within the wider concept of "capabilities" offered by SENTINEL. During Y2, technical partners - as part of activities in WP2, WP3, WP4 and WP5 – have developed from scratch and leveraged tried-and-tested tools and services, which are integrated for the **Full Featured Version (FFV)** (see D5.5) and span several capabilities.<br>- The MITIGATE framework, provided by FP, and integrated with SENTINEL's FFV, is delivering a number of user-facing tools and services: (1) The Vendor and Product Management service which delivers a CPE-based catalogue of vendors' products. It enables SMEs/MEs to identify and select specific versions of products from vendors that correspond to their IT assets aiming to search for security-related information on these products. (2) The asset inventory service (online ISMS for SMEs/MEs), including asset interdependencies and security-related information. (3) The Vulnerability Management service which allows SMEs/MEs to capture information of all vulnerabilities along with their attributes and severity scores identified for the selected products. (4) The Common weaknesses management service which is realized through the Common Weakness Enumeration specification of MITRE and provides a common language of discourse for discussing, finding, and dealing with the causes of software security vulnerabilities as they are found in code, design, or system architecture. (5) The Threat Management service which provides to SMEs/MEs all threat-related information upon specific selected IT products. (6) The Simulation Environment which enables SMEs/MEs to experiment with attack scenarios by selecting specific vendors' products and obtain knowledge on interrelations of corresponding threats and vulnerabilities. All these MITIGATE services are integrated in SENTINEL via the (7) CyberSecurity Risk Assessment (CSRA) tool, available to users via MySentinel (Cybersecurity), enabling SMEs to assess assets grouped under Processing Activities (PAs).<br>- Another novel service is the (8) GDPR Compliance Self-Assessment (GDPRCSA) developed by LIST. GDPRCSA allows SMEs/MEs to determine their compliance level with GDPR and provides a set of recommendations to improve it. GDPRCSA covers all six data protection capabilities (Record, Personal Data Lifecycle Management, Rights Management, Consent Management, Breach notification management, and Data Protection Management System).<br>- The (9) Data Protection Impact Assessment (DPIA) API-based service, provided by STS, allows SMEs to identify (through assessment) and minimise (through recommendations) the data processing-related | | |

<table>
<tr><td colspan="3">risks and is invoked for processing activities that are likely to result in a high risk to individuals.<br>- (10) Security Infusion (SI) is an all-in-one solution provided and supported by ITML, which implements data collection and management services in order to address the need for control baseline of Information and Communications (ICT) operations with integrated risk mitigation and regulatory compliance capabilities. Another indicative example of the SENTINEL platform novel services is the (11) Identity Management Service (IdMS), also provided by ITML, which supports self-service EU-wide and MyData-compliant identity management and data governance with Single Sign-On capabilities.<br>- SENTINEL also provides robust cybersecurity data retrieval, management and dissemination leveraging custom tools that actively connect the (12) Observatory Information Exchange (supported by ITML) with external cybersecurity and open-source threat intelligence, such as MISP, HELK and NIST for browsing, searching, and filtering. Within the same context, the (13) Observatory Knowledge Base is hosting third-party content for cybersecurity and personal data protection, fetched from i) Information Exchange, ii) MITIGATE and iii) open-source content and training material.<br>- SENTINEL's OTM recommendations are accompanied with (14) Open-Source software/plugins and educational or training material, curated by TSI, which helps users better understand, design and implement security and data protection controls within their organization. A major SENTINEL offering is (15) the CyberRange, contributed by ACS, enabling (a) simulation environments (testbeds) and (b) a gamification interface with realistic and SME-focused scenarios, for testing cybersecurity setups before on-site integration for optimizing defences and training end-users.<br>- To the above services we should add core offerings of the integrated SENTINEL platform for cybersecurity and personal data protection. The platform enables users to (16) receive security notifications, through the integration of Security Infusion (SI) with the SENTINEL Notification Aggregator; (17) handle and share cybersecurity incidents and data breaches, as they occur, leveraging the Incident Reporting module; (18) create and edit a data protection-oriented organisational profile, complete with a global asset profile, MITIGATE-modelled asset inventory and a complete Processing Activities data capturing model shared with the self-assessment tools; (19) record their processing activities in a permanent, immutable and auditable ROPA, thus satisfying Art. 30 of the GDPR; (20) obtain tailor-made recommendations of measures (OTMs), software and trainings, based on thorough analysis of every aspect of their profile and processes facilitated through an intelligent synergy of SENTINEL's Recommendation Engine (RE) and Policy Drafting (PD) modules, and, finally, monitor the progress of the enforcement (implementation status) of the aforementioned recommendations through the (21) Policy Enforcement tool, integrated with each policy draft.<br>Details on individual progress and functionalities of these tools and services in the full-featured version (FFV) are found in deliverables D2.2, D3.2, D4.2 and D5.5. Next steps in this KR are to enrich these offerings with functionalities and a better user experience so as to automate cybersecurity and data protection processes for SMEs in the most intuitive way possible, by the final release of SENTINEL (M30). This KR directly linked with iKPI-2.3 and it is currently considered 80% achieved. <b>Linked WPs: 2; 3; 4; 5; Owner: FP</b></td></tr>
<tr><td><b>KR-3.2</b></td><td><b>At least (10) tools and services related to data protection, data privacy management, security assurance and compliance.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The technical work (WP2-WP5) completed by the consortium for the FFV has directly contributed to this Key Result. The SENTINEL tools and services for cybersecurity, data protection and compliance have been identified as such:<br>1. Organisation profiling.<br>2. Cyber asset inventorying (MITIGATE).<br>3. Personal data processing activities capturing.<br>4. GDPR compliant recording of PAs (ROPA).<br>5. GDPR compliance self-assessment (GDPRCSA).<br>6. Data protection impact assessment (DPIA).<br>7. Cybersecurity risk assessment (CSRA/MITIGATE).<br>8. Policy recommendations for OTMs, software and training material.<br>9. Policy enforcement monitoring: tracking the implementation status of OTMs.<br>10. Cyber Range simulations and gaming with realistic SME scenarios (CyberRange).<br>11. Identity management system (IdMS).</td></tr>
</table>

<table>
<tr><td colspan="3">12. Cyber incident reporting and handling.<br>13. Receiving security notifications with Security Infusion (SI, FVT).<br>14. Observatory Knowledge Base (KB).<br>15. Observatory Information Exchange (IE).<br>Some of the above services not only support the integrated SENTINEL solution as a whole but are supported by partner-contributed components. As most of the tools and services targeted above participate in the use cases of the interim full-featured release of SENTINEL allowing us to measure this KR qualitatively and quantitatively. Considering the completion aspects for the individual tools and services in the listing above, we have recorded an overall average progress of ~75% for the KR. <b>Linked WPs: 2; 3; 4; 5; Owner: IDIR</b></td></tr>
<tr><td><b>KR-3.3</b></td><td><b>Update and enrich the SENTINEL OTMs classification and their mappings to adapt to the dynamic properties of the SENTINEL Recommendation Engine.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">After the FFV release, SENTINEL’s Common Service has been enriched with around 50 open-source tools and over 120 courses. Cyber assets in the inventory now support asset locality and ownership. This makes the Recommendation Engine (RE) inputs and outputs even more dynamic and tailored to end-user needs. The above have been reported in D3.2 “The SENTINEL digital core: Full-featured version” and is anticipated to significantly advance SENTINEL services in privacy-aware environments for SMEs/MEs. The RE will be continuously updated and enriched to further increase its accuracy. Thus, this KR is still in progress and will be realised in the final version of the SENTINEL integrated framework. Based on the progress and completion of enrichment of OTMs, new tools and courses mentioned above, we may consider this KR as ~70% achieved. <b>Linked WP: 3; Owner: ITML</b></td></tr>
<tr><td><b>KR-3.4</b></td><td><b>A dynamic Recommendation Engine which is both i) performant, with responsiveness (latency) lower than 3 sec and ii) highly available, with over 99% requests satisfied on average.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The current version of the RE, as included in the FFV has been measured to i) responsiveness of about 50ms and ii) 100% availability. As the rules become more complex in the final version of the platform the inference time is expected to slightly increase the latency. However, we are highly confident that the KR will be met. In Y3, we plan to carry out larger scale stress tests in order to acquire measurements in more complex scenarios of usage, compliance with the goals of the KR. This KR can be considered as 70% achieved. <b>Linked WP: 3; Owner: ITML</b></td></tr>
</table>

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

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

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

Towards experimentation execution, in the M13-M24 period, piloting-related activities have seen progress, including the definition and refinement of experimental setups and relevant infrastructure of the two use case owners. In the meantime, the project has secured the engagement of six (6) extra-consortium SMEs/MEs through Digital Innovation Hubs (DIHs) to trial the SENTINEL platform during the validation phase. A critical milestone achieved as an enabling step towards this objective has been the successful implementation of the MVP. The MVP was demonstrated to internal and external stakeholders and its functionality, usability and performance characteristics were internally evaluated by the SENTINEL user partners. The results informed the development of the FFV. This work will continue in Y3 towards the goal of executing at least five demonstrators in real-life settings. The identification of user personas will assist the user-centric validation process. Another important milestone towards this direction is the definition of the SENTINEL main offerings that aims to 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, including their status update, the activities conducted in Y2 and the strategy towards their successful completion.

*Table 4. KRs status update - Objective 4*

<table>
<tr><td><b>KR-4.1</b></td><td><b><i>Successful collection of data for recommendations of personal data protection technologies and GDPR compliance procedures in complementary SMEs/MEs environments.</i></b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The SENTINEL platform (since it’s MVP version) is fully integrated and provides functionality that successfully collects data from SMEs/MEs to build their profile, provide assessments via the GDPR CSA and DPIA tools and policy recommendations via the policy recommendation engine. The DPIA toolkit underwent improvements to account for the implemented OTMs during the FFV, while FFV of GDPR CSA provides a set of recommendations to improve SMEs/MEs compliance levels. In the final version during Y3, the DPIA questionnaire will be reintroduced with a more complete set of questions. Finally, GDPR CSA module will be improved regarding the accessibility of questionnaires, proposed answers, and proposed improvement. This KR is 75% complete <b>Linked WP: 6; Owner: STS</b></td></tr>
<tr><td><b>KR-4.2</b></td><td><b><i>Delivery of three (3) integrated versions of the SENTINEL framework.</i></b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The MVP constituted the first integrated version of the SENTINEL framework and was delivered in M12 and reported in D5.4, while the FFV was delivered in M18 and reported in D5.5. Both versions were fully integrated. The final platform release is expected in M30 and will be presented in D5.6. This KR is 67% complete and on track to be achieved in M30. <b>Linked WP: 5; Owner: INTRA</b></td></tr>
<tr><td><b>KR-4.3</b></td><td><b><i>Execution of five (5) demonstrators in complementary SMEs/MEs’ industries and environments, together validating at least 95% of tools.</i></b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The consortium has identified six (6) additional SMEs, in addition to the two (2) pilots defined in the GA, as a result of T6.3 activities. In Y2, these demonstrators have been contacted and four of those have been already invited to test the SENTINEL MVP functionalities under four (4) use cases. To assist to understand what the SENTINEL MVP is (scope, functionalities, the use cases etc.), and how to test it a dedicated workshop was organized by the SENTINEL consortium for the SENTINEL pilot partners (CG and TIG) and the external SMEs. After the workshop, the participants were asked to run individual tests and fill in a questionnaire by providing feedback about their experience in testing the SENTINEL MVP. As a result, four (4) out of six (6) demonstrators have successfully tested and provided valuable feedback on the SENTINEL MVP.</td></tr>
</table>

<table>
<tr><td colspan="3">In addition, with the successful release of the SENTINEL FFV, the SENTINEL pilot partners (CG and TIG) have been starting the end-to-end validation of the SENTINEL platform as part of WP6 activities. These activities and the final evaluation of this KR will be accomplished when the projects reach to it's milestone 5 'Demonstration Fire' when the above-mentioned demonstrators (external SMEs, in addition to the two (2) pilots of the project) will finalise the end-to-end validation of the SENTINEL platform. INTRA – as an integration leader – will monitor this KR under T5.2 to determine the percentage of tools validated in each demonstrator. This KR is considered 50% achieved in the sense that we have already secured the SENTINEL demonstrators for end-to-end validation of SENTINEL tools. <b>Linked WPs: 5, 6; Owner: CG</b></td></tr>
<tr><td><b>KR-4.4</b></td><td><b><i>More than ten (10) trials to demonstrate SENTINEL tools' applicability and performance within real-world environments.</i></b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">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 end–users. As mentioned in KR-4.3, as part of the work conducted in WP6 (during the pre-pilot phases), short-run tests were executed by the two end-user partners CG and TIG right after the SENTINEL MVP release (M12) and 4 initial trial executions were conducted for the evaluation of the SENTINEL MVP within M16-M17 period. Specifically, during the latter period, the two end-user partners, and two more external SMEs were engaged via Digital Innovation Hubs (DIHs) and provided initial feedback after trying the SENTINEL MVP. After the SENTINEL FFV release the main pilot phase was commenced in M18 and within M22-M24 the 1st stage of CG pilot was conducted, including the performance of two (2) trial executions by two (2) CG end-users who tested the SENTINEL FFV under specific pilot experiments relying on the healthcare sector. Moreover, the TIG pilot activities have started in M24 and additional trial executions by TIG pilot end-users are currently in progress to assess the SENTINEL FFV towards a pilot experiment associated with socialcare. The plan for Y3 is to keep organising a set of trials allowing both end-user partners and external SMEs engaged by DIHs to test the SENTINEL FFV in a more mature state. Up to M24, six (6) external companies are already engaged. We plan to continue SME end–users' recruitment via DIHs and focused SME-centric workshops towards achieving this KR. According to the above, this KR is considered 60% achieved. <b>Linked WP: 6; Owner: FP</b></td></tr>
<tr><td><b>KR-4.5</b></td><td><b><i>Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.</i></b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">Several meetings have been carried out to define and implement the User Interface (UI) of the SENTINEL platform, namely MySentinel. As part of these meetings, updated versions for the mock ups were presented to the consortium alongside an initial version for the User Journey. Continuous work has been carried out on the UI since the start of the project. By M12, the MySentinel dashboard included links to components that were incorporated in the MVP, as well as the relevant pages. Organization Profile, Processing Activities, Contact Persons, Assets, Self-Assessment tools, Policy Recommendations and a Threat Intelligence Platform (TIP) comprised the modules offered to the end-user by the SENTINEL platform in the MVP phase (more details in D5.1).<br>By M18, the MySentinel dashboard already included links to components and modules that were incorporated in the first complete prototype, as well as the relevant pages. This means that apart from the MySentinel dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts were also included in the second version of the platform. Additionally, feedback from collaborating end-users with diverse backgrounds (under WP6) was taken into consideration in the platform.<br>By M24, several elements of the MySentinel UI in several different pages have been updated. Additionally, a number of bugs/glitches identified by the technical team and/or the end-users have been fixed. Furthermore, the UI has been integrated fully with the backend modules. Moreover, the Cyber Range Gaming Interface, offered by ACS, has been integrated into the platform.<br>Moving forward, we shall continue to do comprehensive work in order to refine and enrich the content of the UI by constantly engaging and closely collaborating with end-users (under WP6), incorporating their feedback and implementing a UI/UX which offers true usability. Additionally, we will make any adaptations required in the communication of the UI with all modules as they progress. This effort will</td></tr>
</table>

result in the final version of the MySentinel UI and will be documented in the subsequent iteration of D5.1 and D5.2, namely D5.3. This KR is 70% complete. **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 Y2, 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 joint Cyber Security webinar organised on the 19th of January 2023 where SENTINEL together with CitySCAPE, HEIR, PUZZLE, SECANT and TRAPEZE projects have presented their results achieved so far and then they had a fruitful open discussion to joining forces about the cyber security challenges and issues in different domains. The event has gathered more than 50 participants and based on the open-session discussion we have already supported CitySCAPE to create useful information for Policy Brief. SENTINEL was actively involved in another webinar named "EU-Made Cybersecurity for Safe, Resilient and Trustworthy Applications and Services" which was jointly organized by ARCADIAN-IoT, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SPATIAL, TRUST aWARE projects. The webinar took place on the 27th of February 2023 and has provided an overview of how novel solutions can protect complex ICT infrastructures and create a stronger, more innovative, and resilient European industry.

In addition to this, the consortium has organized its 3rd SME-centric workshop (on the 25th of October 2022) and Workshop/Training session (on the 26th of September 2022) with SMEs for MVP demonstration, with more than 100 registrations (more than 70 attendees), including SMEs/MEs coming from different application domains and countries across the EU, 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, their perception of technical and organisational measures, infrastructure and awareness of GDPR compliance obligations.

In a co-organization with AI4HealthSec and HEIR H2020 projects, an international workshop on Information & Operational Technology (IT & OT) Security Systems took place on the 23rd – 26th of August 2022. This workshop took place in conjunction with the 17th International Conference on Availability, Reliability, and Security (ARES 2022).

SENTINEL has also engaged different DIHs, at national and EU level, namely Produtech, DIH4CPS, DIHWorld, Madeira DIH, Digital Manufacturing Innovation Hub Wales, DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH.

In terms of SENTINEL exploitation, standardization and ecosystem building roadmap, the M13-M24 period relates to SENTINEL "Sustainability building", which as mainly focused on following activities:

- Employ a clear definition of SENTINEL offerings and value proposition.

- Encourage further engagement with key stakeholders.
- Framing individual and joint exploitation paths.
- Boosting standardisation activities.

From communication perspectives, additional promotional material such as four more (4) newsletters, nine (9) videos (1 promotional and eight (8) other video materials), six (6) SENTINEL podcasts, flyer, brochure, business card, regular posts in social media (LinkedIn, Twitter) were produced during Y2 attracting more and more attention as the project progressed.

Three (3) more papers have been presented in three (3) different conferences including the IEEE cyber security and Resilience (IEEE CSR) conference, the 9th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE 2022) the 30th Annual Network and Distributed system Security Symposium (NDSS 2023). These papers have already been published and are openly accessible to the general public. Two (2) other scientific publications have been submitted to European Conferences and we are waiting for final acceptance.

Finally, the consortium has participated the following major events: FIC Forum 2022, IoTWeek 2022, EU Policy to Projects Seminar (PPS), INTEROP V-LAB General Assembly 2022, CyberHOT Summer School 2022, Digital Transformation Summit 2022, FIC Forum 2023, IDC Security Roadshow 2023 and “Safe Internet Day 2023” February 2023.

In Y3, SENTINEL aims to contribute to the following objectives: (i) Continue with dissemination of the project results; (ii) Creation of the final SENTINEL promotional material; (iii) Organization of the final dissemination activities, and (iv) Support on further take-up of the project’s results.

The table below provides a summary of the KRs related to Objective 5, including their status update, the activities conducted in Y2 and the strategy towards their successful completion.

*Table 5. KRs status update - Objective 5*

<table>
<tr><td><b>KR-5.1</b></td><td><b>All SENTINEL solutions, products and services aligned and harmonized with regulations and EU standards.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">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. In this respect, the CECL scientific officer in collaboration with the project’s Ethics Supervisor, updated the partnership on EDPB and national DPAs’ opinions, relevant to the SENTINEL scope, in real time, as well as through its regular reporting obligations (see D2.4 “Continuous data privacy legislation compliance monitoring and guidelines - interim version”) that was successfully submitted in M18. This KR is 50% complete. <b>Linked WPs: 2, 8; Owner: CECL</b></td></tr>
<tr><td><b>KR-5.2</b></td><td><b>Define a concrete dissemination strategy to raise awareness.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">From an early point of the project, the consortium has defined a structured methodology to disseminate the project’s offerings and preliminary outcomes and raise awareness of SENTINEL’s potential. The SENTINEL dissemination strategy has been already established and documented in D7.3 (M18). Furthermore, the strategy was successfully realised through a plethora of dissemination and communication activities conducted during Y1 and Y2. In Y3, we will increase awareness and disseminate the SENTINEL outcome among wider audiences by following the methodologies and strategy already defined in D7.3. <b>Linked WP: 7; Owner: UNINOVA</b></td></tr>
<tr><td><b>KR-5.3</b></td><td><b>Uptake more than (6) standards from several data privacy and compliance related technologies.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">Several developments during Y2 have taken into account important regulations and standards, such as the NIS Directive, alignment with ENISA’s objectives, the eIDAS regulation, standards related to</td></tr>
</table>

| | | |
|---|---|---|
| Information Security (e.g., ISO/IEC 27000) and standards related to Data protection and privacy (GDPR). In the reference period, STS has prepared a survey on the usage of standards and the interactions with standardisation bodies which has been distributed to all partners in order to record the specific use of standards by all partners. Furthermore, during Y2 SENTINEL successfully applied for the first open call of the Horizon Standardisation Booster, aiming to provide standardization support for H2020 projects (application made on the 5th of July 2022). Several meetings have been already conducted and the expert assigned by HSBooster.eu will assist SENTINEL to (i) analyse CARPA's requirement (conformity assessment of GDPR CSA Assessment Model), (ii) identify extent of existing and additional measures required for CARPA (based on current CSA and ISO standards being followed) and (iii) identify relevant current and upcoming standards that SENTINEL can take advantage of. This KR is 60% achieved. **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.<br>By the end of Y2, UNINOVA had engaged with three (3) more DIHs in addition to previously engaged five (5) DIHs. Thus, in total the project has already engaged eight (8) DIHs namely: Produtech, DIH4CPS, DIHWorld, Madeira DIH, Digital Manufacturing Innovation Hub Wales, DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH. Our plan is to continue promoting the project among new DIHs and fully achieve the KR-5.4 during the third year.During Y3, SENTINEL will keep maintaining direct connections with the DIHs already contacted, so that its members (the SMEs/MEs) will have a chance to trial SENTINEL as part of the validation phase (WP6). This KR is considered 90% achieved. **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 progressed in Y2 by updating its business model which initially was launched in Y1. In particular, among others, SENTINEL value proposition, main offerings, target markets, customer segments, possible revenue streams, individual exploitation plans and expected TRLs have been updated. 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. In Y2, an important milestone achieved towards realising Objective 6 is the release of the FFV version of SENTINEL described in D5.5 (M18). This further initiated the SENTINEL validation phase as well as activated the project's exploitation activities towards creating opportunities for European-based SMEs to use SENTINEL offerings. It will 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 the different networks of DIH previously identified.

The table below provides a summary of the KRs related to Objective 6, including their status update, the activities conducted in Y2 and the strategy towards their successful completion.

*Table 6. KRs status update - Objective 6*

<table>
<tr><td><b>KR-6.1</b></td><td><b>Ready to market integrated solution for the overall security compliance framework and independent privacy and security enhancing solutions (TRL 7).</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The MVP, described in D5.4, was the first step towards an integrated solution, while there have also been significant advancements in various individual solutions. The SENTINEL full-featured version (FFV), described in D5.5, has established a significant improvement in the data protection and cybersecurity services offered. The platform, as well as the individual offerings, are expected to become more mature through the validation and evaluation iterations that will follow, as part of WP6, and provide inputs for further improvements. This KR is 60% achieved. <b>Linked WP: 5; Owner: INTRA</b></td></tr>
<tr><td><b>KR-6.2</b></td><td><b>At least four (4) SENTINEL tools reach market readiness level (8) at the end of the project</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">SENTINEL is based on several mature – in terms of technology and market readiness- components (e.g., MITIGATE, Security Infusion, CyberRange etc), which are already placed at a high TRL, while some of them (Security Infusion and CyberRange) are already launched in the market. In addition, tools newly developed in the project (e.g., IdMS, policy drafting, self-assessment workflow, GDPR CSA module) will also be further improved in Y3 and validated in real-world settings.<br>The project's technical and development procedures further advance the tools contributed by partners, as well as services developed from the ground up, towards market readiness in an agile and continuous process. Project activities 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 process model is adjusted according to the SMEs' specific characteristics. Processes of the DPIA SA tool are also tailored to SMEs and modelled to be as automatic and independent of human assessors as possible. The initial evaluation of TRLs and MRLs of the SENTINEL platform and its components have been already conducted and reported in D7.7 and D8.12. More technical enhancements on the SENTINEL tools are performed progressively within the ongoing project's development works taking into account the feedback that is gradually received from the trials/pilots' execution evaluators. To this aim, different types of personas have been identified from SMEs end-users which will be grouped by specific criteria to better profile the targeted users and thereby improve the linkage between the technical work on the system architecture and the user-centric approach. By utilizing this persona-based validation, we aim to facilitate the identification and development of technical improvements (e.g. UI/UX improvements) which can increase the commercial readiness of the SENTINEL tools towards the current needs of SME markets.<br>Thus, this KR is monitored successively on the technical enhancements carried out after each pilot from the lessons learned and thereby the final calculation of the market readiness level reached by the SENTINEL tools will be assessed and provided in the final reporting period. Considering that initial technical improvements on the SENTINEL tools are already running compared to CG pilot evaluation results captured until M24, the work conducted for this KR may record an overall average progress of 60% in Y2. <b>Linked WPs: 2-5; Owner: FP</b></td></tr>
<tr><td><b>KR-6.3</b></td><td><b>At least six (6) third-party collaborations to be established for further applicability verification.</b></td><td><b>Achieved</b></td></tr>
<tr><td colspan="3">With respect to KR-6.3, SENTINEL has been interacting with several SMEs, since the beginning of the project, under activities of T6.3 and T7.4, with the purpose of establishing partnerships for applicability and testing of the SENTINEL offerings. SENTINEL has organised three SME-centric workshops in total (2 during Y1 and one during Y2), 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 eight (8) DIHs so that their associates (the SMEs) can trial the SENTINEL platform and provide feedback on the SENTINEL offerings. As a result of this collaboration, six (6) external companies have been already engaged among which 4 third-party (SMEs) entities were invited to participate in the MVP demonstration workshop that was organized to showcase the SENTINEL main offerings. A more detailed description of the actions being addressed by SENTINEL towards KR-6.3 and the strategy towards the successful completion, are addressed in Section 3.7 of this report. This KR is achieved and in Y3, the consortium will focus on bringing onboard more potential end-users (from DIHs or other sources) to trial the SENTINEL offerings as part of the activities of T6.3. The consortium will focus on validating the utility of the proposed solution at a larger</td></tr>
</table>

<table>
<tr><td colspan="3">scale with a view to be adopted by several thousand European SMEs/MEs, being part of the activities of T5.3. <b>Linked WPs: 5; 6; 7; Owner: UNINOVA</b></td></tr>
<tr><td><b>KR-6.4</b></td><td><b>More than ten (10) critical aspects (e.g., maintenance and software updates) will be addressed to ensure long-term sustainability of the solution.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">The design and development process of the integrated solution has already made various technical provisions related to long-term sustainability. These include aspects such as extensibility and modularity of the architecture, software maintainability in terms of proper organisation of code repositories, naming conventions in code, common objects libraries, documentation of synchronous and asynchronous APIs), regular backups and automated deployments. As the piloting has started bringing feedback for the platform development, more sustainability aspects are being considered to include ones related with the user feedback and the business landscape. This KR is 80% complete. <b>Linked WP: 5; Owner: INTRA</b></td></tr>
<tr><td><b>KR-6.5</b></td><td><b>A concrete business plan for business continuity (including joint exploitation plans, alliances and collaborations) will be released at the end of the project.</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">This KR is linked to WP7 and T7.1. Activities within this task have been ongoing since the start of the project. As a first step, all consortium partners contributed to the rationale which became the basis for the exploitation plan. Additionally, a questionnaire was created and circulated for gathering insights from many different perspectives including academia, large industries, technology providers and SMEs. These insights contributed to understanding and identifying SENTINEL’s value proposition and supporting its business modelling. This was presented in D7.2 titled “Market analysis and preliminary business modelling” in M6 of the project.<br>Following submission of D7.2, information gathering, and observation of market trends have continued for changes that could affect the elaboration of the joint business plan presented in the deliverable. In this context, as part of the continuous market observation, an intermediate analysis has been carried out resulting in an updated business strategy [value proposition, business model (canvas)] which was included in D7.7, submitted in M18. After D7.7, we have continued monitoring and analysing the market to provide updates to the (i) market analysis, (ii) business model, (iii) business model canvas and (iv) value proposition.<br>In Y3, the business planning will be revisited based on the acceptance of the SENTINEL platform and feedback we shall receive from end-users. This will involve a cooperation between T7.1, T7.2 and T7.3 and will be documented in the final business model, market analysis and long-term sustainability report (D7.9). This KR is currently considered as 70% achieved. <b>Linked WP: 7; Owner: AEGIS</b></td></tr>
</table>

# 3. Explanation of the work carried per WP during the 2nd 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**

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

## 3.2 WP2 – The SENTINEL privacy and personal data protection technologies

**Leader: LIST**

**Involved Partners: LIST, ITML, IDIR, STS, AEGIS, 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. The reference period of this report covers the WP2 activities conducted in the M13-M24 period. All WP2 partners worked intensively towards setting a solid ground for delivering the WP2 outcomes. As part of this work package, MVP version of self-assessment module for GDPR compliance (i.e., GDPR Compliance Self-Assessment), integrated IdMS, and standards-based risk management tool (i.e., MITIGATE) have been released in M12. During the same period, an enriched list with open-source tools and training to be used as external plugins recommended by the SENTINEL platform was produced. Based on these achievements, Y2 covered the release of the Full Featured Version of plugins developed within this work package. In addition, the list of open-source tools and training has been extended, including around 54 tools and 117 training elements, covering a wide range of security/privacy technologies and concepts.

The key achievements of WP2 include:

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

**(ii)** Delivering the integrated Identity Management System.

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

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

During Y2, two (2) deliverables have been prepared and submitted namely: D2.2 “The SENTINEL privacy & data protection suite for SMEs/MEs: FFV” and D2.4 “Continuous data privacy legislation compliance monitoring and guidelines - interim version” (delivered in M18). These deliverables contributed to milestone 3 “Innovation Fire”, due in M18.

### 3.2.2 Key WP2 achievements during reporting period at task level

**T2.1 The privacy and data protection compliance framework**

Led by LIST, T2.1 aims at developing SENTINEL’s privacy and data protection compliance framework that takes the form of a GDPR compliance self-assessment tool: the GDPR Compliance Self-Assessment (GDPR CSA) module. GDPR CSA is a rules-based engine derived from ISO/IEC 330xx family standard compliant expert-based GDPR compliance assessment approach. The task is split into three sub-tasks: T2.1.1, T2.1.2 and T2.1.3.

The work conducted within Sub-task T2.1.1 aimed at collecting and making explicit both GDPR compliance expected evidence and GDPR assessment rules to be achieved through knowledge management activities with experienced GDPR compliance assessors. Such activities aimed at 1) identifying evidence to collect to perform assessment, 2) specifying Organizational and Technical Measures (OTMs) that might meet data protection requirements, 3) defining GDPR compliance assessment rules regarding data protection risk level of Processing Activities (PAs).

Results of these activities have been formalized into a dedicated handbook. This handbook is the main input of T.2.1.2. Results also contributed to the development of SENTINEL's Data Model.

The second sub-task (i.e. T.2.1.2) is aimed at automating GDPR compliance assessment. The work conducted within this task aimed at coding "assessment rules". Particular attention has been paid to the documentation. Hence, in the code, script is explained; a GIT repository describes components of the GDPR CSA module.

The FFV of GDPR CSA has been released in M18. In addition to MVP version (delivered in M12) that covered only one data protection capabilities (i.e. RECORD), the GDPR CSA FFV allows to perform an assessment of the five remaining data protection capabilities: Personal Data Lifecycle Management (PDLM), data protection rights of individuals (RIGHTS), consent management (CONSENT), Data Protection Management System (DPMAN), personal data breach management (BREACH). This new version provides SMEs:

- Compliance level of the relevant data protection capabilities.
- Synthesis of compliance level in dashboard allowing data protection monitoring
- Set of recommendations to improve compliance levels, if necessary.

Finally, the work conducted in Sub-task T2.1.3 aimed at ensuring integration of the GDPR CSA FFV module within SENTINEL's platform. The connection between the SENTINEL's platform and the 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").

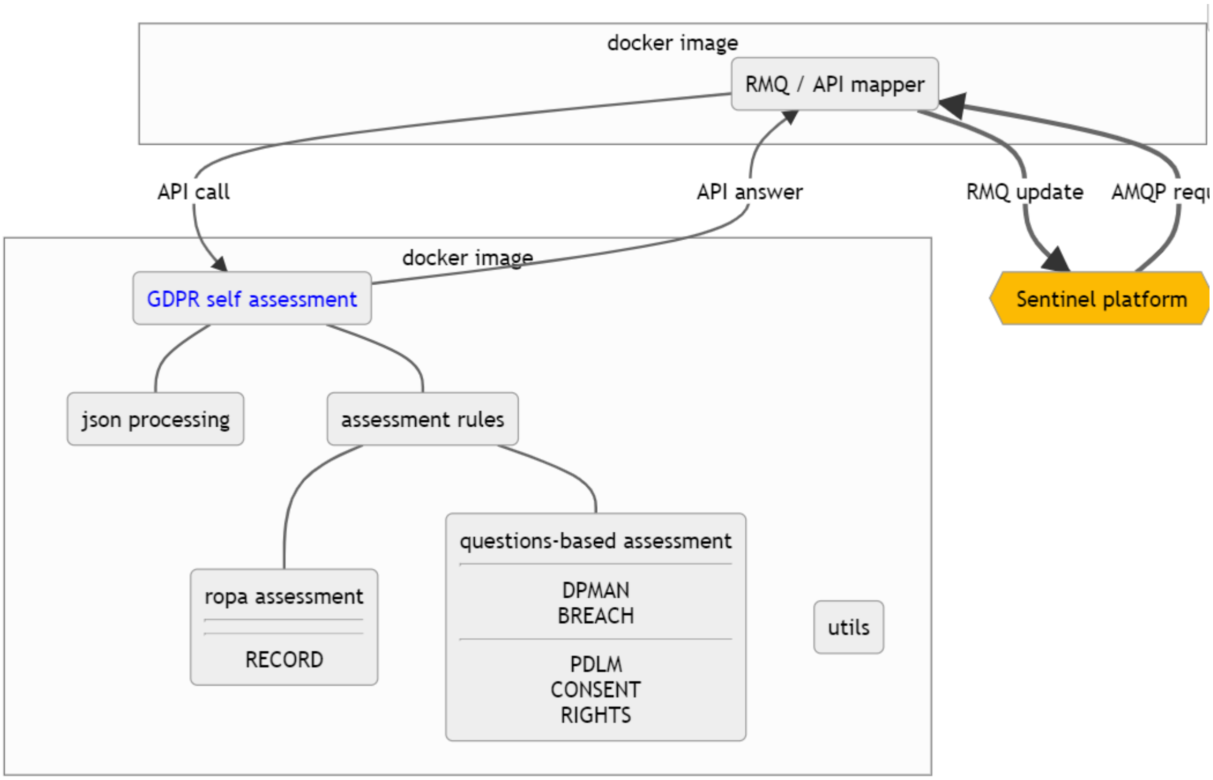


*Figure 1. GDPR CSA docker image*

T2.1 has contributed to the following WP2 objective:

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

The above work comprises significant input to D2.2 "The SENTINEL privacy & data protection suite for SMEs/MEs: FFV", (delivered in M18) while contributing also to milestone 3 "Innovation Fire", due in M18. Additional contributions will also be reported in D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product", contributing to milestone 5 "Demonstration Fire", due in M30.

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

T2.2 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. For the MVP version of IdMS, ITML presented an overview of the desired solution, requirements and constraints, including the detailed examination of the MyData Operator, selection and testing of state-of-the-art security technologies to support the solution, as well as a bottom-up approach to build the initial version of the IdMS, starting from the minimum set of the most fundamental requirements to provide a proof-of-concept demonstrator.

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

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

T2.2 has contributed to the following WP2 objective:

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

The above comprises significant input to D2.2 "The SENTINEL privacy and data protection suite for SMEs/MEs: Full featured version" (delivered in M18) contributing to milestone 3 "Innovation Fire" achieved in M18. Major contributions will also be provided in D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product", contributing to milestone 5 "Demonstration Fire", due in M30.

**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 standards-based risk management tool, providing a collaborative, evidence-driven risk assessment approach, delving into the technical specificities and security particularities of an organisation's infrastructure, analysing assets' interdependencies, detecting all cyber threats and assets' vulnerabilities, and calculating all cyber risks related to the underlined infrastructure, including potential cascading effects.

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

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

These are realized through the following functionalities:

- The vendor and product management, which is based on the CPE catalogue of National Institute of Standards and Technology (NIST). The catalogue is parsed for the embedded vendor names and products along with their CPE identifier, name, version, and edition, which are then extracted and assigned with a unique id.
- The vulnerability management, which allows the exact vulnerabilities related to the declared SENTINEL cyber-asset to be automatically inherited, based on the selected CPE identifier and the vulnerability records, that are replicated in the persistence engine from the *National Vulnerability Database (NVD)*.
- The common weaknesses management, which utilizes the *Common Weakness Enumeration (CWE)* [1] specification, allowing the automated identification of relations with specific vulnerabilities, identified on the selected cyber-assets.
- The threat management, which allows the identification of the threat landscape the underlined organisation's IT infrastructure may be exposed to, from the *Common Attack Pattern Enumeration and Classification (CAPEC*) of MITRE[2].

From this point on, FP has been working in close collaboration with WP2 partners on designing the final integration scenario of the cybersecurity components. More specifically, this scenario improves and properly enhances the first one as follows:

-Significantly enrich the current reports of the Cyber-Security Risk Assessment (CSRA) process.

-Enhance the current threat profile of a SENTINEL cyber-asset with:

- the MITRE Attack Framework, which is a curated knowledge based on the tracks cyber. adversary tactics and techniques used by threat actors across the entire attack lifecycle.
- the MITRE Mitigation strategies, which represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.
- The MITRE D3fend framework, which maps relationships between attacker and defensive countermeasures, providing a model of defensive techniques and artifacts to neutralize or mitigate specific offensive cyberattacks strategies.
- The NIST 800-53 list of (operational, technical and management) controls, which support the development of secure and resilient information systems.

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

T2.3 has contributed to the following WP2 objective:

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

The above provided significant input to D2.2 "The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version" (delivered in M18), contributing also to milestone 3 "Innovation

[1] https://cwe.mitre.org/
[2] https://capec.mitre.org/

Fire", due in M18 of the project. The final integration scenario of the cybersecurity components will be documented in the deliverable D2.3 "The SENTINEL privacy & data protection suite for SMEs/MEs: Final product", due in M30.

### 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 T2.4, 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 version 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) Deliver a curated collection of self-serving, state-of-the-art security- and privacy-enhancing modules, both open-source and contributed by consortium partners, which will be selected to meet individual specific needs of participants.

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

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

In addition, the external plugins were mapped to the respecting OTMs, which occurred during the technical SENTINEL meetings. The implementation of Task 2.4 was presented as part of the deliverable D2.2 “The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version”, which was submitted in M18.

During the last year of SENTINEL, the two lists will be further enhanced based on the upcoming needs of the project and the pilot evaluations. There, it will be validated wherever the selected tools and training elements are appropriate and cover the pilots’ needs, with related updates and adjustments being made. Also, technical aspects will be revisited, especially the descriptive models and the metadata of the two lists, which are processed by the Recommendation Engine in order to make targeted suggestions to the user.

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

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

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

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

T2.5 has contributed to the following WP2 objective:

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

The above provided input D2.4 ‘Continuous data privacy legislation compliance monitoring and guidelines - interim version’ as well as to milestone 3 “Innovation Fire”, due in M18. Final results of this effort will be reported in D2.5 “Continuous data privacy legislation compliance monitoring and guidelines - final version” due in M30.

### 3.2.3 Work carried out in WP2 per partner

| | |
|---|---|
| ITML | As task leader of T2.2, ITML provided the design and development of IdMS as-a-service reported in D2.2, after having completed a proof-of-concept demonstrator as part of the MVP version. 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, which will be used as one of the cybersecurity offerings of SENTINEL. 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. Finally, during Y2, ITML has also contributed to D2.2 providing extensive input regarding the IdMS system. |
| LIST | In Y2, as WP2 leader, LIST has organised coordination meetings with work package task leaders. LIST was also the representative of work done in this WP for review meetings. LIST ensured coordination with other work packages.<br>In addition, 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 D2.2.<br>In Y3, LIST will carry out a set activity to improve reliability of GDPR CSA's assessment model, and to increase usability of GDPR CSA by SMEs. |
| IDIR | In Y2, IDIR has contributed technical work in T2.1 by collaborating with LIST and other technical partners in the further refinement of the project's domain model for profiling, which is driven by privacy and personal data protection (GDPR) requirements and modelled to comply with standardised records of processing activities (ROPA). 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. In Y2, IDIR also contributed to (a) some high-level and strategic design work for T2.2, the design of a proof-of-concept IdMS, (b) technical work towards the design, implementation and refinement of the ROPA as part of the SME profiling and personal data processing activities capturing process (Profile Service), (c) work for the further convergence of the GDPRCSA inputs into the profile (Profile Service), (d) design work for the CSRA (asset capturing) and (e) estimating of the initial risk level associated with PAs (Self-Assessment Service). |
| 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. Finally, STS has contributed to D2.2. |
| AEGIS | AEGIS has contributed to the development of SENTINEL's Data Model and participated in all the relevant discussions and contributed to what was requested in accordance with the instructions provided by the task leaders as well as the WP2 leader. Furthermore, AEGIS developed a sample API to be used by the relevant cybersecurity components and modules to communicate with the front-end. The mentioned modules are integrated within the MySENTINEL UI (see D5.1 and D5.2). Finally, AEGIS participated in all WP2-relevant telcos. |

| | |
|---|---|
| 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. Also, TSI participated in the overall activities of T2.3 concerning the development and integration of the main cybersecurity modules of SENTINEL, focusing on the open-source solutions.<br>Within Y2, TSI significantly enriched and enhanced the list with the trainings and third-party open-source tools to be offered by the SENTINEL platform, as external plugins. The two lists were described in D2.2 "The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version", in which TSI contributed. The external plugins (trainings and open-source tools) recommended by TSI aim to fully cover the SENTINEL OTMs. Finally, TSI participated in the monthly WP2 telcos.<br>For Y3, TSI will further update the contents of the two lists. This will be driven by the technical progress of the platform (i.e., integration with the Recommendation Engine for better suggestions to the user), as well as the evaluation from the piloting environments regarding the appropriateness of the recommended tools and trainings. |
| CECL | The CECL team, being the T2.5 leader, has been continuously monitoring various sources for developments in the data protection landscape. As part of its monitoring activities, CECL identified relevant developments, consulted with the Ethics supervisor, and relayed the relevant information to the coordinator and the partners. Within the M13-M24 project period, CECL carried on its monitoring activities using the same methodology described above and successfully reported monitoring activities in D2.4. The corresponding compliance report codifies relevant opinions of the EDPB and national DPAs, as well as legal and policy developments at the EU level (such as the adoption of the New Standard Contractual Clauses (SCCs) for transfers of personal data from the EU and the European Economic Area (EEA) to third countries). The report emphasises developments relevant to SMEs and MEs and is used to inform the SENTINEL outputs and the content of current and future tasks. |
| FP | During Y2 FP participated in all WP2 meetings for the self-assessment module development. Within these meetings and specifically for T2.3, FP has introduced an approach to properly utilize and integrate the cybersecurity components contributed from the SENTINEL partners. 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. FP has continued to participate in all meetings relevant directly or indirectly to T2.5 by discussing how to align all technologies and solutions developed in the context of SENTINEL with the GDPR, and other EU regulations or best practices dedicated to privacy assessment and personal data protection.<br>FP introduced the Organization and Technical Measure (OTM) classification, based on which many different SENTINEL components and WPs are built upon. Through this classification our focus was to avoid complicated formal policy and procedures and simplify (as much as possible) our approach to make it approachable, understandable, affordable, and practical for smaller enterprises, selectively adopting, however, world-wide accepted and known standards, frameworks, and best practices. Towards this and in accordance with T2.5, in SENTINEL we were based on the hierarchy of the ISO/IEC 27001:2013 standards and ENISA's risk-based approach to protecting data and we built upon these. Towards this, we introduced |

| | |
|---|---|
| | 134 different OTMs grouped in 10 organization and 10 technical categories. These OTMs are further considered from the SENTINEL privacy and data protection compliance framework (T2.1). Upon successfully delivering the FFV of the SENTINEL platform, FP leads the proper design and implementation of the final integration scenario, which will be also realized through the MITIGATE adapter and system. |

### 3.2.4 Status of Deliverables and Milestones

The work conducted in WP2 in Y2 contributed to reaching milestone MS3 and is well-documented in deliverables D2.2 and D2.4.

*Table 7. Status of WP2 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D2.2 | The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version | FP | Demonstrator; PU; M18 | Accepted |
| D2.4 | Continuous data privacy legislation compliance monitoring and guidelines - interim version | CECL | Report, PU, M18 | Accepted |
| MS3 | Innovation Fire | INTRA | M18 | Achieved |

### 3.2.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D2.2 and D2.4 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

In Y3, the WP2 activities will be focused on the following aspects:

- T2.1 – GDPR CSA module
  - Based on Pilots' feedback, improve accessibility of questionnaires, proposed answers, and proposed improvement.
  - Implement additional functionalities as IMPROVE, DEMONSTRATE, and MONITOR compliance with GDPR.
  - Following recommendations made by experts during the interim review meeting, establish conformity assessment of GDPR CSA's assessment model with existing GDPR certification criteria and main data protection standards.
- T2.2 – Integrated Identification Management System
  - Examine further MyData Features that can be covered by the module.
- T2.3 – MITIGATE module
  - Update Cybersecurity Threat Intelligence library
  - Implement both graph visualization of cyber-asset and an executive summary of risk assessment.

- T2.4 – Management and integration of open-source technology offerings and solutions
    - Verify suitability and completeness of open-source technologies and training materials.
- T2.5 – GDPR and data protection regulations continuous monitoring and guidelines
    - Further monitoring of various sources for developments in the data protection landscape.

The envisioned work will be reported in D2.3 and D2.5 in M30.

## 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. Since the first demonstration of WP3 activities (MVP delivered in M12) SENTINEL core has been upgraded to its FFV, after a set of improvements and changes implemented to its comprised modules.

As a result, the key achievements of WP3 in terms of developed technologies, from M13-M24, include:

Open data security platforms as accessed and used by the Observatory: Besides, Malware Information Sharing Platform (MISP), module has been further developed to access and monitor CONCORDIA MISP for retrieving information related to detected and well-known security threats and vulnerabilities.

Recommendation Engine: This module has been implemented to provide recommendations to the users in the form of OTMs, trainings and tools. Within Y2, the recommendation process has been further improved considering enhanced list of trainings and taking into account accuracy and locality of users' assets.

In addition, Policy Drafting, enforcement and orchestration module has been further expanded to implement the Policy enforcement and orchestration module, enhance the policy drafting with more training material and available tools and include Cybersecurity risk assessment results.

Technical details of each module of the FFV are explained in D3.2 "The SENTINEL digital core: Full-featured version" delivered in M18.

### 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, investigated for external open security data sources and presented an outline of the most well-known and widely used to the rest of the consortium. Additionally, functionality of T3.1 and system requirements were identified and discussed with the consortium.

As a result of a series of WP3 meetings since the launch of T3.1, AEGIS alongside 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 and the first complete prototype. This instance consumes open, public sources and feeds to receive updated information on current threats and vulnerabilities. In coordination with T4.4, a decision has been made on the data storing technology that can be used for the Observatory Knowledge Base. By combining the two approaches, a base has been set up on which we were able to build SENTINEL's threat intelligence platform, which not only receives data from the community but also shares and gives back all relevant information. Additionally, it includes other open security data sources and platforms, in order to give the end-user a more concrete approach to assess their organization's security. Furthermore, the user is able to submit incidents identified in their own organization, through a form created for this exact purpose.

T3.1 has contributed to the following WP3 objective:

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

The above comprises significant input to D3.2 “The SENTINEL digital core: Full-featured version”, delivered in M18, contributing also to milestones 3 “Innovation Fire”, due in M18. Major contributions will also be provided in D3.3 “The SENTINEL digital Core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

### T3.2 The incident handling and sharing module

T3.2 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 the end-users to submit incidents as they occur during the operations of an SME/ME.
b) the Notification aggregator that continuously monitors an SME/ME's infrastructure, collects and reports on any event that may be a security breach, vulnerability, threat or attack.

In Y2, the incident handling service has been developed and deployed. The report was separated in two (2) use cases:

1. Receiving security notification which discusses the way the various SENTINEL plugins are sending notifications through the plugin adapter and the notification aggregator to the SENTINEL UI (i.e the user) and

2. Reporting security incidents, where the user is given the option to report security incidents observed internally to the organization to open security platforms in order to share knowledge with anybody interested.

T3.2 has contributed to the following WP3 objective:

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

The above comprises significant input to D3.2 “The SENTINEL digital core: Full-featured version” in M18 and milestone 3 “Innovation Fire”. Final contribution will also be provided in D3.3 “The SENTINEL digital core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

**T3.3 The intelligent recommendation engine**

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

Since M12, the list of OTMs has been expanded to include locality and ownership alongside the recommended tools and trainings. A technical amendment has been applied and submitted in November 2022, so the RE engine to operate on a rule-based approach providing extra scalability and extensibility. The main reasons behind that choice were i) the size and nature of the input dataset; the cybersecurity and data protection measures (OTMs) adopted by SENTINEL, based on ENISA and the ISO 27000 family of international standards, as well as their associated tools and trainings, are low in number, envisioned around the low three-figures; this is even after the additions until the end of the project, ii) with the selected criteria, a rule-based approach would further optimize the recommendation process compared to the ML/DL-based approach. The proposed amendment aims to boost the original proposal with outcomes both more feasible and measurable; the RE will be highly available (>99% requests satisfied), performant (<3 sec latency), functionally suitable and scalable.

T3.3 has contributed to the following WP3 objective:

(i) Deliver the SENTINEL Intelligent Recommendation Engine.

The above comprises significant input to D3.2 “The SENTINEL digital core; Full-featured version”, contributing also to Milestone 3 “Innovation Fire”. Further technical development will be continued and will be finally reported in D3.3 “The SENTINEL digital core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

**T3.4 Policy drafting, enforcement and orchestration module**

T3.4 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. The output policy draft is enriched with organization measures to be taken, specific enforceable and actionable security policies and policy data patterns that are provided by both the Policies repository and the Observatory of the SENTINEL architecture.

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

- Section 1: **Policy details**, which consists of the metadata of the SENTINEL policy (i.e. generation date and time of policy).
- Section 2: **Organization Info**, which includes the most important organization profile details (i.e. name, sector, size, etc.).
- Section 3: **Global Recommendations**, which reports the recommendations that concern the whole organization regardless of the information provided in each one of the Pas.
- Section 4: **PA specific Recommendations**, which reports the recommendations for each completed PA.

Section 3 and 4 consist of the following:

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

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

The latest version (full featured version) of the SENTINEL platform reports on 55 organization and 79 technical (134 total) measures, further analysing these recommendations while considering the following factors:

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

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

- Considers the calculated risk level of the organization and gathers all available measures that need to be recommended to the SME/ME.

- Filters the list of available measures based on the ownership of organization assets.
- Considers the locality of the organization assets recommending the proper policy text for each case.

Additionally, in Y2 effort was spent for the proper design and implementation of the Policy Enforcement module the purpose of which is to track the implementation status of the policy recommendations contained in the policy draft that is generated for the needs of an SME/ME. Specifically, the end-user of the SENTINEL platform may visualize and manage the implementation status of OTMs at the following sections:

- The organization profile, in which global OTMs may be properly set and configured.
- PA level, in which PA specific OTMs may be properly set and configured.
- Policy Recommendations level, in which the implementation status of all recommended OTMs (global and PA specific) is reported.

The implementation statuses the SENTINEL platform supports are as follows:

- “Not Implemented”, which corresponds to the status of an OTM that is both not recommended and not implemented.
- “Pending”, which is the status of a recommended OTM that is not yet implemented.
- “Implemented”, which is the status of an OTM that is implemented regardless of whether it is recommended or not.

All these are realized in the FFV of the SENTINEL platform which was released in M18. From M18 FP is in close collaboration with all technical partners leads the process for finalizing:

- the OTM classification by enriching the current list with privacy aware measures and controls.
- the criteria upon which one or more OTMs may be recommended or not from the SENTINEL policy drafting module.

T3.4 has contributed to the following WP3 objective:

(i) Deliver the SENTINEL Policy Drafting and Enforcement modules.

The above comprises significant input to D3.2 “The SENTINEL digital core: Full-featured version”, delivered in M18, contributing also to milestone 3 “Innovation Fire” due in M18 respectively. Final technical development will be reported in D3.3 “The SENTINEL digital core: Final product”, contributing to milestone 5 “Demonstration Fire”, due in M30.

### 3.3.3 Work carried out in WP3 per partner

| | |
|---|---|
| ITML | As WP3 leader, ITML continued coordinating the discussions for the selection of external open data security platforms and participated in testing the suggested sources. 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. |

| | |
|---|---|
| | Considering the close relationship between T3.3 and T3.4, in Y2, ITML has continued its active participation in the design and deployment of the Policy Drafting module and its dependency to the Recommendation Engine, as well as interfacing of those components within the context of the FFV (M18). Finally, ITML has also led the delivery of D3.2, contributing key content for all sections. |
| IDIR | In Y2, IDIR has kept contributing work to both T3.3 and T3.4, extending and refining Y1 achievements. In T3.3 (Y2) work has been about rethinking the RE design and redesigning it towards a rule-based approach, primarily by recording a number of rules which should be observed for selecting OTMs, open-source software and training material. In T3.4 (Y2) work has focused on further refining the mapping between OTMs and policy templates. This mapping, for which FP has led the work, has been recorded as SENTINEL's global classification sheet, which, in the technical architecture, resides in the Common Repository. IDIR has (a) helped enrich this classification with OTMs, additional metadata (columns), selection rules and other data towards the final release of the platform (M30). |
| 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, by drafting corresponding high-level and system use cases accompanied by corresponding UML sequence diagrams. 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 as well as the design of declarative rules and their capabilities for explainable 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 and implemented. |
| STS | STS has actively participated and contributed to all WP3 discussions. Best practices were investigated and contributions were made in determining the process to identify the risk levels based on the processing activities captured during the initial assessment of the SME/ME. 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. The MVP version of the DPIA toolkit was questionnaire based and was designed, implemented and delivered during Y1.<br>In Y2, STS has continued its contribution to WP3. In particular, the FFV of DPIA toolkit was delivered, which was better integrated to the SENTINEL platform through the orchestration module. Additionally, STS has contributed to D3.2 |
| 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.<br>During Y2, AEGIS continued to work on the implementation of MISP on the SENTINEL platform and its integration with the Observatory Knowledge Base, by |

| | |
|---|---|
| | updating the external open security data sources and developing a form so the user can contribute relevant information back to the community. This form will be redesigned and updated for the final version of the platform. |
| CECL | The CECL has continued to participate in all WP3 related meetings and discussions taken place in the second project year, especially the ones focusing on T3.4 concerning the policy drafting module. |
| FP | During Y2, FP participated in all scheduled meetings and calls related to WP3 as well as to meetings and activities related to the proper design and implementation of the SENTINEL platform and its components. FP contributed to the design of the Data Fusion Bus which is required to allow a trustworthy way of transferring data between the SENTINEL internal and external components. FP also participated in the 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 is 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/ME 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 are recorded and mapped either to the organization profile of the SME/ME and the processing activities and are used at the building process of the human readable policy. Based on these, FP implemented the MVP and the full feature 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, considering the risk level of the organization, the ownership of the assets, and their locality (on-premise, cloud, hybrid).<br>Last but not least, in Y2, FP also led the proper design and implementation of the Policy Enforcement module, the purpose of which is to track the implementation status of the recommended OTMs contained in the policy draft. For this, three different statuses were defined (“Not implemented”, “Pending”, and “Implemented”) that can be applied for both global and PA specific OTMs.<br>From the successful release of the FFV of the SENTINEL platform, FP in close collaboration with all technical partners and privacy experts works on the proper finalization of the OTM classification and the selection criteria of the last mentioned when generating the SENTINEL policy recommendations. |

### 3.3.4 Status of Deliverables and Milestones

The work conducted in WP3 in Y2 contributed to reaching milestone MS3 and is well-documented in deliverable D3.2.

*Table 8. Status of WP3 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| D3.2 | The SENTINEL digital core: Full-featured version | ITML | Demonstrator; PU; M18 | Accepted |
| MS3 | Innovation Fire | INTRA | M18 | Achieved |

### 3.3.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D3.2 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 FFV, the WP3 activities will continue towards the enhancement of the technologies developed as part of the SENTINEL digital core. To that end, WP3 will

- Further enrich MISP feeds/platforms. (T3.1)
- Explore more plugins that offer notifications. (T3.2)
- Improve recommendation process by implementing a rule-based approach. A set of rules will be investigated for producing more targeted recommendations for the user. (T3.3)
- Enhance the current list of OTMs to achieve GDPR compliance. (T3.4)
- Enhance policy drafting and policy enforcement and orchestration modules considering the updates in OTMs, trainings and software. (T3.4)
- Optimise policy enforcement and orchestration modules. (T3.4)

The envisioned work will be reported in D3.3 in M30.

## 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.

In Y2, the key achievements of WP4 include:

- The design and implementation of SENTINEL's FFV of self-assessment services.
- The establishment of a stable shared data model for the SME Profile Service focusing on both PDP aspects (PAs and ROPA) and organization aspects. This data model is common among core SENTINEL modules as well as plugins.
- Simulations and training for SMEs/MEs, integration of ACS's CyberRange platform and new gaming interface in the SENTINEL environment.

- Technical effort towards the development of the expanded SENTINEL Observatory and knowledge base, including external data sources, data formats, storage technologies and user-facing collaborative tools.

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

The SENTINEL services' functional details and their implementation details are updated in D4.2 "The SENTINEL services: Full-featured version" delivered in M18, contributing to milestone 3 "Innovation Fire" due in M18. Final contribution will also be reported in D4.3 "The SENTINEL services: Final product", contributing to milestone 5 "Demonstration Fire", due in M30.

### 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 has been made. A meeting with SMEs to present the CyberRange and involve them in the development process has also taken place. Technical aspects regarding development and implementation of simulation scenarios have been discussed among all involved partners. Furthermore, discussions on how to integrate the CyberRange testbed within SENTINEL have been initiated. Multiple possibilities have been discussed aiming to offer the best user experience for the SMEs. As a result, to comply with the SENTINEL project scope, a solution-based on OpenID Connect was selected as a rational option with the authentication process from the SENTINEL user to the CyberRange platform. On the CyberRange, generic infrastructure of SME has been created, in order to replicate the way most SMEs operate nowadays. Scenarios have been created with Cyber-attack to exploit vulnerabilities, and misconfiguration.

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

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

T4.1 has contributed to the following WP4 objective:

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

All the above-mentioned activities are going to be described in D4.3 "The SENTINEL services: Final product", contributing to milestone 5 "Demonstration Fire", due in M30.

**T4.2 Data protection impact assessment and assurance**

T4.2 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 is provided on the processing activities. A series of specific questions are asked and organizational and technical measures (OTMs) are mapped. Based on the answers provided the processing activity is marked as potentially high risk and the relevant SA tool is triggered.

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

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

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

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

Throughout the period between M7-M24 STS has been chairing a series of weekly MVP/FFV Technical Meetings which all the technical partners were attending and were reporting on the progress of their activities. For the smooth delivery and planning of the MVP, FFV and the final version of SENTINEL, an agile-based approach is being followed. Overall, this approach has been proven to be very helpful as it is very clear which partners are working on what tasks and their dependencies. Their progress is easy to track, sharing comments, files and having a history on every task (GitHub issue). A Slack channel was utilized in parallel for a more immediate communication among technical partners.

T4.2 has contributed to the following WP4 objective:

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

In Y2, a more detailed description and further implementation of the DPIA plugin has been presented in D4.2 “The SENTINEL Services: Full-featured version” which was delivered in M18.

In Y3, STS will reintroduce a questionnaire to the final version of the DPIA toolkit to perform the assessment of a Processing Activity. However, it will still consider the implementation status of the OTMS while processing the “core” data of the SME profile.

### T4.3 Self-assessment and RASE scoring engine

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

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

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

Major T4.3 achievements leading up to M24 have been:

- The design and unification of a stable shared data model for the SME profile, focusing on both PDP aspects (PAs and ROPA) and organization aspects (such as the asset inventory). This data model is common among core SENTINEL 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.
- Detailed UI mockups to showcase the intended functionality, as well as the look and feel, of MySENTINEL, including a UI/UX-optimized dashboard.
- 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, deployment and refinement (M13-M24) of two key technical components of the SENTINEL architecture:
  - The Profile Service
  - The Self-Assessment (SA) Service

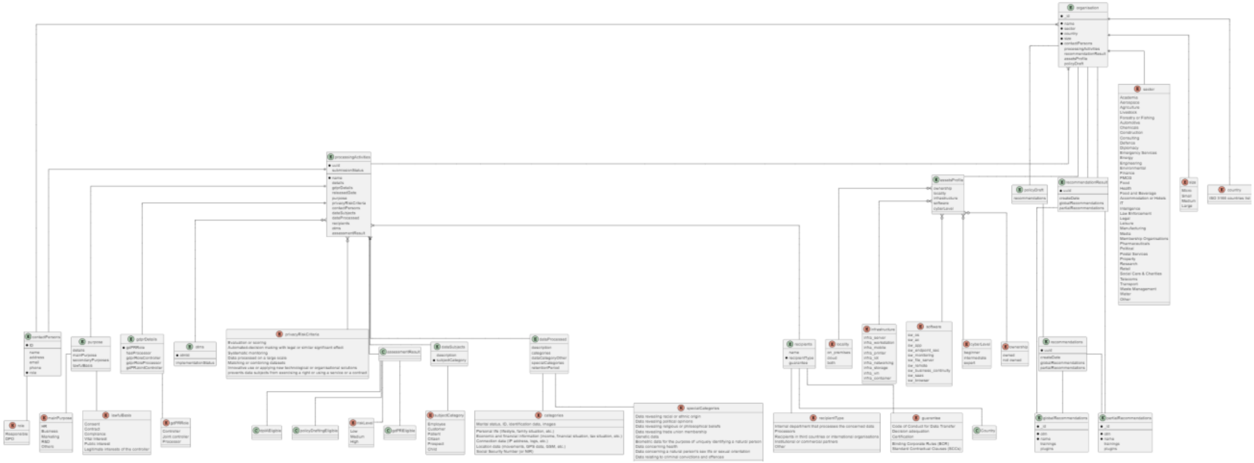


*Figure 2. Updated common SENTINEL Organization Profile data model*

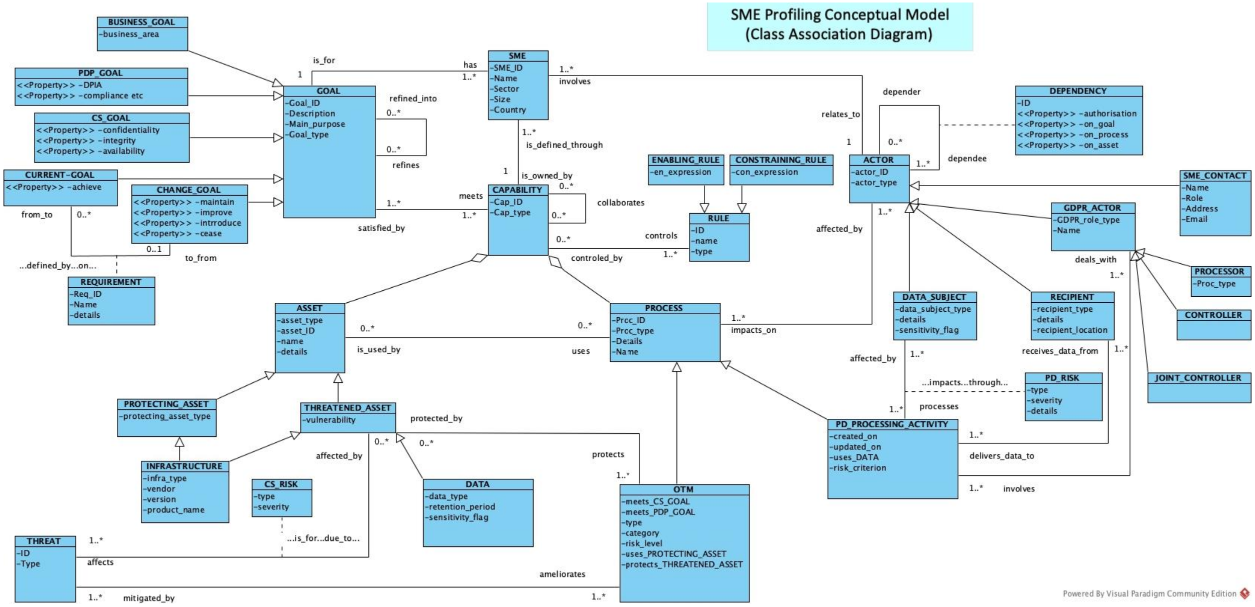


*Figure 3. The conceptual metamodel for SME profiling*

T4.3 has contributed to the following WP4 objective:

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

Overall, T4.3 work has provided key input to deliverables D4.2 “The SENTINEL services: Full-featured version”, delivered in M18, and D4.3 “The SENTINEL services: Final version” due in M30 is (in-progress). It has also contributed to Milestone 3 “Innovation Fire”, delivered in M18.

### T4.4 The SENTINEL Observatory

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

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

T4.4 has contributed to the following WP4 objective:

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

An intermediate version of the Observatory was included in D4.2 “The SENTINEL Services: Full-featured version”, delivered in M18, contributing also to milestone 3 “Innovation Fire”, due in M18.

Further development of this context will be presented in D4.3 “The SENTINEL services: Final product” due in M30.

### 3.4.3 Work carried out in WP4 per partner

| | |
|---|---|
| ITML | In Y2, as T4.4 leader, ITML has initiated and coordinated the discussions for the implementation of the Observatory as part of FFV of the platform, including selection of external data sources, data formats/structure, storage technologies, collaborative tools and UI issues. The implementation and demonstration of the Observatory has been successfully executed while the achieved results have been thoroughly reported in deliverable D4.2. |
| LIST | In Y2, LIST has continued to contribute to T4.2. Based on a previous list of requirements that are common to both DPIA and GDPR CSA, LIST was involved in discussion related to the extension of SENTINEL’s Organisational and Technical Measures (OTMs) taxonomy. LIST proposed to add specific OTMs allowing to meet GDPR requirements not covered by initial OTMs taxonomy. Such extension should ease information sharing between SENTINEL’s plugins, and then, reduce time spent by SMEs to provide expected information. |
| IDIR | In Y2, IDIR, as T4.3 leader, has contributed technical work towards maturing SENTINEL’s Profiling and Self-Assessment modules, along with the leaders of T4.2 and T2.1 which are the key participants. Key contributions towards this end have been (a) participating in key meetings and decisions towards the technical direction of the respective tasks (b) defining and refining a shared data model for the SME profile and the GDPR-compliant ROPA, which is common among core SENTINEL context and modules as well as plugins; (c) proposing a feasible SME profiling and initial assessment process requirements; (d) collaborating towards establishing the appropriate user flow and sequencing among context modules; (e) clarifying organizational and technical measures (OTMs) structure and role and (f) defining the data exchange (inputs and outputs) between the participating self-assessment plugins, namely the GDPR Compliance Self-Assessment (T2.1) and the Data Protection Impact Self-Assessment (T4.2), as well as between SENTINEL’s SA context and the Core context. In M13-M18, technical work and refinements were provided by IDIR to T4.3, related to (a) the full implementation of the ROPA (Profile Service), (b) the implementation of the detailed cyber asset inventory as a prerequisite for the cybersecurity risk assessment (CSRA) (Profile Service), (c) the update of the algorithm which assigns a preliminary risk level to PAs by examining specific risk criteria (Self-Assessment Service), and (d) the unification of the SME profile with the GRPDCSA and DPIA inputs (Profile Service), all towards the full-featured version of the platform. In M19-M24 the work has focused on rethinking the overall user experience in SENTINEL. Key examples of how this would affect the Profile Service and the SA Engine include: (i) the PA templating feature, (ii) tracking the SME Profile completion progress, (iii) saving additional SA tools results (CSRA), (iv) reflecting updates to the domain model in the Profile Service and (v) reflecting changes in how risk is calculated in the SA Engine. |
| INTRA | Within Y2, INTRA actively participated in all Observatory-focused discussions as part of Task 4.4 and contributed to the formulation of the Observatory use case, covering both the threat intelligence and MISP integrations as well as the integration of training material and its presentation for the non-technical users. To that end, INTRA also proposed architectural patterns and information flows to help form the Observatory structure and its interfaces. |

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

| | |
|---|---|
| FP | In Y2, FP participated in all scheduled meetings and calls related to WP4 and led many of the processes required to be implemented in all main components of the SENTINEL platform. Specifically, FP actively participated in the implementation of the SME profiling process, which consists of the data required for performing the initial assessment, the data processing activities, and the proper definition of the organization assets in which the MITIGATE system participates through the mitigate-adapter. At this core process a number of organizational and technical measures are required also since based on these the policy-drafting module builds the human readable policy for the SME. Therefore, much effort was spent on the introduction of the SENTINEL OTM classification with their selection criteria when generating the SENTINEL policy recommendations. For each OTM a list of optional capabilities is mapped, upon which all plugins and training material are also mapped. This mapping allows the Recommendation Engine to generate the proper recommendations for each SME/ME, mainly based on the risk level of the organization.<br>Furthermore, the tasks of this WP contribute to the proper utilization of the SENTINEL plugins (tasks T2.3 and T2.4 in which FP leads and participates correspondingly) since many of these require the list of processing activities and the list of the organizational assets. |

### 3.4.4 Status of Deliverables and Milestones

The work conducted in WP4 contributed to reaching milestone MS3 and is well-documented in deliverable D4.2.

*Table 9. Status of WP4 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D4.2 | The SENTINEL services: Full-featured version | STS | Demonstrator; PU; M18 | Accepted |
| MS3 | Innovation Fire | INTRA | M18 | Achieved |

### 3.4.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D4.2 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 final version of the SENTINEL services in M30. 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 and gaming interface of CyberRange tool based on additional requirements received from end-users as a result of first testing trials.

- Enhance the SENTINEL Observatory and knowledge base, including additional external data sources and data formats. Moreover, redesign the Observatory in alignment with RE so the user can browse through in a more targeted manner.

The envisioned work will be reported in D4.3 in M30.

## 3.5 WP5 – SENTINEL continuous integration and system validation

**Leader: INTRA**

**Involved Partners: INTRA, ITML, LIST, IDIR, STS, 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. Both tasks have made significant progress and are fully on-track.

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 representatives 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, four out of the seven use cases described in D1.2 were selected for implementation in the MVP, while the remaining seven were also implemented and integrated into the platform in the FFV release in M18.

**(iii)** Moreover, 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 into the docker compose environment. Finally, integration tests were conducted in a bilateral manner, which were subsequently followed by end-to-end tests.

Development towards both versions was done in an iterative and agile manner. Starting from the beginning of M10, and M14 respectively, series of meetings were carried out where partners were asked to estimate all the individual pieces of work that needed to be realised from their end to finalise 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 deadline of each respective release as a backup. Sprints were monitored on a weekly basis in dedicated meetings that combined review and planning activities. Moreover, shorter and more concise low-level meetings (similar to daily Scrum) were carried out three times per week (Monday, Wednesday and Friday).

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 MySENTINEL UI, which accommodated all functionalities envisaged for both the MVP and, subsequently, the FFV.

The results are reported in D5.1 and D5.4, which both contribute to milestone 2 ('Innovation Flame', due M12) and D5.2 and D5.5, which contribute to milestone 3 ('Innovation Fire', due M18).

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

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

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

Moving forward, work will continue to be comprehensive to refine and enrich the content of the UI by constantly engaging and closely collaborating with the project's end-users with diverse backgrounds (under WP6). We will make sure to continue incorporating their feedback and implement a UI that offers high levels of usefulness and usability. Additionally, we will make any adaptations required in the communication of the UI with all modules as they progress. All this effort will result in the final version of the MySENTINEL UI dashboard and will be documented in the subsequent iteration of D5.1 and D5.2, namely D5.3.

T5.1 has contributed to the following WP5 objective:

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

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

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

T5.2 is led by INTRA and started in M9. Within this task, a GitHub organization (https://github.com/SENTINEL-EU/) and multiple subsequent repositories (22 at the time of writing this report) 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 and the FFV releases of M12 and M18 respectively. In terms of deployment, all modules are being delivered in a dockerised manner and automatically deployed on INTRA's infrastructure using docker-compose on two deployment environments to cater for development and staging purposes. A docker registry server (JFrog artifactory) has also been deployed to facilitate delivery, storage and deployment of docker images. Corresponding Jenkins pipelines have also been created in order to automate the release process.

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 towards the final release. After the release of M18, a retrospective session was performed where feedback on the development process was provided by software engineers and managers. This resulted in the collection of technical debt and pending issues that needed to be tackled as well as various organizational aspects of the integration process such as the frequency and focus of recurring meetings. Moreover, the feedback of the reviewers as well as the technical partners of the consortium has been incorporated into the backlog of the product, and the work has been broken down in sprints as with previous releases.

T5.2 has contributed to the following WP5 objectives:

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

(ii) Continuously optimizing the SENTINEL platform through an iterative process (testing-improvement-testing).

(iii) Supporting the project's sustainability by putting into place automations and monitoring mechanisms.

The above comprises significant input to D5.5 "The SENTINEL integrated solution – interim version", delivered in M18 contributing also to milestone 3 "Innovation Fire" of the project. Currently T5.2 is focusing on the final release of the integrated SENTINEL platform which is to be reported in M30 in D5.6 "The SENTINEL integrated solution – final version" and achieve the respective milestone 5 "Demonstration Fire".

**T5.3 From the prototype to the final solution**

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

### 3.5.3 Work carried out in WP5 per partner

| | |
|---|---|
| ITML | ITML provided support on integration of SENTINEL's components and the operation of the integrated framework contributing with ideas and experience on continuous integration processes, testing methods, quality assurance tools and infrastructure sizing. Additionally, ITML participated in the configuration and use of the Github project for issue tracking. Finally, ITML has contributed to the D5.2 and D5.5 deliverables. |
| LIST | In the reference period, the contribution of LIST to WP5 consisted in ensuring integration of GDPR CSA Full Featured Version with the SENTINEL's platform. Comparing with the MVP version, this new release encompassed data collected through questionnaire fulfilled by SMEs. An illustration of integration of GDPR CSA with SENTINEL's platform is available in the description of subtask T2.1.3 (see Figure 1). In the coming year, efforts will be focused on UI aspects of GDPR CSA integration with the SENTINEL's platform which include both interfaces and workflow. |
| IDIR | IDIR has been contributing work in T5.2 towards preparing and executing SENTINEL's technical integration, together with other technical project partners, in the timeframe of the deployment of the full-featured version (M13-M18) and beyond (M19-M24) towards final SENTINEL platform. IDIR has also been contributing tools, technologies, and methodologies for integration and for addressing system architecture, deployment, DevOps, interoperability, scalability, performance, and security. |
| INTRA | INTRA has organized and actively participated in all related calls and discussions. INTRA has set up and configured all the required infrastructure, tools and processes to facilitate modules' continuous integration and delivery. Moreover, INTRA participated in the engineering of business requirements, the definition of user journeys and the design of the User Interfaces. INTRA has coordinated the preparation of and provided key content to deliverables D5.4 and D5.5 as well as conducted the internal review of D5.2. |
| STS | STS has been actively involved in the WP5 discussions and integration activities related to its DPIA component and has made significant contributions towards enhancing the integration solution and patterns. |
| 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 MVP stage, the MySENTINEL dashboard included links to components that were 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. At the current stage, the MySENTINEL dashboard includes links to components and modules that are incorporated in the first complete prototype, as well as the relevant pages. This means that apart from the MySENTINEL dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts are also included in the second version of the platform. Additionally, several elements of the MySENTINEL UI in several different pages have been updated and a number of bugs/glitches identified by the technical team and/or the end-users have been fixed. Furthermore, the UI has been integrated fully with the backend modules. Moreover, the Cyber Range Gaming Interface, offered by ACS, has been integrated into the platform. AEGIS has also participated in discussions related to the SENTINEL integration activities. Finally, AEGIS has led D5.2 and delivered content for all sections of it, while it served as a reviewer and contributor for D5.5. |
| 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. TSI participated in every technical and functional telco. In addition, TSI shared the lists with the external plugins (open-source tools and trainings) to be integrated with the SENTINEL platform and the appropriate modules. The integration also includes the definition of relevant models (for tools and training elements) that are processed by the recommendation modules of the SENTINEL platform. The external plugins were also mapped with the corresponding OTMs of SENTINEL. TSI contributed to deliverable D5.5.<br>For Y3, TSI is planning to further enhance the content of the two lists based on feedback from the application of SENTINEL to the piloting environments regarding the appropriateness of the suggested tools and training. Towards this goal, the models and metadata of the two lists will be updated in an attempt to assist the Recommendation Engine and its decision making to derive more targeted recommendations for the end user. |
| 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. ACS has also contributed to D5.5 |
| UNINOVA | No work regarding WP5 has been carried in Y2, thus reporting is not relevant at this stage. |
| 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 the SENTINEL services and tools. After the MVP release, CG executed MVP demo from the real tester in order to get used with the UI. It completed beta trials and made more than 20 suggestions for the improvement of the SENTINEL platform via a given questionnaire. CG users collaborate with technical partners for the improvement and refinement of the SENTINEL platform to address their needs in an iterative process. Furthermore, the CG pilot users have actively participated in the SENTINEL FFV Demonstration workshop, successfully executed 2 experiments, and filled out a |

| | |
|---|---|
| | questionnaire by providing new suggestions regarding the FFV of the SENTINEL platform. |
| TIG | In Y2, TIG has actively participated in all WP5 related calls and discussions. In addition, TIG has engaged and continued to participate in testing and reviewing the SENTINEL platform to:<br>• Assess usability, checking the use of language and structure for SME users who may have limited knowledge and understanding of GDPR, particularly regarding compliance requirements.<br>• Test with dummy information to generate reports.<br>• Identify any areas for development in terms of user experience. This is facilitated with the launch of the TIG pilot (Dimensions Care (DC)) in M24, in which a lead DC colleague with limited knowledge of GDPR/cyber security will access and use the SENTINEL platform. This will provide a "real-world" user scenario, thereby allowing for assessment and evaluation of accessibility and usability.<br>• TIG is presently consulting with other SMEs within the group to provide further piloting opportunities. |
| 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 mainly focused (i) on the visualization of the SENTINEL policy, (ii) the monitoring of the OTMs implementation status, and (iii) the visualization of the results of the cybersecurity risk assessment.<br>For the continuous integration towards the realization of a complete system (T5.2) FP focused on the proper integration of the MITIGATE plugin, enabling the SENTINEL platform to build upon its functionalities, allowing SME/MEs on one hand to build simulation computer security risk assessment scenarios for preferred cyber-assets, and on the other to perform cybersecurity risk assessments on one or more processing activities. In this context, the first version of the mitigate-adapter was successfully deployed, offering all required integration services from the MITIGATE system and providing corresponding REST APIs to the SENTINEL internal components. In parallel and based on the activities performed within T2.3, the final version of the mitigate-adapter is properly under design. This final version will significantly enrich the already integrated services from MITIGATE system, enabling the SME/MEs not only to better understand the nature of the cyber-assets' risks profile but also to find recommendations on how they can take specific actions for mitigating them.<br>Additionally, a full featured version of the policy-drafting module and the policy enforcement component were also implemented and deployed in the SENTINEL system. Since M18 FP leads the proper design and implementation effort for realizing the final version of these components. |

### 3.5.4 Status of Deliverables and Milestones

The work conducted in WP5 in Y2 contributed to reaching milestone MS3 and is well-documented in deliverables D5.2 and D5.5.

*Table 10. Status of WP5 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D5.2 | The SENTINEL visualisation and UI component – second version | AEGIS | Demonstrator; PU; M18 | Accepted |
| D5.5 | The SENTINEL integrated solution - interim version | INTRA | Demonstrator; PU; M18 | Accepted |
| MS3 | Innovation Fire | INTRA | M18 | Achieved |

### 3.5.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D5.2 and D5.5 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 Y3, WP5 will aim at meeting SENTINEL's milestone 5, i.e., the final version of the integrated platform in M30. In this respect, WP5 will:

- Continue UI development with planned user flows beyond the FFV, by incorporating fixes and adjustments received as feedback from the pilot users as well as features that improve the user experience.
- Facilitate the smooth and effective integration of the components by continuing the successful agile approach with iterations and development sprints used in the project.
- Closely monitor WP6 activities to collect and further incorporate feedback and requirements and gradually incorporate it into the platform until its final release in M30.

These activities will be captured in corresponding deliverables, i.e., D5.3 and D5.6 in M30.

## 3.6 WP6 – Real-life experimental evaluations: SENTINEL pilots

**Leader: FP**

**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 and will take effect until the end of the project (M36). Based on the guidelines and parameters formulated in D1.3, the main objectives of WP6 are the following:

- Ensure the finalization of the experimentation protocol based on end-users' requirements.
- Realize real-life demonstrators based on both consortium members and on external entities engaged via DIHs.

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

WP6 activities kicked-off with 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.

Key achievements of WP6 during the M12-M24 period include:

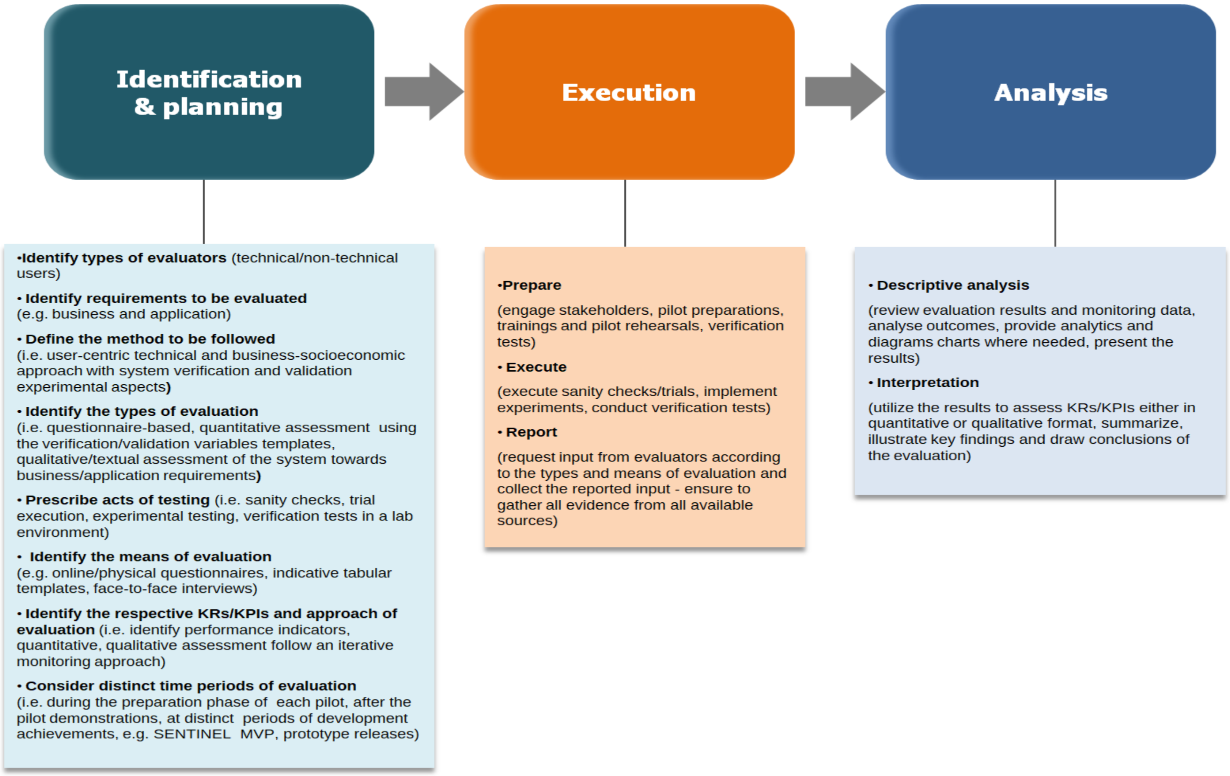
**(i)** the refinement of the SENTINEL experimental protocol, identified in T1.3 of WP1, wherever needed to be aligned with the SENTINEL development progress and meet the pilot requirements and expectations. To this aim, the pilot cases content along with the pilots' experiment were revised and enhanced in the field of genomics and social care characteristics and the DIHs external evaluators testing towards the SENTINEL general functionalities. In addition, the validation and verification variables, which will be utilized during the SENTINEL evaluation process, were reviewed and updated with the contribution of pilot partners and technical partners respectively following quality standards and models. Their mapping with Key Results (KRs) was reviewed and updated accordingly to be in line with the project's technical activities and development plan.

**(ii)** the construction of SENTINEL pilot action plan distinguished into two pre-pilot phases from M10 to M18 (including the Initial Demonstration) and three pilot phases from M19 to M30, prescribing the pilot preparations and activities.

**(iii)** the development of the training process that is utilized to raise the end-users awareness on the SENTINEL platform and facilitates them to get properly prepared for the trial executions and pilot demonstrations. For this purpose, a Training Needs Analysis (TNA) method was adopted to elicit the training requirements and tailor the entire training process. Moreover, a training action plan was set to organise the training process and the type of training material and the technical equipment utilized to support the training procedures was identified.

**(iv)** the development of the SENTINEL User-centric Evaluation Methodology aiming to complement the SENTINEL experimentation protocol to define and prescribe the exact evaluation process that is followed by the project to assess the SENTINEL system throughout its lifecycle development, generate evidence and produce results. The SENTINEL User-centric Evaluation Methodology consists of three (3) main phases; identification and planning, execution and analysis. It encompasses a set of parameters, such as non-technical and technical evaluation considering the SENTINEL platform assessment from business, socio-economic, legal, security, privacy, technical and technological, UI/UX and visualization perspectives, identifying the type of evaluators in each case, examine whether the SENTINEL platform meets specific business and application requirements of SMEs/MEs, identified in T1.1 and T1.2 of WP1, defining the types of calculation (e.g. quantitative, qualitative approach), the acts of testing (e.g. execution of trials, experiments, etc.), the means of evaluation (e.g. questionnaire-based, tabular or textual forms, etc.) and the respective evaluation KRs/KPIs considering distinct time periods of evaluation. Furthermore, it prescribes the preparation procedures (e.g. SMEs/MEs engagement and education) and the execution of the SENTINEL platform evaluation, illustrating how it may be reported and analysed and providing a set of evaluation templates.

The following figure reflects the SENTINEL User-centric Evaluation Methodology:



•**Identify types of evaluators** (technical/non-technical users)

• **Identify requirements to be evaluated** (e.g. business and application)

• **Define the method to be followed** (i.e. user-centric technical and business-socioeconomic approach with system verification and validation experimental aspects**)**

• **Identify the types of evaluation** (i.e. questionnaire-based, quantitative assessment using the verification/validation variables templates, qualitative/textual assessment of the system towards business/application requirements**)**

• **Prescribe acts of testing** (i.e. sanity checks, trial execution, experimental testing, verification tests in a lab environment)

• **Identify the means of evaluation** (e.g. online/physical questionnaires, indicative tabular templates, face-to-face interviews)

• **Identify the respective KRs/KPIs and approach of evaluation** (i.e. identify performance indicators, quantitative, qualitative assessment follow an iterative monitoring approach)

• **Consider distinct time periods of evaluation** (i.e. during the preparation phase of each pilot, after the pilot demonstrations, at distinct periods of development achievements, e.g. SENTINEL MVP, prototype releases)

•**Prepare**

(engage stakeholders, pilot preparations, trainings and pilot rehearsals, verification tests)

• **Execute**

(execute sanity checks/trials, implement experiments, conduct verification tests)

• **Report**

(request input from evaluators according to the types and means of evaluation and collect the reported input - ensure to gather all evidence from all available sources)

• **Descriptive analysis**

(review evaluation results and monitoring data, analyse outcomes, provide analytics and diagrams charts where needed, present the results)

• **Interpretation**

(utilize the results to assess KRs/KPIs either in quantitative or qualitative format, summarize, illustrate key findings and draw conclusions of the evaluation)

*Figure 4. the SENTINEL User-centric Evaluation Methodology*

**(v)** the definition of a set of Key Results (KRs) and Key Performance Indicators (KPIs) at technical and business level as part of the evaluation process and the identification of the SENTINEL KRs/KPIs monitoring approach along with the provision of KRs evaluation template.

**(vi)** the trials execution to test the MVP version of the SENTINEL platform and report the results following a specific timeplan which was carried out after the MVP release in M12 and terminated in M18. The Initial Demonstration workshop was conducted in M16 with a total duration of 1.5 hours and the participation of six (6) stakeholders, including the SENTINEL pilot partners CG and TIG and four (4) external SMEs engaged by DIHs. The workshop aimed at educating end-users on the SENTINEL MVP to be able to try and test it. The MVP was tested under 4 use cases which reflected the MVP experiment's objectives and the results of the initial demonstration were recorded via textual feedback and filled questionnaires developed for the MVP evaluation. In addition, corresponding guidance was prepared.

**(vii)** Since M19, the main SENTINEL pilot phase is running which will be accomplished by M30. Within M22-M24, the first stage of CG pilot experiments was carried out. Specifically, in M22 a focused workshop was conducted by the consortium to demonstrate the functionalities of the SENTINEL FFV to the CG pilot partner and educate CG end-users on GDPR compliance and privacy-wised contents to guide them how to perform the trials execution to test the SENTINEL

FFV. The CG Demo Workshop of the SENTINEL FFV was recorded to be re-used as training material by the CG end-users prior to the trials. The SENTINEL FFV functionalities were tested via the execution of 2 trials performed by 2 CG end-users under the scope of CG pilot experiments addressing different PAs of personal data (i.e., user/client data and genomic data) utilized in the normal operations of CG company which resides in healthcare sector. The pilot experiments contained subsequent steps to realize a set of SENTINEL use cases that reflected FFV functionalities. The 2 CG end-users provided feedback from their pilot testing experience by filling in an online User Evaluation Questionnaire and providing detailed comments in a tabular format of an excel-based evaluation form. Corresponding guidance and evaluation material was prepared under the works of T6.4 to address the needs of CG pilot assessment.

**(viii)** During M23, the TIG pilot preparatory works commenced. Within M24, the TIG Workshop was realized to demonstrate the functionalities of the SENTINEL FFV to the end-users engaged for the TIG pilot. The Demonstration Workshop was focused on training the TIG end-users on the SENTINEL FFV, including a session dedicated to the Cyber Range capabilities of the SENTINEL cybersecurity component. The TIG Demo Workshop of SENTINEL FFV was recorded to enable its re-use as training material by the TIG end-users before performing the trials. The TIG trial execution and evaluation process is currently in progress and it is expected to be accomplished within M25. Respective instructions for the TIG pilot experiment workflow together with an online questionnaire template and evaluation forms are currently prepared. The TIG pilot experiment aims to address different PAs of personal data related to social care (i.e. information related to vulnerable children). After testing the SENTINEL FFV, TIG end-users will be requested to provide feedback from their pilot assessment experience of FFV. Updates on the corresponding guidance and evaluation material carried out in M24 as part of T6.4 works.

**(ix)** Within M19-M24, initial SENTINEL personas were identified from the end-users responses provided so far by adopting a mixed (both quantitative and qualitative) persona-based methodology. The persona-wised profiling of end-users aims to leverage the SME user-centric perspective towards the SENTINEL technical work enhancements.

To coordinate and implement all the above achievements, a series of monthly meetings were organised between WP6 partners from M10 until M18. Specifically, for the experimental protocol refinement, the initial demonstration preparation and the D6.1 reporting, as part of T6.1, T6.2 and T6.3 activities performed between M16 and M18, few additional meetings were organized. Since M19, WP6 digital meetings are conducted constantly on a biweekly basis to better handle the pilots' cooperative works. These WP6 telcos include discussions related to WP6 running tasks activities, i.e., T6.2 - T6.3 (M13-M18) and T6.4 (M22-M24) pertaining to the respective period of time.

All WP6 achievements carried out from M10 to M18 along with the developed questionnaire template and evaluation form utilized to gather end-users feedback from the Initial Demonstration (MVP assessment) were extensively reported and analysed in D6.1 "SENTINEL Demonstration - initial execution and evaluation" which was successfully delivered in M18.

The above also comprises significant input to milestone 3 (MS3) "Innovation Fire" ended in M18.

All achievements fulfilled from M19 to M24 contributed to the accomplishment of milestone 4 (MS4) "Demonstration Flame" which fired a first execution round of pilots and SENTINEL evaluation of FFV.

WP6 plans for Y3 (M24-M36) will be the preparation and complete execution of all three pilots (CG pilot, TIG pilot and DIH pilot) and the implementation of the pilot experiments at all stages, end-users evaluation from the trials execution, the development and update of respective questionnaires and evaluation forms according to the pilot assessment needs, the recruitment of more external companies (e.g. through DIHs), the evaluation report and analysis of the generated evidence both from internal and external evaluators using the SENTINEL evaluation templates, the calculation of verification/validation variables and the SENTINEL quality performance testing against the identified application and business requirements (cf, D6.1; annex evaluation templates), the measurement of “evaluation KRs/KPIs” to assess the project’s success as indicated in the SENTINEL User-centric Evaluation Methodology (cf. D6.1).

### 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 started in M10 and completed in M18. To drive the task activities, a series of discussions about the main aim of the task (considering also input from previous tasks) were carried out during the dedicated session of WP6 monthly meetings. 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 and 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 current reporting period, FP led the continuous process of the experimental protocol refinement, identified in T1.3. Within this framework, pilot partners in collaboration with FP and ITML revised and enhanced the SENTINEL validation templates for each pilot case according to pilot users expectations following prominent quality models and standards (e.g. ISO/IEC 25010, etc.). The revised validation templates aimed at addressing the specified SMEs requirements under real SME environments towards business-specific indicators and user characteristics that will be utilized during the SENTINEL platform non-technical evaluation. In addition, FP in collaboration with technical partners reviewed and updated the SENTINEL verification templates per SENTINEL component and plugin to be in line with the project’s technical developments and provide efficient testing indicators related to the quality of the platform and services’ performance over specified application requirements/characteristics utilizing a set of benchmark standards and other approaches (e.g. ISO/IEC 27001, Google analytics). The revised verification templates will be utilized for the SENTINEL technical evaluation. The mapping of verification and validation variables with the respective KRs, identified in T1.3, was updated as well, according to T6.1 refinements and enhancements.  In addition, specific KRs were identified together with corresponding validation and verification variables to address the Initial Demonstration evaluation of the MVP. Moreover, within the works of T6.1, the SENTINEL User-centric Evaluation Methodology was designed (in consensus with the experimental protocol) to drive the entire SENTINEL evaluation process, which is carried out as an ongoing, agile process of the SENTINEL platform assessment throughout its lifecycle development. In this regard, a variety of SENTINEL evaluation templates were designed as part of T6.1 (verification/validation templates, business and application requirements evaluation templates, KRs/KPIs evaluation templates). The SENTINEL evaluation process is designed to run at distinct time periods (e.g. during the pilot preparations, after the pilot demonstrations, after development achievements, i.e. MVP prototype releases) following a hybrid approach of both technical and non-technical aspects relying on system verification and system validation evaluation criteria as indicated in the methodology.

Furthermore, within T6.1 activities, the evaluation KRs were identified and the way of their monitoring and assessment to measure the project's success considering the produced evaluation results was defined. Through the works of T6.1, the demo execution plans and the overall evaluation time plan were structured. In addition, the SENTINEL training process, the training material and supporting equipment were prescribed, including the development of the questionnaire and instructions utilized in the initial execution and evaluation. These T6.1 activities were presented by FP in the 4th plenary meeting that occurred in late October 2022.

T6.1 has contributed to the following WP6 objective:

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

The above comprises significant input to the produced deliverable D6.1 "SENTINEL Demonstration – initial execution and evaluation", 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 started in M13. CG has already participated and discussed with all the involved partners during the WP6 meetings about the SENTINEL offerings. After the development of the SENTINEL MVP the SENTINEL pilot owners validated the MVP and its functionalities before releasing its full-featured version and identified valuable insights needed to feed in further technical developments. In particular, these short-run experimentations aimed at

- Engaging end-users and engaging them with the main objective of the project piloting activities.
- Uncovering technical problems/bugs of the MVP functionalities and to get feedback for further technical improvements.
- Discovering opportunities to improve the design and learn about users' real needs and preferences.
- Addressing any concerns that the end-users have arisen before starting the real-life demonstration phase of the project.

To support and complement the MVP testing activities, several preparatory activities have been carried out (such as the MVP Use Case selection, the experimental protocol refinement, guidelines and documentation preparation and external end-users' recruitment) by the consortium partners while to perform successful experimental trials and attain valuable insights, a dedicated workshop has been organized jointly by WP5 and WP6 partners. In total, six (6) participants (the SENTINEL pilot partners CG and TIG and four (4) external SMEs were invited as part of Task 6.3 activities) attended the workshop. At the end of the workshop, the participants were provided with supporting material, (reading documentation and video recordings) and kindly invited to take part in a survey campaign and provide feedback via an online questionnaire prepared by FP.

The results achieved are analysed and reported in D6.1 "SENTINEL Demonstration – initial execution and evaluation", delivered in M18.

After the release of the SENTINEL FFV the project's pilot end-users collaborated with technical partners for the improvement and refinement of the SENTINEL platform to address their needs. In particular during M19-M24, CG and TIG pilot activities took over. In particular, in M22 the CG Demonstration Workshop was conducted to demonstrate the SENTINEL FFV capabilities to CG end-users and via two trial executions, performed by two (2) CG end-users, CG pilot experiments were accomplished at a first stage and evaluation feedback was provided by the 2 end-users via filling the online User Evaluation Questionnaire and the excel detailed evaluation form. In addition, within M23-M24, TIG pilot preparatory actions were organized and in M24 the TIG Demo Workshop realized how to demonstrate the SENTINEL FFV capabilities and the CyberRange platform to TIG end-users. Through the next period, CG pilot experiments will be implemented at all stages engaging an additional end-user testing and TIG trial execution and evaluation by relevant end-users will be performed as well.

T6.2 has contributed to the following WP6 objective:

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

The above activities will provide significant input for deliverable D6.2 "SENTINEL Demonstration – final execution", to be delivered in M30.

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

This task is led by UNINOVA and started in M13. UNINOVA, as a task leader, has been in close contact with several DIHs in order to engage European SMEs willing to use and validate the SENTINEL platform. Such engagement activities are being performed through webinars and workshops aiming to present the SENTINEL platform to different SMEs. At the end of such events, participants are requested to fill in a questionnaire, which enables them to understand how such SMEs are willing to use and validate the SENTINEL platform. With this respect, four (4) third parties (SMEs) were already contacted and have participated in the SENTINEL MVP demonstration workshop for SMEs, which was conducted under WP6 scope.

In Y2, SENTINEL was able to engage with the following DIHs and network of DIHs: Produtech, DIH4CPS, DIHWorld, Madeira DIH, Digital Manufacturing Innovation Hub Wales, DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH. As also mentioned previously, the aim is to foster such collaboration with other European DIHs. Regarding this last point, a preliminary contact was established with 39 different European DIHs, seeking the organization of a workshop for demonstrating the SENTINEL platform and recruiting additional SMEs for use and validating SENTINEL offerings. In Y3, we intend to increase the number of external parties willing to test and validate the SENTINEL platform.

### T6.4 Evaluation and impact analysis

This task is led by STS and started in M22. As part of the SENTINEL evaluation process, STS will ensure that KR templates are completed and regularly updated for each KR. In M30, after the final execution of the demonstrators and at the end of the project, each KR will be evaluated. STS will collect and analyze data and feedback from end-users through questionnaires, using a user-centric methodology for impact analysis. The impact analysis will be carried out with respect to the demonstration protocol finalised in T6.1. STS will also arrange to gather feedback from the External Advisory Board members, in addition to feedback from the pilots, and lead the delivery of D6.3.

### 3.6.3 Work carried out in WP6 per partner

| | |
|---|---|
| ITML | In Y2, ITML has participated in all WP6 related discussions providing inputs and valuable insights on planning the execution of both the SENTINEL MVP and FFV trials. Furthermore, ITML has facilitated the organization of the MVP and FFV demonstration workshops by inviting and engaging both internal (SENTINEL pilot 1 and pilot 2) and external SME representatives (pilot 3) and giving short presentations during these sessions. ITML has contributed to and conducted the internal review of D6.1. Finally, ITML has facilitated the successful achievement of MS4 “Demonstration Flame” (M24). Next steps for Y3 include to keep participating and actively supporting the SENTINEL validation, evaluation & impact analysis as part of WP6 activities. |
| LIST | In Y2, LIST continued to actively participate in Pilot preparation meetings. In that context, LIST was responsible for the presentation of Data Protection challenges to the CG pilot. Another content related to how data protection is addressed within SENTINEL is under preparation for the TIG pilot. Experimentation will continue more intensively in Y3. LIST will pursue its contribution to prepare users for trial. In addition, LIST will be involved in the analysis of pilots’ feedback. |
| IDIR | IDIR participated in the discussions concerning the experimentation protocol alignment and refinement process. To this end, IDIR provided updates regarding the verification variables concerning two SENTINEL main system components (the Profiling service and the Self-Assessment engine) and associated KPIs. IDIR also provided input regarding the definition of the user test cases and the user evaluation questionnaire and participated in the SENTINEL MVP demonstration workshop. IDIR also acted as an internal reviewer for the deliverable D6.1. IDIR also participated in the discussion related to the validation of the SENTINEL offerings. In particular, IDIR has participated in the revision of the user questionnaire for obtaining user input and the identification of a suitable methodology for identifying indicative user personas. |
| 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. Moreover, INTRA conducted the demonstration workshops for both the MVP and the FFV versions of the platform to onboard internal users and external SMEs participating in the platform evaluation. |
| STS | STS has participated in all WP6 monthly telcos and discussions as a leader of T6.4. |
| AEGIS | AEGIS participated in all related discussions providing inputs on the evolving system architecture and functionalities. In addition, AEGIS has contributed to the deliverable D6.1. |
| TSI | TSI has participated in all WP6 monthly telcos and discussions (mainly for T6.2 and T6.3). TSI also contributed to D6.1. The main contributions were focused on the recommendation of external tools and trainings, which could potentially assist the pilots to improve their security/privacy status. Currently, the suggestions are mostly based on covering missing functionality and OTMs. A wide list of recommendations is given to the user, who then has to select the most suitable of them.<br>For Y3, TSI will collect feedback from the pilots, concerning the appropriateness of the recommended external tools and training elements. The goal is to assist the |

| | |
|---|---|
| | operation of the Recommendation Engine in order to make tailored and fruitful suggestions to the end user. |
| ACS | ACS has participated in the WP6 monthly call and initiated discussions with SENTINEL pilot owners (TIG, CG) to engage them in the development of CyberRange scenarios. ACS has provided the gaming interface of the CyberRange with four scenarios to be used by the SME's. In Y3, the end-users will use the gaming interface of the CyberRange and will provide feedback based on which ACS will improve the solution and user experience. |
| UNINOVA | In Y2, UNINOVA has participated in WP6 regular calls and has provided input to D6.1, namely on the DIH use case plan and the refinement of the validation template for the SMEs. As previously identified, UNINOVA has been also actively contributing to Task 6.3 by engaging with various DIHs and networks of DIHs. |
| CG | In Y2, CG has validated and identified valuable insights needed to feed in further technical developments. CG worked on refining the verification and validation variables and their respective KRs and provided input to D6.1, regarding the CG's use case plan. In addition, to facilitate the ensuing operational trials, CG has started the process of the replication of CG's software infrastructure by providing the following information to all the involved technical partners:<br>• the OS used<br>• the database with the configuration used<br>• schema of database infrastructure<br>• the applications with the configuration used<br>• the firewall, with the rules and<br>• a network flow matrix<br>a VM with the development environment.<br>CG partners have actively participated in the SENTINEL FFV Demo session, tested the FFV platform and filled in a respective questionnaire. For FFV platform testing CG made a hands-on session within the organisation, to be ready for the experiment's executions. |
| TIG | In Y2, TIG has participated in the WP6 monthly calls and by participating in all related discussions supported the technical partners with pilot requirements. Furthermore, TIG has proposed an SME within the TIG group, Dimensions Care, that will become the pilot organisation. This is a critical case company as it uses a range of highly sensitive information about service users (i.e., children) that should be protected, and not in the least due to the vulnerabilities of service users. During the reference period, the Managing Director of Dimensions Care has been consulted and provided agreement to proceed, subject to the implementation of a robust and comprehensive Data Protection Impact Assessment (DPIA). In this respect, the following items have been identified as the most important requirements to be addressed by the SENTINEL platform:<br>• Enhance the measures taken to protect sensitive information about children and those significant to them (i.e., suitable biological parents, carers, social workers, commissioners, etc.,).<br>• Improve upon the robustness of security measures in place to counter potential threats from ransomware and malware that could result in serious disruption to day-to-day operations, such as the locking of essential communication systems.<br>• Reduce the potential for children to access inappropriate sites and social media platforms that have the potential to cause harm. |

| | |
|---|---|
| | Within M23-M24, TIG was involved in the pilot preparatory actions, by actively participating in the TIG Demo Workshop during which the SENTINEL FFV capabilities and the CyberRange platform were demonstrated the TIG end-users. |
| CECL | In Y2, 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. Moreover, the EDAC finalised the Ethical Controlling Report, which offers a more detailed comparison of the partners' (especially the pilot partners) data protection policies. Both documents will be used as valuable sources and learning materials for pilot partners. |
| FP | After M16, FP leads all WP6 activities and conducts and coordinates corresponding meetings. As T6.1 leader, FP has illustrated the main task objectives to be followed and coordinated all the activities to address T6.1 objectives and proposed directions for their execution. FP actively participated in all WP6 meetings and organised additional web meetings devoted to T6.1 activities to open discussions engaged project partners for the refinement of the SENTINEL experimentation protocol (e.g. regarding the verification/ validation variables and their mapping with respective KRs, pilot cases and experiments). Moreover, FP has proposed the SENTINEL User-centric Evaluation methodology which sets the directions for the SENTINEL evaluation process (identifying all evaluation aspects, type of actors means of evaluation and calculation, time plan, its actual preparation and execution, collection of evidence, reporting and analysis of results). To this aim, FP developed the evaluation templates that will be used to check whether the application and business stakeholders' requirements identified in T1.1 and T1.2 are covered by the SENTINEL platform. In addition, FP initiated the template that will be utilized for the KRs assessment and introduced respective KRs evaluation properties to be considered. Furthermore, FP following the SENTINEL experimental protocol identified in T1.3, updated the structure of the pilot case template and the experiments template that are used to reflect the pilot demonstrations. FP has initiated the training process of SENTINEL and proposed types of material to be utilized. To this aim, FP indicated the adopted training method (Training Needs Analysis method) to elicit the SENTINEL training requirements. In addition, FP in collaboration with ITML, developed the online questionnaire used within the initial trial execution and evaluation and prepared the respective instructions presenting the SENTINEL MVP test cases which were disseminated to the engaged evaluators during the Initial Demonstration workshop. FP together with TIG prepared and submitted D6.1 in M18. From M19 to M24, FP led all CG and TIG pilot activities and coordinated the trials execution and evaluation process performed by CG end-users providing related timeplans and action points for each pilot as well. Moreover, FP prepared the CG pilot instructions which referred to two (2) CG pilot experiments reflecting 2 personal data PAs related to CG user/client data and genomics data. The instructions also indicated the CG experiments workflow and respective SENTINEL use cases to test the SENTINEL FFV functionalities. In addition, FP in collaboration with ITML reviewed the User Evaluation Questionnaire prepared by IDIR for the CG pilot and coordinated the two pilot demo workshops (for CG and TIG). Eventually, FP has proposed in the context of T6.3, DIH recruitment effort to invite Women4Cyber of Greece to participate in external end-users trial executions. |

### 3.6.4 Status of Deliverables and Milestones

The work conducted in WP6 in Y2 is well-documented in deliverables D6.1 which also contributed to reaching milestone MS4.

*Table 11. Status of WP6 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D6.1 | SENTINEL Demonstration - initial execution and evaluation | TIG | Report; CO; M18 | Accepted |
| MS4 | Demonstration Flame | TIG | M24 | To be achieved in M24 |

### 3.6.5 Deviations from Work Plan

There has been one deviation from the GA which has resulted in changing the engaged corporate SME of the TIG pilot from Juventas Services to Dimensions Care. This necessitated a change in the scheduled piloting arrangements resulting in CG to become the first to conduct the pilot SME activities. In addition, CG pilot experiments PAs reported in D6.1 were modified and enhanced to better address the GDPR and privacy requirements of the CG pilot case. Nevertheless, the writing process of D6.1 started and executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

### 3.6.6 WP6 planned activities for the next period

In the course of the project's Y3, (M24-M36) all required pilot preparations and auxiliary activities will be undertaken to promote the final execution of all three pilots (CG pilot, TIG pilot and DIH pilot) considering:

- the implementation of all planned trials to conduct the pilot experiments at all stages (which will be reported in D6.2).
- the end-users' evaluation from the trials execution.
- the development and update of respective questionnaires, evaluation forms and pilot instructions according to the pilot assessment needs.
- the recruitment of additional external companies (via DIHs).
- the evaluation report and analysis of the generated evidence both from internal and external evaluators using the SENTINEL evaluation templates to develop focused personas which will allow the consortium to better profile the engaged end-users and provide indications for technical enhancements.
- the calculation of verification/validation variables and the SENTINEL quality performance testing against the identified application and business requirements (cf, D6.1; annex evaluation templates).
- the monitoring and measurement of "evaluation KRs/KPIs" to assess the project's success as indicated in the SENTINEL User-centric Evaluation Methodology (cf. D6.1).

Furthermore, it was decided by the majority of the consortium during the 5th plenary meeting to conduct a short final round of trials after the final SENTINEL platform release in M30 and provide evidence from this final end-to-end evaluation which will be reported in D6.3 and may activate eventual technical improvements of SENTINEL recommended by the end-users and contribute to Milestone 6 (MS6) related to "Consolidation" phase. To this end, these activities will be captured in the corresponding deliverables, i.e., D6.2 and D6.3 due in M30 and M36 respectively.

## 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 Y2, WP7 activities focused on updating and maintaining the fundamental communication and dissemination channels for the project. In addition, SENTINEL has produced additional dissemination materials: four (4) newsletters, 9 videos [one (1) promotional video, and eight (8) other dissemination related videos], six (6) SENTINEL podcasts, which have been prepared and electronically distributed via the established online channels and in physical meetings.

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

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

- SENTINEL MVP demonstration, Online
- 3rd SME-centric workshop as part of the Digital Transformation Summit 2022, Madeira

In addition to this, the partners have managed to submit three (3) additional publications. One has already been published while acceptance notifications are pending for the other two.

- Kostas Drakonakis, Sotiris Ioannidis, Jason Polaki "ReScan: A Middleware Framework for Realistic and Robust Black-box Web Application Scanning", 30th Annual Network and Distributed system Security Symposium (NDSS 2023) (**published**).
- Y. Skourtis, P. Loucopoulos, E. Kavakli "Supporting Profiling and Self-assessment for Cybersecurity and Personal Data Processing of SMEs", 35th International Conference on Advanced Information Systems Engineering (CAiSE'23), Zaragoza, 12-16 June, 2023 (**submitted**).
- S. Cortina, M. Picard, S Renault, P. Valoggia., "An illustration with GDPR Compliance Self-Assessment for SMEs", EuroSPI: European Conference on Software Process Improvement, 2023 (**submitted**).

In Y2, the SENTINEL partners have participated (or jointly organised) and presented the project in events and conferences:

- FIC 2022 International Cybersecurity Forum, 7-9 June 2022.
- IoT Week 2022 workshop, 20-23 June 2022.
- EU Policy to Projects Seminar (PPS), event invited by REA 30th June 2022.
- INTEROP V-LAB General Assembly, 30th June 2022.

- IEEE International Conference on Cyber Security and Resilience, 27th July 2022.
- International workshop on Information & Operational Technology (IT & OT) Security Systems in conjunction with the 17th International Conference on Availability, Reliability, and Security, 23-26 August 2022.
- 9th International Workshop on Evolving Security & Privacy Requirements Engineering, 15-19 August 2022.
- CyberHOT summer school, 29-30 September 2022.
- ETSI conference on cybersecurity certification October 2022.
- Digital Transformation Summit, 25-27 October 2022.
- Joint cybersecurity webinar 19th January 2023.
- Joint workshop "EU-Made cybersecurity for safe, resilient and trustworthy applications and services" 27th February 2023.
- Safe Internet Day 2023" February 2023.
- FIC 2023 International Cybersecurity Forum, 5-7 April 2023.
- IDC Security Roadshow, 20th April 2023.
- 30th Annual Network and Distributed System Security Symposium, 27th of February to 3rd of March 2023.

SENTINEL has reached and secured the interest for further trialling of the SENTINEL framework of eight (8) Digital Innovation Hubs:

- DIH-WORLD
- PRODUTECH – Production Technologies Cluster
- DIH4CPS
- Madeira DIH
- Digital Manufacturing Innovation Hub Wales
- DataLife DIH
- Images-et-reseaux DIH
- ICE RWTH DIH

In Y2, SENTINEL was engaged with four (4) new projects and continued to liaise with ten (10) EU projects engaged during Y1.

- PALANTIR-883335
- TRAPEZE-883464
- PUZZLE-883540
- ARCADIAN-IoT-101020259
- IRIS-101021727
- ERATOSTHENES -101020416
- IDUNN-101021911
- SECANT-101019645
- CyberKit4SME-883188
- CONCORDIA-830927
- CitySCAPE - 883321
- TRUST aWARE - 101021377
- HEIR - 883275

- ELECTRON - 101021936

During Y2, the project partners organized one SME-centric workshop with a release of the SME engagement survey, which, in conjunction with the MVP release, has triggered the intensification of the exploitation activities. Furthermore, we gave training on "Cybersecurity Policies and Practices in the EU – for non-IT Experts" by presenting and talking about the SENTINEL project as well as organized training for the SENTINEL end-users and showcased the SENTINEL MVP.

The above was comprised significant input to D7.3 "Dissemination strategy and activities - interim version" (delivered in M18), D7.5 "Ecosystem building and SMEs engagement report - interim version" (delivered in M18), D7.7 "Exploitation strategy, standardisation activities and best practices - interim version" (delivered in M18). Furthermore, D7.3, D7.5 and D7.7 contributed to milestone 3 "Innovation Fire" due M18.

### 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 in. The design of the questionnaire was aimed at gathering insights from many different perspectives including Academia, large industries, technology providers and SMEs. The insights emerged from this process were contributed to better understand and identify SENTINEL competitive advantage and value proposition and form the preliminary business modeling that was successfully presented in D7.2 titled "Market analysis and preliminary business modeling" in M6 of the project.

After the successful submission of the D7.2 "Market analysis and preliminary business modelling", AEGIS 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 and the FFV as part of brainstorming, as well as based on the feedback we will 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. In addition, as part of the continuous market observation, an intermediate analysis has been carried out for M18 resulting in an updated business strategy [value proposition, business model (canvas)] which was included in D7.7 "Exploitation strategy, standardisation activities and best practices - interim version".

T7.1 has contributed to the following WP7 objectives:

(i) To develop the SENTINEL business model and strategies for incentivizing/promoting project adoption by various stakeholders within the SMEs/MEs ecosystem during and after the project.
(ii) Create a marketing strategy that focuses on commercialization including the products costs (TCO), benefits (TBO), and return on investment.

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

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

T7.2 is led by UNINOVA and started in M1. 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 peek was presented during the kick-off meeting, followed by the social media channels (LinkedIn, Twitter and YouTube).

With respect to the reporting period of this deliverable, SENTINEL has released four (4) new newsletters (M14, M18, M21 and M24). The SENTINEL promotional video was released at the end of M12 and early M13 was already available under the YouTube channel.

Considering attendance at events, SENTINEL was present at different events, as already presented previously. In parallel to participation in multiple events, SENTINEL has also organized webinars and workshops aiming to invite and engage target audiences and potential end-users. The full list of activities and events where SENTINEL participated is described under D7.3” Dissemination strategy and activities - interim version”.

With respect to academic publications, SENTINEL has submitted three (3) conference papers, among which one has been presented and accepted for publication on conference proceedings, the remaining two are still waiting for acceptance.

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

T7.2 has contributed to the following WP7 objectives:

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

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

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

Points (i) and (ii) mentioned above are mainly covered in Y1. In Y2, we updated the project’s visual identity (where needed), continued raising awareness about the project, developed the project’s dissemination and communication strategy and proceeded in implementing the main aspects mentioned in point (iii). The respective activities are well demonstrated in D7.3 “Dissemination strategy and activities – interim version”, delivered in M18.

Further actions towards points (i), (ii) and (iii) will comprise input for future deliverable of WP7, namely D7.4 "Dissemination strategy and activities-final version" to be delivered in M36, contributing also to milestone 6 'Consolidation', due in M36.

### T7.3 Exploitation and standardization activities and best practices

T7.3 started in M13 and is led by STS. In the context of designing and developing the exploitation strategy and standardisation activities of SENTINEL, STS circulated a questionnaire and all the partners were kindly requested to fill it in.

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

Furthermore, as part of this questionnaire, the SENTINEL partners examined their individual exploitation plans, gave details about completed and current exploitation actions and detailed their short-term future exploitation plans and long-term sustainability plans. They also described the standardisation activities they are engaged in and their expected impact, all of which were included in the D7.7 report, submitted successfully within the given timeline.

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

At an upcoming workshop, the members of the consortium will review the outcome of these questionnaires filled out as well as discuss and plan joint exploitation activities for the remainder of the SENTINEL project. In addition, each partner will be able to share their individual exploitation plans and ideas that may inspire others. The objective of the workshop is to both review the exploitation results already attained and to map out future plans.

In Y2, SENTINEL has applied for the Horizon Standardisation Booster[3] to seek help in identifying relevant current and upcoming standards that SENTINEL can take advantage of. At the stage of writing this deliverable several meetings took place with the assigned expert and based on the discussions made a report with valuable suggestions and recommendations will be prepared by the assigned expert.

Additionally, STS has applied for two modules under the service 1 "Portfolio Dissemination and Exploitation Strategy" of the Horizon Results Booster[4] to strengthen SENTINEL's dissemination and exploitation strategy and maximise the impact of the project. Currently, only introductory meetings take place with further arrangements that will take place mainly in Y3.

[3] HSbooster.eu

[4] https://www.horizonresultsbooster.eu/

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

T7.4 is led by UNINOVA and started in M1. The ecosystem building task was very active during the first 24 months, three (3) different SME-centric workshops were organized. The third SME-centric workshop was held on the 25th of October 2022 co-located with the Digital Summit event (Funchal, Madeira), organized by UNINOVA.

We received more than 100 registrations for the workshop, which accounted for more than 70 people attending physically. During the workshop, participants had the chance to participate in our SME questionnaire, where we were able to collect 52 responses. The focus of the 3rd SME-centric workshop was to present the SENTINEL project to regional SMEs and to have a first glimpse of the SENTINEL MVP features and services. The idea was to have a first contact with the SMEs regarding MVP usability, UI and UX.

Aligned with T7.2, a joint Cyber Security webinar was organised on the 19th of January 2023 where SENTINEL together with CitySCAPE, HEIR, PUZZLE, SECANT and TRAPEZE projects have presented their results achieved. SENTINEL was actively involved in another webinar named “EU-Made Cybersecurity for Safe, Resilient and Trustworthy Applications and Services” which took place on the 27th of February 2023 and gathered ARCADIAN-IoT, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SPATIAL, TRUST aWARE 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”, “IoT Week”, “Projects to Policy Seminar (PPS)” events also paved the way for reaching out to a wider audience of SMEs.

Overall, during Y2 SENTINEL was able to establish contacts with the following DIHs and DIHs networks: Produtech, DIH4CPS, DIHWorld, Madeira Digital Innovation Hub, Digital Manufacturing Innovation Hub Wales, DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH.

SENTINEL was also presented along with an oral speech concerning “Internet & Social Media Safety” for raising awareness during the global *Safe Internet Day 2023*, in February 2023. The talk took place on the premises of the Metropolitan College in Heraklion, Greece. It was attended by students and staff of various backgrounds (Informatics, Economics & Management, Tourism, Phycology, Legal). There were around 30 participants, half of them were women. Moreover, it was a joint event with the privacy-focused project CAP-A[5] (ttps://cap-a.eu), part of the CAPRICE community[6].

Within this task, SENTINEL is engaging 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.

T7.4 has contributed to the following WP7 objective:

(i) To raise awareness about the project concept, developments and findings to all key actors (the cybersecurity and data protection industry, SMEs/MEs, academics, policy

[5] https://cap-a.eu/
[6] https://www.caprice-community.net

makers, general public) by participating and organizing outreach activities, international events (e.g., conferences and seminars) and INFO days.

The above comprised significant input to D7.5 “Ecosystem building and SMEs engagement report – interim version”, delivered in M18, contributing also to milestone 3 “Innovation Fire”, due in M18.

### 3.7.3 Work carried out in WP7 per partner

| | |
|---|---|
| ITML | In Y2, ITML has contributed to all the dissemination and exploitation strategy activities which took place during this reporting period. In this context, 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 to promote the project offerings. Also, ITML participated in all the crucial discussions which took place to build a thorough exploitation strategy plan, target market and standardisations activities plan also (T7.3). In addition, ITML has provided input for all deliverables of WP7, and conducted a review process wherever assigned. In this regard, ITML, elaborated on deliverables D7.3 and D7.7 as well as conducted the internal reviews of D7.3, D7.5 and D7.7 which are linked to T7.3 and T7.4. The 4th plenary meeting of SENTINEL was co-located with the Digital Transformation Summit that was held on 24-27 October 2022, Funchal, Madeira, Portugal. During this event a dedicated interactive workshop session took place on the 25th of October, to promote the project during the Digital Transformation Summit event. In this event, ITML, has moderated the workshop session along with UNINOVA and INTRA, and has presented the SENTINEL project as a whole. Regarding the event participation, ITML has disseminated the SENTINEL project in IoT Week, FIC 2022, PPS 2022, and Digital Transformation Summit event. ITML has prepared and released posts relevant to SENTINEL, GDPR compliance, data protection and security in SENTINEL’s social media (LinkedIn, Twitter), as well as in its own media channels (social media and website). ITML has supported the project’s exploitation and standardization activities by actively participating in all relevant meetings and discussions.<br>In Y3, ITML is looking forward to providing additional support in the next Clustering Event which will be hosted by UNINOVA within the next months and probably in Portugal. Finally, ITML will continuously provide support in the contributing tasks of WP7 as assigned, participate in the dissemination activities, and particularly focus on defining a thorough exploitation strategy plan concerning maximizing the project’s product exploitation in order to reach a long-term impact. |
| LIST | In Y2, LIST has participated in the Digital Transformation Summit that was co-located with the SENTINEL plenary meeting in Madeira, Portugal (October 2022) and contributed to D7.3 and D7.7. LIST also submitted a paper describing GDPR CSA and providing its conformity assessment with ISO/IEC 330xx family standard. In Y3, LIST will continue to actively participate in the definition of dissemination and exploitation strategy of SENTINEL. |
| 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).<br>**Since M6, the partner SHELL has been terminated from ECAS.** |

| | |
|---|---|
| IDIR | IDIR has participated at all four WP7 tasks active in Y2 (M13-M24). Specifically, it has participated in all major WP7 meetings, contributed to social media content dissemination and creation. IDIR has also made contributions towards the common effort to define SENTINEL's business value for different stakeholders 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.<br>IDIR has also contributed and presented a paper in the 9th International Workshop on Evolving Security & Privacy Requirements Engineering which took place virtually on August 15th-19th, 2022 (M15). The workshop included invited talks and paper presentations from distinguished members of the Requirements Engineering community and brought together practitioners and researchers interested in security and privacy requirements coming from 3 continents. Another publication was submitted by IDIR to the 35th International Conference on Advanced Information Systems Engineering, which will take place in June 2023 in Zaragoza, Spain. IDIR participated in the Digital Transformation Summit that was co-located with the SENTINEL plenary meeting in Madeira, Portugal (October 2022). Finally, IDIR has participated in exploitation activities within Task 7.3. |
| INTRA | In Y2, INTRA has participated continuously in all the meetings concerning the WP7. Occasionally, input for the SENTINEL website and SENTINEL social media channels (e.g., newsletters) has been provided also. INTRA has participated in meetings and discussions dedicated to dissemination and exploitation strategy. Within this period, INTRA has demonstrated the SENTINEL platform in SENTINEL events/workshops such as the MVP demonstration workshop and the demonstration to SMEs in the Digital Transformation Summit in Madeira. Moreover, INTRA led the demo session along with covering technical aspects to the 1st Pilot Workshop with CG.<br>Furthermore, INTRA contributed to the definition of the business value of SENTINEL, portraying its main virtues and helping the consortium find pitching points for engaging external SMEs.<br>Finally, INTRA has participated in meetings concerning T7.3, regarding the standardisation activities and in crucial discussions which occurred in Y2 focusing on exploitation strategy.<br>Work will continue implementing for the next months as is requested and wherever contribution is needed. This may include the final deliverables submission, linked with the tasks that INTRA is a contributor (T7.1-T7.4). |
| STS | In Y2, STS participated in all WP7 relevant telcos, discussions and provided content for producing social media posts. In addition, STS supported SENTINEL in the International Workshop on Information & Operational Technology (IT & OT) Security Systems (IOSec 2022) that was co-organised by STS. STS has circulated an exploitation questionnaire by collecting and analysing the KERs and exploitation strategies of the SENTINEL partners. This helped to prepare and submit D7.7.<br>Furthermore, STS has engaged with Horizon standardisation Booster (HSbooster.eu) to seek help in Identifying relevant current and upcoming standards that SENTINEL can take advantage of. Additionally, STS applied for two modules from service 1 provided by the Horizon Results Booster (HRB) to strengthen the dissemination and exploitation strategy of the project. |
| 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. These activities resulted in preparation and submission of D7.2. 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.<br>Additionally, during Y2, as part of the continuous market observation, AEGIS carried out an intermediate market analysis for M18 resulting in an updated business strategy [value proposition, business model (canvas)] which was included in D7.7 "Exploitation strategy, standardisation activities and best practices - interim version". 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. Finally, AEGIS has conducted an internal review of deliverables D7.3, D7.7. |
| TSI | TSI has participated in all WP7 meetings and discussions. In addition, during M1-M12, TSI has made three (3) posts on the 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 the European Workshop on Systems Security (EUROSEC '22).<br>During months M13-M18, TSI published two (2) LinkedIn posts on SENTINEL's LinkedIn page. Also, TSI co-organized and participated in the CyberHOT summer school (Chania, Crete, September 2022) and produced a relevant webpage post to promote it. SENTINEL was promoted there with a poster exhibition. Finally, TSI participated in the Digital Transformation Summit that was co-located with the SENTINEL plenary meeting in Madeira, Portugal (October 2022). Moreover, TSI members gave a speech concerning "Internet & Social Media Safety" for raising awareness on university students, during the global Safe Internet Day 2023, in February. In addition, TSI contributed to Deliverables D7.3 and D7.7. This also included the update of the individual exploitation plan of TSI. For Y3, TSI will assist again in the organization of the CyberHOT summer school of 2023 (probably in September). Moreover, TSI will assist the organization of workshops under scientific conferences, focusing on conferences where CERTs can be reached (i.e., FIRST CTI conference 2023 in Berlin). |
| 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 also provided input for the 2nd newsletter of SENTINEL about the CyberRange platform and contributed to D7.7 by providing input about the company's exploitation activities. Finally, ACS has participated in Madeira's Digital Transformation Summit in October 2022 and FIC 2023 in Lille where the ACS partners made a presentation about the SENTINEL project. |
| UNINOVA | During Y2, as the leader of the WP7 UNINOVA has conducted the following activities.<br>• Organization and leading of monthly WP7 telcos.<br>• Organization the 3rd SENTINEL SME-centric workshop.<br>• Contribution to the exploitation questionnaire.<br>• Continuously creating awareness, promoting SENTINEL through social media channels and providing content to social media on a regular basis<br>• Design of the SENTINEL brochure, business card and roll-up.<br>• Engagement of relevant stakeholders through social media channels.<br>• Supporting the definition of the online questionnaire for collecting insights from EU SMEs. |

| | |
|---|---|
| | • Preparation of the SENTINEL newsletters.<br>• Leading the creation of the SENTINEL podcast series.<br>• Promotion on bilateral meetings with other EU projects, seeking potential synergies.<br>• Targeting industrial events for SME engagement.<br>• Participation in several EU events aiming to disseminate SENTINEL achievements. |
| CG | CG has participated in all meetings regarding the WP7 and was actively following the SENTINEL social media profiles. It also produced content for a post in SENTINEL's LinkedIn channel and participated in all discussions regarding stakeholder engagement activities. |
| TIG | During Y2, TIG worked with relevant partners to fulfil the requirements of WP7 and participated in all meetings regarding WP7. Furthermore, provided input concerning the exploitation plan of TIG. Finally, TIG has contributed to D7.3 and D7.7. |
| CECL | CECL has participated in all meetings regarding the WP7. During Y2 CECL has reviewed the D7.5 and contributed to the development of Exploitation strategy and standardisation activities questionnaire. CECL contributed to D7.3 and D7.7. 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 | In Y2, FP has regularly participated in all meetings regarding WP7. In addition, FP has participated in the "CyberHOT" summer school (27-28 September 2022), boosting interested parties' acknowledgement about the project.<br>FP researcher gave training on "Cybersecurity Policies and Practices in the EU – for non-IT Experts" and talked about the SENTINEL project as well and also participated in ETSI conference on cybersecurity certification 3-5 October 2022<br>FP researcher Thanos Karantjias was part of the team who successfully submitted a position paper to the IEEE CSR 2022.<br>Furthermore, FP has contributed to deliverables D7.3 and D7.7 and reviewed D7.5 as FP was one of the assigned internal reviewers for this deliverable alongside with CECL.<br>FP has been active in social media of the project by creating new posts about the project. We will keep pushing to disseminate the project across multiple events. Next one is CyberHOT summer school 29th September 2023 where FP is one of the co-organizers. |

### 3.7.4 Status of Deliverables and Milestones

The work done under WP7 is well-documented in three deliverables D7.3, D7.5 and D7.7.

*Table 12. Status of WP7 Deliverables and Milestones*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D7.3 | Dissemination strategy and activities - interim version | UNINOVA | Report; Public; M18 | Accepted |
| D7.5 | Ecosystem building and SMEs engagement report - interim version | UNINOVA | Report; Public; M18 | Accepted |
| D7.7 | Exploitation strategy, standardisation activities and best practices - interim version | STS | Report; CO; M18 | Accepted |
| MS3 | Innovation Fire | INTRA | M18 | Achieved |

### 3.7.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D7.3, D7.5 and D7.7 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

### 3.7.6 WP7 planned activities for the next period

In Y3, the SENTINEL project will intensify its activities, from dissemination and communication, project exploitation as well as standardization point of view. In particular, WP7 will:

- Enhance the project's exploitation strategy and lay the ground for the long-term sustainability plan and next best actions for contribution to and leverage of relevant standards.
- Finalise the market analysis and formulate the final business model of the project.
- Shape the "Intensify Communication" and "Market outreach" phases of the SENTINEL dissemination and exploitation strategy respectively.
- Intensify event participation at both consortium level as well as at a partner level.
- Trigger engagement with other DIHs and boost the SENTINEL ecosystem building.
- Organization of physical project-cluster meeting.
- Organization of SENTINEL final event.
- Conducting preparation webinars with SMEs, for SENTINEL platform validation and testing.

These activities will be reported in corresponding deliverables, i.e., D7.4, D7.6, D7.8 and D7.9 due in M36.

## 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. In Y2, the WP8 activities have focused on updating the expected coordination bodies and procedures (if needed) as well as maintaining the efficient communication among the project partners and ensuring smooth implementation of the project's objectives and expected impact.

The key achievements of WP8 in **Y2** include:

**(i)** Maintaining the day-to-day project management structure and procedures already established in Y1.
**(ii)** Ensuring the existence of collaborative tools to enable effective internal and external communication and decision making.
**(iii)** Updating the External Advisory Board (EAB) and the Ethical & Data privacy Advisory Committee (EDAC).
**(iv)** Initiation and successful completion of the project's 2nd amendment processes (submitted in November 2022, M18) after the unfortunate event of Dr. Christopher Konialis – the CEO and founder of CG - passing away in M16.
**(v)** Managing the preparatory activities towards the production of the project's 1st Periodic Report (PART A, PART B and financial reporting) as well as coordinating the preparation of 13 deliverables (all submitted on time, except D5.5, which was submitted with only two-week delay).

Within Y2, WP8 was dedicated to regular coordination activities. A tight control over the project activities has been taking place regularly by organizing and executing regular meetings at different levels:

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

In Y2, five (5) deliverables of WP8 have been successfully produced and submitted, namely D8.6, D8.12, D8.14 and D8.2 (current document), D8.11 in M18 and M24 respectively.

### 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 it has been an active task since the beginning of the project. In Y2, the project's quality planning and monitoring has been further updated in D8.6 "The SENTINEL QA plan and periodic monitoring report – second version" in M18. This report provides updates on the project's organization, procedures, roles and responsibilities in addition to the management, coordination, control and quality assurance activities of the SENTINEL project that were previously presented in D8.5 "The SENTINEL QA plan and periodic monitoring report – first version". In addition, it contains updates regarding the production and reviewing of project deliverables, along with the involved partner roles and outputs.

In Y2, the project partners experienced only one risk (#6 as stated in the GA) and undertook an effective action as follows:

| Risk Number and Description | Mitigation Measures |
|---|---|
| **Risk #6**: Project milestones or deliverables are delayed | In Y2, only D5.5 deliverable was delayed. The Project Coordinator requested a two-week extension for this report. The report was successfully submitted within the requested extension period. The main reason of this delay was that D5.5 was a core document representing the project's technical activities conducted since M12 covering the most relevant information regarding the 1st integrated SENTINEL platform reflecting the technical progress being reported in D2.2, D3.2, D4.2, D5.2 in parallel. Thus, a short time of extension was required to crystalize the respective work by depicting the achieved results in a constructive and organized manner. This justification was communicated in advance with the Project Officer. |

In Y2, T8.1 has continued to contribute to the following WP8 objectives:

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

The above comprise significant input to D8.6 "The SENTINEL QA plan and periodic monitoring report – second version" due in M18 and D8.11 "The SENTINEL project handbook – third version" due in M24.

**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, ITML has been actively monitoring all the activities of the project in Y2 within all WPs and tasks to ensure that the time plan is well-followed by providing clarifications (when needed) and ensure the SENTINEL partners follow the same project mission towards the fulfillment of the project's objectives as defined in the GA. Furthermore, ITML has organised the 1st interim review meeting (M18) with the PO including the preparation of the technical and financial reports.

Also, a project handbook (D8.11 (third version), has been produced summarizing the key project management procedures which was made available to the Consortium as soon as it was submitted.

During Y2, a 2nd amendment was initiated, primarily needed for changing WP6 leadership from CG to FP due to the unfortunate event of Chris Konialis – the CEO and founder of CG - passing away in September 2022.

Finally, D8.2 (current document due in M24) has been prepared by presenting the work accomplished during the second project year. It elaborates on the advancements in relation to the project objectives and provides an in-depth description of the technical progression in all the WPs including work carried out per task and per partner, submitted deliverables, achieved milestones, potential deviations and corrective actions.

In Y2, project coordination has organized the following consortium meetings with the purpose of ensuring a synergistic collaboration among partners and brainstorming on technical and management issues:

- The 4th Plenary meeting, hosted by UNINOVA in Funchal, Madeira, on 25-26 October 2022.
- The 5th Plenary meeting, hosted by ACS in Paris, France, on 26-27 April 2023.
- 8 more monthly Scientific and Technical Meetings
- The 1st Interim Review Preparation meeting (3rd of February 2023, online)
- The 1st Interim Review Official Rehearsal meeting (13th of February 2023, online)
- 1st Interim Review Meeting (16th of February 2023, online)

T8.2 has continued to the following WP8 objectives:

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

The above comprise significant input to D8.2 “Yearly project management report -second version” and D8.11 “The SENTINEL project handbook – third version”, delivered in M24.

**T8.3 Technical and innovation management**

T8.3 is led by INTRA and started in M1. During Y2, INTRA continued the organization of monthly Scientific and Technical meetings on a regular basis. The main purpose of this series was for the partners to align monthly with respect to the latest developments and achievements of the project, potential risks and future plans. To facilitate the design and development of the SENTINEL FFV, during the Scientific and Technical meetings, the roles and expected contributions of each partner were clarified and key technology assets were presented by their owners. Moreover, Key Results and Performance Indicators were revisited and discussed defining their quantitative progress for the reference period.

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 were intensified after the delivery of the MVP and led to the production of D8.12 “The SENTINEL technical and innovation management report – interim version”. In particular, this report set the common rules that will govern the exploitation and commercialization of SENTINEL results, including the management of IPR and the relative competitiveness of the end results. It presents the strategic plans for innovation assurance, including coordination and management procedures of the technical evolutions within the project, as well as the project progress in terms of achieved innovation, evolving market needs/changes and business models linked to the project objectives.

T8.3 has contributed to the following WP8 objectives:

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

The above comprised significant input to D8.12 "The SENTINEL technical and innovation management report – interim version", (delivered in M18), contributing also to milestone 3 "Innovation Fire", due in M18. Further actions towards points (i), (ii) and (iv) of WP8 objectives will comprise input for future deliverable D8.13 "The SENTINEL technical and innovation management report - final version" to be delivered in M36.

### 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. Following the unfortunate passing away of Dr. Christopher Konialis, Dr. Tanya Kyriakou (hitherto alternate member of the EDAC) took over as a regular member on the 5th of October 2022, after consultation with the partnership and the coordinator.

In the reference period, 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 was finalised following input from all partners and delivered according to the plan initially defined in the GA. Moreover, the Ethics supervisor, in collaboration with the EDAC, prepared the first draft version of the SENTINEL Ethical Controlling report, and circulated it for comment to the partnership and specific reviewers on 12 July 2022. The report contains a detailed comparison of the partners' data protection policies against the standards identified in the Ethics Manual, assesses the level of data protection currently achieved and proceeds to formulate recommendations for its improvement. The final version of the report, following review by all designated reviewers, was finally adopted on the 26th of October 2022, at which point the Ethics Manual and Ethical controlling report were collated into a single document (D8.14 "Ethics manual and ethical controlling report - interim version"), delivered in M18, in accordance with the project's timeline.

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 comprised of significant input to milestone 3 "Innovation Fire", due in M18.

### 3.8.3 Work carried out in WP8 per partner

| | |
|---|---|
| ITML | In Y2, ITML has organized the SENTINEL M18, M24 plenary meetings, 1st Interim Review preparation and official meetings creating the agenda, minutes and the action items. ITML has maintained the smooth operation of the NextCloud repository for the project-related entries (deliverables, minutes, reports, etc.) and the project's mailing list. To manage and control the status update of the project KPIs/KRs, ITML has also facilitated the updating process of the SENTINEL KPI/KR evaluation matrix. ITML followed all the necessary procedures for keeping regular communications with the project Officer and the respective members of the EAB and EDAC. ITML actively participated in the scientific-technical monthly teleconference meetings.<br>In addition, ITML has initiated, coordinated and submitted the 2nd amendment after the unfortunate event of Chris Konialis (the CEO, founder of CG, WP6 leader) passing away in M16. ITML proceeded with all the necessary actions to organise the mid-term project review report. In detail, it initiated all the procedures to collect input for the report (cost claims, technical report (PART A and PART B).<br>ITML has been constantly monitoring the quality of the deliverables through a thorough final quality review process before the final submission based on its established Quality Assurance Plan. Apart from this, ITML has also been contributing to T8.3 by discussing with INTRA the time plan and the monitoring means that will be used for the innovation tracking. Finally, ITML has produced and successfully submitted the D8.6, D8.2 (current document) and D8.11, extensively contributed to D8.12 and conducted the internal review of D8.14. |
| LIST | In Y2, LIST has participated in all WP8 relevant telcos, meetings and discussions as well as plenary meetings and scientific and technical meetings. It will pursue its participation in Y3 as well. |
| IDIR | During Y2, IDIR has participated in all project management and resource monitoring activities either standalone, as is the case when reviewing deliverables (e.g., the D8.2 and D8.11 review) or collaboratively as in the participation in the SENTINEL Scientific and Technical monthly meetings, the monthly WP meetings and other administrative work, between M13 and M24. |
| 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 to ensure the scientific soundness, technical integrity and innovation potential of the SENTINEL platform. |
| STS | STS has participated in all WP8 relevant telcos, technical and plenary meetings. In addition, STS has participated in the interim review meeting and provided the necessary contribution for the Interim Review Report. |
| AEGIS | AEGIS has participated in all scientific and technical meetings and plenary meetings. Apart from this, during Y2 AEGIS has conducted an internal review of the deliverable D8.12, while it provided input for D8.2. |
| TSI | TSI participated in all project's relevant telcos (e.g., scientific and technical telcos), plenary meetings and contributed to quarterly reports and D8.2. In Y3, TSI will continue supporting these procedures. |
| ACS | ACS participated in all relevant meetings related to T8.2. ACS contributed to D8.2 and reviewed D8.12 deliverables. |

| | |
|---|---|
| UNINOVA | UNINOVA has participated in all WP8 relevant telcos and discussions. Contributed to D8.2 and Interim Review Report. |
| CG | In Y2, CG actively participated in all plenary & technical meetings and discussions of the project organised by the project coordinator and scientific, technical and innovation manager of SENTINEL. CG has also participated in the interim review meeting and provided the necessary contribution for the Interim Review Report. |
| TIG | TIG has regularly participated in WP8 scientific and technical telcos, plenary and meetings during the second project year. In addition, TIG has provided the necessary contribution for the Interim Review Report, participated in the Interim review meeting and contributed to D8.2. |
| CECL | In Y2, CECL participated in project meetings. It has provided input for the 2nd 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 also provided input for D8.2.<br>As part of T8.4 activities, 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 the first draft of the Ethics manual and circulated draft document for comments. The final version of the Ethics Manual was finalized following input from all partners and is expected according to the plan initially defined in GA. CECL prepared the first draft of the Ethical Controlling report and circulated it to EDAC and the partnership for comments and review. CECL finalised the Ethical Controlling report following comments by the reviewers, collated it with the final version of the Ethics Manual formed D8.14 and delivered to the coordinator for submission one month ahead of schedule. The final version of the Ethics Manual is going to be delivered in M36. Finally, CECL has proposed and discussed the appointment of new EDAC member Dr. Tania Kyriakou. |
| FP | In Y2, 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 the project's quality assurance plan. Furthermore, FP contributed to D8.2 "Yearly project management report – second version" as well as conducted the peer review of D8.14 "Ethics manual and ethical controlling report – Interim version" and D8.6 "The SENTINEL QA plan and periodic monitoring report – second version". |

### 3.8.4 Status of Deliverables and Milestones

The work done under WP8 in Y2 is well-documented in five (5) deliverables listed below.

*Table 13. Status of WP8 Deliverables*

| Del/MS # | Del/MS name | Leader | Type; dissemination level; Due date | Status |
|---|---|---|---|---|
| D8.2 | Yearly project management report – second version | ITML | Report, PU, M24 | Prepared; To be submitted in M24 |
| D8.6 | The SENTINEL QA plan and periodic monitoring report- second version | ITML | Report; PU; M18 | Accepted |

| | | | | |
|---|---|---|---|---|
| D8.11 | The SENTINEL project handbook - third version | ITML | Report, PU, M24 | Prepared; To be submitted in M24 |
| D8.12 | The SENTINEL technical and innovation management report - interim version | INTRA | Report; CO; M18 | Accepted |
| D8.14 | Ethics manual and ethical controlling report - interim version | CECL | Report; CO; M18 | Accepted |

### 3.8.5 Deviations from Work Plan

There were no deviations from the GA. The writing process of D8.2, D8.6, D8.11, D8.12 and D8.14 started and was executed in accordance with guidelines and procedures presented in the SENTINEL quality assurance protocol.

### 3.8.6 WP8 planned activities for the next period

For Y3, 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 Final Review Meeting foreseen for M36. In terms of technical and innovation management, the plan for Y3 is to foster integration activities within and between all technical WPs as well as support validation, evaluation & impact analysis.

### 3.8.7 GA 2nd Amendment

During Y2, the 2nd amendment was initiated primarily needed for changing WP6 leadership from CG to FP due to the unfortunate event of Chris Konialis (the CEO and founder of CG and WP6 leader of the SENTINEL project) passing away in M16. Towards this direction, the coordinator together with the consortium has carefully examined the situation regarding the WP6 activities and proposed that FP -who is already leading the pilots' preparation activities (T6.1) – becomes the new WP6 leader. The amendment that was submitted in M18 has been approved by the European Commission. Thanks to the proactiveness of the coordinator and the careful and detailed mitigation actions undertaken by the new WP6 leader, all WP6 activities smoothly continued without delays.

## 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 focus 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.

Within Y2 the project mainly focused on monitoring all the activities to comply with all the pre- and post-grant ethics and legal requirements as described in D9.1.

D9.1 has contributed to the following WP9 objective:

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

### 3.9.2 Work carried out in WP9 package

| | |
|---|---|
| ITML | ITML is leading WP9 and within Y2 closely collaborated with CECL to continuously monitor all the project activities by providing guidance and assistance to all partners related to ethics issues and ensuring that the project fully complies with all legal and ethical requirements set in this project. |

### 3.9.3 Status of Deliverables and Milestones

No deliverables to report in Y2.

### 3.9.4 Deviations from Work Plan

No deviations from Work plan.

### 3.9.5 WP9 planned activities for the next period

In Y3, ITML, together with CECL and 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. This will be achieved via continuous monitoring and controlling all the project activities.

# 4. Impact

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

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

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

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

Aiming to monitor the progress and measure the respective achievements, well-defined iKPIs have already been identified by the SENTINEL consortium since Y1. Moreover, we rely on specific measures aiming to maximize the impact of SENTINEL. The measures include the establishment of the External Advisory Board (EAB) and the External Ethics and Data Advisory Committee (EDAC), communication and dissemination plan and activities, continuous stakeholder engagements, a concrete exploitation strategy and management of knowledge and Intellectual Property. The activities towards the successful completion for each impact iKPI conducted in Y2 are reported below.

## 4.1 Impact related to the work programme

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

| | | |
|---|---|---|
| **iKPI-1.1** | **At least four (4) privacy and personal data protection technologies delivered** | **Achieved** |
| Within the SENTINEL project, technology-driven compliance services are developed according to a 3 steps engineering approach that illustrates "readiness" of service (MVP, First Integrated version, Final Version). Although the platform as a whole provides an integrated and extendable solution for multiple privacy and data protection technologies, the four most significant contributions to that end are: 1) GDPR Compliance Self-Assessment, 2) Integrated Identity Management System, 3) Data Protection Impact Assessment and 4) the Record of Processing Activities, as required by GDPR article 30. The two first are managed in WP2, respectively T2.1 and T2.2, while the third one is the expected outcome of T4.2. Finally, the fourth privacy and personal data protection technology has been introduced as part of the overall platform, so can be considered as an outcome of T5.2. All these services have been already successfully released. **Linked WPs: 2, 4, 5; Owner: LIST** | | |
| **iKPI-1.2** | **At least six (6) standards, regulations and directive incorporated within SENTINEL** | **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 tracks the CERTS / CSIRTS engaged by TSI and other partners for the duration of the project. In this context, TSI and other SENTINEL partners contacted several H2020 European projects (e.g., PUZZLE, CONCORDIA, PALANTIR, CAPA-A) to promote the dissemination of the project. A considerable number of the liaised organizations including **CERT/CSIRT teams approached are 11** so far. TSI plans to engage more CERTs/CSIRTs by presenting SENTINEL during an online event in the following months. In this regard, TSI is in contact with the EU projects JCOP and CyberExchange, which have several CERTs as consortium members, to facilitate the process. Also, TSI members are members of the Forum of Incident Response and Security Teams (FIRST), where more CERTs can be reached. **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** | | |

<table>
<tr><td>**iKPI-2.3**</td><td>**More than 20 novel services, tools and modules within the SENTINEL platform**</td><td>**In progress**</td></tr>
<tr><td colspan="3">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**</td></tr>
<tr><td>**iKPI-3.1**</td><td>**At least three (3) improved business model developed within the SENTINEL project**</td><td>**In progress**</td></tr>
<tr><td colspan="3">The preliminary business model was presented in D7.2, as part of the ongoing process related to T7.1. An intermediate update of the market analysis and the business model has been performed in the context of D7.7 “Exploitation strategy, standardisation activities and best practices – interim version” (M18). 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). This iKPI is considered 70% achieved. **Linked WP: 7; Owner: AEGIS**</td></tr>
<tr><td>**iKPI-3.2**</td><td>**At least 40% reduction of compliance – related costs**</td><td>**In progress**</td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-1.3, please refer to Sec. 2.1; KR-1.3; **Linked WP: 6; Owner: STS**</td></tr>
<tr><td>**iKPI-4.1**</td><td>**At least 4 tools reach market readiness level eight (8)**</td><td>**In progress**</td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-6.2, please refer to Sec. 2.6; KR-6.2; **Linked WPs: 2-5; Owner: FP**</td></tr>
<tr><td>**iKPI-4.2**</td><td>**More than 10 critical aspects addressed to ensure long-term sustainability**</td><td>**In progress**</td></tr>
<tr><td colspan="3">This iKPI is directly linked with KR-6.4, please refer to Sec. 2.6; KR-6.4; **Linked WP: 5; Owner: INTRA**</td></tr>
<tr><td>**iKPI-4.3**</td><td>**10.000 smaller enterprises entities and third parties reached**</td><td>**In progress**</td></tr>
<tr><td colspan="3">Regarding iKPI4.3, all the dissemination and communication activities conducted since M1, are seen as actions to reach out to SMEs and third parties. In particular, the events organized by SENTINEL (1st, 2nd, 3rd SME-centric workshops, 1st clustering webinar, MVP demonstration workshop, “A privacidade e a proteção de dados pessoais no panorama nacional das PMEs” webinar) have reached more than **200 participants in total**. We believe that our participation in major events (such as IoT week, Madeira digital transformation summit, FIC Forum (both in 2022 and 2023)) strongly contributed towards this iKPI as well. For example, the FIC event reports more than 13.000 participants every year while the last edition of IoT week attracted about 1600 participants. The Madeira digital transformation summit has received more than 300 registrations.<br>Regarding the outreach of third parties through the SENTINEL social media, the numbers indicate good progress towards this KPI as well: during the first 24 months in LinkedIn, we reached more than **1100 unique visitors,** in Twitter, we’ve reached more than **5000 visits,** in our YouTube channel we reached around **500 views** while in the SENTINEL Zenodo Community we recorded around **50 views.** Considering such numbers for the first 24 months of project duration, we can estimate that our progress towards this KP roughly targets 65% of completeness. Efforts to disseminate SENTINEL and reach out to a larger audience will be conducted in Y3 as well through the upcoming events, newsletters, podcasts and social media campaigns, which will increase the number of third parties to be reached. **Linked WP: 7; Owner: UNINOVA**</td></tr>
<tr><td>**iKPI-9**</td><td>**At least four (4) innovative technologies advanced within SENTINEL**</td><td>**In progress**</td></tr>
<tr><td colspan="3">SENTINEL combines a set of tried-and-tested innovative solutions (MITIGATE, Security Infusion, CyberRange, GDPR CSA etc) that are further advanced throughout the project, with a set of components/modules newly developed within the project (IdMS, DPIA, etc). During Y2, the consortium has made significant progress in advancing at least six technologies by integrating them within the 1st integrated version of the SENTINEL platform and anticipates that both the newly developed technologies, as well as the technologies already brought by partners will lead to further advancements. Although the number of core components of the project are already fixed, this iKPI is obviously still in progress, as the advancement activities continue and will be finalised in M30 when the 2nd version of the SENTINEL platform is released. This KR is considered ~80% achieved. **Linked WPs: WP2-WP4; Owner: ITML**</td></tr>
<tr><td>**iKPI-10**</td><td>**At least five (5) cases testing and validating the innovative capacity of the SENTINEL’s offerings**</td><td>**In progress**</td></tr>
<tr><td colspan="3">Considering that a testing refers to an end-to-end validation of one of the SENTINEL innovative services/tools we anticipate having at least 5 cases testing from already identified end–users. As mentioned previously in KR-4.3, in the frame of WP6 activities, we have already executed early testing and validation of the SENTINEL MVP through CG, TIG and two (2) external end-users. Following the</td></tr>
</table>

<table>
<tr><td colspan="3">same paradigm, the consortium partners will focus on testing and validation activities of the 1st integrated SENTINEL platform under WP6 by organising SME-centric workshops and recruiting more external end-users' via DIHs, towards achieving this KR. This KR is considered 50% achieved in a sense that we have already secured the SENTINEL demonstrators for end-to-end validation of SENTINEL tools. <b>Linked WP: 6; Owner: UNINOVA</b></td></tr>
<tr><td><b>iKPI-11.1</b></td><td><b>At least 20 third-party entities (SMEs/MEs) directly using SENTINEL's tools/services</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">To achieve this iKPI, SMEs (other than the ones included in the consortium) should first become aware of the SENTINEL services. This demands the consortium to have a solid dissemination strategy and conduct multiple dissemination and communication activities. In this regard, since the launch of the project the consortium partners have approached SMEs in several targeted events (SME-centric workshops, several talks and events co-organised with DIHs and relevant projects) outlining the project objectives and main project offerings. In Y2, aiming to intensify the SME's engagement, the project partners have organised two more workshops (Demonstration of the SENTINEL MVP and 3rd SME-centric workshop at the Digital Transformation Summit) by demonstrating the SENTINEL MVP and inviting wider audiences to short run trials. As a result, and in addition to its pilot owners (CG and TIG) the consortium has secured 5 DIHs (PRODUTECH, DIH4CPS, DIH-WORLD, Madeira DIH and Digital Manufacturing Innovation Hub Wales), invited 4 external SMEs to trial the SENTINEL MVP. By the end of Y2, UNINOVA has engaged with three (3) more DIH (DataLife DIH, Images-et-reseaux DIH and ICE RWTH DIH) in addition to previously engaged five (5) by increasing the number of potential channels for inviting more SMEs to test the final release of the SENTINEL platform (M30). Currently six (6) external SMEs are identified and within Y3 the partners will intensify these activities towards the successful achievement of this iKPI. This KR is considered 30% achieved. <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-11.2</b></td><td><b>At least 10% increase of market share for SMEs/MEs exploiting SENTINEL</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">To monitor the project's impact on the market share, based on the Innovation Radar components already identified and reported in D8.12, STS has updated a questionnaire to circulate among the project's SMEs/MEs partners and collect insights about the basic financial figures of their companies. The current position regarding the targeted markets and the relevant increments in the project partners will be captured early in Y3 and will follow up towards the end of the project to verify the accomplishment of this iKPI. The estimated progress of this iKPI is 30% and the core activities are going to be executed during Y3. <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-12.1</b></td><td><b>At least four (4) start-ups and spin-offs boosted exploiting SENTINEL security services</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">This iKPI necessitates that the SENTINEL complete suite of services is launched (M30), trialled by external end users and fully evaluated in terms of – among others - (i) usability, (ii) user acceptance, (iii) cost-efficiency, (iv) automation. In SENTINEL, third-party collaborations have been started since the beginning of the project as part of T6.3 and T7.4 activities. So far, eight (8) DIHs have engaged that helped to approach six (6) external enterprises and invite them to test the final SENTINEL platform. Currently this iKPI is considered ~20% achieved in a sense that we have already secured eight (8) DIHs having solid experience in working not only with SMEs/MEs but also with startups and spin-offs ecosystem thus can help to engage with those parties as well. <b>Linked WP: 7; Owner: STS</b></td></tr>
<tr><td><b>iKPI-12.2</b></td><td><b>At least 15% increase in sales for the pilot partners exploiting the SENTINEL platform</b></td><td><b>In progress</b></td></tr>
<tr><td colspan="3">Similarly, to iKPI-12.1, this iKPI necessitates that the SENTINEL complete suite of services is launched, trialled by CG and TIG end users and fully evaluated in terms of – among others - (i) usability, (ii) user acceptance, (iii) cost-efficiency, (iv) automation. Within M22-M24, the first stage of CG and TIG pilot experiments have been initiated. To this end, two (2) CG end-users have provided feedback on the SENTINEL FFV based on their pilot testing experience by filling out an online User Evaluation Questionnaire regarding usability, user acceptance, cost efficiency etc. After the final execution of the SENTINEL demonstrators (M30) the pilot partners will provide detailed information on the usability, user acceptance, cost-efficiency, automation of the final version of the platform as well as estimate (in the long term) the impact of the SENTINEL platform on their business operations. This iKPI is directly related with WP6 activities and currently considered ~20% achieved in the sense that pilot evaluation methodologies have been established and real-world pilot testing activities have been launched. Within</td></tr>
</table>

Y3 the corresponding measures will continue to take place to monitor and assess this iKPI. **Linked WP: 7; Owner: STS**

## 4.2 Measures to maximize impact

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

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

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

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

- **Prof. Fereniki Panagopoulou:** Assistant Professor of Constitutional Law, Panteion University, Athens, Greece.
- **Dr. Tania (Konstantina) Kyriakou**: Dr. Kyriakou has a well-demonstrated track record on data protection law, EU law and cultural heritage law. Dr. Kyriakou has a full membership of EDAC, as she has already worked on several tasks for the EDAC as a deputy member. She has replaced Dr. Chris Konialis because of the unfortunate event of his passing away in M16 of the project.
- **Dr. Tal Soffer**: Head of the unit of Technology and Society Foresigh, Tel Aviv University, Israel.

During Y2, EDAC has successfully produced the Ethics Manual and Ethical Controlling reports, which comprised D8.14 delivered in M18. This process involved holding several meetings among the three EDAC members to draft the Ethical and legal controlling form, which was distributed to all SENTINEL partners. The form aimed to serve as a blueprint for the SENTINEL partners to record their legal and ethical policies in terms of personal data protection.

The second EAB meeting was successfully conducted on the 26-27th of April 2023, during the second day of the SENTINEL's 5th plenary meeting, held in Paris, France. The purpose of the meeting was to introduce the SENTINEL project and present the main achievements up to M24, aiming to receive valuable feedback for the next steps. The meeting consisted of four parts: (i) SENTINEL project status and progress since M18, (ii) SENTINEL technical overview and workshop session (iii) SENTINEL testing and validation (iv) an overview towards implementing the final SENTINEL platform.

A fruitful discussion was held during this meeting where the EAB member Prof. João Mendonça provided feedback and valuable recommendations aiming to ensure high quality and excellence in the project. The comments were focused on the challenges that SENTINEL is facing related to the i) user experience, ii) UX/UI improvements, iii) enhancement of guidance/instructions within the SENTINEL platform for the potential users, iv) final integration of all SENTINEL tools and services and v) engagement of external stakeholders. In addition, Prof. João Mendonça expressed willingness to test the platform and provide useful insights as an external end user.

For the third year of the project, the plan is to organise at least one more meeting with the EAB co-hosted with the SENTINEL's 6th plenary meeting (scheduled in October 2023) and continue our efforts.

### 4.2.2 Communication and dissemination activities conducted in 2nd Year

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 were presented.

With respect to activities conducted in Y2, SENTINEL social media channels have been engaging with different users almost daily (please refer to the dissemination dKPIs identified in the tables below). The 2nd year resulted in the consolidation of our recent SENTINEL YouTube channel, which has been used to promote SENTINEL videos and the SENTINEL podcast series.

Regarding the marketing material, during Y2 we initiated the design and development of SENTINEL "product". This material is planned to be used online, but also in physical events when promoting the SENTINEL offerings.

Considering participations in events and conferences, in Y2 SENTINEL has participated in the **FIC Forum** 7-8 June 2022, **IoTWeek** 20-23 June 2022, **Policy to Projects Seminar (PPS)** 30 June 2022, **INTEROP V-LAB General Assembly** 30 June 2022, **IEEE International Conference on Cyber Security and Resilience** 27th July 2022, **International workshop on Information & Operational Technology** (IT & OT) Security Systems in conjunction with the 17th International Conference on Availability, Reliability, and Security, **9th International Workshop on Evolving Security & Privacy Requirements Engineering** 15-19 August 2022, **CyberHOT Summer School** 29-30 September 2022, **ETSI conference on cybersecurity certification** 3-5 October 2022, **Digital Transformation Summit** 25-27 October 2022, **Joint cybersecurity webinar** 19th January 2023, **Joint workshop "EU-Made cybersecurity for safe, resilient and trustworthy applications and services"** 27th February 2023, **30th Annual Network and Distributed system Security Symposium (NDSS 2023)** 27 Feb–3 March 2023, **FIC Forum** 5–7 of April 2023, **IDC SECURITY ROADSHOW** 20th of April 2023, "**Safe Internet Day 2023**" February 2023.

Regarding the organization of events, SENTINEL has organized the following events: **Workshop/Training session with SMEs for MVP demonstration** 26 September 2023, **Digital Transformation Summit: SME-centric Workshop III** 24-27 October 2022.

Regarding the upcoming events, SENTINEL will be attending **IT Security Conference** 12 October 2023 (not confirmed yet), "**European Big Data Value Forum**" 25 October 2023 (not confirmed yet); **B-sides Lisbon** 16-17 November 2023". SENTINEL is also planning to organize a project cluster physical meeting and promote the SENTINEL final event in M36.

In Y2 SENTINEL has continued promoting synergies with cluster projects with fourteen (14) projects engaged so far. With this respect, besides the organization of a physical meeting, we are also planning to promote the development of a joint publication on policy priorities and joint training sessions on projects technical innovations.

The visibility of the project and transferability of the project outcomes has been promoted through the generation of promotional material. In this context, four (4) additional SENTINEL newsletters were released within Y2, highlighting some of the SENTINEL components as part of the SENTINEL technical suite, but also dissemination and communication achievements. Several SENTINEL videos and podcasts were also released and are available under the SENTINEL YouTube channel.

With respect to academic publications, SENTINEL has submitted three (3) conference papers. One paper has already been approved, the other two are currently under review.

The WP7 monthly meetings also take 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.

The following table lists the dKPIs related to communication and dissemination activities and summarizes the progress for year 2. The aim of these KPIs is to measure the impact of the related activities.

*Table 15. SENTINEL Website - KPIs status update*

| **SENTINEL website** | **dKPI** | **Frequency** | **Threshold** | **Achieved/In progress** |
|---|---|---|---|---|
| | 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. In the second year (**M13-M24**) we had **1544 number of visitors**, which is approximately **128 visitors monthly.** Even with good numbers, the consortium aims to keep maintaining more than 100 visitors per month to aim for at least 1200 visitors in Y3 as well. The estimated progress of this dKPI is ~ 69%. | | | |
| | 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. In the first year (**M1-M12**), the **number of the SENTINEL website views** was **4,502.** This was highly related to the fact that it was the first year of the project, where awareness and loyalty starts being built. For the second year of project (**M13-M24**) the **number of the SENTINEL website page views increased significantly by reaching to 6.498**, and the project achieved more than the expected KPI with 11.000 page views in total. The estimated progress of this dKPI is ~ 73%. | | | |
| | 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 in Y1.** In the second year (**M13-M24**), we had **276 files downloaded**, totalizing **385 downloads** since the beginning of the project. The progress of the achievement of this KPI is less than 10%. To address this KPI in Y3 the consortium will take advantage of the Zenodo Open Access repository[7] as well and make all scientific material, presentations, and public deliverables available for the audience's reference via this channel too. |

*Table 16. 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**. This was highly related to the fact that it was the first year of the project, where awareness and loyalty starts being built. In Y2, **the number of followers** in twitter was **287,** which equals to approximately **23 monthly.** The consortium aims to keep maintaining more than 20 monthly followers in Y3 as well. The estimated progress of this dKPI is ~ 65%. | | | |
| | 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, the **number of tweets** per month was approximately **17**. We are planning to leverage more of our public content and keep up with this KPI in Y3. The estimated progress of this dKPI is ~ 45%. | | | |
| | dKPI#6: Number of unique visitors | Monthly | ≥ 30 | **Achieved** |
| | Although the twitter analytics provide no information about unique visits, we keep monitoring the total number of visitors via this channel. In Y1, we recorded 2,313 twitter visitors (approximately **192 visitors monthly**). In Y2 (M13-M23 data) we recorded approx. 3,500 twitter visitors (approximately **290 visitors monthly).** This KPI is 100% achieved and the consortium aims to keep maintaining these numbers in Y3 as well. | | | |

*Table 17. 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**. In Y2, the **number of follower**s in LinkedIn was **272**, which accounts for approximately **22 monthly**. This KPI is 100% achieved, and we will keep monitoring this during 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 achieved approx. **18** (M24 data), and we are optimistic about the third year, when we are planning to leverage more of our public content and keep up with this KPI. The estimated progress of this dKPI is ~ 48%. | | | |
| | dKPI#9: Number of unique visitors | Monthly | ≥ 20 | **Achieved** |
| | In Y1, we recorded approx. **60 visitors monthly** (M11 data)**.** In Y2, we recorded approx. **45 unique visitors monthly**. This KPI is 100% achieved and we will keep monitoring this during Y3. | | | |

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

*Table 18. 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 now, 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 (especially in Y1), thus this KPI experienced a deviation to the initial plan. In Y2, we participated in more than eight **(8) physical events** and were able to distribute more materials through participants, which totalized more than **480** distributed brochures in the second year. In total, we distributed approximately **560 brochures in 11 events,** and we will keep monitoring this during Y3. The estimated progress of this dKPI is ~ 56%. | | | |
| | dKPI#11: Number of electronic SENTINEL brochures | End of project | ≥1000 downloads | **In progress** |
| | To address this KPI, the SENTINEL consortium has continued to create a number of informative materials such as flyer, brochure, newsletters (all available in the SENTINEL's website) in Y2 as well. Based on the tendency of people to read and "save" whatever they are most interested in terms of interesting material, we decided that "views" is a more relevant aspect to track for this KPI compared to "downloads". Following up on this deviation, this KPI was recorded **426 views** of all our electronic material in Y1 and **151 views** in Y2. To achieve this KPI, in Y3 the consortium will take advantage of the Zenodo Open Access repository[8] as well and make all informative materials available for the audience's reference via this channel too. The estimated progress of this dKPI is ~ 58%. | | | |
| | dKPI#12: Regular newsletters | End of project | ≥9 newsletters | **In progress** |
| | In Y1, we have released **3 high-quality Newsletters**, while in Y2 we released **four (4)** additional newsletters. Thus, we believe we are on track towards achieving this KPI in Y3 as well. The estimated progress of this dKPI is ~ 78%. | | | |
| | dKPI#13: Number of SENTINEL videos and number of views | End of project | 3 videos with >1000 views each | **In progress** |
| | In Y1, we released the first promotional video of SENTINEL. In Y2, we released more than 14 video materials (including the SENTINEL podcasts) on our channel, with a total of **535 views**. For Y3 we are planning to produce more content about training and events to achieve the number of views expected for this KPI. The estimated progress of this dKPI is ~ 50%. | | | |

*Table 19. 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 | Envisioned to be assessed in Y3 |
| | To address 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. We expect that with the release of the final SENTINEL platform, a lot of research material is available to be published to address this KPI. | | | |

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

| | | | | |
|---|---|---|---|---|
| | dKPI#15: Number of special issues in international referred journals | End of project | >2 | Envisioned to be assessed in Y3 |
| | The technical implementation has been amplified in Y2, so we are expecting that the consortium will have produced a significant load of research material published in Y3 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 address this KPI in the next project period. | | | |
| | dKPI#16: Number of publications in international (printed or online) magazines | End of project | >6 | **In progress** |
| | SENTINEL has been published in **four (4) different conference proceedings**, we are still expecting the final outcome of **other 2 publications** and also working towards a joint publication with other cluster projects. The estimated progress of this dKPI is ~ 67%. | | | |
| | dKPI#17: Number of conference presentations by SENTINEL partners | End of project | ≥12 | **In progress** |
| | Regarding this KPI, SENTINEL has participated in **six (6) conferences** highlighted previously, 4 of them are scientific conferences with paper publication while **2 conference papers** are currently under review process. This KPI is on track, and we will keep monitoring it in Y3 to ensure that it will be achieved by the end of the project. The estimated progress of this dKPI is ~ 50%. | | | |

*Table 20. 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 | **Achieved** |
| | To address this KPI, the consortium worked as a team and each partner utilised their network and individual dissemination plans. This KPI is well on track as within the first and second years of the project, SENTINEL participated in **16 large events with >60 attendees.** This KPI is 100% achieved nevertheless during Y3, we have already planned to participate in other large events (such as C-DAYS 2023, B-sides Lisbon, European Big Data Value Forum 2023 etc.). | | | |
| | dKPI#19: Number of audience contacts | End of project | ≥50% of the participants | **Achieved** |
| | It is difficult to address this KPI where most of the events take place virtually thus, we utilised a combination of means such as online surveys, personal contacts and website statistics on the day of the event. For Y2, the KPI was on average accomplished with approximately 55% of the participants registered as audience contacts. Nevertheless, we will keep up monitoring this in Y3 as well. | | | |
| | dKPI#20: Number of participants interested in SENTINEL project | End of project | ≥40% of the participants | **Achieved** |
| | Similar to dKPI#19, to address this KPI we utilised a combination of means such as online surveys, personal contacts and website statistics on the day of an event or at any other occasion where we made contact with potential SENTINEL stakeholders. The KPI was on average accomplished during Y1 and slightly overachieved during Y2 with approximately 45% of participants demonstrating their interest in SENTINEL. Nevertheless, we will keep monitoring it in Y3 as well and record our stakeholders' attitude during the next SME-centric workshops. | | | |

*Table 21. 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 organised the 3rd SME-centric workshop, one (1) Workshop/Training session with SMEs for MVP demonstration with **≥100 registrations** in total. Furthermore, with AI4HealthSec and HEIR H2020 projects we co-organized an international workshop on Information & Operational Technology (IT & OT) Security Systems took place on the 23rd – 26th of August 2022. This workshop took place in conjunction with the 17th International Conference on Availability, Reliability, and Security (ARES 2022). The event reported ≥**100 attendees**. In Y3, we plan to organise at least three (3) more major events, thus we anticipate that this KPI will be achieved by the end of the project. The estimated progress of this dKPI is ~ 64%. | | | |
| | dKPI#22: Number of audience contacts | End of project | ≥50% of the participants | **Achieved** |
| | To address this KPI we utilised a combination of means such as online surveys, personal contacts and website statistics on the day of the event. This KPI was on average accomplished with approximately 50% of the participants registered as audience contacts. Nevertheless, we will keep up monitoring this in Y3 as well. | | | |
| | dKPI#23: Number of participants interested in SENTINEL project | End of project | ≥50% of the participants | **Achieved** |
| | In Y2 during the 3rd workshop where the SENTINEL MVP demonstration took place 42% of attendees expressed interest about the SENTINEL project by answering that they could consider investing in tools/services similar to SENTINEL within the next 2 years. SENTINEL is committed to organise several events within the 3rd year of the project and thus will keep up monitoring this in Y3 as well. As an example, UNINOVA is working towards the organization of a scientific conference in 2024, where SENTINEL is planning to promote a satellite event. | | | |

*Table 22. 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 all partners 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. In addition to this, in Y2, we engaged with **four (4) more** new projects thus, this KPI is 100% achieved and we will continue to liaise with similarly themed projects and relevant stakeholders to intensify dissemination and exploitation actions in Y3 as well. |

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

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

### 4.2.3 Exploitation strategy and activities conducted in 2nd Year

The SENTINEL exploitation activities officially started in M13 of the project thus the project consortium has intensified the respective activities in Y2. Particularly in Y2 the SENTINEL exploitation activities were focused on the following actions:

- Organisation of further SME-centric workshop and engagement with potential SMEs for further exploration of the SENTINEL platform. In Y2, the 3rd SME-centric workshop took place aiming at discussing SMEs challenges, needs, their view of SENTINEL offerings and revealing their willingness to trial the SENTINEL integrated solution.
- Creating an SME-centric questionnaire distributed to the above SME/ME participants to better reflect aspects, such as their awareness of GDPR obligations, their needs, challenges, application domain, etc.
- Liaising with similarly themed projects to ensure common exploitation pathways and synergies. Like Y1, special communications and discussions took place in Y2 as well and the efforts culminated with two (2) clustering webinars, where more than 10 project representatives elaborated on outcomes, offerings and innovations of their projects and discussed openly common exploitation & dissemination possibilities.
- Further exploration of individual components and technology offerings provided by the project partners.

In Y2, we have prepared the ground for the SENTINEL exploitation plan. The exploitation manager designed a questionnaire and collected the renewed exploitation interest of the project partners. The objective of the survey was 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 identified various opportunities to leverage the project's outcomes in their ongoing and/or future activities. To highlight these opportunities, technology and knowledge transfer actions from the individual viewpoint perspective D7.7 delivered in M18 illustrates updated exploitation strategies reported by all the SENTINEL partners including both current and future exploitation activities.

After successfully realizing D7.7 and aiming at further enhancing the SENTINEL exploitation activities, SENTINEL has applied for the Horizon Results Booster[9], which is an initiative aiming to boost the exploitation potential of EU projects' results. Two modules have been selected: **Module A** "Identifying and creating the portfolio of R&I project results" and **Module C** "Assisting projects to improve their existing exploitation strategy" as part of Service 1 "Portfolio Dissemination & Exploitation Strategy". The application was made by STS (a leader of the SENTINEL exploitation activities). Our aim is to receive advice and guidance from exploitation experts on how to prepare the ground for exploiting the SENTINEL platform and its services and to enhance partners' competence in enriching their exploitation strategy. Two experts have been assigned to our project, the first introductory meetings have already taken place and the agreed start of the service is at the end of M25.

We plan to intensify these actions in Y3 towards effective exploitation of the SENTINEL key exploitable results. In particular, STS plans to apply for Service 2 "Business Plan Development" under HRB, which will offer guidance and support to SENTINEL's consortium in preparing their project results for the market. This service will provide tailor-made training and support in enhancing the project's business plan, which will incorporate a market analysis, a business strategy, operations plan, competitor identification and analysis and a clear action plan to be implemented by the project with an estimation of time to market.

The outcome of these services will be reported in D7.8 and D7.9 in M36.

# 5. Innovations

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

During Y2, and after the SENTINEL MVP release, the consortium has proceeded with respect to the project's product definition by updating the SENTINEL business model and value proposition elaborating on the project's three main offerings, which provides the foundation for innovation management and exploitation activities.

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

[9] https://www.horizonresultsbooster.eu/

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.

In Y2, these offerings have been investigated more in parallel with the project's technical developments. The SENTINEL consortium has further defined its innovations and track their progress utilizing the Innovation Radar Methodology[10] and leveraging the related questionnaire and instructions for its analysis. As a result, a preliminary Technology and Innovation Radar was constructed based on the technologies and innovations identified with respect to their potential and maturity. Key internal milestones to construct the Radar were the release of the SENTINEL 1st integrated solution (M18-MS3) and the initial demonstration and assessment of the SENTINEL platform and technologies (M24-MS4).

As a result, we delivered D8.12 which presents i) the list of technological innovations and their convergence in SENTINEL, ii) Technical and Innovation Strategy Plan, iii) innovation management approach including a thorough assessment framework of project innovation. It is worth mentioning that this work was used as input not only to manage innovation strategy of the project but also for the overall exploitation and long-term sustainability plan as well as for the individual exploitation plans of each consortium partner for their future developments and their contribution to the European Economy. To this end, D7.5, D7.7 and D5.5 (in addition to D8.12) have been prepared and released showing a strong link between innovations and activities within T7.1, T7.3, T7.4, T8.3 as well as T5.3.

It should be noted that this work will continue to evolve in Y3, therefore, the Radar will be revisited again to decide if technologies and innovations should move in terms of maturity, or if any other technologies and innovations rise by the end of the project. The consortium will focus on the better-shaped innovations for M36 by identifying actions to support the partners involved in each innovation to bring their innovation result closer to market after the project ends.

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

# 6. Conclusions

This document presents the work accomplished mainly during the second year of the project [M13-M24 (June 2022 to May 2023)]. The SENTINEL project had several intensive activities in the course of this period in a sense of delivering tangible results and achievements. In particular, it illustrates i) activities that the SENTINEL project successfully accomplished the Innovation Phase (M7- M18) and ii) progress of some actions as part of the Demonstration Phase (M19-M30). Additionally, it provides an overview of the consortium plans for the third and final year of the project.

In Y2, the SENTINEL project has delivered its interim full-featured platform together with its tools and services such as GDPR Compliance Self-Assessment (GDPR CSA) module, Identity Management System (IdMS), Data Protection Impact Assessment (DPIA) toolkit, GDPR compliant recording of PAs (ROPA), Cybersecurity risk assessment (CSRRA/MITIGATE), Cyber Range simulations, Policy recommendation and enforcement, Cyber incident reporting and handling, Observatory. In addition, the project has reported on its activities related to exploitation, standardization, dissemination and stakeholder engagement as well as released the work carried out on the SENTINEL initial execution and evaluation.

Moving forward, in the last project year, the Demonstration phase will be concluded, and the project will approach the Consolidation & Sustainability Management Phase (M31-M36). By the end of the demonstration phase the project partners will reach MS5 by delivering the final version of SENTINEL integrated framework together with its technologies and services. The phase can be considered accomplished when nine (9) deliverables within WP2, WP3, WP4, WP5 and WP6 are produced and successfully submitted to the REA (M30). Lastly, in the final project phase (Consolidation & Sustainability Management Phase) the project partners will join their forces to conduct the final framework's evaluation and impact assessment, deliver the final business plan and produce the final dissemination and exploitation reports.